เอกสารทบทวนแนวปฏิบัติด้านรักษาความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
หมวดที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements For Access Control)	
๑. การควบคุมการเข้าถึงข้อมูลสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูล ให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัย ดังนี้ ๑.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ ต้องสอดคล้อง และเป็นไปตามคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ ๑.๒ เจ้าของระบบมีหน้าที่ในการอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้กับผู้ใช้งาน ๑.๓ ผู้ดูแลระบบมีหน้าที่กำหนดสิทธิให้แก่ผู้ใช้งานตามที่เจ้าของระบบอนุมัติ ๑.๔ ผู้ดูแลระบบมีหน้าที่ในการสร้างบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน สำหรับการเข้าระบบคอมพิวเตอร์และระบบสารสนเทศ ตลอดจนควบคุม การใช้งานและดูแลรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบสารสนเทศ ๑.๕ ผู้ใช้งานสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น ๑.๖ เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ ต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจจากเจ้าของระบบ และต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหาย บุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน ๑.๗ การเข้าถึงห้องศูนย์ข้อมูล (Data Center) ให้ดำเนินการ ดังนี้ ๑.๗.๑ กลุ่มเทคโนโลยีสารสนเทศต้องกำหนดข้อปฏิบัติสำหรับการปฏิบัติงานในห้องศูนย์ข้อมูล (Data Center) ๑.๗.๒ การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใด ๆ ออกจากห้องศูนย์ข้อมูล (Data Center) ต้องได้รับอนุมัติจากผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ ๑.๗.๓ ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์ข้อมูล (Data Center) เว้นแต่ได้รับอนุญาตจากผู้ได้รับมอบหมายดูแลห้องศูนย์	๑. การควบคุมการเข้าถึงสินทรัพย์ทางสารสนเทศ ให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัย ดังนี้ ๑.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ ต้องสอดคล้อง และเป็นไปตามคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ ๑.๒ เจ้าของระบบมีหน้าที่ในการอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้กับผู้ใช้งาน ๑.๓ ผู้ดูแลระบบมีหน้าที่กำหนดสิทธิให้แก่ผู้ใช้งานตามที่เจ้าของระบบอนุมัติ ๑.๔ ผู้ดูแลระบบมีหน้าที่ในการสร้างบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน สำหรับการเข้าระบบคอมพิวเตอร์และระบบสารสนเทศ ตลอดจนควบคุม การใช้งานและดูแลรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบสารสนเทศ ๑.๕ ผู้ใช้งานสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น ๑.๖ เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ ต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจจากเจ้าของระบบ และต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหาย บุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน ๑.๗ การเข้าถึงห้องศูนย์ข้อมูล (Data Center) ให้ดำเนินการ ดังนี้ ๑.๗.๑ กลุ่มเทคโนโลยีสารสนเทศต้องกำหนดข้อปฏิบัติสำหรับการปฏิบัติงานในห้องศูนย์ข้อมูล (Data Center) ๑.๗.๒ การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใด ๆ ออกจากห้องศูนย์ข้อมูล (Data Center) ต้องได้รับอนุมัติจากผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ ๑.๗.๓ ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์ข้อมูล (Data Center) เว้นแต่ได้รับอนุญาตจากผู้ได้รับมอบหมายดูแลห้องศูนย์ข้อมูล (Data Center) ๑.๗.๔ ห้ามนำอาหาร เครื่องดื่ม เข้ามาในห้องศูนย์ข้อมูล (Data Center) ๑.๗.๕ ห้ามถ่ายรูป อุปกรณ์ภายในห้องศูนย์ข้อมูล (Data Center) ก่อนได้รับอนุญาตจากผู้ได้รับมอบหมายดูแลห้องศูนย์ข้อมูล (Data Center)

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
ข้อมูล (Data Center) ๑.๗.๔ ห้ามนำอาหาร เครื่องดื่ม เข้ามาในห้องศูนย์ข้อมูล (Data Center) ๑.๗.๕ ห้ามถ่ายรูป อุปกรณ์ภายในห้องศูนย์ข้อมูล (Data Center) ก่อนได้รับอนุญาตจากผู้ได้รับมอบหมายดูแลห้องศูนย์ข้อมูล (Data Center)	
หมวดที่ ๒ การบริหารจัดการเข้าถึงของผู้ใช้งาน (User Access Management)	
๑. การลงทะเบียนผู้ใช้งาน ให้ดำเนินการ ดังนี้ ๑.๑ ผู้รับผิดชอบด้านสารสนเทศของหน่วยงานต้องกำหนดแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ที่สามารถนำข้อมูลไปตรวจสอบได้ ประกอบด้วยชื่อ 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 หรือหนังสือขอเข้าใช้งานจากบริษัท/หน่วยงานต้นสังกัด ๒. ให้หน่วยงานพิจารณาเหตุผล และดำเนินการส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้เจ้าของระบบที่	๑. การลงทะเบียนผู้ใช้งาน ให้ดำเนินการ ดังนี้ ๑.๑ ผู้รับผิดชอบด้านสารสนเทศของหน่วยงานต้องกำหนดแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ 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 หรือหนังสือขอเข้าใช้งานจากบริษัท/หน่วยงานต้นสังกัด ๒. ให้หน่วยงานพิจารณาเหตุผล และดำเนินการส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้เจ้าของระบบที่ขอใช้งาน ๓. ให้เจ้าของระบบพิจารณาและอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ๔. ให้ผู้ดูแลระบบกำหนดสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ พร้อมทั้งแจ้งให้หน่วยงานเจ้าของระบบรับทราบ ๑.๓ การสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่าน (Password) ให้ดำเนินการ ตามหลักเกณฑ์ ดังนี้ ๑.๓.๑ การสร้างบัญชีผู้ใช้งาน (Username) ให้เจ้าของระบบ กำหนด เช่น ชื่อภาษาอังกฤษตามด้วยเครื่องหมาย “_”

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
ขอใช้งาน ๓. ให้เจ้าของระบบพิจารณาและอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ๔. ให้ผู้ดูแลระบบกำหนดสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ พร้อมทั้งแจ้งให้หน่วยงานเจ้าของบุคลากรรับทราบ ๑.๓ การสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่าน (Password) ให้ดำเนินการ ตามหลักเกณฑ์ ดังนี้ ๑.๓.๑ การสร้างบัญชีผู้ใช้งาน (Username) ให้เจ้าของระบบ กำหนด เช่น ชื่อภาษาอังกฤษ หรือบัตรประจำตัวประชาชนตามด้วยเครื่องหมาย “_” หรือ “.” ตามด้วยอักษรนามสกุลตัวแรก หรือลักษณะอื่นใดตามที่เจ้าของระบบ ที่มีการตกลงร่วมกัน ๑.๓.๒ การกำหนดรหัสผ่าน (Password) ประกอบไปด้วย ชุดของตัวอักษรภาษาอังกฤษ ตัวเลข และอักขระพิเศษ อย่างน้อย 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(Username) และแจ้งกลับไปยังหน่วยงานรับทราบ ภายใน ๑ เดือน ๒.๑.๒ กรณีผู้ดูแลระบบ ให้ดำเนินการยกเลิกสิทธิการใช้งานของตนเองทุกระบบงาน ทั้งนี้ให้ดำเนินการแจ้งหน่วยงานต้นสังกัดหรือเจ้าของระบบรับทราบการยกเลิกสิทธิการใช้งาน ภายใน ๑ วัน ๓. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้ใช้งาน ให้ดำเนินการ ดังนี้ ๓.๑ ในกรณีที่มีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ให้	หรือ “.” ตามด้วยอักษรนามสกุลสองตัวแรก หรือลักษณะอื่นใดตามที่เจ้าของระบบ ที่มีการตกลงร่วมกัน ๑.๓.๒ การกำหนดรหัสผ่าน (Password) ประกอบไปด้วย ชุดของตัวอักษรภาษาอังกฤษ ตัวเลข และอักขระพิเศษ อย่างน้อย ๘ ตัวขึ้นไป และยากต่อการคาดเดา ๑.๓.๓ การกำหนดบัญชีผู้ใช้งานครั้งแรกให้ผู้ดูแลระบบ แจ้งบัญชีผู้ใช้งาน (Username) และรหัสผ่านชั่วคราว (Temporary Password) ให้ผู้ใช้งาน ทราบโดยตรง และเมื่อผู้ใช้งานเข้าใช้งานระบบต้องมีการบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่าน (Password) ในการนำไปลงชื่อเข้าสู่ระบบครั้งแรก ๑.๓.๔ เมื่อผู้ใช้งานมีการเปลี่ยนแปลงข้อมูลให้หน่วยงานทำการแจ้งเจ้าของระบบ เพื่อปรับปรุงข้อมูลให้เป็นปัจจุบัน ๒. การยกเลิกสิทธิการใช้งานของบุคลากรหรือบุคคลภายนอกและผู้ดูแลระบบให้ดำเนินการ ดังนี้ ๒.๑ ให้หน่วยงานแจ้งเจ้าของระบบ เพื่อขอยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของบุคลากร เมื่อมีการลาออก โอนย้าย หรือสิ้นสุดการจ้าง ๒.๑.๑ กรณีบุคลากรหรือบุคคลภายนอก ให้ผู้ดูแลระบบดำเนินการปิดบัญชีผู้ใช้งาน (Username) และแจ้งกลับไปยังหน่วยงานรับทราบ ภายใน ๑ เดือน ๒.๑.๒ กรณีผู้ดูแลระบบ ให้ดำเนินการยกเลิกสิทธิการใช้งานของตนเองทุกระบบงาน ทั้งนี้ให้ดำเนินการแจ้งหน่วยงานต้นสังกัดหรือเจ้าของระบบรับทราบการยกเลิกสิทธิการใช้งาน ภายใน ๑ 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) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้ ๔.๑ ในกรณีผู้ใช้งานลืมรหัสผ่าน (Password) ให้แจ้งหน่วยงานที่รับผิดชอบ โดยใช้วิธีการของระบบโปรแกรม ตามที่เจ้าของระบบได้กำหนดไว้ ๔.๒ ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๓ - ๖ เดือน ตามความเสี่ยงของระบบโปรแกรม และรหัสผ่าน (Password) ใหม่ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม ๕. ผู้ดูแลระบบ ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสุดสิ้นการจ้าง เพื่อกำหนดสิทธิให้สอดคล้องตามภารกิจที่เปลี่ยนไป และการรักษาความมั่นคงปลอดภัย ตามที่พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์กำหนดไว้

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
หน่วยงานแจ้ง เจ้าของระบบ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ๓.๒ ในกรณีที่ผู้ใช้งาน ต้องการสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ที่สูงกว่าระดับสิทธิที่ได้รับ ขอให้แจ้งความประสงค์พร้อมเหตุผลต่อเจ้าของระบบ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้ดำเนินการ ตามหลักเกณฑ์ ดังนี้ ๔.๑ ในกรณีผู้ใช้งานลืมรหัสผ่าน (Password) ให้แจ้งหน่วยงานที่รับผิดชอบ โดยใช้วิธีการของระบบโปรแกรม ตามที่เจ้าของระบบได้กำหนดไว้ ๔.๒ ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๓ - ๖ เดือน หรือ ๑ ปี ตามความเสี่ยงของระบบโปรแกรม และรหัสผ่าน (Password) ใหม่ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม ๕. ผู้ดูแลระบบ ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสุดสิ้นการจ้าง เพื่อกำหนดสิทธิให้สอดคล้องตามภารกิจที่เปลี่ยนไป และการรักษาความมั่นคงปลอดภัย ตามที่พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์กำหนดไว้	
หมวดที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)	
๑. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการ ดังนี้ ๑.๑ ผู้ใช้งานต้องกำหนดรหัสผ่าน(Password) ตามหมวดที่ ๒ ข้อ ๑.๓ และต้องเปลี่ยนรหัสผ่านตาม ข้อ ๔.๒ ๑.๒ผู้ใช้งานต้องไม่ใช้รหัสผ่าน(Password)ร่วมกับบุคคลอื่นและไม่ควรให้ระบบคอมพิวเตอร์หรือระบบสารสนเทศจำรหัสผ่าน (Password) ในการเข้าใช้งานโดยอัตโนมัติ ๑.๓ ผู้ใช้งานต้องไม่เปิดเผยรหัสผ่าน(Password) สำหรับการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้บุคคลอื่นรับรู้ โดยเก็บเป็นความลับเสมือนเป็น	๑. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการ ดังนี้ ๑.๑ ผู้ใช้งานต้องกำหนดรหัสผ่าน (Password) ประกอบไปด้วย ชุดของตัวอักษรภาษาอังกฤษ ตัวเลข และอักขระพิเศษอย่างน้อย ๘ ตัวขึ้นไปและยากต่อการคาดเดา ต้องไม่ใช้รหัสผ่านเดียวกันกับระบบอื่น และต้องเปลี่ยนรหัสผ่าน(Password) ใหม่ทุก ๓ - ๖ เดือน หรือ ๑ ปี ตามความเสี่ยงของระบบโปรแกรม และรหัสผ่าน (Password) ใหม่ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม ๑.๒ ผู้ใช้งานต้องไม่ใช้รหัสผ่าน(Password) ร่วมกับบุคคลอื่นและไม่ควรให้ระบบคอมพิวเตอร์หรือระบบสารสนเทศจำรหัสผ่าน (Password) ในการเข้าใช้งานโดยอัตโนมัติ ๑.๓ ผู้ใช้งานต้องไม่เปิดเผยรหัสผ่าน(Password) สำหรับการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้บุคคลอื่นรับรู้ โดยเก็บเป็นความลับเสมือนเป็นสมบัติส่วนตัว ห้ามจดหรือเขียนรหัสผ่าน (Password) ที่ใช้งานไว้ในที่เปิดเผย ๑.๔ หากมีความจำเป็นต้องบอกรหัสผ่าน (Password) แก่บุคคลอื่นเนื่องจากความจำเป็นเมื่อมีการเข้าถึงหลังจากดำเนินการเสร็จสิ้นแล้วให้เปลี่ยนรหัสผ่าน (Password) ใหม่ทันที

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
สมบัติส่วนตัว ห้ามจดหรือเขียนรหัสผ่าน (Password) ที่ใช้งานไว้ในที่เปิดเผย ๑.๔ หากมีความจำเป็นต้องบอกรหัสผ่าน (Password) แก่บุคคลอื่นเนื่องจากความจำเป็นในการเข้าถึงหลังจากดำเนินการเสร็จสิ้นแล้วให้เปลี่ยนรหัสผ่าน (Password) ใหม่ทันที ๑.๕ หากมีการกระทำความผิดเกิดขึ้นจากบัญชีผู้ใช้งาน(Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องมีส่วนร่วมในการรับผิดชอบต่อการกระทำความผิดนั้น เว้นแต่เจ้าของ บัญชีผู้ใช้งาน (Username) ได้กระทำการป้องกันตามแนวปฏิบัติที่กำหนดแล้ว ๒. ผู้ใช้งานต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ ๓. การควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้ ๓.๑ ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงอุปกรณ์ในการประมวลผลข้อมูล(ProcessDevice) มีวัตถุประสงค์เพื่อใช้ในการปฏิบัติงานของหน่วยงานเท่านั้น ๓.๒ ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ (Asset)ของหน่วยงาน และให้ใช้งานด้วยความระมัดระวังเสมือนเป็นทรัพย์สินส่วนตน ๓.๓ผู้ใช้งานต้องไม่ดัดแปลงหรือไม่ติดตั้งอุปกรณ์หรือซอฟต์แวร์ใดๆที่เครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์พกพาหรือระบบคอมพิวเตอร์และระบบสารสนเทศในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์พร้อมเหตุผลต่อผู้ดูแลระบบสารสนเทศของ หน่วยงานต้นสังกัด ๓.๔ผู้ใช้งานต้องใช้ความระมัดระวังในการบันทึกข้อมูลสารสนเทศไว้ในอุปกรณ์บันทึกข้อมูลแบบพกพาหรือการ์ดความจำในโทรศัพท์มือถือ เพื่อป้องกันการรั่วไหลของข้อมูล ๓.๕ บุคคลภายนอกที่เกี่ยวข้องกับการดำเนินงานด้านสารสนเทศ ต้องขออนุมัติเป็นลายลักษณ์อักษรก่อนเข้าปฏิบัติงาน ๓.๖ การทำลายอุปกรณ์บันทึกข้อมูลให้ดำเนินการ ดังนี้	๑.๕ หากมีการกระทำความผิดเกิดขึ้นจากบัญชีผู้ใช้งาน(Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องมีส่วนร่วมในการรับผิดชอบต่อการกระทำความผิดนั้น เว้นแต่เจ้าของ บัญชีผู้ใช้งาน (Username) ได้กระทำการป้องกันตามแนวปฏิบัติที่กำหนดแล้ว ๒. ผู้ใช้งานต้องออกจากระบบ (Log Out) ทันทีเมื่อไม่ได้ใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ โดยไม่เปิดระบบสารสนเทศที่สำคัญ ทิ้งไว้โดยไม่มีใครดูแล ๓. การควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้ ๓.๑ ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงอุปกรณ์ในการประมวลผลข้อมูล(ProcessDevice)มีวัตถุประสงค์เพื่อใช้ในการปฏิบัติงานของหน่วยงานเท่านั้น ๓.๒ ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ (Asset) ของหน่วยงาน และให้ใช้งานบริหารจัดการทรัพยากรด้วยความระมัดระวังเสมือนเป็นทรัพย์สินส่วนตน ๓.๓ผู้ใช้งานต้องไม่ดัดแปลงหรือไม่ติดตั้งอุปกรณ์หรือซอฟต์แวร์ใดๆที่เครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์พกพาหรือระบบคอมพิวเตอร์และระบบสารสนเทศในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์พร้อมเหตุผลและได้รับอนุญาตจากผู้ดูแลระบบสารสนเทศของหน่วยงานต้นสังกัด ๓.๔ผู้ใช้งานต้องใช้ความระมัดระวังในการบันทึกข้อมูลสารสนเทศไว้ใน อุปกรณ์บันทึกข้อมูลแบบพกพาหรือการ์ดความจำในโทรศัพท์มือถือ หลีกเลี่ยงการทิ้งไว้ที่สาธารณะ เพื่อป้องกันการรั่วไหลของข้อมูล ๓.๕ บุคคลภายนอกที่เกี่ยวข้องกับการดำเนินงานด้านสารสนเทศ ต้องขออนุมัติเป็นลายลักษณ์อักษรก่อนเข้าปฏิบัติงาน ๓.๖ การทำลายอุปกรณ์บันทึกข้อมูลให้ดำเนินการ ดังนี้

ประเภทสื่อบันทึก	นำสื่อบันทึกกลับมาใช้ ใหม่	บันทึกข้อมูลชั้นความลับและนำสื่อบันทึกกลับมาใช้	ไม่นำสื่อบันทึกกลับมา ใช้ใหม่
CD/DVD	-	-	ใช้การทุบ หรือทำลายให้เสียหายหรือเผา
สื่อบันทึกข้อมูลแบบปฏิบัติการ	ใช้การ Factory Data Reset	- ระบบปฏิบัติการ IOS ให้ใช้การ Factory Data Reset - ระบบปฏิบัติการอื่นๆ ใช้การลบและเขียนข้อมูลทับจนเต็มพื้นที่จัดเก็บ	ใช้การทุบหรือทำลายให้เสียหายหรือเผา
สื่อบันทึกข้อมูลแบบถอดแยกได้	ใช้การ Format	ใช้การ Format แบบ Zero-filling	ใช้การทุบหรือทำลายให้เสียหายหรือเผา

แนวปฏิบัติ (เดิม)

ประเภทสื่อบันทึก	นำสื่อบันทึกกลับมาใช้ ใหม่	บันทึกข้อมูลชั้นความลับและนำสื่อบันทึกกลับมาใช้	ไม่นำสื่อบันทึกกลับมา ใช้ใหม่
CD/DVD	-	-	ใช้การทุบหรือทำลายให้เสียหายหรือเผา
สื่อบันทึกข้อมูลแบบปฏิบัติการ	ใช้การ Factory Data Reset	- ระบบปฏิบัติการ IOS ให้ใช้การ Factory Data Reset - ระบบปฏิบัติการอื่นๆ ใช้การลบและเขียนข้อมูลทับจนเต็มพื้นที่จัดเก็บ	ใช้การทุบหรือทำลายให้เสียหายหรือเผา
สื่อบันทึกข้อมูลแบบถอดแยกได้	ใช้การ Format	ใช้การ Format แบบ Zero-filling	ใช้การทุบหรือทำลายให้เสียหายหรือเผา
เทปบันทึกข้อมูล	ใช้การ Format	ใช้การ Format แบบ Zero-filling	ใช้การทุบหรือทำลายให้เสียหายหรือเผา
ฮาร์ดไดรฟ์ (Hard Drive)	ใช้การ Format โดยการเขียนทับข้อมูลเป็นจำนวนหลายๆรอบ	ใช้การ Format แบบ Zero-filling	ใช้การทุบหรือทำลายให้เสียหายหรือเผา
กระดาษ	ขีดข้อความทิ้งก่อนนำไปใช้เป็นกระดาษ Reuse	ห้ามนำกลับมาใช้ใหม่	ใช้เครื่องทำลายเอกสารก่อนทิ้ง

แนวปฏิบัติ (ปรับปรุง)

เทปบันทึกข้อมูล	ใช้การ Format	ใช้การ Format แบบ Zero-filling	ใช้การทุบหรือทำลายให้เสียหายหรือเผา
ฮาร์ดไดรฟ์ (Hard Drive)	ใช้การ Format โดยการเขียนทับข้อมูลเป็นจำนวนหลายๆรอบ	ใช้การ Format แบบ Zero-filling	ใช้การทุบหรือทำลายให้เสียหายหรือเผา
กระดาษ	ขีดข้อความทิ้งก่อนนำไปใช้เป็นกระดาษ Reuse	ห้ามนำกลับมาใช้ใหม่	ใช้เครื่องทำลายเอกสารก่อนทิ้ง

๓.๗การนำอุปกรณ์บันทึกข้อมูลกลับมาใช้งานใหม่ให้ดำเนินการนำอุปกรณ์บันทึกข้อมูลไปใช้งานใหม่ให้ฟอร์แมต (Format)อุปกรณ์บันทึกข้อมูลนั้นโดยใช้วิธีการฟอร์แมต(Format)ตามมาตรฐานสากลหรือตามที่พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กำหนดไว้ และตรวจสอบอุปกรณ์ว่ามีสื่อจัดเก็บข้อมูลก่อนนำกลับมาใช้ใหม่หรือไม่

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
๓.๗การนำอุปกรณ์บันทึกข้อมูลกลับมาใช้งานใหม่ให้ดำเนินการนำ อุปกรณ์บันทึกข้อมูลไปใช้งานใหม่ให้ฟอร์แมต(Format)อุปกรณ์บันทึกข้อมูลนั้นโดยใช้วิธีการฟอร์แมต(Format)ตามมาตรฐานสากลหรือ ตามที่พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์กำหนดไว้	
หมวดที่ ๔ การควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ (Computer Network Access Control)	
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 ต้องระมัดระวังการดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมต่างๆ เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุก โจมตีระบบคอมพิวเตอร์และระบบสารสนเทศ โดยแจ้งให้ผู้ดูแลระบบสารสนเทศของหน่วยงานต้นสังกัดทราบก่อนติดตั้งใช้งาน ๑.๒ การใช้งานโดเมนเนม (Domain Name) ของหน่วยงานให้ดำเนินการ ดังนี้ ๑.๒.๑ ห้ามนำโดเมนเนม (Domain Name) ในทางที่ไม่ถูกต้อง ผิดกฎหมาย	๑ การเข้าถึงเครือข่ายของผู้ใช้งาน ๑.๑ การใช้งานระบบเครือข่ายคอมพิวเตอร์ (Internet) ให้ดำเนินการ ดังนี้ ๑.๑.๑ มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงด้วยการใช้รหัสผ่าน (Password) ๑.๑.๒ ผู้ใช้งานสามารถเข้าบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองที่ได้รับอนุญาตจากหน่วยงาน เพื่อเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์ (Internet) ๑.๑.๓ ควรควบคุมการใช้งานระบบเครือข่ายคอมพิวเตอร์ (Internet) ที่มีการครอบครองแบรนด์วิดท์ (Bandwidth) สูง และที่ไม่เกี่ยวข้องกับการปฏิบัติหน้าที่ราชการ เช่น รายการบันเทิงต่าง ๆ ในเวลาราชการ เป็นต้น ๑.๑.๔ ห้ามเข้าชมเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดศีลธรรม ลามกอนาจาร เว็บไซต์ที่มีเนื้อหาที่ทำให้สถาบันชาติ ศาสนา และพระมหากษัตริย์เสื่อมเสีย เป็นต้น ๑.๑.๕ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของหน่วยงาน เว้นแต่ได้รับ อนุญาตจากเจ้าของข้อมูล ๑.๑.๖ ต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พระราชบัญญัติการ รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยเคร่งครัด ๑.๑.๗ ต้องระมัดระวังการดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมต่าง ๆ เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุก โจมตีระบบคอมพิวเตอร์และ ระบบสารสนเทศ โดยแจ้งให้ผู้ดูแลระบบสารสนเทศของหน่วยงานต้นสังกัดทราบก่อนติดตั้งใช้งาน ๑.๑.๘ หลังจากใช้งานระบบเครือข่ายภายนอก (Internet) แล้ว ต้องออกจากระบบ (Logout) ก่อนปิดเว็บบราวเซอร์ (Web Browser) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งาน ๑.๒ การใช้งานโดเมนเนม (Domain Name) ของหน่วยงานให้ดำเนินการ ดังนี้ ๑.๒.๑ ห้ามนำโดเมนเนม (Domain Name) ไปใช้ในทางที่ไม่ถูกต้อง ผิดกฎหมาย ละเมิดศีลธรรม ๑.๒.๒ ต้องไม่แสวงหาผลประโยชน์หรือให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจด้วยการใช้โดเมนเนม (Domain Name) ของหน่วยงาน ๑.๒.๓ หลังจากการใช้งานโดเมนเนม (Domain Name) ของหน่วยงาน ต้องออกจากระบบ (Logout) ทันที

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
ละเมิดศีลธรรม ๑.๒.๒ ต้องไม่แสวงหาผลประโยชน์หรือให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจด้วยการใช้โดเมนเนม (Domain Name) ของหน่วยงาน ๑.๒.๓ หลังจากการใช้งานโดเมนเนม (Domain Name) ของหน่วยงาน ต้องออกจากระบบ (Log Out) ทันที ๑.๓ การใช้งานเครือข่าย Local Area Network (LAN) ให้ดำเนินการ ดังนี้ ๑.๓.๑ ผู้ดูแลระบบต้องทำการคอนฟิกกูเรชั่น(Configuration) เลขที่อยู่ไอพี (IP Address) เมื่อนำอุปกรณ์มาใช้ภายในหน่วยงาน ๑.๓.๒ ผู้ใช้งานต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่าย Local Area Network (LAN) ๑.๔ การใช้งานเครือข่ายไร้สาย (WiFi) ให้ดำเนินการ ดังนี้ ๑.๔.๑ ผู้ดูแลระบบต้องทำการเปลี่ยนค่า Service Set Identifier (SSID) ที่ถูกกำหนดจากผู้ผลิตทันที เมื่อนำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาติดตั้งเพื่อใช้งาน ๑.๔.๒ ผู้ใช้งานต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (WiFi) 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 โดยการนำเข้าข้อมูลต้องเป็นผู้ที่ได้รับ	๑.๓ การใช้งานเครือข่าย Local Area Network (LAN) ให้ดำเนินการ ดังนี้ ๑.๓.๑ ผู้ดูแลระบบต้องทำการตั้งค่า (Configuration) เลขที่อยู่ไอพี (IP Address) เมื่อนำอุปกรณ์มาใช้ภายในหน่วยงาน ๑.๓.๒ ผู้ใช้งานต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่ เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่าย Local Area Network (LAN) ๑.๔ การใช้งานเครือข่ายไร้สาย (Wi-Fi) ให้ดำเนินการ ดังนี้ ๑.๔.๑ ผู้ดูแลระบบต้องทำการเปลี่ยนค่า Service Set Identifier (SSID) ที่ถูกกำหนด จากผู้ผลิตทันที เมื่อนำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาติดตั้งเพื่อใช้งานภายในหน่วยงาน ๑.๔.๒ ผู้ใช้งานต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (Wi-Fi) ๑.๔.๓ ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ ที่เป็นทรัพย์สินของหน่วยงานไปใช้งานเครือข่ายไร้สาย (Wi-Fi) ที่ไม่น่าเชื่อถือ ๑.๔.๔ ผู้ใช้งานควรระมัดระวังในการทำธุรกรรมทางการเงินทางอิเล็กทรอนิกส์ระหว่าง การใช้งานเครือข่ายไร้สาย (Wi-Fi) เนื่องจากอาจเกิดความไม่ปลอดภัยและอาจขาดการเชื่อมต่อของสัญญาณ ๑.๔.๕ ห้ามผู้ใช้งานติดตั้งและเปิดการทำงานโปรแกรมดักจับข้อมูล (Network Sniffer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สาย (Wi-Fi) ของหน่วยงานและมีความผิดตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม ๑.๕ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการ ดังนี้ ๑.๕.๑ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ภายใต้ หน่วยงาน ควรนำเสนอเกี่ยวกับภารกิจงานของหน่วยงาน เช่น ผลการดำเนินงาน และข่าวสาร โดยการนำเข้าข้อมูล ต้องเป็นผู้ที่ได้รับมอบหมายจากหน่วยงาน และต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม ๑.๕.๒ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ภายใต้ หน่วยงาน ผู้รับผิดชอบต้องแสดงตำแหน่ง และหน่วยงาน ให้ชัดเจน เพื่อความน่าเชื่อถือ โดยอาจใช้รูปสัญลักษณ์หรือเครื่องหมายแสดง ๑.๕.๓ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับของหน่วยงานผ่านเครือข่ายสังคมออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล ๑.๕.๔ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่าง ต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงต่อไป ๑.๕.๕ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากหน่วยงาน และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว ๑.๕.๖ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งานต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทันที ทั้งนี้ให้แจ้งผู้บังคับบัญชารับทราบ

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
มอบหมายจากหน่วยงาน 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 หรือตามความเหมาะสม ๒.๒ การนำเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ มาใช้งานบนเครือข่ายต้องได้รับอนุญาตจากผู้รับผิดชอบด้านสารสนเทศของหน่วยงาน เช่น แท็ปเลต โทรศัพท์มือถือ เป็นต้น ๓. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) ให้ดำเนินการ ดังนี้ ๓.๑ หน่วยงานที่ดูแลด้านสารสนเทศต้องดูแล/ตรวจสอบพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) รวมทั้งการควบคุมการเข้าถึงพอร์ตทางกายภาพและเครือข่าย ๓.๒ หน่วยงานที่ดูแลด้านสารสนเทศต้องเปิดใช้งานเฉพาะพอร์ตที่จำเป็นสำหรับการใช้งานเท่านั้น และต้องตรวจสอบพอร์ตที่เปิดให้บริการ อย่างน้อย ๖	๒. การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ให้ดำเนินการ ดังนี้ ๒.๑ ผู้รับผิดชอบด้านสารสนเทศของหน่วยงานต้องจัดทำผังระบบเครือข่าย (Network Diagram) พร้อมรายละเอียดอุปกรณ์บนเครือข่ายที่จำเป็นต่อการใช้งาน ได้แก่ กลุ่มอุปกรณ์ เลขที่อยู่ไอพี (IP Address) และหมายเลขเฉพาะอุปกรณ์ (MAC Address) โดยให้ปรับปรุงทุก ๑ ปี หรือตามความเหมาะสม ๒.๒ การนำเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ มาใช้งานบนเครือข่ายต้องได้รับ อนุญาตจากผู้รับผิดชอบด้านสารสนเทศของหน่วยงาน เช่น แท็ปเลต โทรศัพท์มือถือ เป็นต้น ๓. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) ให้ดำเนินการ ดังนี้ ๓.๑ หน่วยงานที่ดูแลด้านสารสนเทศต้องดูแล/ตรวจสอบพอร์ตที่ใช้สำหรับตรวจสอบและ ปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) รวมทั้งการควบคุมการเข้าถึง พอร์ตทางกายภาพและเครือข่าย ๓.๒ หน่วยงานที่ดูแลด้านสารสนเทศต้องเปิดใช้งานเฉพาะพอร์ตที่จำเป็นสำหรับการใช้งาน เท่านั้น และต้องตรวจสอบพอร์ตที่เปิดให้บริการ อย่างน้อย ปีละ ๒ ครั้ง หรือตามความเหมาะสม ๔. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ให้ดำเนินการ ดังนี้ ๔.๑ หน่วยงานที่ดูแลด้านสารสนเทศควรมีระบบป้องกันการบุกรุกโจมตีทางเครือข่าย Firewall เพื่อใช้เป็นจุดควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ๔.๒ ผู้ดูแลระบบต้องไม่เปิดเผยข้อมูลการเชื่อมต่อทางเครือข่าย ก่อนได้รับอนุญาตจาก หน่วยงานที่ดูแลด้านสารสนเทศ ๔.๓ ผู้ดูแลระบบมีหน้าที่ในการควบคุมการเชื่อมต่อสัญญาณหรือยกเลิก การเชื่อมต่อสัญญาณ ตามที่ได้รับอนุญาตจากหน่วยงานที่ดูแลด้านสารสนเทศทั้งนี้ หากพบข้อผิดพลาดหรือเห็นว่า หมดความจำเป็นใน การเชื่อมต่อสัญญาณให้รายงานหน่วยงานที่ดูแลด้านสารสนเทศทันที ๔.๔ การเชื่อมต่อเครือข่ายสารสนเทศกับหน่วยงานภายนอกหรือเชื่อมต่อผ่านระบบเครือข่าย คอมพิวเตอร์ของผู้ให้บริการที่มีความน่าเชื่อถือ ต้องได้รับอนุญาตจากผู้บังคับบัญชาของหน่วยงาน ๕. การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ให้ดำเนินการ ดังนี้ ๕.๑ ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศเป็นไปอย่างมีประสิทธิภาพ และการรับ – ส่ง หรือการไหลเวียนของข้อมูลหรือสารสนเทศเป็นไปอย่างรวดเร็ว ๕.๒ ผู้ดูแลระบบต้องเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ของผู้ใช้งานเป็นระยะเวลาไม่ น้อยกว่า ๙๐ วัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
เดือน หรือตามความเหมาะสม ๔. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ให้ดำเนินการ ดังนี้ ๔.๑ หน่วยงานที่ดูแลด้านสารสนเทศควรมีระบบป้องกันการบุกรุกโจมตีทางเครือข่าย Firewall เพื่อใช้เป็นจุดควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ๔.๒ ผู้ดูแลระบบต้องไม่เปิดเผยข้อมูลการเชื่อมต่อทางเครือข่าย ก่อนได้รับอนุญาตจากหน่วยงานที่ดูแลด้านสารสนเทศ ๔.๓ ผู้ดูแลระบบมีหน้าที่ในการควบคุมการเชื่อมต่อสัญญาณหรือยกเลิก การเชื่อมต่อสัญญาณตามที่ได้รับอนุญาตจากหน่วยงานที่ดูแลด้านสารสนเทศทั้งนี้ หากพบข้อผิดพลาดหรือเห็นว่า 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	๖. มาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Data Center) ๖.๑ ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการบันทึกข้อมูลลงในสมุดบันทึกการเข้า-ออก พื้นที่ประจำห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Data Center) ๖.๒ ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ในสมุดบันทึกการเข้า-ออกพื้นที่ ให้ครบถ้วน ถูกต้อง ชัดเจน ๖.๓ ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกแบบฟอร์มการขออนุญาตเข้า-ออกเป็นประจำ ๗. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ ๘. ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)
หมวดที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)	
๑.การกำหนดขั้นตอนการปฏิบัติงาน ดังนี้ ๑.๑ ผู้ใช้งานไม่มีสิทธิ์เปลี่ยนแปลงแก้ไขค่าต่าง ๆ ของระบบปฏิบัติการ เช่น Product Key หรือ License ของระบบปฏิบัติการ และค่า	๑.การกำหนดขั้นตอนการปฏิบัติงาน ดังนี้ ๑.๑ ผู้ใช้งานไม่มีสิทธิ์เปลี่ยนแปลงแก้ไขค่าต่าง ๆ ของระบบปฏิบัติการ เช่น Product Key หรือ License ของระบบปฏิบัติการ และการตั้งค่า (Configuration) ต่าง ๆ เช่น Computer Name, IP Address เป็นต้น

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
คอนฟิกกูเรชั่น (Configuration) ต่าง ๆ เช่น Computer Name, IP Address เป็นต้น ๑.๒ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ ๑.๓ หลังจากผู้ดูแลระบบติดตั้งระบบปฏิบัติการเสร็จ ผู้ใช้งานต้องบริหารจัดการรหัสผ่านหรือเปลี่ยนรหัสผ่านที่กำหนดไว้ตั้งแต่ต้นโดยทันที ๑.๔ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งานเป็นเวลา ๑๐ นาที หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน - ก่อนการเข้าใช้ระบบปฏิบัติการผู้ใช้งานจะต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง - ห้ามให้ผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพไม่เหมาะสม หรือขัดต่อศิลธรรม บนระบบปฏิบัติของหน่วยงาน - ห้ามผู้ใช้งานของหน่วยงานเข้าควบคุมระบบปฏิบัติการคอมพิวเตอร์หรือระบบสารสนเทศจากภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน - ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer โปรแกรมประเภทดักจับข้อมูล (Network Sniffer) โปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer) และโปรแกรมประเภท Formatter หรือโปรแกรมที่มีความเสี่ยง เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน - ซอฟต์แวร์ที่หน่วยงาน ใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว - ซอฟต์แวร์ที่หน่วยงานจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น - ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของกระทรวงสาธารณสุขเพื่อประโยชน์ทางการค้า - ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์	๑.๒ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ ๑.๓ หลังจากผู้ดูแลระบบติดตั้งระบบปฏิบัติการเสร็จ ผู้ใช้งานต้องบริหารจัดการรหัสผ่านหรือเปลี่ยนรหัสผ่านที่กำหนดไว้ตั้งแต่ต้นโดยทันที ๑.๔ ผู้ดูแลระบบต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งานเป็นเวลา ๑๕ นาที หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน(Password)เพื่อเข้าใช้งาน - ก่อนการเข้าใช้ระบบปฏิบัติการผู้ใช้งานจะต้องทำการบันทึกเข้าใช้งาน (Login) ทุกครั้ง - ห้ามให้ผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพไม่เหมาะสม หรือขัดต่อศิลธรรม บนระบบปฏิบัติของหน่วยงาน - ห้ามผู้ใช้งานของหน่วยงานเข้าควบคุมระบบปฏิบัติการคอมพิวเตอร์หรือระบบสารสนเทศจากภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน - ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer โปรแกรมประเภทดักจับข้อมูล (Network Sniffer) โปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer) และโปรแกรมประเภท Formatter หรือโปรแกรมที่มีความเสี่ยง เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน - ซอฟต์แวร์ที่หน่วยงาน ใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว - ซอฟต์แวร์ที่หน่วยงานจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น - ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของหน่วยงาน เพื่อประโยชน์ทางการค้า - ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ - ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศจากภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน ๒.การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมสำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ ให้ดำเนินการ ดังนี้ ๒.๑ การใช้งานโปรแกรมยูทิลิตี้ต้องได้รับการอนุมัติจากผู้ดูแลระบบ เพื่อจำกัดและควบคุมการใช้งาน ๒.๒ โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์ ๒.๓ ผู้ดูแลระบบต้องยกเลิกหรือลบโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ - ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน ๒.การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมสำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ ให้ดำเนินการดังนี้ ๒.๑ การใช้งานโปรแกรมยูทิลิตี้ต้องได้รับการอนุมัติจากผู้ดูแลระบบ เพื่อจำกัดและควบคุมการใช้งาน ๒.๒ โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์ ๒.๓ ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้	
หมวดที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ	
๑. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น ๒. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ ๓.ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๓๐ นาที ระบบจะยุติการใช้งานผู้ใช้งานต้องทำการการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง ๔.ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้ ๔.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งาน	๑. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น x. ผู้ดูแลระบบ ต้องมีการจัดทำนโบบายคุกกี้ (Cookie Policy) โดยแจ้งวัตถุประสงค์ของการจัดเก็บคุกกี้ พร้อมทั้งระบุระยะเวลาในการจัดเก็บ x. ต้องมีการขอความยินยอมคุกกี้ (Consent) และมีการทบทวนความยินยอม ตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงการจัดเก็บคุกกี้ ๒. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๒ ครั้ง ๓.ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๓๐ นาที ระบบจะยุติการใช้งานผู้ใช้งานต้องทำการการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง ๔.ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้ ๔.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบ ลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
ระบบ ลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน ๔.๒ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง ๔.๓ กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน ๔.๔ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้า ถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ ๕.ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้ ๕.๑ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ๕.๒ ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล ๕.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว ๕.๔ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น ๕.๕ กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล ๕.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออก นอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น ๕.๗ ต้องสำรองข้อมูลและระบบ และทดสอบการกู้คืนข้อมูลและระบบอย่างสม่ำเสมอโดยกำหนดความถี่ในการดำเนินงานอย่างชัดเจนในแต่ละระบบ ๕.๘ ไม่เก็บข้อมูลสำคัญขององค์การไว้บนอุปกรณ์แบบพกพา เว้นแต่มีความจำเป็น และ ข้อมูลดังกล่าวจะต้องมีการเข้ารหัส	๔.๒ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ หรือในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง ๔.๓ กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน ๔.๔ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้า ถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ ๕.ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้ ๕.๑ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ๕.๒ ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล ๕.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว ๕.๔ การรับส่งข้อมูลสำคัญหรือข้อมูลที่มีชั้นความลับผ่านระบบเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น ๕.x การรับส่งข้อมูลที่มีชั้นความลับผ่านช่องทางอีเมล ต้องใช้โปรโตคอลการเข้ารหัสแบบ PGP (Pretty Good Privacy) ๕.๕ กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล ๕.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออก นอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น ๕.๗ ต้องสำรองข้อมูลและระบบ และทดสอบการกู้คืนข้อมูลและระบบอย่างสม่ำเสมอโดยกำหนดความถี่ในการดำเนินงานอย่างชัดเจนในแต่ละระบบ ๕.๘ ไม่เก็บข้อมูลสำคัญขององค์การไว้บนอุปกรณ์แบบพกพา เว้นแต่มีความจำเป็น และ ข้อมูลดังกล่าวจะต้องมีการเข้ารหัสข้อมูลที่เป็นมาตรฐาน ๕.๙ ข้อมูลที่มีชั้นความลับที่ต้องส่งออกไปนอกองค์การ โดยถูกจัดเก็บไว้บนอุปกรณ์แบบพกพาหรือถูกส่งผ่านระบบเครือข่ายไร้สาย ต้องผ่านการอนุมัติจากเจ้าของระบบงานและธุรกรรมและทำการเข้ารหัสข้อมูลและระบบเครือข่ายไร้สายก่อนเท่านั้น ๕.๑๐ การเคลื่อนย้ายข้อมูลที่มีชั้นความลับ ต้องกระทำโดยบุคคลที่เจ้าของระบบงานและธุรกรรมกำหนด และจะต้องทำลายข้อมูลดังกล่าวทันทีเมื่อไม่มีการใช้งานแล้ว

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
ข้อมูลที่เป็นมาตรฐาน ๕.๙ ข้อมูลที่มีชั้นความลับที่ต้องส่งออกไปนอกองค์การ โดยถูกจัดเก็บไว้บนอุปกรณ์แบบพกพาหรือถูกส่งผ่านระบบเครือข่ายไร้สาย ต้องผ่านการอนุมัติจากเจ้าของระบบงานและธุรกรรมและทำการเข้ารหัสข้อมูลและระบบเครือข่ายไร้สายก่อนเท่านั้น ๕.๑๐ การเคลื่อนย้ายข้อมูลที่มีชั้นความลับ ต้องกระทำโดยบุคคลที่เจ้าของระบบงานและธุรกรรมกำหนด และจะต้องทำลายข้อมูลดังกล่าวทันทีเมื่อไม่มีการใช้งานแล้ว ๖. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้ ๖.๑ ระบบที่ไวต่อการรบกวน โดยมีผลกระทบและมีความสำคัญสูง ได้แก่ระบบข้อมูลผู้ป่วยที่เป็นข้อมูลที่เกี่ยวข้องกับการรักษาพยาบาล และข้อมูลทางการแพทย์ระบบบุคลากรที่เป็นข้อมูลส่วนบุคคลของเจ้าหน้าที่ภายในกรมสนับสนุนบริการสุขภาพ ๖.๒ ต้องมีการควบคุมสภาพแวดล้อมของระบบที่ไวต่อการรบกวนโดยเฉพาะ ๖.๓ มีห้องปฏิบัติงานแยกเป็นสัดส่วนและต้องกำหนดสิทธิ์ให้เฉพาะผู้ที่ได้รับมอบหมายเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว ๖.๔ ติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่นและกำหนดสิทธิ์ในการเข้าถึงข้อมูล ๖.๕ ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร ๗. การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องปฏิบัติดังต่อไปนี้ ๗.๑ ตรวจสอบความพร้อมของคอมพิวเตอร์และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์ ๗.๒ ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้เว้นแต่ข้อมูลที่ได้มีการเผยแพรเป็นการทั่วไป ๗.๓ เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที ๗.๔ เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อม	๖. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้ ๖.๑ ระบบที่ไวต่อการรบกวน โดยมีผลกระทบและมีความสำคัญสูง ได้แก่ระบบข้อมูลผู้ป่วยที่เป็นข้อมูลที่เกี่ยวข้องกับการรักษาพยาบาล และข้อมูลทางการแพทย์ระบบบุคลากรที่เป็นข้อมูลส่วนบุคคลของเจ้าหน้าที่ภายในกรมสนับสนุนบริการสุขภาพ ๖.๒ ต้องมีการควบคุมสภาพแวดล้อมของระบบที่ไวต่อการรบกวนโดยเฉพาะ ๖.๓ มีห้องปฏิบัติงานแยกเป็นสัดส่วนและต้องกำหนดสิทธิ์ให้เฉพาะผู้ที่ได้รับมอบหมายเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว ๖.๔ ติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่นและกำหนดสิทธิ์ในการเข้าถึงข้อมูล ๖.๕ ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร ๗. การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องปฏิบัติดังต่อไปนี้ ๗.๑ ตรวจสอบความพร้อมของคอมพิวเตอร์และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์ ๗.x ห้ามนำอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ไปใช้งานในเรื่องที่ไม่เกี่ยวข้องกับการปฏิบัติงาน ๗.x ต้องไม่ติดตั้งโปรแกรมลงในอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่เอง หากมีความจำเป็นต้องใช้โปรแกรมเฉพาะทาง ให้แจ้งเจ้าหน้าที่ที่รับผิดชอบเพื่อพิจารณาในการดำเนินการติดตั้งให้เป็นครั้งคราวหรือตามความเหมาะสม ๗.x หากพบว่าอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ เกิดการทำงานที่ผิดปกติ ให้รีบดำเนินการแจ้งเจ้าหน้าที่ที่รับผิดชอบโดยเร็ว ๗.x ห้ามผู้ที่ไม่เกี่ยวกับการปฏิบัติงานหรือบุคคลภายนอกทำการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ในระยะไกล (Remote Desktop) ๗.๒ ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้เว้นแต่ข้อมูลที่ได้มีการเผยแพรเป็นการทั่วไป ๗.๓ เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที ๗.๔ เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย ๗.๕ หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาท

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
ใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย ๗.๕ หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาท อย่างร้ายแรงของผู้นำไปใช้ผู้นำไปใช้ต้องรับผิดชอบ ต่อความเสียหายที่เกิดขึ้น	อย่างร้ายแรงของผู้นำไปใช้ผู้นำไปใช้ต้องรับผิดชอบ
หมวดที่ ๗ การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล	
ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล ๑.กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล ๑.๑จัดทำบัญชีฐานข้อมูลการจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน ๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้ ๑.๒.๑ กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง - อ่านอย่างเดียว - สร้างข้อมูล - ป้อนข้อมูล - แก้ไข - อนุมัติ - ไม่มีสิทธิ์ ๑.๒.๒ กำหนดเกณฑ์การระงับสิทธิ์การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้ ๑.๒.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้า หน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย ๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล ๑.๓.๑ จัดแบ่งประเภทของข้อมูล ออกเป็น - ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น - ข้อมูลสารสนเทศด้านการแพทย์ที่ให้บริการ เช่น ข้อมูลผู้ป่วย	ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล ๑.กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล ๑.๑จัดทำบัญชีฐานข้อมูลการจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน ๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้ ๑.๒.๑ กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง - อ่านอย่างเดียว - สร้างข้อมูล - ป้อนข้อมูล - แก้ไข - อนุมัติ - ไม่มีสิทธิ์ ๑.๒.๒ กำหนดเกณฑ์การระงับสิทธิ์การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้ ๑.๒.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขอ อนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้า หน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย ๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล ๑.๓.๑ จัดแบ่งประเภทของข้อมูล ออกเป็น - ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น - ข้อมูลสารสนเทศด้านที่ให้บริการตามภารกิจ เช่น ข้อมูลผู้รับบริการ ข้อมูลสถานพยาบาล ข้อมูลสถานประกอบการเพื่อสุขภาพ เป็นต้น ๑.๓.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
ข้อมูลยาและเวชภัณฑ์ ข้อมูลสถานพยาบาล เป็นต้น ๑.๓.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ - ข้อมูลที่มีระดับความสำคัญมากที่สุด - ข้อมูลที่มีระดับความสำคัญปานกลาง - ข้อมูลที่มีระดับความสำคัญน้อย ๑.๓.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล - ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้าย แรงที่สุด - ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่าง ร้ายแรง - ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย - ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้ ๑.๓.๔ จัดแบ่งระดับชั้นการเข้าถึง - ระดับชั้นสำหรับผู้บริหาร - ระดับชั้นสำหรับผู้ใช้งานทั่วไป - ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย ๑.๓.๕ การกำหนดเวลาที่ได้เข้าถึง ๑.๓.๖ การกำหนดจำนวนช่องทางที่สามารถเข้าถึง ๒.ข้อมูลข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย ๓.การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วย การรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ๔. หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของ ผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิ์และจัดให้มีแฟ้มลงบันทึกเข้า ออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการ	- ข้อมูลที่มีระดับความสำคัญมากที่สุด - ข้อมูลที่มีระดับความสำคัญปานกลาง - ข้อมูลที่มีระดับความสำคัญน้อย ๑.๓.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล - ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด - ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง - ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย - ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้ ๑.๓.๔ จัดแบ่งระดับชั้นการเข้าถึง - ระดับชั้นสำหรับผู้บริหาร - ระดับชั้นสำหรับผู้ใช้งานทั่วไป - ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย ๑.๓.๕ การกำหนดเวลาที่ให้เข้าถึงข้อมูล ๑.๓.๖ การกำหนดจำนวนช่องทางที่สามารถเข้าถึงข้อมูล ๒.ข้อมูลข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย ๓.การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วย การรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ๔. หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิ์และจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล ๕. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการ หรือแลกเปลี่ยน หรือขอใช้ข้อมูลจากส่วนราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานกับหน่วยงานภายนอก ดังต่อไปนี้ ๕.๑ กำหนดนโยบาย ขั้นตอนปฏิบัติและมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง ๕.๒ กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการ ใช้ข้อมูลร่วมกัน หรือแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น ๕.๓ กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
ตรวจสอบความถูกต้องของ การใช้งานฐานข้อมูล ๕. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการ หรือแลกเปลี่ยน หรือขอใช้ข้อมูล จากส่วนราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานกับ หน่วยงานภายนอก ดังต่อไปนี้ ๕.๑ กำหนดนโยบาย ขั้นตอนปฏิบัติและมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง ๕.๒ กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกัน หรือแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น ๕.๓ กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล ๕.๔ กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธ ๕.๕ กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น ๕.๖ กำหนดสิทธิ์การเข้าถึงข้อมูล ๕.๗ กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์ ๕.๘ กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น ส่วนที่ ๒ การสำรองข้อมูล ๑. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย ๒. ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล ๓. ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง ๔. ต้องกำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูลหากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่	๕.๔ กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้ รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธ ๕.๕ กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น ๕.๖ กำหนดสิทธิ์การเข้าถึงข้อมูล ๕.๗ กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์ ๕.๘ กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส,ตั้งค่าการเข้ารหัสในทุกระดับของทรัพยากร, เป็นต้น ส่วนที่ ๒ การสำรองข้อมูล ๑. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย ๒. ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล ๓. ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง ๔. ต้องกำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย กำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้ ๔.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้และความถี่ในการ สำรอง ๔.๒ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง ข้อมูล ๔.๓ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ, วัน/เวลาชื่อข้อมูลที่สำรอง ,สำเร็จ/ไม่สำเร็จ ระยะเวลา, วิธีการสำรองข้อมูล เป็นต้น ๔.๔ ตรวจสอบค่าคอนฟิกกูเรชันต่าง ๆ ของระบบการสำรองข้อมูล ๔.๕ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ๔.๖ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน ๔.๗ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่ เช่น จัดการการเข้าถึงทางกายภาพโดยการให้สิทธิ์เฉพาะกับบุคคลที่ได้รับอนุญาต,ติดตั้งระบบกล้องวงจรปิดเพื่อตรวจสอบและบันทึกการเข้าถึง เป็นต้น ๔.๙ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้ ๔.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้และความถี่ในการสำรอง ๔.๒ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล ๔.๓ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น ๔.๔ ตรวจสอบค่าคอนฟิกกูเรชันต่าง ๆ ของระบบการสำรองข้อมูล ๔.๕ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ๔.๖ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอก สถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน ๔.๗ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่ ๔.๘ ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ ๔.๙ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้ ๔.๑๐ ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น ๔.๑๑ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้ ๕.ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการ ทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย ๕.๑ มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด ๕.๒ มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้	๔.๑๐ ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น ๔.๑๑ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้ ๕.ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย ๕.๑ มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด ๕.๒ มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น ๕.๓ มีการกำหนดขั้นตอนปฏิบัติในการสำรอง กู้คืน และทดสอบกู้คืนระบบสารสนเทศที่ทำการสำรองไว้ ๕.๕ มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เพื่อใช้ในการติดต่อเมื่อเกิดเหตุจำเป็น ๕.๖ การสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น ๖. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง ๗.ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรองและการจัดทำแผนเตรียมพร้อม กรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ๘. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ ๙. มีการทบทวนระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น ๕.๓ มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ ๕.๔ มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้ ๕.๕ มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่ายฮาร์ดแวร์ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ ๕.๖ การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น ๖. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง ๗.ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรองและการจัดทำแผนเตรียมพร้อม กรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ๘. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผน เตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ ๙. มีการทบทวนระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง	
หมวดที่ ๘ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	
ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง ๑. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้อง	ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง ๑. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) **หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก** (External Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
คำนึงถึง ดังนี้ ๑.๑ จัดลำดับความสำคัญของความเสี่ยง ๑.๒ ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง ๑.๓ ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง ๑.๔ สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้ ๑.๕ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ ๑.๖ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้ ๑.๖.๑ กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว ๑.๖.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี ๑.๖.๓ กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย ๑.๖.๔ กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ ๑.๖.๕ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบ เทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆ ได้ ๔ ประเภท ดังนี้ <u>ประเภทที่ ๑</u> ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่นเจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้านHardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงันหรือหยุดทำงาน และ	๑.๑ จัดลำดับความสำคัญของความเสี่ยง ๑.๒ ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง ๑.๓ ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง ๑.๔ สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้ ๑.๕ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ ๑.๖ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้ ๑.๖.๑ กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว ๑.๖.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี ๑.๖.๓ กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย ๑.๖.๔ กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อก แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ ๑.๖.๕ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนาและมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบ เทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆ ได้ ๔ ประเภท ดังนี้ <u>ประเภทที่ ๑</u> ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ไว้ดังนี้ ๑) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human error ลดน้อยลง (๒) จัดทำหนังสือแจ้งเวียนหน่วยงานทั้งส่วนกลางและส่วนภูมิภาค เรื่อง การใช้และการ ประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง <u>ประเภทที่ ๒</u> ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือ ระบบเครือข่ายคอมพิวเตอร์

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
ส่งผลให้ ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพได้ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ดังนี้ ๑) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจในด้าน Hardwareและ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human error ลดน้อยลง ๒) จัดทำหนังสือแจ้งเวียนหน่วยงานทั้งส่วนกลางและส่วนภูมิภาค เรื่อง การใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง <u>ประเภทที่ ๒</u> ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเทอร์เน็ต(Internet Worm), ม้าโทรจัน (Trojan Horse), และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้ ๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก ๒) ติดตั้งซอฟต์แวร์ Anti virus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์ <u>ประเภทที่ ๓</u> ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ดังนี้ ๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย ๒) ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟ	ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนอินเทอร์เน็ต (Internet Worm) ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่าย คอมพิวเตอร์ใช้งานไม่ได้ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้ (๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก ๒) ติดตั้งซอฟต์แวร์ Anti virus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์ <u>ประเภทที่ ๓</u> ภัยจากไฟไหม้หรือระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้ ๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย ๒) ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟ เกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ ๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ <u>ประเภทที่ ๔</u> ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับ สถานการณ์ ดังนี้ ๑) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา ๒) ถอดเทป Back up ข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย ๓) ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเบรคเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า ๔) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในที่สูง ๕) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่าย สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ๖) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบ Network ว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่ ๗) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งให้

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
เกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงทีซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ ๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ <u>ประเภทที่ ๔</u> ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วมจัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ดังนี้ ๑) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา ๒) ถอดเทป Back up ข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย ๓) ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเบรกเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า ๔) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในที่สูง ๕) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่ายว่า สามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ๖) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ตรวจสอบระบบ Network ว่า สามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่ ๗) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ	หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ
หมวดที่ ๙ การรักษาความปลอดภัยด้านกายภาพ สถานที่และสภาพแวดล้อม	
๑. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์	๑. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน ๒. ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ต้องมีลักษณะ ดังนี้ ๒.๑ กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตาม ความสำคัญแล้วแต่กรณี ๒.๒ ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออก ของบุคคลเป็นจำนวนมาก ๒.๓ จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว ๒.๔ จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่ ๒.๕ หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยก ออกมาจาก บริเวณดังกล่าว ๒.๖ ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด ๒.๗ จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศ จัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต ๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย ๓.๑ มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ ๓.๒ กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้ง จัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area)พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ	๒. ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ต้องมีลักษณะ ดังนี้ ๒.๑ กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตาม ความสำคัญแล้วแต่กรณี ๒.๒ ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออก ของบุคคลเป็นจำนวนมาก ๒.๓ จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว ๒.๔ จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่ ๒.๕ หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยก ออกมาจาก บริเวณดังกล่าว ๒.๖ ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด ๒.๗ จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศ จัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต ๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย ๓.๑ มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ ๓.๒ กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้ง จัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area)พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN CoverageArea) เป็นต้น ๔. การควบคุมการเข้าออก อาคารสถานที่ ๔.๑ กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน ๔.๒ การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor) ๔.๓ ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors) ๔.๔ ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน ๔.๕ บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน ๔.๖ จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
(IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN CoverageArea) เป็นต้น ๔. การควบคุมการเข้าออก อาคารสถานที่ ๔.๑ กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออก ในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน ๔.๒ การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษา ความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor) ๔.๓ ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors) ๔.๔ ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน ๔.๕ บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน ๔.๖ จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น ๔.๗ ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและ จากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ๔.๘ มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และ ต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว ๔.๙ สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ	๔.๗ ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและ จากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ๔.๘ มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และ ต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว ๔.๙ สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ ๔.๑๐ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่ ๔.๑๑ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต ๔.๑๒ มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center) ๔.๑๓ จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ ๔.๑๔ จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญ อย่างน้อยปีละ ๑ ครั้ง ๕. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) ๕.๑ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบอย่างน้อยดังต่อไปนี้ ๕.๑.๑ ระบบสำรองกระแสไฟฟ้า (UPS) ๕.๑.๒ ระบบระบายอากาศ ๕.๑.๓ ระบบปรับอากาศ และควบคุมความชื้น ๕.๒ ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ ๕.๓ ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน ๖. การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling Security) ๖.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ ๖.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย ๖.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ ๔.๑๐ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่ ๔.๑๑ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต ๔.๑๒ มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center) ๔.๑๓ จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ ๔.๑๔ จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญ อย่างน้อยปีละ ๑ ครั้ง ๕. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) ๕.๑ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้ ๕.๑.๑ ระบบสำรองกระแสไฟฟ้า (UPS) ๕.๑.๒ เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator) ๕.๑.๓ ระบบระบายอากาศ ๕.๑.๔ ระบบปรับอากาศ และควบคุมความชื้น ๕.๒ ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ ๕.๓ ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน ๖. การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling Security)	๖.๔ ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น ๖.๕ จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้องเป็นปัจจุบัน ๖.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงจากบุคคลภายนอก ๖.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี ๗. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance) ๗.๑ ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต ๗.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ ๗.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง ๗.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว ๗.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน ๗.๖ จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ๘. การนำทรัพย์สินของหน่วยงานออกไปใช้นอกหน่วยงาน (Removal of Property) ๘.๑ ให้มีการขออนุญาตก่อนนำทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน ๘.๒ กำหนดผู้รับผิดชอบในการเคลื่อนย้ายทรัพย์สินออกนอกหน่วยงาน ๘.๓ กำหนดระยะเวลาของการนำทรัพย์สินออกไปใช้งานนอกหน่วยงาน ๘.๔ เมื่อมีการนำทรัพย์สินส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของทรัพย์สิน ๘.๕ บันทึกข้อมูลการนำทรัพย์สินของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำทรัพย์สินส่งคืน ๙. การป้องกันทรัพย์สินที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises) ๙.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับทรัพย์สิน ๙.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยในที่สาธารณะโดยไม่มีเจ้าหน้าที่รับผิดชอบดูแล ๙.๓ เจ้าหน้าที่มีหน้าที่รับผิดชอบดูแลทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
๖.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ ๖.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย ๖.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน ๖.๔ ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น ๖.๕ จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง ๖.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิทเพื่อป้องกันการเข้าถึงของบุคคลภายนอก ๖.๗ พิจารณาใช้งานสายไฟเบอร์ออปติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่นสายสัญญาณแบบ coaxial cable) สำหรับระบบสารสนเทศที่สำคัญ ๖.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี ๗. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance) ๗.๑ ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต ๗.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ ๗.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง ๗.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ	๑๐. การใช้ซ้ำหรือกำจัดทิ้งอย่างปลอดภัย ดังนี้ ๑๐.๑ ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว ๑๐.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
เพื่อใช้ในการประเมินและ ปรับปรุงอุปกรณ์ดังกล่าว ๗.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษา อุปกรณ์ภายในหน่วยงาน ๗.๖ จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจาก ภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ๘. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property) ๘.๑ ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน ๘.๒ กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน ๘.๓ กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน ๘.๔ เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและ ตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย ๘.๕ บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็น หลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน ๙. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises) ๙.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์ ๙.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ	

แนวปฏิบัติ (เดิม)	แนวปฏิบัติ (ปรับปรุง)
๙.๓ เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง ๑๐. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง ดังนี้ ๑๐.๑ ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว ๑๐.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้	