ประกาศกรมส่งเสริมอุตสาหกรรม
เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมส่งเสริมอุตสาหกรรม
พ.ศ. ๒๕๕๕

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมส่งเสริมอุตสาหกรรมมีความมั่นคงปลอดภัย และสามารถใช้งานได้อย่างมีประสิทธิภาพ อันจะทำให้การดำเนินธุรกรรมมีความถูกต้องและน่าเชื่อถือ จึงกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ดังนี้

นิยามศัพท์

กรมฯ	หมายถึง กรมส่งเสริมอุตสาหกรรม
ผู้บังคับบัญชา	หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการแบ่งส่วนราชการ
ระบบเครือข่าย กสอ.	หมายถึง ระบบเครือข่ายคอมพิวเตอร์ของกรมส่งเสริมอุตสาหกรรม ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานที่กล้วยน้ำไท และระบบเครือข่ายคอมพิวเตอร์ศูนย์ภาคฯ ทั้งหมด
ระบบงานภายใน	หมายถึง ระบบเว็บท่า (portal.dip.go.th) ของกรมส่งเสริมอุตสาหกรรม เนื่องจากทุกระบบงาน จะต้องเข้าผ่านทางระบบเว็บท่า
ผู้ดูแลระบบ	หมายถึง เจ้าหน้าที่ผู้ปฏิบัติงานในส่วนหรือศูนย์ที่ทำหน้าที่ดูแลด้านระบบเครือข่าย กสอ. และดูแลด้านระบบสารสนเทศในภาพรวมของ กรมส่งเสริมอุตสาหกรรมซึ่งมีอำนาจและหน้าที่ในการบริหารระบบเครือข่ายให้มีประสิทธิภาพ
ระบบป้องกันเครือข่าย	หมายถึง ระบบที่ผู้ดูแลระบบพิจารณานำมาใช้งานร่วมกับระบบเครือข่าย เพื่อทำหน้าที่ป้องกันการโจมตี เพื่อให้การทำงานของระบบเครือข่ายมีเสถียรภาพหรือเพื่อความมั่นคงของระบบสารสนเทศของกรมฯ
ระบบเฝ้าระวังเครือข่าย	หมายถึง ระบบที่ทำหน้าที่ Network Monitoring Tools
เหตุการณ์นอกเหนือการควบคุม	หมายถึง เหตุการณ์ที่เกิดขึ้นและไม่อาจควบคุมได้ด้วยเหตุสุดวิสัย หรือนอกเหนือจากการทำงานของอุปกรณ์ในสภาพปกติ
ผู้ใช้งาน	หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างตามสัญญาจ้างของกรมฯ หรือเจ้าหน้าที่ของหน่วยงานที่ดำเนินงานให้กับกรมฯ
ผู้ใช้งานชั่วคราว	หมายถึง บุคคลภายนอกที่ขอใช้งานระบบโดยมีการสร้างสิทธิ์ในการใช้งานแบบกำหนดระยะเวลา
สิทธิของผู้ใช้งาน	หมายถึง สิทธิการใช้งานตามหน้าที่ของระบบงานนั้นๆ หรือตามที่เจ้าหน้าที่ผู้ดูแลระบบกำหนด

การพิสูจน์ตัวตน	หมายถึง ขั้นตอนการยืนยันชื่อผู้ใช้งานและการยืนยันรหัสผ่าน เพื่อการได้รับสิทธิเข้าใช้งาน
การละเมิดข้อมูล	หมายถึง การเข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาตหรือไม่สิทธิ์ในการเข้าถึงข้อมูล ไม่ว่าจะเป็นการเข้าถึงอุปกรณ์จัดเก็บข้อมูลโดยทางตรง หรือการเข้าถึงโดยผ่านระบบเครือข่าย
เลขหมายประจำเครื่อง	หมายถึง IP Address ซึ่งบริหารและควบคุมการใช้งานสำหรับเครื่องคอมพิวเตอร์ลูกข่ายโดยผู้ดูแลระบบ
สินทรัพย์ (asset)	หมายถึง สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร
สินทรัพย์คอมพิวเตอร์	หมายความว่า โปรแกรมคอมพิวเตอร์ เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และให้หมายความรวมถึงอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้องด้วย
อุปกรณ์บันทึกข้อมูล-ชนิดพกพา	หมายถึง เครื่องหรืออุปกรณ์คอมพิวเตอร์ที่สามารถบันทึกข้อมูลได้โดยตรงและสามารถเคลื่อนย้ายไปใช้งานร่วมกับเครื่องคอมพิวเตอร์เครื่องอื่นได้โดยไม่จำเป็นต้องติดตั้งใช้งานภายในตัวเครื่อง (Internal) เช่น ฮาร์ดดิสก์ภายนอก (External Hard Disk), แผ่นบันทึกข้อมูลชนิดต่าง, การ์ดหน่วยความจำชนิดต่างๆ, เครื่องมือที่สามารถบันทึกข้อมูลได้ในตัว, Flash Drive เป็นต้น

หมวด ๑.
แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

ข้อ ๑. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องจัดการควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานดังนี้

๑.๑ ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ตนต้องใช้งานได้ก็ต่อเมื่อได้รับอนุญาตจากผู้ดูแลข้อมูล และ/หรือ ผู้ดูแลระบบงาน ตามความจำเป็นต่อการใช้งานแล้วเท่านั้น

๑.๒ ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบ ผู้ขอใช้ระบบงานจะต้องมีการทำเป็นบันทึกและกรอกแบบเอกสารที่กรมฯ กำหนดเพื่อขออนุญาตเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้บังคับบัญชาหรือผู้รับมอบอำนาจจากผู้บังคับบัญชาเพื่อการจัดเก็บไว้เป็นหลักฐาน จากนั้น ผู้ดูแลระบบจะสร้างบัญชีสำหรับการเข้าถึงโดยอนุญาตเฉพาะในส่วนที่จำเป็น

๑.๓ ผู้ดูแลระบบงาน ต้องอนุญาตให้ผู้ใช้งานเข้าสู่ระบบตามหน้าที่งานเท่านั้นเนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นเท่านั้น

๑.๔ ผู้ดูแลระบบ ต้องกำหนดไม่ให้ผู้ใช้งานเข้าสู่ระบบได้ หากผู้ใช้งานใส่รหัสผ่านเข้าระบบผิด ๓ ครั้ง จนกว่าจะยื่นเรื่องพร้อมหลักฐานแสดงความเป็นตัวตนต่อเจ้าหน้าที่ดูแลระบบ เพื่อขอรหัสใหม่อีกครั้ง

๑.๕ ผู้ดูแลระบบ ต้องกำหนดให้การ Log-in เพื่อเข้าใช้ระบบงานใด ๆ จะต้องมีการตรวจจับการเปิดระบบงานไว้ เมื่อไม่มีการใช้งาน จะทำการ log-out ระบบให้อัตโนมัติ ในระยะเวลาที่เหมาะสม

ข้อ ๒. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องจัดการควบคุมการเข้า-ออกพื้นที่ควบคุม เช่น หน่วยงานที่รับผิดชอบระบบสารสนเทศของกรมฯ ดังนี้

๒.๑ ผู้มาติดต่อจากหน่วยงานภายนอก มีแนวปฏิบัติดังนี้

๒.๑.๑ ติดต่อผู้ดูแลระบบของกรมฯ เพื่อแจ้งความประสงค์และเหตุผลในการขอเข้า-ออก ห้องเครื่องแม่ข่าย

๒.๑.๒ หากได้รับอนุญาตให้ผู้ดูแลระบบเป็นผู้พาเข้า-ออก ห้องควบคุมระบบเครือข่าย และจะต้องลงรายชื่อในสมุดบันทึก พร้อมแจ้งเวลาเข้า-ออก และกิจกรรมที่เข้ามาทำด้วย

๒.๒ ผู้ดูแลระบบและควบคุมห้องเครื่องแม่ข่าย มีแนวทางปฏิบัติดังนี้

๒.๒.๑ ผู้ดูแลระบบห้องเครื่องแม่ข่าย ต้องกำหนดสิทธิ์บุคคลเข้า-ออก ห้องเครื่องแม่ข่าย โดยผ่าน Finger Scan

๒.๒.๒ ให้มีระบบเก็บบันทึกการเข้าออกหน่วยงานที่รับผิดชอบระบบสารสนเทศของกรมฯ จากบุคคลภายนอก โดยในบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้า-ออก และควรมีการตรวจสอบบันทึกดังกล่าวอยู่เสมอ

๒.๒.๓ ผู้ดูแลระบบห้องเครื่องแม่ข่ายจะต้องเป็นผู้ควบคุม และรับผิดชอบต่อบุคคลภายนอกที่เข้ามาในห้องเครื่องแม่ข่าย โดยการ Login เข้าสู่ระบบให้

ข้อ ๓. ผู้ดูแลระบบสารสนเทศ ต้องกำหนดการจัดวางและการป้องกันฮาร์ดแวร์และอุปกรณ์ต่างๆ ดังนี้

๓.๑ จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงของบุคคลภายนอก

๓.๒ เอกสาร สื่อบันทึกข้อมูลในการทำงานหรืออุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่มีความมั่นคงปลอดภัยเพียงพอ เช่น ใส่ตู้ หรือ โต๊ะ ที่สามารถล็อคกุญแจได้

๓.๓ สื่อประเภทสิ่งพิมพ์ ให้ทำลายตามระเบียบสารบรรณ สื่อบันทึกข้อมูล แฟ้มข้อมูล ให้ทำลายข้อมูลตามมาตรฐาน DoD ๕๒๒๐-๒๒M ของกระทรวงกลาโหมสหรัฐอเมริกาถ้าเป็นการทำลายแบบถาวรให้ทำลายโดยการบดขยี้

ข้อ ๔. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องกำหนดระบบและอุปกรณ์สนับสนุนการทำงาน ดังนี้

๔.๑ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

๔.๑.๑ ระบบสำรองกระแสไฟฟ้า (UPS)

๔.๑.๒ ระบบปรับอากาศและควบคุมความชื้น

๔.๒ ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๔.๓ ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๕. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องควบคุมการนำอุปกรณ์คอมพิวเตอร์ของกรมฯ ออกนอกหน่วยงาน ดังนี้

๕.๑ ให้มีการขออนุญาตก่อนนำสิ่งอุปกรณ์หรือทรัพย์สินออกนอกหน่วย

๕.๒ บันทึกข้อมูลการนำสิ่งอุปกรณ์ของกรมฯ ออกนอกหน่วย เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

หมวด ๒.
แนวปฏิบัติในการบริหารจัดการสิทธิการเข้าถึง

ข้อ ๑. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน ดังนี้

๑.๑ ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ต้องปฏิบัติตามขั้นตอนลงทะเบียนในแบบฟอร์มที่กรมฯ กำหนดขึ้น เพื่อให้มีสิทธิในการใช้งานระบบสารสนเทศ ตามความจำเป็น รวมทั้งปฏิบัติตามขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป ย้ายออก เกษียณอายุ เป็นต้น

๑.๒ กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบเว็บท่า (Portal) ระบบรับ-ส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบงานภายในต่าง ๆ ระบบเครือข่ายไร้สาย (Wireless LAN) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชา เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๒. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (user account) และรหัสผ่านของเจ้าหน้าที่ดังนี้

๒.๑ กำหนดบัญชีชื่อผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดบัญชีชื่อผู้ใช้งานซ้อนกัน

๒.๒ ไม่อนุญาตให้ผู้ร้องขอใช้ระบบงานเข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้น

๒.๓ จัดเก็บข้อมูลการลงทะเบียนของผู้ที่ร้องขอใช้ระบบไว้เพื่อเอาไว้ใช้อ้างอิงหรือตรวจสอบในภายหลัง

๒.๔ ทบทวนบัญชีผู้ใช้งานทั้งหมดอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้งเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทางดังนี้

๒.๔.๑ พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงานภายในของกรมฯ

๒.๔.๒ จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานภายในนั้นเพื่อดำเนินการทบทวนว่าเจ้าหน้าที่มีการเลื่อนตำแหน่ง,ย้าย,ลาออก หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้มีการแก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่

๒.๔.๓ ผู้บังคับบัญชาของหน่วยงานภายในแจ้งกลับว่ามีรายชื่อใดที่ต้องดำเนินการแก้ไขให้ถูกต้อง

๒.๔.๔ ดำเนินการแก้ไขข้อมูลสิทธิให้ถูกต้องตามที่ได้รับแจ้ง

ข้อ ๓. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องจัดให้มีการพิสูจน์ตัวตนเพื่อเข้าใช้ระบบงานสำคัญสำหรับผู้ใช้ที่อยู่ภายนอกสถานที่ดังนี้

ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบของกรมฯ ต้องผ่านการพิสูจน์ตัวตนจากระบบของกรมฯ โดยมีแนวปฏิบัติดังนี้

๓.๑ การแสดงตัวตนด้วยชื่อบัญชีผู้ใช้งาน

๓.๒ การพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน

๓.๓ การเข้าสู่ระบบงานสำคัญของกรมฯ ผ่านเครือข่ายอินเทอร์เน็ตนั้น จะมีการตรวจสอบผู้ใช้งานด้วย

ข้อ ๔. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องกำหนดหลักเกณฑ์ที่เข้มงวดเกี่ยวกับการใช้และการเปลี่ยนรหัสผ่านสำหรับใช้ในการเข้าถึงฐานข้อมูลของเจ้าหน้าที่ อาทิ

๔.๑ การกำหนดรหัสผ่านควรมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการผสมผสานกันระหว่างตัวอักษรตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และ สัญลักษณ์เข้าด้วยกัน)

๔.๒ ไม่ควรกำหนดรหัสผ่านจากชื่อ สกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือ จากคำศัพท์ที่ใช้ในพจนานุกรม

๔.๓ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ที่เจ้าหน้าที่ครอบครองอยู่

๔.๔ ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

๔.๕ ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default) หรือได้รับรหัสผ่านใหม่ต้องเปลี่ยนแปลงรหัสผ่านนั้นโดยทันที

๔.๖ ไม่อนุญาตให้เจ้าหน้าที่ใช้รหัสผ่านร่วมกัน

๔.๗ ให้เจ้าหน้าที่ที่ได้รับมอบหมายให้สามารถเข้าถึงฐานข้อมูลเปลี่ยนรหัสผ่านที่ใช้อย่างสม่ำเสมอ โดยในการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรกำหนดรหัสผ่านใหม่ซ้ำของเดิมครั้งสุดท้าย

๔.๘ ให้เจ้าของหน่วยงานแจ้งยกเลิกการใช้งานของเจ้าหน้าที่ทันทีในกรณีลาออกจากงานหรือพ้นจากหน้าที่ ให้ผู้ดูแลระบบทราบ

๔.๙ ถ้ารหัสผ่านถูกเปิดเผยบนระบบต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

๔.๑๐ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์ ในการพิมพ์แต่ละตัวอักษร

๔.๑๑ ผู้ใช้งานต้องไม่เปลี่ยนรหัสผ่านของผู้อื่น ยกเว้นผู้มีหน้าที่ในการบริหารจัดการรายชื่อผู้ใช้งานและรหัสผ่าน

๔.๑๒ ถ้ามีการเปิดให้บุคคลทั่วไปใช้ Guest Account ควรทำการจำกัดสิทธิ์ในการใช้งานอย่างรัดกุม หรือหากเป็นไปได้ให้งดใช้งาน Guest Account

๔.๑๓ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๑๕ นาทีให้ยุติการใช้งาน (Session Time - Out) สำหรับระบบที่มีความสำคัญสูง ให้ผู้ดูแลระบบต้องกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) สูงสุดไม่เกิน ๑๘๐ นาที ต่อการเชื่อมต่อในแต่ละครั้ง

๔.๑๔ ผู้ใช้งานระบบควรทำการแจ้งผู้ดูแลระบบ หากต้องการทำกิจกรรมที่อาจมีผลกระทบต่อความปลอดภัยของระบบ และผู้ใช้งานระบบควรจะแจ้งผู้ดูแลระบบความปลอดภัยของระบบทันที ถ้าหากสงสัยว่าได้กระทำกิจกรรมที่มีผลต่อความปลอดภัยของระบบ

๔.๑๕ กำหนดสิทธิ์ให้ผู้ใช้แต่ละระดับ (Access Right) มีระบบรักษาความปลอดภัยที่อนุญาตให้ผู้ใช้งาน สามารถเข้าสู่ระบบได้ตามขอบเขตงานที่รับผิดชอบดังนี้

- Guests คือ กลุ่มผู้ใช้ข้อมูลทั่วไปสามารถอ่านได้อย่างเดียว
- Users คือ กลุ่มที่สามารถอ่านและแก้ไขข้อมูลได้ โดยสามารถแก้ไขเฉพาะข้อมูลที่รับผิดชอบเท่านั้น
- Admin คือ กลุ่มผู้ดูแลระบบสามารถปรับปรุงและเข้าถึงระบบได้ทั้งหมด

๔.๑๖ กำหนดลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล มีการบริหารจัดการดังนี้

- การรักษาความลับ (Confidentiality) ให้บุคคลผู้มีสิทธิ์เท่านั้น เข้าถึงเรียกดูข้อมูลได้ โดยมีการควบคุมการเข้าถึงข้อมูล โดยข้อมูลที่เป็นความลับผู้มีสิทธิ์ใช้ข้อมูลต้องไม่เปิดเผยกับผู้อื่น
- ความถูกต้องเหมาะสม (Integrity) มีระบบป้องกันความถูกต้องครบถ้วนและสมบูรณ์ของข้อมูล และวิธีประมวลผลต้องมีการควบคุมและป้องกันความผิดพลาด กรมฯ ไม่กำหนดให้ผู้ไม่มีสิทธิ์เข้ามาเปลี่ยนแปลงแก้ไขข้อมูล
- ความสามารถพร้อมใช้ (Availability) ให้บุคคลผู้มีสิทธิ์ใช้ข้อมูลเท่านั้นสามารถเข้าถึงข้อมูลได้ทุกเมื่อที่ต้องการ ผู้ดูแลระบบต้องมีการควบคุมไม่ให้ระบบใช้งานไม่ได้ ไม่ให้ผู้ไม่มีสิทธิ์ทำให้ระบบเกิดความเสียหาย

๔.๑๗ ผู้ใช้งานสามารถเข้าถึงข้อมูลระบบงานภายในด้วยความเร็วในการเข้าใช้งานได้ไม่เกิน ๓๐ วินาที การควบคุมการเข้าถึง มี ๒ วิธี คือ

- การควบคุมการเข้าถึงระบบงานภายในจะต้องมีการควบคุมสิทธิ์ใน การเข้าถึงและสิทธิ์ในการใช้ข้อมูลภายใน ซึ่งถูกจัดเก็บไว้ในระบบ ฐานข้อมูล

- การควบคุมการเข้าถึงระบบเครื่องแม่ข่ายจะต้องมีการควบคุมสิทธิ์ในการเข้าสู่การใช้งานเครื่องแม่ข่าย

หมวด ๓.
แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

ข้อ ๑. ผู้บังคับบัญชาหน่วยงานภายในกรมฯ ต้องจัดให้มีวิธีการจัดการ การเข้าถึงข้อมูลตามระดับชั้นความลับ ซึ่งเบื้องต้นกรมฯ ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ อาศัยอำนาจตามความในมาตรา ๑๖ และมาตรา ๒๖ วรรคห้า แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ ในการกำหนดชั้นความลับของข้อมูล จึงกำหนดให้มีแนวปฏิบัติ ดังนี้

๑.๑ ผู้ใช้งาน ต้องจัดการกับข้อมูลตามชั้นความลับของข้อมูล กรมฯ ได้กำหนดชั้นความลับของข้อมูลดังนี้

ลับที่สุด (Top Secret), หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด

ลับมาก (Secret), หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

ลับ (Confidential) หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

ข้อ ๒. ในการจัดการกับไฟล์ข้อมูลลับ ให้ปฏิบัติดังนี้

๒.๑ ระมัดระวังการกระจาย หรือแจกจ่ายข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับของกรมส่งเสริมอุตสาหกรรมไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

๒.๒ ผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ต้องตรวจสอบความถูกต้องของข้อมูลอิเล็กทรอนิกส์ก่อนนำไปใช้งาน

๒.๓ ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยการใช้รหัสผ่านที่มีความมั่นคงปลอดภัย เมื่อมีการนำไฟล์ข้อมูลลับไปใช้งานผู้ใช้งานต้องมีการเข้ารหัส โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๒.๔ ห้าม Share ไฟล์ข้อมูลลับบนเครือข่ายของกรมฯ เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ (ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการ Share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)

๒.๕ ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลลับว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

๒.๖ ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่เพื่อแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่

๒.๗ ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

๒.๘ ต้องทำลายข้อมูลอิเล็กทรอนิกส์บนฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์ที่ถูกยกเลิกการใช้งาน

ข้อ ๓ ประเภทข้อมูล

๓.๑ ข้อมูลสารสนเทศเพื่อการบริหาร เช่น ข้อมูลสารสนเทศที่ใช้ภายในกรมส่งเสริมอุตสาหกรรม เช่น ข้อมูลเงินเดือน ข้อมูลระบบสารบรรณ ข้อมูลแผนงานงบประมาณ เป็นต้น

๓.๒ ข้อมูลสารสนเทศเพื่อการบริการ เช่น ข้อมูลเว็บไซต์ กสอ. ข้อมูลห้องสมุด ข้อมูลปรึกษาแนะนำ เป็นต้น

หมวด ๔.
แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

ข้อ ๑. การใช้คอมพิวเตอร์ของ กรมฯ ให้เจ้าหน้าที่ปฏิบัติดังต่อไปนี้

๑.๑ ต้องตรวจสอบว่าโปรแกรมป้องกันไวรัสยังทำงานตามปกติและมีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ หากพบว่าโปรแกรมดังกล่าวทำงานผิดปกติให้รีบแจ้งหน่วยงานที่รับผิดชอบระบบสารสนเทศ เพื่อดำเนินการแก้ไขโดยเร็ว

๑.๒ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกจากโปรแกรมมาตรฐานที่กำหนด

๑.๓ ห้ามเปลี่ยนแปลงหรือแก้ไขซอฟท์แวร์ที่มีลิขสิทธิ์ถูกต้องของกรมส่งเสริมอุตสาหกรรม

๑.๔ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย

๑.๕ ต้องลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากคอมพิวเตอร์เพื่อประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

๑.๖ ต้องออกจากระบบ (Log off) ทุกครั้งที่มิได้ปฏิบัติงานอยู่หน้าคอมพิวเตอร์ รวมทั้งปิดคอมพิวเตอร์เมื่อใช้งานประจำวันเสร็จสิ้น

๑.๗ การนำคอมพิวเตอร์ส่วนตัวมาใช้กับระบบเครือข่ายของกรมฯ ต้องได้รับการตรวจสอบและอนุญาตจากหน่วยงานที่รับผิดชอบระบบสารสนเทศ และต้องสแกนไวรัสก่อนการใช้งานทุกครั้ง

ข้อ ๒. การใช้คอมพิวเตอร์เพื่อประโยชน์ส่วนตัวของเจ้าหน้าที่ให้ใช้ได้ภายในสถานที่ที่กรมฯ จัดไว้เป็นการเฉพาะเท่านั้น

ข้อ ๓. การเข้าถึงระบบงานเทคโนโลยีสารสนเทศ เจ้าหน้าที่ใช้งานต้องปฏิบัติตาม ข้อกำหนดดังต่อไปนี้

๓.๑ ให้ผู้ใช้งานใหม่ทำการขอลงทะเบียน เพื่อให้ผู้ดูแลระบบกำหนดสิทธิ์ต่าง ๆ ตามที่ได้รับและให้ผู้ใช้งานทำงานได้ตามที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๓.๒ ต้องไม่เข้าถึงระบบงานอื่นที่ตนไม่ได้รับอนุมัติให้ใช้งาน

๓.๓ ต้องออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

ข้อ ๔. การใช้งานอินเทอร์เน็ต ผู้ใช้งานต้องปฏิบัติตาม ข้อกำหนด ดังต่อไปนี้

๔.๑ ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้

(ก) การพนัน

(ข) การประมูล

(ค) วิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และ พระมหากษัตริย์

(ง) ลามก อนาจาร

(จ) อื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือผิดศีลธรรม จริยธรรม

๔.๒ ห้ามใช้อินเทอร์เน็ตเพื่อส่ง กระจาย หรือ แจกจ่าย ดังต่อไปนี้

(ก) สื่อสิ่งพิมพ์อิเล็กทรอนิกส์ที่เป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของ

(ข) ข้อมูลประเภทสื่อลามกอนาจาร

(ค) ข้อมูลที่เป็นความลับของกรมฯ ไปยังบุคคลที่ไม่ได้รับอนุญาต

(ง) ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

๔.๓ ห้ามใช้อินเทอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์ หรือชื่อเสียงของกรมฯ

ข้อ ๕. การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องปฏิบัติตาม ข้อกำหนด ดังต่อไปนี้

๕.๑ ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ตามที่กรมฯ กำหนดเท่านั้น

๕.๒ ห้ามดู ใช้ หรือเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ของบุคคลอื่นโดยไม่ได้รับอนุญาต

๕.๓ ห้ามปลอมแปลง รับหรือส่งจดหมายอิเล็กทรอนิกส์ของบุคคลอื่นโดยไม่ได้รับอนุญาต

๕.๔ ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้

(ก) จดหมายขยะ (Spam Mail)

(ข) จดหมายลูกโซ่ (Chain Letter)

(ค) จดหมายที่ละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น

(ง) จดหมายที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

๕.๖ ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีขนาดใหญ่เกินกว่าที่กรมฯ กำหนด

๕.๗ ต้องระบุชื่อเรื่อง (Subject) และชื่อผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป

๕.๘ ต้องใช้คำที่สุภาพในการส่งจดหมายอิเล็กทรอนิกส์

หมวด ๕.
แนวปฏิบัติและหน้าที่ของผู้ดูแลระบบสารสนเทศ/ผู้ดูแลเครือข่าย

ข้อ ๑ เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๑.๑ การลงทะเบียนผู้ใช้งาน (User Registration) มีการกำหนดขั้นตอนปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานใหม่ เพื่อกำหนดสิทธิ์ต่างๆ ในการใช้งานตามสิทธิ์ที่ได้รับ รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกหรือเปลี่ยนหน่วยงานภายในองค์กร เป็นต้น

๑.๒ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) ผู้ดูแลระบบ ต้องจัดให้การควบคุมและจำกัดสิทธิ์การใช้งานระบบตามความเหมาะสมในการใช้งาน และการเข้าถึงข้อมูล

๑.๓ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ผู้ดูแลระบบต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม เพื่อให้มีความมั่นคงปลอดภัย

๑.๔ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Right) ผู้ดูแลระบบและเจ้าของระบบงาน ต้องจัดให้มีกระบวนการทบทวนสิทธิ์การเข้าถึงผู้ใช้งาน-ระบบตามระยะเวลาที่กำหนดไว้

ข้อ ๒ ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

ข้อ ๓ ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) ระบบงานสารสนเทศ และระบบเครือข่าย

ข้อ ๕ บริหารจัดการบัญชีผู้ใช้งานตามอำนาจหน้าที่ที่ตนเองรับผิดชอบเท่านั้น

ข้อ ๖ บริหารจัดการระบบงานสารสนเทศ และระบบเครือข่ายตามอำนาจหน้าที่ที่ตนเองรับผิดชอบเท่านั้น

ข้อ ๗ บริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตามอำนาจหน้าที่ที่ตนเองรับผิดชอบเท่านั้น

ข้อ ๘ ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งาน ที่ใช้งานระบบคอมพิวเตอร์ ระบบสารสนเทศ และระบบเครือข่ายโดยไม่มีเหตุผลอันสมควร

ข้อ ๙ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งาน ที่ใช้งานระบบคอมพิวเตอร์ ระบบสารสนเทศ และระบบเครือข่าย โดยไม่มีเหตุผลอันสมควร

ข้อ ๑๐ ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่สามารถเปิดเผยได้ให้บุคคลอื่นทราบ โดยไม่มีเหตุผลอันสมควร

ข้อ ๑๑ เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็น เพื่อให้สามารถระบุตัวตนผู้ใช้งานและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า ๙๐ วัน นับแต่การใช้บริการสิ้นสุดลง

หมวด ๖.
แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย

ข้อ ๑. กำหนดมาตรการทางเครือข่ายสื่อสารข้อมูลเพื่อป้องกันข้อมูลในเครือข่าย ระบบงาน หรือบริการต่างๆ จากการถูกเข้าถึงหรือถูกทำลายโดยไม่ได้รับอนุญาต ดังต่อไปนี้

๑.๑ กำหนดบุคลากรผู้มีหน้าที่รับผิดชอบ ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล

๑.๒ กำหนดมาตรการป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ เช่น เครือข่ายอินเทอร์เน็ต เครือข่ายไร้สาย เป็นต้น

๑.๓ กำหนดมาตรการเพื่อป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

๑.๔ กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่างๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

๑.๕ มีการบันทึกข้อมูลพฤติกรรมการใช้งานเก็บ Log ของอุปกรณ์เครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

ข้อ ๒. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ผู้ดูแลต้องปฏิบัติตาม ข้อกำหนดดังต่อไปนี้

๒.๑ ผู้ดูแลระบบ ต้องมีการออกแบบแบ่งระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งานตามกลุ่มของผู้ใช้ เพื่อเป็นการควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๒.๒ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๒.๓ ผู้ดูแลระบบ ต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน โดยกำหนด IP Routing บนอุปกรณ์เลือกเส้นทาง (Router & Switch) รวมทั้งตรวจสอบและปิดพอร์ต (Port) ของอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๒.๔ ระบบเครือข่ายทั้งหมดของหน่วยที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering ผ่านระบบ Firewall

๒.๕ มีการติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IPS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย

๒.๖ การเข้าสู่ระบบงานเครือข่ายภายในหน่วยงาน ผ่านทางอินเทอร์เน็ตต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๒.๗ ข้อมูลหมายเลขชุดอินเทอร์เน็ตของคอมพิวเตอร์ (IP Address) ภายใน (Local) ของระบบงานเครือข่ายภายในของกรมฯ จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของกรมฯ ได้โดยง่าย

๒.๘ จัดทำแผนผังระบบเครือข่าย (Network Diagram) พร้อม IP address และ MacAddress เพื่อระบุอุปกรณ์เครือข่าย ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๙ จัดให้มีการใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้รับมอบอำนาจ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒.๑๐ การบริหารจัดการการบันทึกและตรวจสอบ กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้ไม่น้อยกว่า ๓ เดือน หรือไม่ต่ำกว่า ๙๐ วัน

๒.๑๑ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

ข้อ ๓. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องจัดการควบคุมการเข้าใช้งานระบบจากภายนอก หน่วยงานที่มีระบบสารสนเทศ ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งเอาไว้ภายในหน่วยของตนเอง เพื่อดูแลรักษาความปลอดภัยของระบบภายในจากการเข้าถึงระบบจากภายนอก โดยมีแนวปฏิบัติ ดังนี้

๓.๑ การเข้าสู่ระบบจากระยะไกล (remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ของกรมฯ ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของกรมฯ การควบคุม

บุคคลที่เข้าสู่ระบบของกรมฯ จากระยะไกลจึงต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน ผ่านระบบ VPN จากบัญชีรายชื่อผู้ใช้งาน (Active Directory)

๓.๒ วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้ที่ได้รับการมอบอำนาจก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๓.๓ ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับกรมฯ อย่างเพียงพอและต้องได้รับอนุมัติจากผู้บังคับบัญชา และกำหนดให้มีการยืนยันตัวบุคคล ผ่านระบบ VPN จากบัญชีรายชื่อผู้ใช้งาน (Active Directory)

ข้อ ๔. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ผู้ดูแลต้องปฏิบัติตาม ข้อกำหนด ดังต่อไปนี้

๔.๑ ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในกรมฯ จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาก่อนการใช้งาน

๔.๒ ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๔.๓ ผู้ดูแลระบบควรใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

หมวด ๗.
แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

ข้อ ๑. ผู้ใช้งานควรยืนยันตัวตนด้วย User account ของตนเองก่อนเข้าใช้งานระบบปฏิบัติการเครื่องคอมพิวเตอร์ทุกครั้ง

ข้อ ๒. ผู้ใช้งานไม่ควรอนุญาตให้บุคคลอื่นใช้ User account ของตนเองในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

ข้อ ๓. ผู้ใช้งานควรทำการลงบันทึกออก (Log off) ทุกครั้งที่มิได้ปฏิบัติงานอยู่หน้าคอมพิวเตอร์ รวมทั้งปิดคอมพิวเตอร์เมื่อใช้งานประจำวันเสร็จสิ้น

หมวด ๘.
แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

ข้อ ๑. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องกำหนดแนวปฏิบัติในการสำรองและกู้คืนข้อมูล เมื่อมีระบบงานใหม่ เกิดข้อมูลใหม่ หรือข้อมูลที่มีการเปลี่ยนแปลงใหม่ ควรกำหนดให้ใช้แนวทางการสำรองและกู้คืนข้อมูลดังนี้

๑.๑ พิจารณาระบบงานที่มีความสำคัญและขั้นตอนในการสำรองข้อมูล

๑.๒ กำหนดผู้ดูแลในการสำรองข้อมูล

๑.๓ กำหนดความถี่ในการสำรองข้อมูลของระบบงาน เช่น ระบบงานที่มีการเปลี่ยนแปลงบ่อย ควรมีความถี่ในการสำรองข้อมูลมากขึ้น เป็นต้น

๑.๔ กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์ที่ใช้ในการสำรองข้อมูล

๑.๕ ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ และควรนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด

๑.๖ ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้น สำเร็จครบถ้วน หรือไม่

๑.๗ ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ในระบบที่สำคัญ รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ หรือไม่ อย่างน้อยปีละ ๑ ครั้ง

๑.๘ จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนด แผนควรมีรายละเอียดอย่างน้อยดังต่อไปนี้

๑.๘.๑ การกำหนดหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด

๑.๘.๒ การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๑.๘.๓ การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน

๑.๘.๔ การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

หมวด ๙.
แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

ข้อ ๑. การแจ้งเหตุการณ์ทางด้านความมั่นคงปลอดภัย

๑.๑ ให้เจ้าหน้าที่หรือผู้ปฏิบัติงานแจ้งไปยังหน่วยงานที่รับผิดชอบระบบสารสนเทศ ทันทีที่พบเห็นเหตุการณ์ที่อาจเป็นปัญหาต่อความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของกรมฯ อันได้แก่

(ก) มีโปรแกรมไม่ประสงค์ดีเข้ามาในระบบ
(ข) มีการบุกรุกเข้ามาในเครือข่าย
(ค) ข้อมูลสำคัญเปลี่ยนแปลง หรือสูญหาย
(ง) มีการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต
(จ) มีการนำข้อมูลสำคัญไปใช้ผิดวัตถุประสงค์
(ฉ) มีการใช้ระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์
(ช) พบจุดอ่อนในระบบงาน ซอฟต์แวร์ หรือฮาร์ดแวร์ที่ใช้งาน
(ซ) มีการโจมตีเข้ามาในระบบจนไม่สามารถให้บริการได้
(ฌ) ระบบเทคโนโลยีสารสนเทศชำรุด หรือสูญหาย
(ญ) บุคคลภายนอกเข้าใช้ระบบงานของกรมฯ โดยไม่ได้รับอนุญาต
(ฎ) มีการติดตั้งซอฟต์แวร์เพื่อขโมยข้อมูลหรือเข้าถึงข้อมูลในเครือข่าย หรือ
(ฏ) เหตุการณ์อื่นๆ ที่เป็นการละเมิดความมั่นคงปลอดภัยของกรมฯ

๑.๒ ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชา หรือหน่วยงานที่รับผิดชอบระบบสารสนเทศ ในการตรวจสอบเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้น

ข้อ ๒. ผู้ดูแลระบบสารสนเทศของกรมฯ เมื่อได้รับแจ้งจากผู้ใช้งานเกี่ยวกับเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้นหรือที่พบ ให้ปฏิบัติตามขั้นตอนดังต่อไปนี้

๒.๑ ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้นว่ามีผลกระทบในระดับใด (สูง กลาง หรือต่ำ)

๒.๒ แจ้งให้ผู้บังคับบัญชาตามลำดับชั้นได้รับทราบตามระดับของผลกระทบ กล่าวคือ รายงานไปสู่ระดับชั้นของผู้บังคับบัญชาที่สูงขึ้นตามลำดับสำหรับเหตุการณ์ที่มีผลกระทบสูงกว่า

๒.๓ จัดทำรายงานสรุปเหตุการณ์นับตั้งแต่ได้รับแจ้งเฉพาะเหตุการณ์ที่มีผลกระทบตั้งแต่ระดับปานกลาง ขึ้นไปและแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ โดยมีข้อมูลอย่างน้อยในรายงานดังนี้

- รายละเอียดเหตุการณ์
- วันเวลาที่เกิดขึ้น
- ชื่อผู้แจ้ง/หน่วยงานผู้แจ้ง
- สถานะของเหตุการณ์ในแต่ละช่วงเวลา
- ความคืบหน้าในการดำเนินการในแต่ละช่วงเวลา
- สาเหตุและวิธีการแก้ไข
- ข้อเสนอแนะเพื่อป้องกันการเกิดซ้ำ

ข้อ ๓. ความรับผิดชอบของผู้บังคับบัญชากรณีที่มีการละเมิดการปฏิบัติ นี้

๓.๑ ให้แจ้งรายงานตามสายการบังคับบัญชาให้หน่วยที่เกี่ยวข้องทราบ

๓.๒ สั่งการสอบสวนหาตัวผู้กระทำผิดและผู้รับผิดชอบโดยเร็วที่สุด

๓.๓ พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เช่นนี้อุบัติซ้ำอีก

ข้อ ๔. ความรับผิดชอบของหน่วยงานที่รับผิดชอบระบบงานสารสนเทศ เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัยของข้อมูล ให้ส่วนราชการเจ้าของระบบสารสนเทศดำเนินการดังนี้

๔.๑ พิจารณาด้านความเสียหายของข้อมูลสารสนเทศมีผลกระทบกระเทือนเสียหายอย่างใดหรือไม่

๔.๒ แก้ไขหรือขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันทีในการนี้อาจจะต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติพร้อมทั้งปัจจัยต่างๆ ที่เกี่ยวข้องตามที่เห็นสมควร

ข้อ ๕. ความรับผิดชอบของผู้ใช้งานต่อประกาศฉบับนี้มีดังนี้

๕.๑ ปฏิบัติตามประกาศนี้อย่างเคร่งครัดและต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง

๕.๒ ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ได้รับอนุญาต หรือทำให้เสียหายต่อระบบคอมพิวเตอร์และเครือข่ายของกรมฯ

๕.๓ ไม่รบกวนหรือแทรกแซงการสื่อสารข้อมูลในเครือข่ายคอมพิวเตอร์ของกรมฯ

๕.๔ รายงานเหตุการณ์ความเสี่ยง จุดอ่อน หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบไปยังหน่วยงานผู้ดูแลระบบโดยเร็วที่สุด

หมวด ๑๐.
แนวปฏิบัติในการจัดซื้อจัดจ้างระบบเทคโนโลยีสารสนเทศ

ข้อ ๑. การจัดหาเพื่อให้ได้มาซึ่งระบบสารสนเทศ จะต้องดำเนินการตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมฯ โดยเคร่งครัด และให้ครอบคลุมถึง

๑.๑ การเชื่อมโยงหรือทำงานร่วมกันกับระบบงานเดิมต่าง ๆ ที่กรมฯ มีใช้งานอยู่

๑.๒ การจัดหาเครื่องแม่ข่ายเพื่อรองรับระบบสารสนเทศใหม่ให้รวมอยู่ในการจัดหาด้วย รวมถึงการดูแลระบบ การดูแลข้อมูล การสำรองข้อมูล และการ update ระบบต่าง ๆ ให้เป็นหน้าที่ของผู้พัฒนาระบบ

๑.๓ การดูแลการเชื่อมต่อกับระบบเครือข่ายกรมฯ ให้เป็นหน้าที่ของผู้ดูแลระบบ

๑.๔ การจัดหาระบบงานจะต้องรวมถึงการอบรมหรือการแนะนำการใช้งานด้วย

ข้อ ๒. ภายหลังจากที่ได้มีการตรวจรับระบบที่พัฒนาขึ้นใหม่แล้ว ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องกำหนดการควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์ที่ให้บริการ

๒.๑ ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบงานของหน่วย

๒.๒ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

๒.๓ กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบงาน เป็นต้น

๒.๔ ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

๒.๕ ในกรณีที่เป็นการติดตั้งระบบเพื่อทดแทนระบบงานเดิม ให้ทำการสำรองข้อมูลที่จำเป็น เช่น ฐานข้อมูล ซอฟต์แวร์ ค่าคอนฟิกกูเรชัน หรืออื่นๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งทำไม่สำเร็จจะได้สามารถถอยหลังกลับไปใช้ระบบงานเดิมได้

๒.๖ ในกรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบงานเดิมไปสู่ข้อมูลในระบบงานที่จะทำการติดตั้ง ให้กำหนดแผนการถ่ายโอนหรือแปลงข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ ถ่ายโอนข้อมูลตามแผนฯ และร่วมกับผู้ใช้งานเพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้องและครบถ้วนหรือไม่

๒.๗ ให้กำหนดแผนการติดตั้งสำหรับระบบงานซึ่งรวมถึงระยะเวลาที่จะดำเนินการ รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า เช่น แผนการติดตั้งฮาร์ดแวร์ ซอฟต์แวร์ และอื่นๆ

๒.๘ สำหรับซอฟต์แวร์ที่จะทำการติดตั้ง ให้ตรวจสอบก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตซอฟต์แวร์นั้น

๒.๙ ให้อ่านและปฏิบัติตามเงื่อนไขหรือข้อตกลงการใช้งานซอฟต์แวร์ที่จะทำการติดตั้งอย่างเคร่งครัด

๒.๑๐ สำหรับการติดตั้งซอฟต์แวร์ยูทิลิตี้ (utility software) ต้องตรวจสอบก่อนว่าเป็นซอฟต์แวร์ที่มีการทำงานที่ถูกต้องและเชื่อถือได้ โดยห้ามมิให้ติดตั้งโปรแกรม (utility software) หากไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๒.๑๑ ติดตั้งโปรแกรมแก้ไขช่องโหว่ต่างๆ (patch) ที่เกี่ยวข้องกับระบบงานตามความจำเป็น เช่น โปรแกรมแก้ไขช่องโหว่สำหรับระบบปฏิบัติการ โปรแกรมแก้ไขช่องโหว่สำหรับระบบบริหารจัดการฐานข้อมูล เป็นต้น

๒.๑๒ ตรวจสอบและปิดพอร์ต (port) บนระบบงานที่ไม่มีความจำเป็นในการใช้งานก่อนเปิดระบบให้บริการ

๒.๑๓ จัดให้มีการป้องกันไวรัสคอมพิวเตอร์บนระบบงานที่ทำการติดตั้ง

๒.๑๔ จำกัดการเชื่อมต่อทางเครือข่ายเพื่ออนุญาตให้เฉพาะกลุ่มผู้ใช้งานที่เกี่ยวข้องเท่านั้นจึงจะสามารถเชื่อมต่อเพื่อเข้าสู่ระบบงานที่ทำการติดตั้งนั้น

ข้อ ๓. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องกำหนดให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (technical review of applications after operating system changes) ดังนี้

๓.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๓.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้าน งบประมาณที่จำเป็นต้องใช้ ในกรณีที่กรมฯ ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

หมวด ๑๑.
แนวปฏิบัติในการเผยแพร่ข้อมูลสาธารณะ

ข้อ ๑. การเผยแพร่ข้อมูลในความรับผิดชอบของกรมส่งเสริมอุตสาหกรรมสู่สาธารณะโดยผ่านระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมอุตสาหกรรม หน่วยงานเจ้าของข้อมูลจะต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำออกเผยแพร่ และหากข้อมูลที่นำออกเผยแพร่เกี่ยวข้องกับเรื่องนโยบายจะต้องได้รับความเห็นชอบจากอธิบดีกรมส่งเสริมอุตสาหกรรม หรือผู้ซึ่งอธิบดีกรมส่งเสริมอุตสาหกรรมมอบหมายก่อนนำออกเผยแพร่

ข้อ ๒. การเผยแพร่ข้อมูลสู่สาธารณะโดยผ่านระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมอุตสาหกรรมให้ดำเนินการโดยหน่วยงานเจ้าของข้อมูล เว้นแต่กรณีที่อธิบดีกรมส่งเสริมอุตสาหกรรมหรือผู้ซึ่งอธิบดีกรมส่งเสริมอุตสาหกรรมมอบหมายได้สั่งการหรือเห็นชอบไว้เป็นอย่างอื่น

ประกาศ ณ วันที่ ๔ เดือน พ.ค. พ.ศ. ๒๕๕๕

(นายพสุ โลหารชุน)
อธิบดีกรมส่งเสริมอุตสาหกรรม

ภาคผนวก ก

ใบคำขอใช้สิทธิ์ระบบสารสนเทศ กสอ.

เลขที่ _____

คำขอใช้สิทธิ์ระบบสารสนเทศ กสอ.

ข้อมูลผู้ขอใช้สิทธิ์

สถานการณ์ทำงาน ☐ ข้าราชการ ☐ ลูกจ้างประจำ ☐ พนักงานราชการ ☐ ลูกจ้างชั่วคราว ☐ บุคคลภายนอก

สถานะปัจจุบัน ☐ สมัครใหม่ (ยังไม่มีสิทธิ์เข้าระบบ DIP-Portal) ☐ มีสิทธิ์เข้าระบบ DIP-Portal แล้ว

ชื่อ – สกุล (ไทย) (นาย/นาง/นางสาว) _____

ชื่อ – สกุล (อังกฤษ) (Mr./Mrs.) _____

เลขที่บัตรประชาชน ☐-☐☐☐☐-☐☐☐☐☐-☐☐-☐

หน่วยงาน (ระบุฝ่าย/ส่วน/สำนัก) _____

โทรศัพท์ _____ มือถือ _____

ความเห็นของผู้บังคับบัญชา	
เรียน ผอ.สส.สบย.กสอ. เพื่อโปรดดำเนินการต่อไป ลงชื่อ _____ (_____) วัน/เดือน/ปี _____	เรียน _____ เพื่อโปรดดำเนินการต่อไป ลงชื่อ _____ ผอ.สส.สบย.กสอ. วัน/เดือน/ปี _____

ระบบสารสนเทศด้านเครือข่ายที่ต้องการใช้

☐ ระบบ e-Mail (ปกติจะให้พื้นที่ (Mail Box) ๕๑๒ MB., แนบไฟล์ (Attach) ครั้งละไม่เกิน ๑๐ MB.)

☐ ระบบ Wireless LAN หมายเลขครุภัณฑ์ของอุปกรณ์ _____

ระบบงานภายในเว็บท่าที่ต้องการใช้

☐ ระบบสารบรรณอิเล็กทรอนิกส์
☐ ระบบฐานข้อมูลสมาชิก
☐ ข้อมูลส่วนตัว
☐ ประชุมผู้บริหาร
☐ ระบบ e-Learning
☐ ระบบจัดเก็บเอกสารอิเล็กทรอนิกส์
☐ ระบบบันทึกข้อมูลผลงานผู้รับจ้าง
☐ ระบบรายงานสารสนเทศ
☐ ปฏิทินผู้บริหาร
☐ ลงข้อมูลระบบเว็บไซต์ กสอ.
☐ ระบบ SMS
☐ สมุดโทรศัพท์ส่วนรวม
☐ ลงข้อมูลประชุม

* โดยปกติทุกท่านจะสามารถใช้สิทธิ์ดูได้ทุกระบบงานอยู่แล้ว

*** สำหรับ ๑. ระบบแผนงบประมาณ ชื่อผู้ประสานงาน คุณฐิติพร วิเศษพจนกิจ สำนัก สผ.สบย. เบอร์โทร. ๐๒๒๐๒๔๕๐๙

๒. ระบบเตือนภัย ชื่อผู้ประสานงาน คุณประเทือง พฤกษาพิทักษ์กุล สำนัก สต.สบย. เบอร์โทร. ๐๒๒๐๒๔๕๑๒

๓. โครงการ สอช. ผู้ประสานงาน คุณบุญวดี เกตุเหล็ก สำนัก สพช. ๐๒๓๖๗๘๓๕๘

๔. โครงการ bds ผู้ประสานงาน คุณวิทัศนีย์ จาดเสม สำนัก สพบ. ๐๒๒๐๒๔๔๙๓

ให้ติดต่อขอใช้สิทธิ์ที่มากกว่าการดูได้ที่หน่วยงานเจ้าของระบบโดยตรง

บันทึกการดำเนินงานของ สส.สบย.กสอ.

รายละเอียด	ผู้ดำเนินงาน	วันที่
๑. สร้างสิทธิ์ระบบ Portal		
๒. สร้างสิทธิ์ระบบ _____		
๓. สร้างสิทธิ์ระบบ _____		
๔. สร้างสิทธิ์ระบบ _____		
๕. สร้างสิทธิ์ระบบ _____		
๖. ดำเนินการแจ้งผู้ขอใช้สิทธิ์แล้ว		
ตรวจสอบการดำเนินงานแล้ว		

ภาคผนวก ข
โปรแกรมมาตรฐานในการใช้งานของกรมส่งเสริมอุตสาหกรรม

๑. Microsoft Windows

๒. Microsoft Office

๓. Acrobat Reader

๔. Anti-virus