สำนักงานสนับสนุนบริการสุขภาพ
เขต 10 จังหวัดอุบลราชธานี

นโยบายระเบียบและแนวทางปฏิบัติ
ด้านการรักษาความมั่นคงและปลอดภัยของระบบสารสนเทศ

โดย

คณะกรรมการการรักษาความมั่นคงและ
ปลอดภัยของระบบสารสนเทศ
ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

พ.ศ.๒๕๖๔

คำนำ

เอกสารฉบับนี้จัดทำขึ้น โดยมีวัตถุประสงค์เพื่อให้ระบบสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ มีความมั่นคงและปลอดภัยของสารสนเทศ สามารถดำเนินงานได้อย่างต่อเนื่องป้องกันปัญหาที่อาจเกิดขึ้นจากการทำงาน และจากการถูกคุกคามจากภัยต่างๆ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ จึงได้กำหนดนโยบาย ระเบียบ แนวปฏิบัติและขั้นตอนการปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงและปลอดภัยของระบบสารสนเทศและการถูกคุกคามจากภัยต่างๆ เพื่อเผยแพร่ให้เจ้าหน้าที่ในสำนักงานฯ ได้รับทราบและให้เจ้าหน้าที่ทุกคนต้องปฏิบัติตามเอกสารนี้โดยเคร่งครัด

คณะกรรมการการรักษาความมั่นคงและปลอดภัยด้านสารสนเทศ
ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐
กรกฎาคม พ.ศ.๒๕๖๓

สารบัญ

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
(Information Technology Security Policy)
ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ เป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัยและสามารถสนับสนุนการดำเนินงานของศูนย์ได้อย่างต่อเนื่อง มีการใช้งานระบบในลักษณะที่ถูกต้องสอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่ อาจก่อให้เกิดความเสียหายแก่งานราชการ ศูนย์ฯ จึงกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

คำนิยาม

คำนิยามในส่วนนี้เป็นการให้คำจำกัดความสำหรับศัพท์ที่ใช้งานในนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ เพื่อให้มีความหมายที่ชัดเจนและเข้าใจตรงกัน

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ

“สำนักงานฯ” หมายถึง ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

“การเข้าถึง” หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนการกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“ผู้ใช้งาน” หมายถึง บุคคลที่ได้รับอนุญาต ให้สามารถใช้งานสารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

“รหัสผ่าน” (Password) หมายถึง ตัวอักษรหรืออักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

“สินทรัพย์” หมายถึง ข้อมูลระบบ ข้อมูลทรัพย์สินด้านระบบสารสนเทศหรือสิ่งใดก็ตามที่มีคุณค่าของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ เช่น อุปกรณ์ ระบบเครือข่าย ซอฟต์แวร์ที่สำนักงานพัฒนา เป็นต้น

“ข้อมูล” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดในระบบคอมพิวเตอร์ในสภาพที่มีระบบคอมพิวเตอร์ที่อาจประมวลผลได้ และให้ความหมายรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบสารสนเทศต่างๆ ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ เช่น ระบบแลน (LAN) อินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

“ภัยพิบัติ” หมายถึง ภัยที่ก่อให้เกิดความเสียหายต่อชีวิต และทรัพย์สิน โดยส่งผลกระทบต่อภาวะเศรษฐกิจ และวิถีชีวิตของผู้คนในสังคมทั้งในระยะสั้น และระยะยาว ภัยพิบัติแบ่งเป็น ๒ ประเภท คือ ภัยพิบัติทางธรรมชาติ และภัยพิบัติที่มนุษย์สร้างขึ้น

“เจ้าหน้าที่” หมายถึง บุคลากรและเจ้าหน้าที่ที่ปฏิบัติงาน ในศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

“เจ้าหน้าที่ผู้รับผิดชอบ” หมายถึง เจ้าหน้าที่ที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

ส่วนที่ ๑
ระเบียบการใช้สารสนเทศ

๑. วัตถุประสงค์

สารสนเทศสำนักงาน ถือเป็นทรัพย์สินที่มีความสำคัญต่อการดำเนินงานของสำนักงานฯ จำเป็นต้องได้รับการดูแลรักษา เพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการทำงานได้อย่างมีประสิทธิภาพ คณะกรรมการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศของสำนักงานฯ ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบให้ข้อมูลและสารสนเทศ รวมทั้งระบบอุปกรณ์เสียหายได้

๒. ระเบียบการใช้สารสนเทศ ภายในศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

(๑) ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ ดำเนินกิจการภายใต้กฎหมายไทย ดังนั้น การใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อทาง อินเทอร์เน็ต ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๒) ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ ไม่สนับสนุน หรือยินยอมให้เจ้าหน้าที่ของ สำนักงานฯ กระทำผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายประกอบอื่นๆที่เกี่ยวข้อง

(๓) ระบบคอมพิวเตอร์และอุปกรณ์เครือข่ายถือเป็นทรัพย์สินของสำนักงานฯ ห้ามผู้ไม่ได้รับการอนุญาตหรือผู้ที่ไม่เกี่ยวข้องใช้งานโดยมิได้รับอนุญาต หากผู้ใดกระทำการใดๆ เป็นการบุกรุกเขตหวงห้ามหรือพยายามบุกรุกเข้าสู่ระบบเครือข่าย ถือเป็นการละเมิดตามกฎหมาย ต้องได้รับโทษตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายประกอบอื่นๆ ที่เกี่ยวข้อง

(๔) การยืม/คืน ทรัพย์สินสารสนเทศจะต้องทำตามขั้นตอนแบบฟอร์มการยืม/คืน ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

(๕) การทำลายอุปกรณ์หรือสื่อบันทึกข้อมูล สารสนเทศ ต้องทำตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการพัสดุ พ.ศ. ๒๕๓๕

(๖) เครื่องคอมพิวเตอร์ และอุปกรณ์ประกอบที่สำคัญของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ จะต้องมีการกำหนดรหัสผ่าน (PASSWORD) เพื่อควบคุมการเข้าถึงและเพื่อป้องกันการเข้าถึงข้อมูลสำนักงานโดยไม่ได้รับอนุญาต

(๗) เมื่อสิ้นสุดการใช้งานหรือสิ้นสุดสัญญาหรือสิ้นสุดข้อตกลงการจ้าง จะต้องคืนทรัพย์สินทั้งหมดที่ถือครองคืนให้ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

(๘) อุปกรณ์ของผู้ใช้งาน ที่เสื่อมสภาพ หรือไม่มีการใช้งาน ให้ปฏิบัติตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการพัสดุ พ.ศ. ๒๕๓๕

๓. ระเบียบการใช้คอมพิวเตอร์ตั้งโต๊ะ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

(๑) เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบถือเป็นทรัพย์สินของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ ผู้ใช้งานหรือเจ้าหน้าที่มีหน้าที่ ดูแลและรักษา หากมีข้อสงสัยหรือเหตุขัดข้าง ให้รีบแจ้งเจ้าหน้าที่ผู้รับผิดชอบ

(๒) ห้ามไม่ให้เคลื่อนย้าย เปลี่ยนแปลง แก้ไข เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ที่อยู่ภายใต้การดูแลของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ โดยไม่ได้รับอนุญาต หากมีความจำเป็นจะต้องแจ้งเจ้าหน้าที่ผู้รับผิดชอบ

(๓) หากมีความจำเป็นต้องนำเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ ไปใช้นอกสถานที่ เจ้าหน้าที่มีหน้าที่ดูแลและรักษา หากมีข้อสงสัยหรือเหตุขัดข้าง ให้รีบแจ้งเจ้าหน้าที่ผู้รับผิดชอบ

(๔) เครื่องคอมพิวเตอร์หรืออุปกรณ์ประกอบอื่นที่มิใช่ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ หากมีความจำเป็นต้องใช้งานในภารกิจของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ ให้แจ้งเจ้าหน้าที่ผู้รับผิดชอบและให้ใช้ชื่อผู้ใช้ (USERNAME) และรหัสผ่าน (PASSWORD) ของเจ้าของเครื่อง

(๕) ห้ามติดตั้ง อัพเดท ระบบปฏิบัติการและ โปรแกรมป้องกันไวรัส ซอฟต์แวร์ หรือชุดคำสั่งไม่พึงประสงค์ ใดลงบนเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ที่อยู่ภายใต้การดูแลของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ โดยไม่ได้รับอนุญาต หากมีความจำเป็นจะต้องแจ้งเจ้าหน้าที่ผู้รับผิดชอบ

(๖) เมื่อพบปัญหาหรือมีข้อสงสัยในการใช้งานด้านฮาร์ดแวร์/ซอฟต์แวร์ ให้ติดต่อแจ้งเจ้าหน้าที่ผู้รับผิดชอบ

(๗) เจ้าหน้าที่ผู้รับผิดชอบ จะต้องมีการกำหนดหมายเลขไอพีแอดเดรส สำหรับเครื่องคอมพิวเตอร์ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ หากมีเหตุขัดข้อง เกี่ยวกับหมายเลขไอพีแอดเดรส ให้รีบแจ้งเจ้าหน้าที่ผู้รับผิดชอบทราบ

๔. ระเบียบการใช้คอมพิวเตอร์พกพา ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

(๑) เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบถือเป็นทรัพย์สินของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ ผู้ใช้งานหรือเจ้าหน้าที่มีหน้าที่ดูแลและรักษา หากมีข้อสงสัยหรือเหตุขัดข้อง ให้รีบแจ้งเจ้าหน้าที่ผู้รับผิดชอบ

(๒) เจ้าหน้าที่ หากมีความจำเป็นต้องนำเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ ไปใช้นอกสถานที่ให้ทำตามขั้นตอนแบบฟอร์มการยืม/คืน ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ เจ้าหน้าที่มีหน้าที่ผู้ใช้งานมีหน้าที่ดูแลและรักษา หากมีข้อสงสัยหรือเหตุขัดข้อง ให้รีบแจ้งเจ้าหน้าที่ผู้รับผิดชอบและความเสียหายเกิดจากความประมาทของผู้ยืมจะต้องรับผิดชอบความเสียหายและต้องดำเนินการให้อยู่ในสภาพที่ใช้การได้โดยเร็ว

(๓) เครื่องคอมพิวเตอร์หรืออุปกรณ์ประกอบอื่นที่มิใช้ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ หากมีความจำเป็นต้องใช้งานในภารกิจของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ ให้แจ้งเจ้าหน้าที่สารสนเทศและให้ใช้ชื่อผู้ใช้ (USERNAME) และรหัสผ่าน (PASSWORD) ของเจ้าของเครื่อง

(๔) ห้ามติดตั้ง อัพเดท ระบบปฏิบัติการและ โปรแกรมป้องกันไวรัส ซอฟต์แวร์ หรือชุดคำสั่งไม่พึงประสงค์ ใดลงบนเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ที่อยู่ภายใต้การดูแลของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ โดยไม่ได้รับอนุญาต หากมีความจำเป็นจะต้องแจ้งเจ้าหน้าที่ผู้รับผิดชอบสนเทศ

(๕) เมื่อพบปัญหาหรือมีข้อสงสัยในการใช้งานด้านฮาร์ดแวร์/ซอฟต์แวร์ ให้ติดต่อแจ้งเจ้าหน้าที่ผู้รับผิดชอบ

๕. ระเบียบข้อกำหนดในการเข้าถึงข้อมูลอินเตอร์เน็ตและเครือข่าย ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

(๑) ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ จะจัดให้มีชื่อผู้ใช้ (USERNAME) และรหัสผ่าน (PASSWORD) ให้กับเจ้าหน้าผู้มีหน้าที่เกี่ยวข้องกับการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อกับ อินเทอร์เน็ต เป็นรายบุคคล ทั้งนี้เพื่อความปลอดภัยของระบบโดยรวม

(๒) รหัสผ่านของเจ้าหน้าที่ถือเป็นทรัพย์สินของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ ไม่อนุญาตให้มีการแจ้งรหัสผ่านที่เป็นข้อมูลส่วนตัวให้กับบุคคลอื่น และเจ้าหน้าที่ทุกคนมีหน้าที่ในการป้องกันรหัสผ่านขององค์กรอย่างเคร่งครัด ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ ไม่อนุญาตให้ใช้ชื่อและรหัสผ่านร่วมกัน หากมีการใช้งานผู้ใช้ (USERNAME) และรหัสผ่าน (PASSWORD) ผู้เป็นเจ้าของมีหน้าที่รับผิดชอบ หากมีการกระทำผิด

(๓) บุคคลผู้มีสิทธิเข้าถึงข้อมูลอินเตอร์เน็ตและเครือข่ายไร้สาย ได้แก่ เจ้าหน้าที่ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

(๔) การเข้าถึงข้อมูลอินเตอร์เน็ตและเครือข่ายไร้สาย จะต้องมีรหัสในการใช้งานที่ออกโดยศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

(๕) การเพิ่ม/แก้ไข/ยกเลิก ข้อมูลรหัสในการใช้งานเพื่อการเข้าเข้าถึงสารสนเทศจะต้องแจ้งให้กับเจ้าหน้าที่ผู้รับผิดชอบ

(๖) บุคคลภายนอกหากต้องการใช้งานอินเตอร์เน็ตและเครือข่ายไร้สายจะต้องลงทะเบียนและแจ้งกับเจ้าหน้าที่ผู้รับผิดชอบ

(๗) ไม่อนุญาตให้ผู้ที่ไม่เกี่ยวข้องเข้าถึงการใช้ PORT สำหรับการเชื่อมต่อเครือข่าย หากมีความจำเป็นจะต้องแจ้งเจ้าหน้าที่ผู้รับผิดชอบและได้รับคำยินยอมในการแก้ไขจากผู้รับผิดชอบสารสนเทศเขตหรือกรมสนับสนุนบริการสุขภาพ

(๘) ไม่อนุญาตให้ผู้ที่ไม่เกี่ยวข้องเข้าถึง Vlan(Virtual Area Network) หากมีความจำเป็นจะต้องแจ้งเจ้าหน้าที่ผู้รับผิดชอบและได้รับคำยินยอมในการแก้ไขจากผู้รับผิดชอบสารสนเทศเขตหรือกรมสนับสนุนบริการสุขภาพ

(๙) ไม่อนุญาตให้ผู้ที่ไม่เกี่ยวข้องเข้าถึง Firewall หากมีความจำเป็นจะต้องแจ้งเจ้าหน้าที่ผู้รับผิดชอบและได้รับคำยินยอมในการแก้ไขจากผู้รับผิดชอบสารสนเทศเขตหรือกรมสนับสนุนบริการสุขภาพ

๖. ระเบียบข้อกำหนดในการการใช้จดหมายอิเล็กทรอนิกส์, การสนทนา และการติดต่อสื่อสารทางอิเล็กทรอนิกส์อื่นๆ (e-mail, chat, and others digital communication) ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

ในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นจดหมายอิเล็กทรอนิกส์ การสนทนา หรือการติดต่อสื่อสารใดๆ ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ ต้องปฏิบัติดังนี้

(๑) การรักษาความลับของเอกสาร ห้ามส่งเอกสารความลับโดยจดหมายอิเล็กทรอนิกส์ ยกเว้นได้รับการยินยอมจากหัวหน้าหรือผู้บังคับบัญชา

(๒) ห้ามส่งข้อมูลที่เป็นเท็จ ห้ามส่งรูปหรือข้อความที่เกี่ยวข้องกับเรื่องลามก อนาจาร หรือข้อมูลที่ก่อให้เกิดความเสียหายต่อ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ หรือบุคคลอื่นๆ

(๓) การส่งข้อมูลใดๆ ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๔) หากพบว่ามีการส่งข้อมูลที่ผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือผิดต่อกฎระเบียบของ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ ให้แจ้งต่อผู้รับผิดชอบสารสนเทศและผู้รับผิดชอบสารสนเทศรายงานผู้บังคับบัญชา

(๕) ห้ามส่งจดหมายอิเล็กทรอนิกส์หรือการสื่อสารทางอิเล็กทรอนิกส์ใดๆ โดยไม่ระบุชื่อผู้ส่ง (SPAM e-mail)

(๖) การส่งข้อความทางอิเล็กทรอนิกส์ของกระทรวงไอซีที(mail.go.th) ใช้เฉพาะงานที่เกี่ยวข้องกับงานราชการเท่านั้น

ส่วนที่ ๒
การควบคุมการเข้าถึงและใช้งานสารสนเทศ
(Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศขององค์การและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศให้หยุดชะงักและทาให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของสำนักงานฯ ได้อย่างถูกต้อง

๒. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

๒.๑ จัดทำทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๒.๒ สถานที่ตั้งของระบบสารสนเทศที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๒.๓ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึง ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๔ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

๓. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๓.๑ ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารหรือกรอกแบบฟอร์ม เพื่อขอสิทธิในการเข้าสู่ระบบ

๓.๒ เจ้าของข้อมูลและเจ้าของระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๓.๓ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

๔. การบริหารจัดการการเข้าถึงของผู้ใช้

๔.๑ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

– อ่านอย่างเดียว

- ป้อนข้อมูล /แก้ไข
- ไม่มีสิทธิ์

(๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของสำนักงานฯ จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากประธานคณะกรรมการการรักษาความมั่นคงและปลอดภัยสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒ กำหนดสิทธิการใช้ระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร

๔.๓ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของเจ้าหน้าที่

๔.๓.๑ ผู้ที่รับผิดชอบงานนั้นๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบสารสนเทศแต่ละระบบรวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ

๔.๓.๒ การกำหนดการเปลี่ยนแปลงและยกเลิกรหัสผ่านต้องปฏิบัติตาม “ระเบียบข้อกำหนดในการเข้าถึงข้อมูลอินเตอร์เน็ตและเครือข่าย ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐”

๔.๓.๓ ควรมีการทบทวนการเปลี่ยนรหัสผ่าน ทุกๆ ๑ ปี

๕. ระดับความสำคัญของข้อมูล

สำนักงานฯ จัดแบ่งระดับความสำคัญของข้อมูลออกเป็น ๓ ระดับ คือ

๕.๑ ข้อมูลที่มีความสำคัญมากที่สุด

๕.๒ ข้อมูลที่มีระดับความสำคัญปานกลาง

๕.๓ ข้อมูลที่มีระดับความสำคัญน้อย

๖. ระดับความลับของข้อมูล

สำนักงานฯ จัดแบ่งระดับความลับของข้อมูลออกเป็น ๔ ระดับ คือ

๖.๑ ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

๖.๒ ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

๖.๓ ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๖.๔ ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๗. ระดับชั้นการเข้าถึง

สำนักงานฯ จัดแบ่งระดับชั้นการเข้าถึงออกเป็น ๓ ระดับ คือ

๗.๑ ระดับชั้นสำหรับผู้บริหาร

๗.๒ ระดับชั้นสำหรับผู้ใช้งานทั่วไป

๗.๓ ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๘. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection)

๘.๑ ผู้ดูแลระบบต้องกำหนดการเปิด-ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่างๆ โดยจะปิดพอร์ตที่เสี่ยงที่ก่อให้เกิดความเสียหายต่อระบบเครือข่าย

๘.๒ ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

ส่วนที่ ๓
การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

๑. วัตถุประสงค์

กำหนดขึ้นด้วยวัตถุประสงค์เพื่อป้องกันการใช้งานเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต อันจะเป็นการป้องกันทรัพยากรและข้อมูลของสำนักงานฯ ให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๒.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๒.๒ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๒.๓ ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ Password ทุกครั้ง

๒.๔ ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของสำนักงานฯ ร่วมกัน

๒.๕ ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๓. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๓.๑ การพิสูจน์ตัวตนสำหรับผู้ใช้งาน ผู้ดูแลระบบสารสนเทศต้องให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

๓.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๓.๓ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๓.๔ ผู้ใช้งานจะต้องลง Login โดยใช้ชื่อบัญชีผู้ใช้บริการ (Account) ของตนเอง และ Logout ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๔. การบริหารจัดการรหัสผ่าน (Password Management System)

๔.๑ วิธีการบริหารจัดการรหัสผ่านของผู้ใช้ให้มีความมั่นคงปลอดภัย กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน แต่ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๔.๒ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๔.๓ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password)

๔.๔ ควรทำการเปลี่ยนรหัสผ่าน เพื่อใช้งานเครื่องคอมพิวเตอร์ของสำนักงานฯ ทุก ๖ – ๑๒ เดือน หรือเปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

๕. การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

การควบคุมการใช้งานโปรแกรมอรรถประโยชน์ ผู้ดูแลระบบกำหนดให้มีการควบคุมการใช้โปรแกรมอรรถประโยชน์สำหรับการเข้าระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

๕.๑ มีการพิสูจน์ตัวตนสำหรับผู้ใช้งาน

๕.๑.๑ ต้องแสดงตัวตนสำหรับผู้ใช้งาน

๕.๑.๒ ต้องพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน

๕.๒ การติดตั้งโปรแกรมอรรถประโยชน์เพื่อใช้งานร่วมกับระบบปฏิบัติการ

๕.๒.๑ ให้ทำการแยกโปรแกรมอรรถประโยชน์ออกจากโปรแกรมระบบงาน

๕.๒.๒ จำกัดการใช้งานโปรแกรมอรรถประโยชน์ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น

๕.๒.๓ หลีกเลี่ยงการติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์

๕.๒.๔ ต้องติดตั้งโปรแกรมตามภารกิจและไม่ติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

๕.๓ จำกัดช่วงวันหรือช่วงเวลาในการอนุญาตให้เข้าสู่ระบบตามความจำเป็น

๕.๓.๑ จำกัดระยะเวลาการใช้งานระบบปฏิบัติการที่เชื่อมต่อ เช่น ตัดการเชื่อมต่อเมื่อใช้งานได้ระยะหนึ่งซึ่งได้กำหนดไว้ล่วงหน้า จำกัดการเชื่อมต่อระบบปฏิบัติการให้เป็นเฉพาะภายในระยะเวลาทำการ ให้ตรวจสอบยืนยันตัวตนใหม่ทุกช่วงเวลาที่กำหนด

๖. เมื่อมีการวางเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

๖.๑ เมื่อใช้งานในระยะหนึ่ง ระบบจะดำเนินการตัดสัญญาณอินเตอร์เน็ต (session timeout) เพื่อนำสัญญาณไปให้ผู้ที่ร้องขออื่นต่อไป

๖.๒ ต้องกำหนดให้ระบบสารสนเทศตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เช่น ระบบ GF-MIS เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ส่วนที่ ๔
การจัดทำระบบสำรองข้อมูล
(Creating a backup system)

๑. วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติการสำรองข้อมูลและกู้คืนระบบ โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบสามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น

๒. แนวปฏิบัติการสำรองข้อมูลและระบบคอมพิวเตอร์

๒.๑ บุคคลผู้ที่มีหน้าที่รับผิดชอบส่งข้อมูลสำรองด้านสารสนเทศที่สำคัญของสำนักงานฯ ได้แก่ เจ้าหน้าที่ได้รับมอบหมายในการสำรองข้อมูล ในแต่ละกลุ่ม/ฝ่าย โดยการสำรองข้อมูลตามความถี่ (ต่อสัปดาห์, ต่อเดือน, ต่อไตรมาส, อื่นๆ) และส่งมอบข้อมูลให้กับเจ้าหน้าที่ผู้รับผิดชอบ

๒.๒ การสำรองข้อมูลการทำงานเบื้องต้น อื่นๆ เช่น ข้อมูลการทำงานส่วนตัว ฯลฯ เป็นหน้าที่ของเจ้าของข้อมูลนั้นๆ ในการเก็บข้อมูลสำรองผ่าน อุปกรณ์การเก็บข้อมูลสำรอง เช่น External hard disk , Usb drive

๒.๓ การขอข้อมูลสำรองย้อนหลัง สามารถขอตามขั้นตอนที่คณะกรรมการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกำหนด และสามารถขอข้อมูลสำรองไม่เกิน ๓ เดือนย้อนหลัง

๒.๕ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อประธานคณะกรรมการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๖ ให้ผู้ดูแลระบบกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมี ๒ ชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๔. การกู้คืนระบบ

๔.๑ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบ ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อประธานคณะกรรมการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๒ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๔.๓ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ ให้แจ้งผู้ใช้งานทราบทันที

ส่วนที่ ๕
แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติด้านเทคโนโลยีสารสนเทศ
(IT Contingency Plan)

๑.วัตถุประสงค์

๑.๑ เพื่อใช้เป็นแนวทางการรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

๑.๒ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาความปลอดภัยของฐานข้อมูลและสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

๑.๔ เพื่อให้การปฏิบัติเป็นไปอย่างมีระบบและต่อเนื่องและสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดเหตุการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อสารสนเทศ

๑.๕ เพื่อให้สอดคล้องตามโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๒. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

๒.๑ วิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของสำนักงานฯ สามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่

๒.๒.๑ ภัยพิบัติจากภายนอก

ก) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่อระบบเทคโนโลยีสารสนเทศ ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย ความชื้น อุณหภูมิ แผ่นดินไหว ฯลฯ

ข) การโจรกรรมอุปกรณ์คอมพิวเตอร์เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

ค) ระบบการสื่อสารที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

ง) ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

จ) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

ฉ) ไวรัสคอมพิวเตอร์

๒.๒.๒ ภัยพิบัติจากภายใน

ก) ระบบกระจายสัญญาณอินเตอร์เน็ตหลักเสียหาย หรือข้อมูลถูกทำลาย

ข) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในสำนักงานฯ

ค) เจ้าหน้าที่หรือบุคลากรของสำนักงานฯ ขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์ คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๓. การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation assessment)

เมื่อสำนักงานฯ มีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรง ภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย เพื่อนำมาสรุปเป็นข้อมูลต่อไป

๓.๑ กำหนดเกณฑ์ลำดับ ความเสี่ยงไว้ ๕ ลำดับ คือ

๓.๑.๑ ลำดับ ๕ หมายถึง ความเสี่ยงสูงสุด

- งดใช้ ชั่วคราว
- ติดป้ายเตือน
- ออกข้อกำหนด มาตรการ หรือออกกฎ
- ให้ความสำคัญ เช่น อุปกรณ์เครื่องดับเพลิง
- ดำเนินการแก้ไขเร่งด่วน

๓.๑.๒ ลำดับ ๔ หมายถึง ความเสี่ยงปานกลาง

- งดใช้ ชั่วคราว
- ติดป้ายเตือน
- ออกข้อกำหนด มาตรการ หรือออกกฎ
- ให้ความสำคัญ เช่น อุปกรณ์เครื่องดับเพลิง
- ดำเนินการแก้ไขโดยด่วน

๓.๑.๓ ลำดับ ๓ หมายถึง เกิดบ่อยแต่ไม่รุ่นแรง

- งดใช้ ชั่วคราว
- ออกข้อกำหนด มาตรการ หรือออกกฎ
- ดำเนินการแก้ไขโดยเร็ว

๓.๑.๔ ลำดับ ๒ หมายถึง เกิดไม่บ่อยและไม่รุนแรง

- งดใช้ ชั่วคราว
- ดำเนินการแก้ไข

๓.๑.๕ ลำดับ ๑ หมายถึง เกือบจะเกิดแต่ยังไม่เกิด

- งดใช้ ชั่วคราว
- ดำเนินการแก้ไขเป็นกรณี

๓.๒ การประเมินสถานการณ์และกำหนดระดับความรุนแรง

พื้นที่	โอกาส (L)	ผลกระทบ (C)	ระดับความเสี่ยง	ลำดับความเสี่ยง	ระดับความเสี่ยง	หมายเหตุ
ไฟไหม้	๒	๔	๘	๑	**๕**	
กรณีไฟดับ / หม้อไฟระเบิด	๒	๒	๔	๒	**๓**	
กรณีแผ่นดินไหว	๒	๒	๔	๒	**๒**	
กรณีโดนเจาะระบบและภัยคุกคามทางคอมพิวเตอร์	๒	๒	๒	๓	**๒**	
จลาจล การชุมนุม / เหตุการณ์ความไม่สงบ	๑	๑	๑	๔	**๑**	
น้ำท่วม	๑	๑	๑	๔	**๑**	

๓.๓. ลำดับความสำคัญทรัพย์สินสารสนเทศกรณีเหตุการณ์ภัยพิบัติ

หากเกิดเหตุภัยพิบัติ ต้องคำนึงถึงความปลอดภัยของเจ้าหน้าที่เป็นลำดับแรกและทรัพย์สินสารสนเทศตามลำดับ และให้ปฏิบัติตามกระบวนการแต่ละกระบวนการในการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดกับสารสนเทศศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

๓.๓.๑ กำหนดเกณฑ์ลำดับความสำคัญอุปกรณ์สารสนเทศเหตุการณ์ภัยพิบัติ เมื่อมี ๕ ลำดับ คือ

๓.๓.๑.๑ ความสำคัญลำดับ ๑

- เข้าตรวจสอบระบบและอุปกรณ์สารสนเทศ พร้อมทั้งทำรายงานความเสียหาย เพื่อแจ้งประธานคณะกรรมการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ภายใน ๒๔ ชั่วโมง
- ขนย้ายอุปกรณ์สารสนเทศออกจากที่เกิดเหตุโดยเร่งด่วน

๓.๓.๑.๒ ความสำคัญลำดับ ๒

- ตรวจสอบระบบและอุปกรณ์สารสนเทศ พร้อมทั้งทำรายงานความเสียหาย เพื่อแจ้งประธานคณะกรรมการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- ขนย้ายอุปกรณ์สารสนเทศออกจากที่เกิดเหตุโดยด่วน

๓.๓.๑.๓ ความสำคัญลำดับ ๓

- ตรวจสอบระบบและอุปกรณ์สารสนเทศ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งประธานคณะกรรมการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- ขนย้ายอุปกรณ์สารสนเทศหากมีความจำเป็น

๓.๓.๑.๔ ความสำคัญลำดับ ๔

- ตรวจสอบความเสียหายโดยเร็วและรายงานต่อผู้บังคับบัญชา

๓.๓.๑.๕ ความสำคัญลำดับ ๕

- ตรวจสอบความเสียหายและรายงานต่อผู้บังคับบัญชา

๓.๓.๒ การแบ่งลำดับทรัพย์สินสารสนเทศดังนี้

รายการ	โอกาส (L)	ผลกระทบ (C)	ระดับความเสี่ยง (LxC)	ลำดับความสำคัญ	หมายเหตุ
Firewall	๓	๓	๙	**๑**	
CCTV และ DVR	๓	๓	๙	**๑**	
Computer	๓	๒	๖	**๒**	
Notebook	๓	๒	๖	**๒**	
Projector	๒	๓	๖	**๒**	
Router ๓BB fiber	๒	๓	๖	**๒**	
Printer	๒	๒	๔	**๓**	
Wireless	๒	๒	๔	**๓**	
Switch	๒	๒	๔	**๓**	
HDD External ๑ TB	๒	๒	๔	**๓**	
Scanner	๒	๑	๒	**๔**	
UPS	๒	๑	๒	**๔**	
Screen Projector	๒	๑	๒	**๔**	
Lan point	๑	๑	๒	**๔**	
Wireless External usb	๑	๑	๑	**๕**	

๔. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดกับสารสนเทศศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

การป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ กำหนดแนวทางให้เจ้าหน้าที่ปฏิบัติดังนี้

๔.๑ กรณีจากไฟไหม้

๔.๑.๑ ก่อนเกิดเหตุ

๔.๑.๑.๑ เจ้าหน้าที่ผู้รับผิดชอบอุปกรณ์ ตรวจเช็คอุปกรณ์และสภาพแวดล้อมหากพบปัจจัยที่ทำให้เกิดไฟไหม้ให้รีบแจ้งหัวหน้ากลุ่ม/ฝ่าย เพื่อ ให้ผู้ที่เกี่ยวข้องตรวจสอบต่อไป

๔.๑.๑.๒ ปฏิบัติตามขั้นตอนแผนภัยพิบัติ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

๔.๑.๑.๓ กลุ่มงานจะต้องจัดเตรียมอุปกรณ์ เครื่องดับเพลิง ไว้ใช้บริเวณใกล้เคียงที่จำสามารถใช้งานได้โดยสะดวกในกรณีเกิดไฟไหม้

๔.๑.๑.๔ ไม่เก็บสารไวไฟหรือวัตถุเชื้อเพลิง ไว้ใกล้อุปกรณ์คอมพิวเตอร์

๔.๑.๒ ระหว่างเกิดเหตุ

๔.๑.๒.๑ เจ้าหน้าที่ผู้รับผิดชอบอุปกรณ์ ดำเนินการป้องกันมิให้เกิดความเสียหายในเบื้องต้นโดยการเคลื่อนย้ายอุปกรณ์สารสนเทศไปที่ปลอดภัยและแจ้งคณะกรรมการที่รับผิดชอบด้านสารสนเทศและผู้บังคับบัญชาเพื่อให้ อุปกรณ์สารสนเทศเสียหายน้อยที่สุด

๔.๑.๒.๒ หากเหตุเกิดวันหยุดราชการให้ดำเนินการแก้ไขปัญหาเบื้องต้นมิให้เกิดความเสียหาย โดยแจ้งคณะกรรมการที่รับผิดชอบด้านสารสนเทศและเจ้าหน้าที่รักษาความปลอดภัยเพื่อให้อุปกรณ์สารสนเทศเสียหายน้อยที่สุด

๔.๑.๒.๓ ปฏิบัติตามขั้นตอนแผนภัยพิบัติ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

๔.๑.๒.๔ ใช้อุปกรณ์ที่น้ำยาดับเพลิง ฉีดควบคุมเพลิงดับและจัดการขนย้ายอุปกรณ์ที่สามารถขนย้ายได้ (บางส่วน) ไปยังสถานที่ที่ปลอดภัยได้แก่ นอกตึกอาคารสำนักงานหรือแล้วแต่เหตุไฟไหม้และความเหมาะสม แต่ถ้าไม่สามารถแก้ไขหรือควบคุมเพลิงได้ต้องดำเนินการในข้อ ต่อไป

๔.๑.๒.๕ แจ้งสถานีดับเพลิงที่ใกล้ที่สุด คือ สถานีดับเพลิงเทศบาลนครอุบลราชธานี จังหวัดอุบลราชธานี เบอร์โทรศัพท์ ๙๑๑ เพื่อดำเนินการต่อไป

๔.๑.๓ หลังเกิดเหตุ

๔.๑.๓.๑ เจ้าหน้าที่ผู้รับผิดชอบ ดำเนินการเข้าตรวจสอบระบบและอุปกรณ์สารสนเทศพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งประธานคณะกรรมการที่รับผิดชอบด้านสารสนเทศและผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ทราบ

๔.๒ กรณีไฟดับ / หม้อไฟระเบิด

๔.๒.๑ ก่อนเกิดเหตุ

๔.๒.๑.๑ เจ้าหน้าที่ผู้รับผิดชอบอุปกรณ์ ตรวจเช็คอุปกรณ์เครื่องสำรองไฟพบปัญหาอุปกรณ์ให้แจ้งเจ้าหน้าที่ผู้รับผิดชอบ

๔.๒.๑.๒ กลุ่มงานวิศวกรรมการแพทย์ ทำการตรวจเช็คหม้อแปลงไฟฟ้าอย่างน้อยปีละ ๑ ครั้ง

๔.๒.๒ ระหว่างเกิดเหตุ

๔.๒.๒.๑ เจ้าหน้าที่ผู้รับผิดชอบอุปกรณ์ ดำเนินการป้องกันมิให้เกิดความเสียหายในเบื้องต้น โดยการบันทึกข้อมูลและปิดเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศเพื่อให้ อุปกรณ์สารสนเทศเสียหายน้อยที่สุด

๔.๒.๒.๒ ปฏิบัติตามขั้นตอนแผนภัยพิบัติ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

๔.๒.๒.๓. แจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการโดย การไฟฟ้าส่วนภูมิภาค เขต ๒ จังหวัดอุบลราชธานี เบอร์โทรศัพท์ ๐๔๕-๒๔๒๔๓๔-๖ เพื่อดำเนินการต่อไป

๔.๒.๓ หลังเกิดเหตุ

๕.๒.๓.๑ เจ้าหน้าที่ผู้รับผิดชอบอุปกรณ์ ที่ตรวจสอบตรวจสอบระบบและอุปกรณ์สารสนเทศ หากพบอุปกรณ์สารสนเทศเสียหายให้แจ้งเจ้าหน้าที่ผู้รับผิดชอบ

๔.๓ กรณีน้ำท่วม

๔.๓.๑ ก่อนเกิดเหตุ

๔.๓.๑.๑ เจ้าหน้าที่ผู้รับผิดชอบอุปกรณ์ ตรวจเช็คอุปกรณ์ หากพบปัญหาอุปกรณ์ให้แจ้งเจ้าหน้าที่ผู้รับผิดชอบ

๔.๓.๒ ระหว่างเกิดเหตุ

๔.๓.๒.๑ ผู้รับผิดชอบอุปกรณ์ ดำเนินการป้องกันมิให้เกิดความเสียหายในเบื้องต้น โดยการขนย้ายอุปกรณ์ขึ้นที่สูง เพื่อให้อุปกรณ์สารสนเทศเสียหายน้อยที่สุด

๔.๓.๓ หลังเกิดเหตุ

๔.๓.๓.๑ เจ้าหน้าที่ผู้รับผิดชอบอุปกรณ์ ตรวจสอบตรวจสอบระบบและอุปกรณ์สารสนเทศ หากพบอุปกรณ์สารสนเทศเสียหายให้แจ้งเจ้าหน้าที่ผู้รับผิดชอบ

๔.๔ กรณีแผ่นดินไหว

๔.๔.๑ ก่อนเกิดเหตุ

๔.๔.๑.๑ ผู้รับผิดชอบอุปกรณ์ ตรวจเช็คอุปกรณ์ หากพบปัญหาอุปกรณ์ให้แจ้งเจ้าหน้าที่ผู้รับผิดชอบ

๔.๔.๒ ระหว่างเกิดเหตุ

๔.๔.๒.๑ เจ้าหน้าที่ผู้รับผิดชอบอุปกรณ์ ดำเนินการป้องกันมิให้เกิดความเสียหายในเบื้องต้น โดยการเคลื่อนย้ายอุปกรณ์สารสนเทศไปที่ปลอดภัยและแจ้งคณะกรรมการที่รับผิดชอบด้านสารสนเทศและผู้บังคับบัญชาเพื่อให้อุปกรณ์สารสนเทศเสียหายน้อยที่สุด

๔.๔.๒.๒ หากเหตุเกิดวันหยุดราชการให้ดำเนินการแก้ไขปัญหาเบื้องต้นมิให้เกิดความเสียหาย โดยแจ้งคณะกรรมการที่รับผิดชอบด้านสารสนเทศและเจ้าหน้าที่รักษาความปลอดภัยเพื่อให้อุปกรณ์สารสนเทศเสียหายน้อยที่สุด

๔.๔.๒.๓ ปฏิบัติตามขั้นตอนแผนภัยพิบัติ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

๔.๔.๒.๔ แจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้ การไฟฟ้าส่วนภูมิภาคจังหวัดอุบลราชธานี เบอร์โทรศัพท์ ๐๙๔ - ๙๐๖๘๙๐๘ เพื่อดำเนินการต่อไป

๔.๔.๓ หลังเกิดเหตุ

๔.๔.๓.๑ เจ้าหน้าที่ผู้รับผิดชอบ ดำเนินการเข้าตรวจสอบระบบและอุปกรณ์สารสนเทศ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งประธานคณะกรรมการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๕ กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์

๔.๕.๑ ก่อนเกิดเหตุ

๔.๕.๑.๑ เจ้าหน้าที่ผู้รับผิดชอบอุปกรณ์ ตรวจเช็คอุปกรณ์ หากพบปัญหาอุปกรณ์ให้แจ้งเจ้าหน้าที่ผู้รับผิดชอบ

๔.๕.๒ ระหว่างเกิดเหตุ

๔.๕.๒.๑ ผู้รับผิดชอบสนเทศของสำนักงานฯ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์สารสนเทศ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งประธานคณะกรรมการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศทราบ

๔.๕.๓ หลังเกิดเหตุ

๔.๕.๓.๑ ให้ผู้รับผิดชอบสนเทศของสำนักงานฯ ตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถแก้ไขปัญหาได้แจ้งเหตุขัดข้องให้กรมฯ เพื่อแก้ไขปัญหาต่อไป

๔.๖ กรณีจลาจล การชุมนุม / เหตุการณ์ความไม่สงบ

๔.๖.๑ ก่อนเกิดเหตุ

๔.๖.๑.๑ เจ้าหน้าที่ผู้รับผิดชอบอุปกรณ์ ตรวจเช็คอุปกรณ์ หากพบปัญหาอุปกรณ์ให้แจ้งเจ้าหน้าที่ผู้รับผิดชอบ

๔.๖.๒ ระหว่างเกิดเหตุ

๔.๖.๒.๑ บันทึกข้อมูลสำคัญและปิดคอมพิวเตอร์อุปกรณ์สารสนเทศ ล๊อคประตูและล๊อคอาคารสำนักงานฯ

๔.๖.๓.๑ แจ้งเจ้าหน้าที่รักษาความปลอดภัยเพื่อปิดประตูสำนักงานฯ เพื่อลดความเสียหายเบื้องต้น

๔.๖.๓ หลังเกิดเหตุ

๔.๖.๓.๑ เจ้าหน้าที่ผู้รับผิดชอบ ดำเนินการเข้าตรวจสอบระบบและอุปกรณ์สารสนเทศ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งประธานคณะกรรมการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศทราบ

ส่วนที่ ๖
การควบคุมตู้กระจายสัญญาณและการป้องกันความเสียหาย

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการและแนวทางในการป้องกันตู้กระจายสัญญาณและอุปกรณ์ในตู้กระจายสัญญาณ เนื่องจากตู้กระจายสัญญาณ ใช้สำหรับกระจายสัญญาณและนำเข้าสัญญาณเครือข่ายที่สำคัญและจัดเก็บอุปกรณ์เครือข่ายหลัก ดังนั้น เพื่อให้การเข้าใช้ตู้กระจายสัญญาณเป็นไปด้วยความสะดวก เรียบร้อย มีความปลอดภัยทั้งข้อมูลและอุปกรณ์ จึงได้กำหมดสิทธิ์การเข้าออกห้องเซิร์ฟเวอร์ เฉพาะเจ้าหน้าผู้เกี่ยวข้องและบุคคลที่มีความจะเป็นต้องเข้าใช้ห้องเซิร์ฟเวอร์

๒. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานตู้กระจายสัญญาณ

๒.๑ บุคคลผู้มีสิทธิเข้าใช้ตู้กระจายสัญญาณ ได้แก่ เจ้าหน้าผู้รับผิดชอบดูแลเครือข่าย ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

๒.๒ บุคคลภายนอกที่จะขอเข้าใช้ตู้กระจายสัญญาณ เช่น ติดตั้งและซ่อมบำรุงรักษาอุปกรณ์ต่างๆ ภายในห้องเซิร์ฟเวอร์ และต้องแจ้งเจ้าหน้าที่ผู้รับผิดชอบ

๒.๓ วันและเวลาการใช้ตู้กระจายสัญญาณ คือวันและเวลาราชการที่มีการทำงานตามปกติคือ ๘.๓๐ น.–๑๖.๓๐ น. ยกเว้นวันหยุดราชการ

๒.๔ กรณีที่มีเหตุฉุกเฉินที่จะเข้าใช้ตู้กระจายสัญญาณ ให้รีบแจ้งเจ้าหน้าที่ผู้รับผิดชอบ

๓. ข้อปฏิบัติการบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

๓.๑ ตรวจสอบความพร้อมของระบบรักษาความปลอดภัยสม่ำเสมอ

๓.๒ กำหนดขั้นตอนแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน เช่น ไฟไหม้ หรือมีผู้บุกรุก เป็นต้น

๓.๓ มีตารางการเข้าบำรุงรักษาอุปกรณ์

ส่วนที่ ๗
การใช้งานคอมพิวเตอร์สำนักงาน
(Using a personal computer for office)

๑. บทนำ

การใช้งานเครื่องคอมพิวเตอร์ภายในสำนักงานฯ มีการเชื่อมต่อเครือข่ายภายในและภายนอกในระบบเครือข่ายแบบอินทราเน็ตและเครือข่ายอินเทอร์เน็ต ซึ่งอาจมีการติดไวรัสคอมพิวเตอร์หรือ malware ต่างๆ เครื่องคอมพิวเตอร์เหล่านี้อาจถูกโจมตีและเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต เพื่อให้การทำงานเป็นไปอย่างมีประสิทธิภาพ จึงต้องมีการกำหนดการใช้คอมพิวเตอร์ส่วนบุคคล เพื่อให้มีความเข้าใจที่ตรงกันเกี่ยวกับการใช้งานคอมพิวเตอร์ส่วนบุคคลภายในสำนักงานฯ

๒. วัตถุประสงค์

เพื่อให้มีการจัดการด้านความมั่นคงปลอดภัยด้านสารสนเทศเป็นไปอย่างมีระบบ มีแบบแผนและสามารถจัดการแก้ปัญหาความปลอดภัยที่อาจจะเกิดขึ้นได้อย่างรวดเร็ว

๓. ข้อปฏิบัติ

๓.๑ ข้อปฏิบัติการใช้งานสำหรับผู้ใช้

๓.๑.๑ มิให้มีการเปิดระบบแชร์แฟ้มข้อมูลหรือโฟลเดอร์ระหว่างเครื่องคอมพิวเตอร์โดยไม่มีความจำเป็นและให้ปรึกษาผู้รับผิดชอบสารสนเทศ

๓.๑.๒ หากเครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ตามปกติ ผู้ใช้งานสามารถแจ้งผู้รับผิดชอบสารสนเทศ เพื่อแก้ปัญหาได้ ห้ามมิให้ผู้ใช้งานติดตั้ง ปรับแก้ และเปลี่ยนแปลง Hardware/Software ด้วยตนเอง

๓.๑.๓ ไม่เปิดอ่าน E-Mail ที่ไม่มั่นใจว่าผู้ส่งเป็นผู้ใด เนื่องจากอาจมีโปรแกรมไวรัสคอมพิวเตอร์และโปรแกรมประเภท Malware ต่างๆ ติดมาพร้อมกับ E-Mail

๓.๑.๔ ห้ามติดตั้ง Software ที่ผิดกฎหมายหรือละเมิดลิขสิทธิ์ หรือที่ไม่เกี่ยวข้องกับการทำงาน

๓.๑.๕ การติดตั้ง Software ที่ไม่เกี่ยวข้องกับการทำงานโดยตรงให้ติดต่อเจ้าหน้าที่ผู้รับผิดชอบ

๓.๑.๖ ผู้ใช้งานประจำเครื่องมีหน้าที่สำรองข้อมูลงานของตนและบำรุงรักษาเครื่องคอมพิวเตอร์ขั้นต้น

๓.๑.๗ แจ้งสิ่งผิดปกติที่เกิดขึ้นกับเครื่องคอมพิวเตอร์ ผู้รับผิดชอบสารสนเทศ

๓.๒ ข้อปฏิบัติการใช้งานของเจ้าหน้าที่ผู้รับผิดชอบ

๓.๒.๑ กำหนดรหัสผ่านให้กับเครื่องคอมพิวเตอร์ทุกเครื่อง

๓.๒.๒ ติดตั้ง Software ต่างๆ ที่จำเป็นต่อการใช้งานให้พอเพียงต่อการใช้งานในแต่ละระดับ

๓.๒.๓ ทำการ Update โปรแกรมต่างๆ เช่น Windows, Antivirus, และ Antispyware

๓.๒.๔ ทำการ Scan ไวรัสคอมพิวเตอร์และ Malware ให้ Scan อัตโนมัติ และตรวจสอบทุกรอบ ๖ เดือน

๓.๒.๕ ปิดระบบการให้บริการของระบบปฏิบัติการบางส่วนที่อาจะทาให้เป็นช่องทางในการเข้า จู่โจมของ Hacker และระบบการให้บริการที่ไม่เกี่ยวข้องกับการทำงานของผู้ใช้โดยตรง

๕.๒.๖ ผู้ดูแลระบบบันทึกรายงานผลการปฏิบัติงานเสนอต่อคณะกรรมการการรักษาความมั่นคงและปลอดภัยสารสนเทศ เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น เช่น มีการโจมตีจาก Hacker

๕.๒.๗ ทำการตรวจซ่อมบำรุงรักษาโดยการเป่าและทำความสะอาดเครื่องคอมพิวเตอร์อย่างน้อย ๑ ครั้งต่อปี

๕.๒.๘ รายงานผู้ใช้ที่ฝ่าฝืนข้อปฏิบัติด้านสารสนเทศ ให้ประธานคณะกรรมการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๘
การบริหารระบบเครือข่ายคอมพิวเตอร์
(Computer Network Management)

๑. บทนำ

การบริหารระบบเครือข่ายคอมพิวเตอร์ ครอบคลุมการบริหารระบบเครือข่ายทั้งด้าน Hardware และ Software ตลอดจนข้อกำหนดเกี่ยวกับการเข้าถึงเครือข่ายคอมพิวเตอร์จากระยะไกล การแบ่งแยกระบบเครือข่าย การตรวจสอบระบบเครือข่าย ตลอดจนการซ่อมบำรุงรักษาในกรณีที่เกิดเหตุระบบขัดข้อง ทั้งนี้ เพื่อให้เกิดความเข้าใจที่ตรงกันตลอดจนทำให้การบริหารระบบเครือข่ายคอมพิวเตอร์ของสำนักงานฯ ได้อย่างถูกต้องและตรงตามวัตถุประสงค์การใช้งาน

๒. วัตถุประสงค์

เพื่อการกำหนดมาตรการและแนวทางในการบริหารระบบเครือข่าย ทั้งในด้าน Hardware และ Software ข้อกำหนดเกี่ยวกับการจัดการ IP Address การตรวจสอบระบบเครือข่าย การเข้าถึงระบบจากระยะไกล การซ่อมบำรุง และการดาเนินการเมื่อระบบขัดข้อง

๓. การจัดการ IP Address

๓.๑ ผู้ดูแลระบบมีหน้าที่จัดสรร IP Address สำหรับสำนักงานฯ

๓.๒ ผู้ดูแลระบบมีหน้าที่ประเมินปริมาณความต้องการใช้งาน IP Address ของสำนักงานฯ เพื่อประกอบการพิจารณาจัดสรร IP Address

๔. การจัดการระบบจากระยะไกล (VPN)

๔.๑ เจ้าหน้าที่ผู้รับผิดชอบมีหน้าที่ประสานหากมีการใช้งานระบบจากระยะไกลจากกรมสนับสนุนบริการสุขภาพ

ส่วนที่ ๙
การบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์
(Log files Management)

๑. บทนำ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กำหนดให้ต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน นับตั้งแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลเท่าที่จำเป็นเพื่อสามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้ไม่น้อยกว่า ๙๐ วันนับตั้งแต่การบริการสิ้นสุดลง ผู้ให้บริการผู้ใดไม่ปฏิบัติตาม มาตรานี้ ต้องระวางโทษปรับไม่เกิน ๕๐๐,๐๐๐ บาท มีผลบังคับใช้ในวันที่ ๒๓ สิงหาคม ๒๕๕๑

๒. วัตถุประสงค์

เพื่อบันทึกข้อมูลจราจรทางคอมพิวเตอร์ ให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

๓. ข้อปฏิบัติ

๓.๑ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ๙๐ วันตาม กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กำหนด ให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

๓.๒ ข้อมูลการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นความลับและบุคคลทั่วไปไม่มีสิทธิ์ในการเข้าถึงข้อมูลยกเว้น ในทางการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

๓.๒.๑ มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

๓.๒.๒ พนักงานเจ้าหน้าที่มีอำนาจด้านการสืบสวนสอบสวนเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

๓.๒.๓ ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

๓.๒.๔ ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการ

กระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์

๓.๓ การดูแล Hardware และ Software ของอุปกรณ์ข้อมูลจราจรเป็นหน้าที่เป็นหน้าที่เจ้าหน้าที่ผู้รับผิดชอบ โดยไม่ได้รับอนุญาต หากมีความจำเป็นจะต้องแจ้งเจ้าหน้าผู้รับผิดชอบสนเทศ

ส่วนที่ ๑๐
การบริหารจัดการทรัพย์สินสารสนเทศ
(Asset Management)

๑.วัตถุประสงค์

เพื่อการกำหนดมาตรการและแนวทางในการบริหารจัดการทรัพย์สินสำนักงาน

๒. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

๒.๑ จัดทำทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๒.๓ การจัดหมวดหมู่ทรัพย์สินสารสนเทศ

๒.๔ จัดทำกฎ ระเบียบ หลักเกณฑ์ในการจัดสรรอุปกรณ์คอมพิวเตอร์ให้เหมาะสม

๓. การจัดหมวดหมู่ทรัพย์สินสารสนเทศ

สำนักงานฯ จัดแบ่งหมวดหมู่ทรัพย์สินสารสนเทศออกเป็น ๔ ระดับ คือ

๓.๑ ฮาร์ดแวร์

๓.๒ ซอร์ฟแวร์

๓.๓ ข้อมูลสารสนเทศ

๓.๔ ผู้ใช้งาน

๔. ระดับชั้นความลับของสารสนเทศ

สำนักงานฯ จัดแบ่งระดับความลับออกเป็น ๔ ประเภท คือ

๔.๑ ลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

๔.๒ ลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

๔.๓ ลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๔.๔ ปกติ หมายถึง ไม่กำหนดชั้นความลับ

๕. ระดับการเข้าถึงสารสนเทศ

สำนักงานฯ จัดแบ่งระดับการเข้าถึงสารสนเทศเป็น ๔ ระดับ คือ

๕.๑ ลับที่สุด หมายถึง ผู้บริหารระดับสูง

๕.๒ ลับมาก หมายถึง หัวหน้าฝ่าย/กลุ่ม

๕.๓ ลับ หมายถึง ผู้ที่เกี่ยวข้องกับงาน

๕.๔ ไม่ลับ หมายถึง สามารถเผยแพร่ได้

๖. ระดับความเสี่ยง

สำนักงานฯ กำหนดเกณฑ์ระดับความเสี่ยงไว้ ๔ ระดับ ได้แก่ ต่ำ ปานกลาง สูง และสูงมาก ดังนี้

- ระดับความเสี่ยงต่ำ หมายถึง ปัจจัยเสี่ยงที่มีระดับคะแนนความเสี่ยง ๑-๓ คะแนน
- ระดับความเสี่ยงปานกลาง หมายถึง ปัจจัยเสี่ยงที่มีระดับคะแนนความเสี่ยง ๔-๙ คะแนน
- ระดับความเสี่ยงสูง หมายถึง ปัจจัยเสี่ยงที่มีระดับคะแนนความเสี่ยง ๑๐-๑๖ คะแนน
- ระดับความเสี่ยงสูงมาก หมายถึง ปัจจัยเสี่ยงที่มีระดับคะแนนความเสี่ยง ๑๗-๒๕ คะแนน

๗. หมวดหมู่ทรัพย์สินสารสนเทศ

๗.๑ ฮาร์ดแวร์

ลำดับที่	รายการ	จำนวน	ระดับความลับ	ระดับการเข้าถึง	หมายเหตุ
๑	Computer	๒๔ เครื่อง	ลับ	ลับ	
๒	Notebook	๑๙ เครื่อง	ลับ	ลับ	
๓	Switch	๑๐ เครื่อง	ลับ	ลับ	
๔	Wireless	๓ เครื่อง	ลับ	ลับ	
๕	Printer	๒๒ เครื่อง	ปกติ	ไม่ลับ	
๖	Projector	๑ เครื่อง	ปกติ	ไม่ลับ	
๗	Screen Projector	๒ อัน	ปกติ	ไม่ลับ	
๘	CCTV และ DVR	๑๖ ตัว	ลับมาก	ลับมาก	
๙	Router ๓BB fiber	๓ เครื่อง	ลับมาก	ลับมาก	
๑๐	Scanner	๑ เครื่อง	ปกติ	ไม่ลับ	
๑๑	HDD External ๑ TB	๑ อัน	ลับ	ลับ	
๑๒	Wireless External usb	๒ อัน	ปกติ	ไม่ลับ	
๑๓	Lan point	๕๐ จุด	ปกติ	ไม่ลับ	
๑๔	UPS	๒๔ เครื่อง	ปกติ	ไม่ลับ	
๑๕	Firewall	๑ เครื่อง	ลับมาก	ลับมาก	

๗.๒ ข้อมูลสารสนเทศ

ลำดับที่	รายการ	จำนวน	ระดับความลับของข้อมูล	ระดับการเข้าถึงสารสนเทศ	หมายเหตุ
๑	Website ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐	๑	ลับ	ลับ	เป็นเว็บไซต์ ประชาสัมพันธ์ เผยแพร่ข้อมูลข่าวสาร รับเรื่องร้องเรียน สำนักงานฯ
๒	ระบบ GFMIS	๑	ลับมาก	ลับมาก	ระบบการจัดสรรงบประมาณ,กาพาระบบบริหาร/ติดตามการใช้งบประมาณ ระบบบัญชีแยกประเภท
๓	ระบบ SMART	๑	ลับ	ลับ	ระบบรายงานผล บริหารแผนงาน งบประมาณ และตัวชี้วัด
๔	ระบบ RMC	๑	ลับ	ลับ	โปรแกรมรายงานผลการบำรุงรักษาในโรงพยาบาล
๕	Facebook ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐	๑	ลับ	ลับ	เป็นสื่อโซเชียลมีเดีย ในการ ประชาสัมพันธ์ สำนักงานฯ
๖	ระบบ EGP	๑	ลับมาก	ลับมาก	ระบบการจัดซื้อจัดจ้างของภาครัฐ

๘. การประเมินความเสี่ยง ทรัพย์สินสารสนเทศ

๘.๑ ฮาร์ดแวร์

รายการ	ความเสี่ยง	ปัจจัยเสี่ยง	โอกาส (L)	ผลกระทบ (C)	ระดับความเสี่ยง (LxC)	ลำดับความเสี่ยง	หมายเหตุ
Firewall	๑. เครื่อง Firewall ไม่สามารถใช้งานได้ตามปกติ	๑. อุปกรณ์เสื่อมสภาพ ๒. ติดไวรัส	๓	๓	๙	๑	
CCTV และ DVR	เครื่อง CCTV และ DVR ไม่สามารถบันทึกข้อมูลได้	๑. อุปกรณ์เสื่อมสภาพ	๓	๓	๙	๑	
Computer	๑. คอมพิวเตอร์ใช้งานไม่ได้ ๒. คอมพิวเตอร์ไม่สามารถเข้าอินเตอร์เน็ตได้	๑. อุปกรณ์เสื่อมสภาพ ๒. ติดไวรัส ๓. ผู้ใช้งานขาดความรู้	๓	๒	๖	๒	
Notebook	๑. คอมพิวเตอร์ใช้งานไม่ได้ ๒. คอมพิวเตอร์ไม่สามารถเข้าอินเตอร์เน็ตได้	๑. อุปกรณ์เสื่อมสภาพ ๒. ติดไวรัส ๓. ผู้ใช้งานขาดความรู้	๓	๒	๖	๒	
Projector	๑. เครื่อง Projector ใช้งานไม่ได้	๑. อุปกรณ์เสื่อมสภาพ ๒. ผู้ใช้งานขาดความรู้	๒	๓	๖	๒	
Router ๓BB fiber	๑. เครื่อง Router ๓BB fiber ไม่สามารถใช้งานได้ตามปกติ ๒. ไม่สามารถเข้าอินเตอร์เน็ตได้	๑. อุปกรณ์เสื่อมสภาพ	๒	๓	๖	๒	
Printer	๑. ไม่สามารถพิมพ์งานได้ตามปกติ	๑. อุปกรณ์เสื่อมสภาพ ๓. ผู้ใช้งานขาดความรู้	๒	๒	๔	๓	

รายการ	ความเสี่ยง	ปัจจัยเสี่ยง	โอกาส (L)	ผลกระทบ (C)	ระดับความเสี่ยง (LxC)	ลำดับความเสี่ยง	หมายเหตุ
Wireless	๑. เครื่อง Wireless กระจายอินเตอร์เน็ตไม่กระจายสัญญาณ	๑. อุปกรณ์เสื่อมสภาพ	๒	๒	๔	๓	
Switch	๑. เครื่อง SWITCH ในการกระจายสัญญาณ ไม่สามารถติดต่อเครือข่ายได้และไม่กระจายสัญญาณอินเตอร์เน็ต	๑. อุปกรณ์เสื่อมสภาพ	๒	๒	๔	๓	
HDD External ๑ TB	๑. HDD External ไม่สามารถใช้งานได้ตามปกติ	๑. อุปกรณ์เสื่อมสภาพ	๒	๒	๔	๓	
Scanner	๑. ไม่สามารถใช้งานได้ตามปกติ	๑. อุปกรณ์เสื่อมสภาพ	๒	๑	๒	๔	
UPS	๑. ไม่สามารถใช้งานได้ตามปกติ	๑. อุปกรณ์เสื่อมสภาพ	๒	๑	๒	๔	
Screen Projector	๑. ไม่สามารถใช้งานได้ตามปกติ	๑. อุปกรณ์เสื่อมสภาพ	๒	๑	๒	๔	
Lan point	๑. สัญญาณอินเตอร์เน็ตใช้ไม่ได้	๑. จุดและสายสัญญาณเสื่อมสภาพ	๑	๑	๒	๔	
Wireless External usb	๑. ไม่สามารถใช้งานได้ตามปกติ	๑. ไม่ได้ลง Driver ๒. อุปกรณ์เสื่อมสภาพ	๑	๑	๑	๕	

๘.๒ ข้อมูลสารสนเทศ

รายการ	ความเสี่ยง	ปัจจัยเสี่ยง	โอกาส (L)	ผลกระทบ (C)	ระดับความเสี่ยง (LxC)	ลำดับความเสี่ยง	หมายเหตุ
Website สำนักงานฯ	๑. ไม่สามารถใช้งานได้ตามปกติ	๑. Host จากกรมฯ มีปัญหา	๓	๓	๙	๑	
ระบบ GFMIS	๑. ไม่สามารถใช้งานได้ตามปกติ	๑. ระบบมีปัญหาจากหน่วยงานที่รับผิดชอบ ๒.ผู้ใช้งานขาดความรู้	๒	๓	๖	๒	
ระบบ SMART	๑. ไม่สามารถใช้งานได้ตามปกติ	๑. ระบบมีปัญหาจากการคีย์ข้อมูล ๒.ผู้ใช้งานขาดความรู้	๒	๓	๖	๒	
ระบบ RMC	๑. ไม่สามารถใช้งานได้ตามปกติ	๑. ระบบมีปัญหาจากการคีย์ข้อมูล ๒.ผู้ใช้งานขาดความรู้	๒	๓	๖	๒	
Facebook สำนักงานฯ	๑. ไม่สามารถใช้งานได้ตามปกติ	๑. ระบบมีปัญหาจากหน่วยงานที่รับผิดชอบ	๒	๓	๖	๒	
ระบบ EGP	๑. ไม่สามารถใช้งานได้ตามปกติ	๑. ระบบมีปัญหาจากหน่วยงานที่รับผิดชอบ ๒.ผู้ใช้งานขาดความรู้	๒	๓	๖	๒	

ส่วนที่ ๑๑
ขั้นตอนการใช้งาน ด้านสารสนเทศ

๑๑.๑ ขั้นตอนการขอเบิกวัสดุ/อุปกรณ์สารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

๑. เจ้าหน้าผู้เบิก กรอกแบบฟอร์ม วัสดุ/อุปกรณ์สารสนเทศ โดยระบุรายการที่เบิกพร้อมด้วยเหตุผลความจำเป็น โดยใช้ แบบฟอร์มขอยืมอุปกรณ์คอมพิวเตอร์

๒. เจ้าหน้าผู้เบิกให้หัวหน้า กลุ่ม/งาน พิจารณาตรวจสอบ ความต้องการของผู้เบิก หากอนุมัติให้ไปขั้นตอนต่อไป หากไม่อนุมัติให้ ระบุเหตุผล

๓. คณะกรรมการสารสนเทศพิจารณา หากอนุมัติให้ไปขั้นตอนต่อไป หากไม่อนุมัติให้ ระบุเหตุผล

๔. เจ้าหน้าที่พัสดุพิจารณา อนุมัติ หากอนุมัติให้ไปขั้นตอนต่อไป หากไม่อนุมัติให้ ระบุเหตุผล

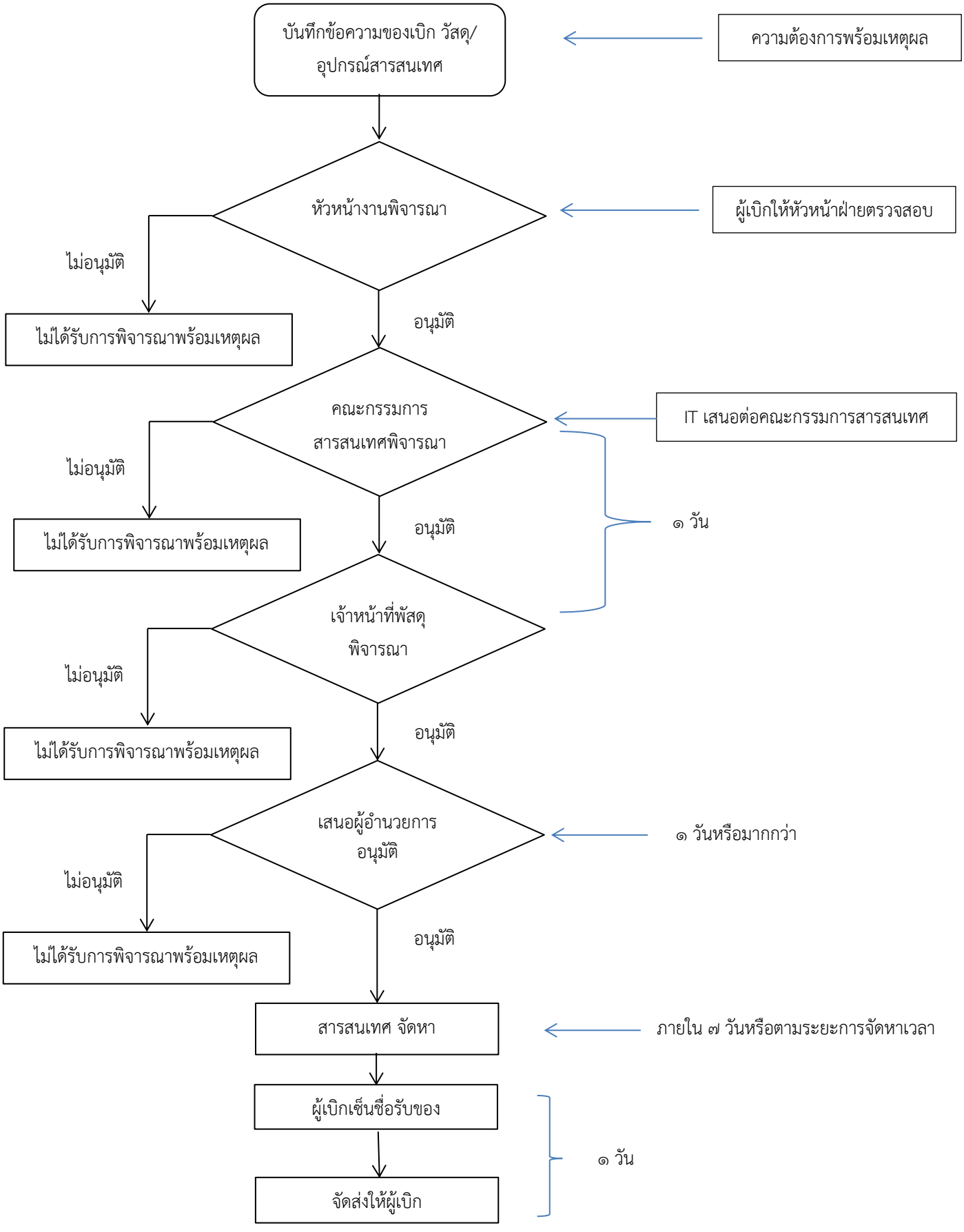
๕. เสนอผู้อำนวยการ อนุมัติ หากอนุมัติให้ไปขั้นตอนต่อไป หากไม่อนุมัติให้ ระบุเหตุผล

๖. ผู้รับผิดชอบสารสนเทศจัดหาตามรายการเจ้าหน้าผู้เบิก

๗. ผู้รับผิดชอบสารสนเทศจัดส่งให้เจ้าหน้าผู้เบิก

๘. เจ้าหน้าผู้เบิก เซ็นรับ พร้อมตรวจเช็คความเรียบร้อยอุปกรณ์ ก่อนใช้งาน

Flowchart ขั้นตอนการเบิก วัสดุ/อุปกรณ์สารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐



๑๑.๒ ขั้นตอนการขอส่งซ่อมวัสดุ/อุปกรณ์สารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

๑. เจ้าหน้า กรอกแบบฟอร์ม ขอส่งซ่อมวัสดุ/อุปกรณ์สารสนเทศ โดยระบุรายการที่ซ่อมพร้อมด้วยเหตุผลความจำเป็น

๒. เจ้าหน้า ให้หัวหน้า กลุ่ม/ฝ่าย พิจารณาตรวจสอบความจำเป็น หากอนุมัติให้ไปขั้นตอนต่อไป หากไม่อนุมัติให้ ระบุเหตุผล

๓. คณะกรรมการสารสนเทศพิจารณา หากอนุมัติให้ไปขั้นตอนต่อไป หากไม่อนุมัติให้ ระบุเหตุผล

๔. เจ้าหน้าที่พัสดุพิจารณา อนุมัติ หากอนุมัติให้ไปขั้นตอนต่อไป หากไม่อนุมัติให้ ระบุเหตุผล

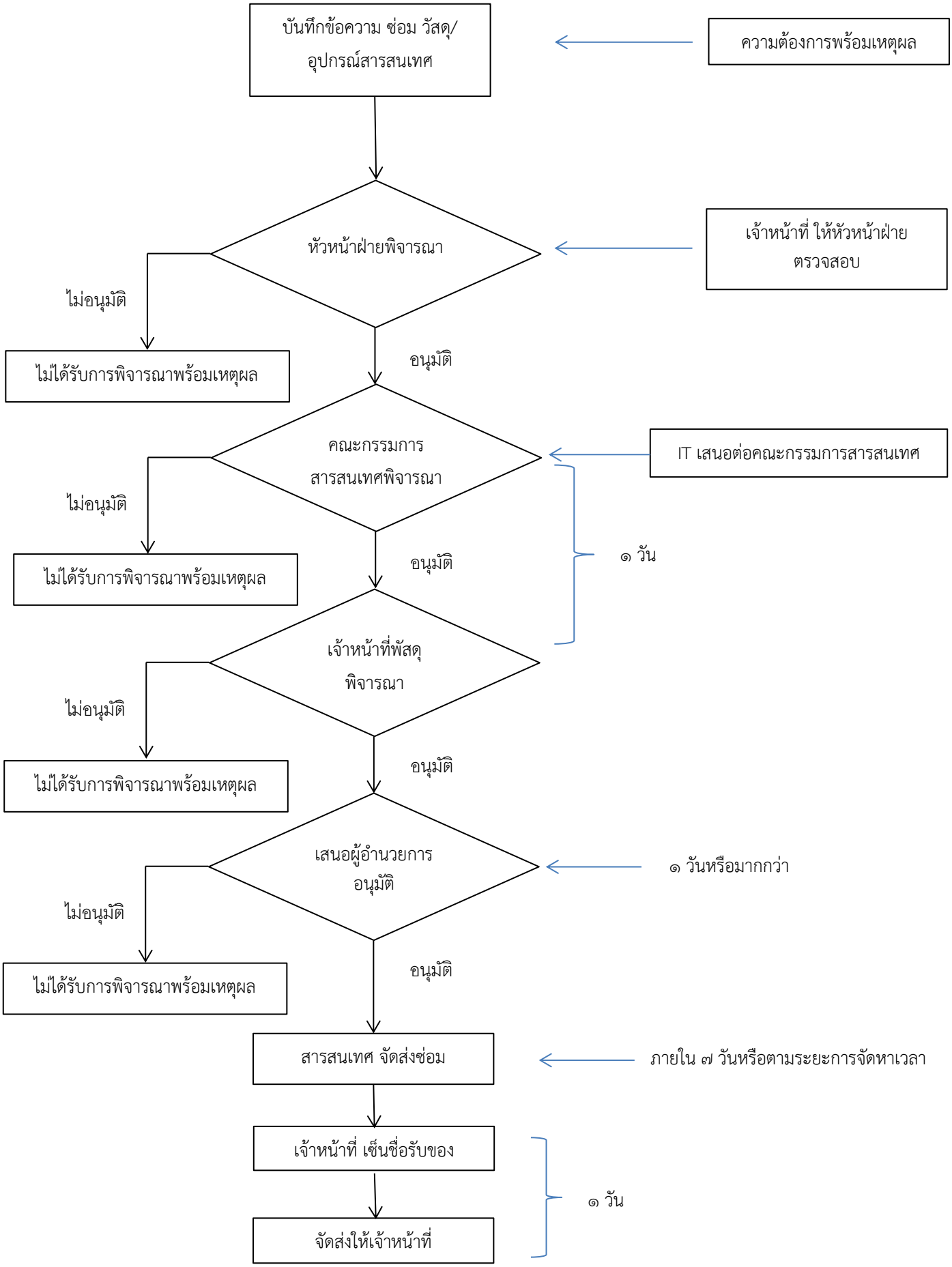
๕. เสนอผู้อำนวยการ อนุมัติ หากอนุมัติให้ไปขั้นตอนต่อไป หากไม่อนุมัติให้ ระบุเหตุผล

๖. ผู้รับผิดชอบสารสนเทศจัดหาตามรายการที่ส่งซ่อมวัสดุ/อุปกรณ์สารสนเทศ

๗. ผู้รับผิดชอบสารสนเทศจัดส่งให้เจ้าหน้า

๘. เจ้าหน้า เซ็นรับ พร้อมตรวจเช็คความเรียบร้อยอุปกรณ์ที่ส่งซ่อม

Flowchart ขั้นตอนการซ่อม วัสดุ/อุปกรณ์สารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐



๑๑.๓ ขั้นตอนการยืม วัสดุ/อุปกรณ์สารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

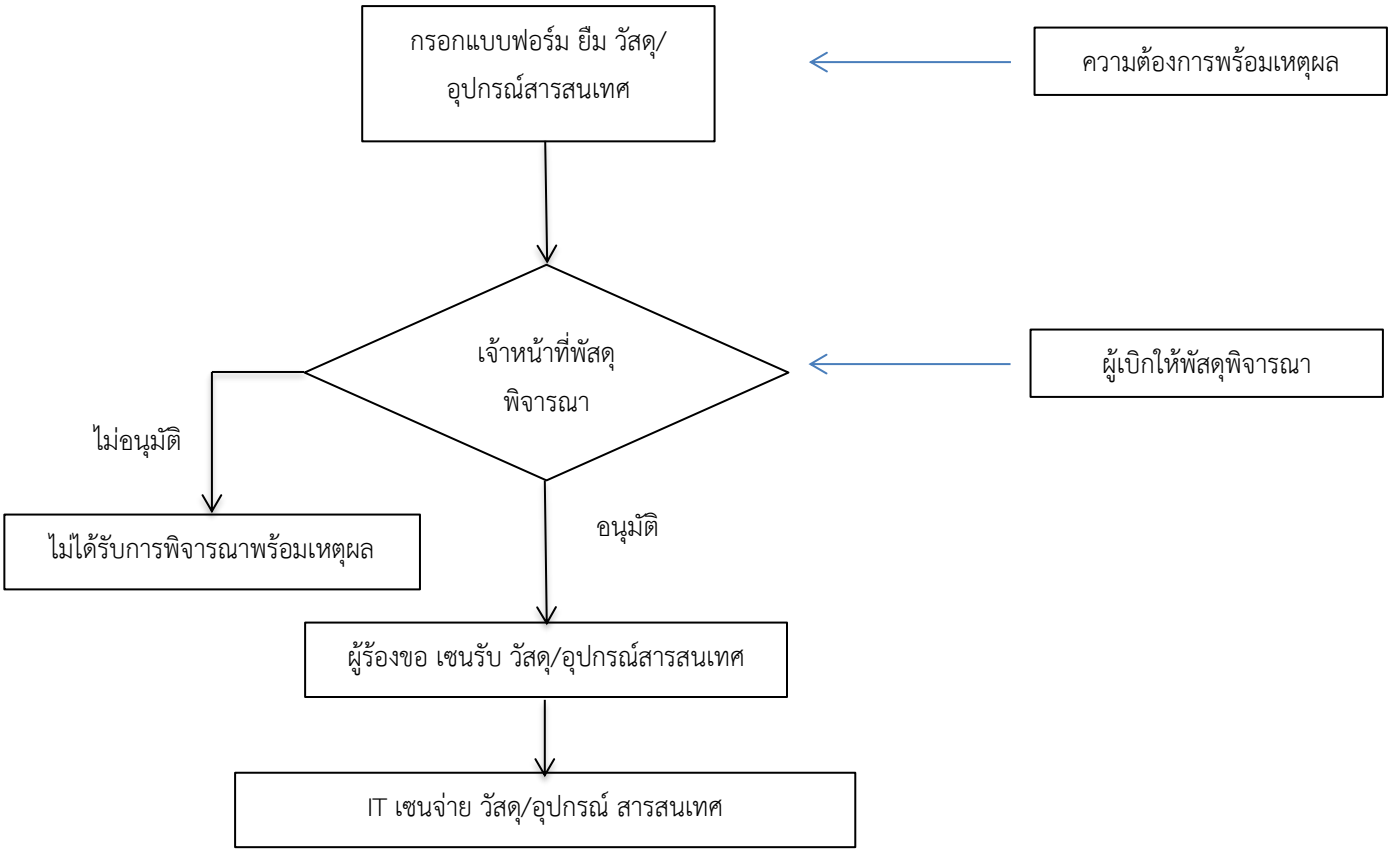
๑. เจ้าหน้าผู้เบิก กรอกแบบฟอร์มยืม วัสดุ/อุปกรณ์สารสนเทศ โดยระบุความประสงค์ขอยืม/ใช้ อุปกรณ์

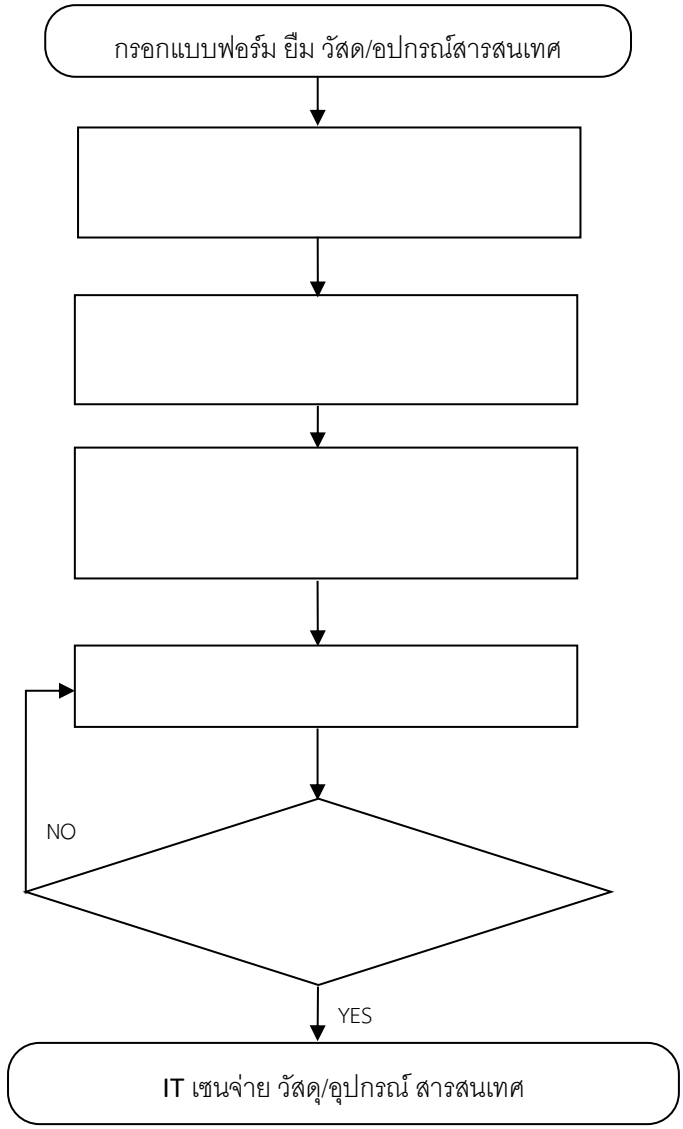
๒. เจ้าหน้าที่พัสดุพิจารณา อนุมัติ หากอนุมัติให้ไปขั้นตอนต่อไป หากไม่อนุมัติให้ ระบุเหตุผล

๓. เจ้าหน้าผู้เบิก เซ็นรับ วัสดุ/อุปกรณ์สารสนเทศ พร้อมตรวจเช็คความเรียบร้อยอุปกรณ์ที่ยืมก่อนนำไปใช้

๔. ผู้รับผิดชอบสารสนเทศ เซ็นจ่าย วัสดุ/อุปกรณ์สารสนเทศ

Flowchart ขั้นตอนการยืม วัสดุ/อุปกรณ์สารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐



ลำดับ	กระบวนงาน	มาตรฐานเวลา (ชม.)	ข้อกำหนดของกระบวนการ	ผู้รับผิดชอบ
๑		.... นาที		
๒		..... นาที		
๓		..... นาที		
๔		..... นาที		
๕		..... นาที		
๖		..... นาที		
๗		..... นาที		
	รวม	ประมาณ ..... ชม.		

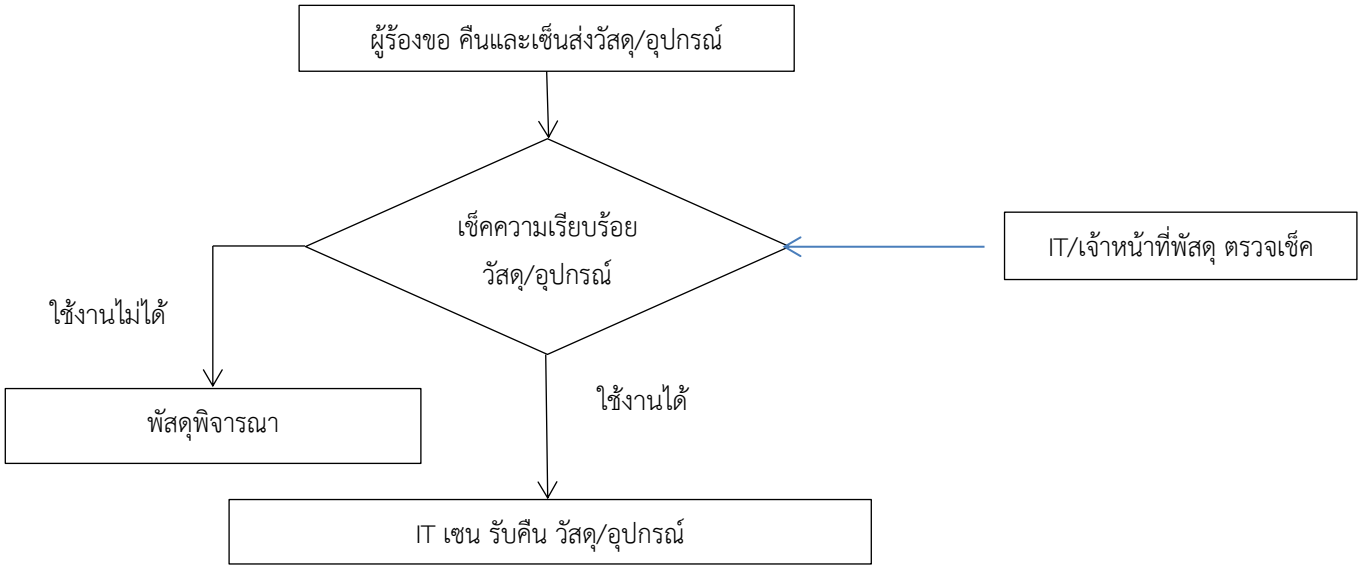
๑๑.๔ ขั้นตอนการคืน วัสดุ/อุปกรณ์สารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

๑. เจ้าหน้าที่ผู้เบิก เซ็นส่ง วัสดุ/อุปกรณ์สารสนเทศ

๒. ผู้รับผิดชอบสารสนเทศ/เจ้าหน้าที่พัสดุ ตรวจเช็คความเรียบร้อย อุปกรณ์ที่ยืม วัสดุ/อุปกรณ์สารสนเทศ หลังนำไปใช้ หากพิจารณา เกิดความเสียหาย ให้เจ้าหน้าที่พัสดุพิจารณาต่อไป

๓. ผู้รับผิดชอบสารสนเทศ เซ็นคืน วัสดุ/อุปกรณ์สารสนเทศ

Flowchart ขั้นตอนการคืน วัสดุ/อุปกรณ์สารสนเทศ

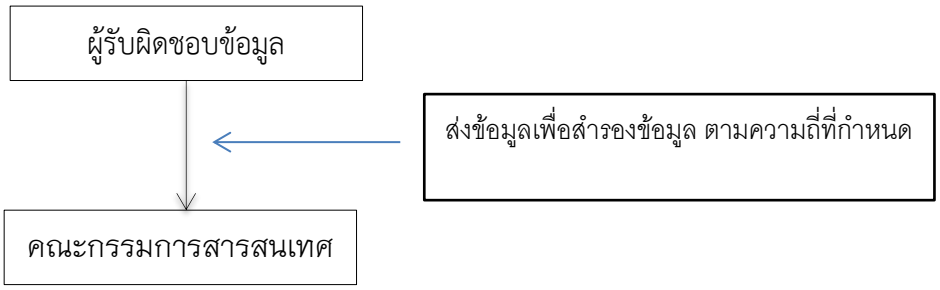


๑๑.๕ ขั้นตอนการสำรองข้อมูลสารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

๑. ผู้รับผิดชอบข้อมูลในการรวบรวมข้อมูลแต่ละกลุ่ม/ฝ่ายสำรองข้อมูลและส่งมอบให้ผู้รับผิดชอบสารสนเทศ

๒. ผู้รับผิดชอบสารสนเทศทำการ สำรองข้อมูล

Flowchart ขั้นตอนการสำรองข้อมูลสารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐



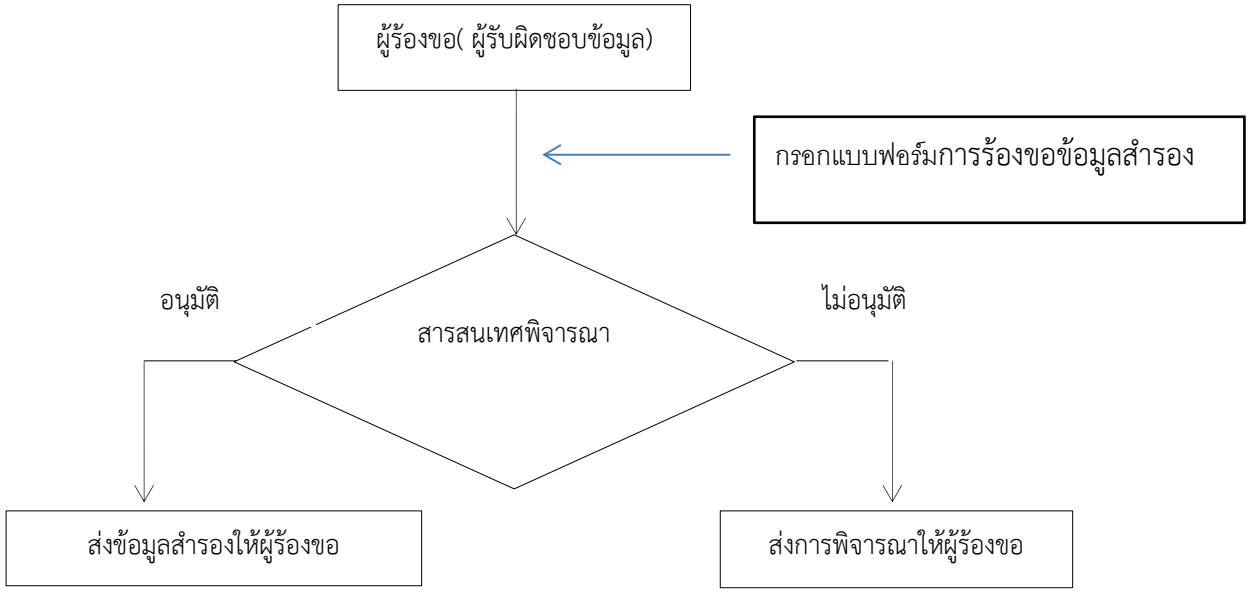
๑๑.๖ ขั้นตอนการร้องขอข้อมูลสำรอง ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

๑.ผู้ร้องขอ (ผู้รับผิดชอบข้อมูล) กรอกแบบฟอร์มการร้องขอ (แบบฟอร์ม สารสนเทศ – ๐๗)

๒. สารสนเทศพิจารณา อนุมัติ หากอนุมัติให้ไปขั้นตอนต่อไป หากไม่อนุมัติให้ ระบุเหตุผล

๓. ส่งข้อมูลสำรองให้ผู้ขอ (ผู้รับผิดชอบข้อมูล)

Flowchart ขั้นตอนการร้องขอข้อมูลสำรอง



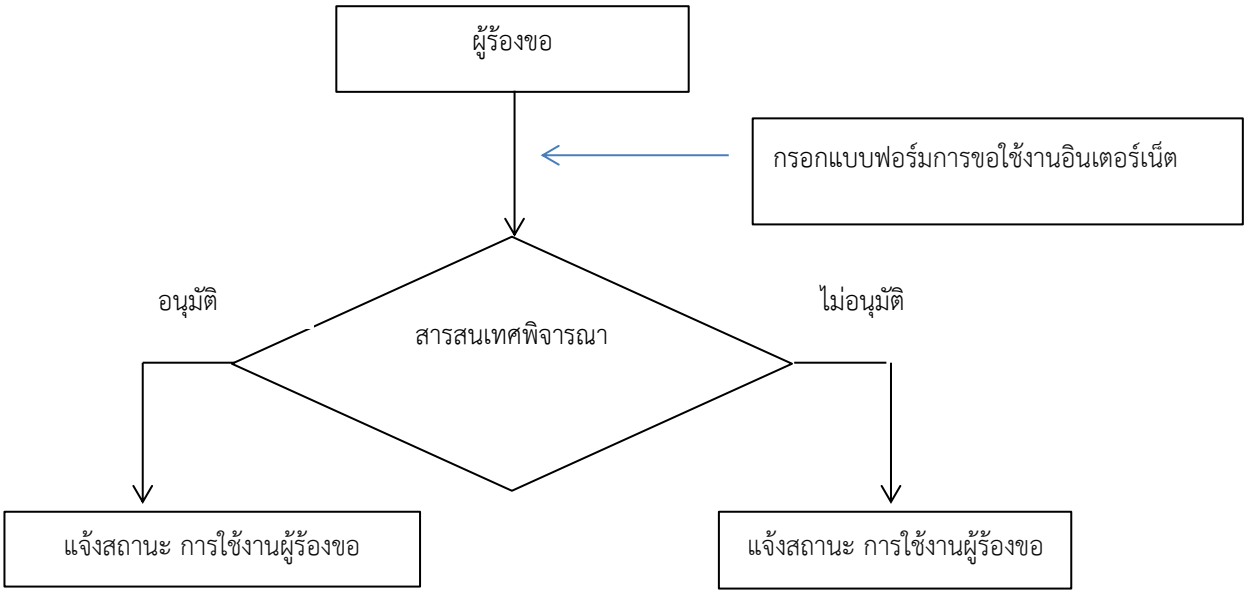
๑๑.๗ ขั้นตอนการใช้งานขอใช้งานอินเตอร์เน็ต ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

๑.ผู้ร้องขอ กรอกแบบฟอร์มขอใช้งานอินเตอร์เน็ต

๒. สารสนเทศพิจารณา อนุมัติ หากอนุมัติให้ไปขั้นตอนต่อไป หากไม่อนุมัติให้ ระบุเหตุผล

๓. แจ้งสถานะ การใช้งานผู้ร้องขอ

Flowchart ขั้นตอนการใช้งานขอใช้งานอินเตอร์เน็ต



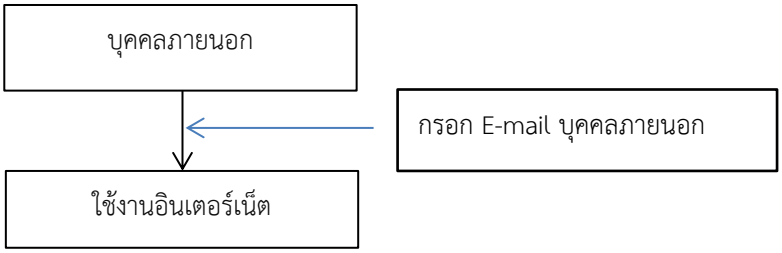
๑๑.๘ ขั้นตอนการใช้งานขอใช้งานอินเตอร์เน็ต สำหรับบุคคลภายนอก

๑. สำหรับบุคคลภายนอกสามารถใช้งานได้ โดยใช้งาน เครื่องกระจายสัญญาณ ชื่อ HSS๑๐_Guest เท่านั้น

๒. กรอกรหัสผ่าน เครื่องกระจายสัญญาณ ชื่อ HSS๑๐_Guest รหัสผ่าน ตามที่เจ้าหน้าที่ออกให้

๓. เข้าเว็บไซต์ กรอก E-mail ของผู้ใช้งาน

Flowchart ขั้นตอนการใช้งานขอใช้งานอินเตอร์เน็ต สำหรับบุคคลภายนอก



ส่วนที่ ๑๒
การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวทางและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้องได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๒.๑ จัดทำเล่มด้านการรักษาความมั่นคงและปลอดภัยของระบบสารสนเทศ เพื่อแนวทางปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง

๒.๓ ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๒.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ

จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ ๓ มกราคม ๒๕๖๔

(นายชาลี สร้างดี)
ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑๐