นโยบายระบบสารสนเทศ

บริษัท ฟิวเจอร์ เมดิคอล ซัพพลาย จำกัด

อนุมัติโดย : _____

(คุณสมนึก วงษ์สมิง)

กรรมการผู้จัดการ

ประกาศใช้ครั้งที่ 00

วันที่ ...08.AUG.2025

ส่วนที่ 1

แนวนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยระบบสารสนเทศ

(Acceptable Use Policy)

ด้วยบริษัทได้กำหนดให้มี นโยบายว่าด้วยความปลอดภัยระบบสารสนเทศ บริษัท ฟิวเจอร์ เมดิคอล ซัพพลาย จำกัด แล้วนั้นเพื่อให้เกิดผลเป็นรูปธรรม ตามนโยบายดังกล่าวอาศัยอำนาจพระราชบัญญัติ ว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงได้จัดทำหนังสือยินยอมรับเงื่อนไขนโยบายว่าด้วย ความปลอดภัยระบบสารสนเทศขึ้นประกอบด้วย 10 หมวด โดยมีรายละเอียด ดังต่อไปนี้

วัตถุประสงค์

1. เพื่อเป็นหลักฐานเชิงประจักษ์ (ลายลักษณ์อักษร) สำหรับผู้ใช้งานระบบสารสนเทศของบริษัท ว่า ยินยอมรับเงื่อนไขตามนโยบาย ว่าด้วยความปลอดภัยระบบสารสนเทศบริษัททุกประการ

2. เพื่อให้ผู้ใช้งานระบบสารสนเทศของบริษัทได้รับทราบถึงข้อห้าม และข้อปฏิบัติ ที่จะส่งผลให้เกิด ความปลอดภัยต่อระบบ สารสนเทศ และเกิดการใช้งานตรงตามวัตถุประสงค์การใช้งานระบบสารสนเทศของ บริษัท รวมทั้งไม่ละเมิดระเบียบกฎหมาย หรือทำให้เกิด ความเสียหายในการปฏิบัติงาน

ขอบเขต

หนังสือนี้มีผลบังคับใช้กับผู้ใช้งานระบบสารสนเทศ ทุกระดับชั้น ตำแหน่ง โดยไม่มีการยกเว้นผู้ใช้งาน รวมถึงผู้บริหาร พนักงาน ลูกจ้างทดลองงาน บุคคลภายนอก ที่ต้องใช้ระบบสารสนเทศของบริษัท

นิยามศัพท์

“บริษัท” หมายความถึง บริษัท ฟิวเจอร์ เมดิคอล ซัพพลาย จำกัด และบริษัทในกลุ่มหรือที่จะเกิดขึ้น ในอนาคตที่ใช้ระบบเครือข่ายคอมพิวเตอร์และระบบ ข้อมูลร่วมกัน

“เครื่องคอมพิวเตอร์” หมายความว่า อุปกรณ์ประมวลผลข้อมูลที่ทำงานด้วยระบบอิเล็กทรอนิคส์ที่มี ความเร็วสูง โดยทำงานตามคำสั่ง ผ่านทางซอฟต์แวร์ให้ได้ผลตามที่ต้องการ ได้แก่ คอมพิวเตอร์แม่ข่าย (Server) คอมพิวเตอร์ส่วนบุคคล (Personal Computer) และคอมพิวเตอร์ แบบพกพา (Notebook Computer) รวมถึงแท็บเล็ตคอมพิวเตอร์

“สมาร์ทโฟน” หมายความว่า อุปกรณ์สื่อสาร (โทรศัพท์) ที่ใช้งานร่วมกับระบบสารสนเทศของบริษัท

“อุปกรณ์คอมพิวเตอร์” หมายความว่า อุปกรณ์อิเล็กทรอนิคส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์เพื่อสนับสนุนให้ เครื่องคอมพิวเตอร์ ปฏิบัติงานได้ตามต้องการ รวมถึงเครื่องคอมพิวเตอร์

“เครือข่ายคอมพิวเตอร์” หมายความว่า เครือข่ายคอมพิวเตอร์ของบริษัท

“ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างของบริษัท

“บุคลากร” หมายความว่า พนักงานบริษัท รวมถึงลูกจ้างทดลองงาน ของบริษัท หรือบุคคลอื่นที่ได้รับมอบหมายให้ปฏิบัติงานตามสัญญาของบริษัท

“ผู้ใช้งาน” หมายความว่า พนักงานบริษัทหรือบุคคลภายนอกที่ได้รับสิทธิ์ให้ใช้งานระบบคอมพิวเตอร์ของบริษัท

“บัญชีผู้ใช้งาน” หมายความว่า บัญชีที่ผู้ใช้งานใช้ในการเข้าถึงและใช้งานระบบคอมพิวเตอร์ ซึ่งเป็นไปตามข้อตกลง ระหว่างผู้ใช้งานกับผู้ให้บริการระบบคอมพิวเตอร์

“ข้อมูล” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใดๆไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่ง นั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะทำในรูปแบบเอกสารแฟ้มรายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย การบันทึกภาพ หรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีการอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“การพิสูจน์ตัวตน” หมายความว่า ขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

“ผู้ดูแลระบบ” หมายความว่า ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ที่ได้รับมอบหมายจากบริษัท

ข้อบังคับ

ผู้ใช้งานระบบสารสนเทศของบริษัท มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

หมวด 1

ว่าด้วยการพิสูจน์ตัวตน

(Accountability, Identification and Authentication)

ข้อ 1 ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคน ต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่นรวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้ รหัสผ่าน (Password)

ข้อ 2 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งาน หรือไม่ก็ตาม

ข้อ 3 ผู้ใช้งานควรตั้งรหัสผ่านให้ตรงตาม นโยบายการจัดการรหัสผ่าน

นโยบายการจัดการรหัสผ่าน

(Password management)

รหัสผ่านครอบคลุมบัญชีชื่อผู้ใช้งานดังนี้

ข้อ 1 Computer User ทั้งที่เป็น Domain User และ Local User, E-mail 365 System, Internet, Microsoft Dynamic 365, Bplus HRM, Win Wpeed หรือ บัญชีผู้ใช้งานระดับบริหารจัดการระบบสารสนเทศต่างๆ

ข้อ 2 รหัสผ่านต้องมีอย่างน้อย 8 ตัวอักษร

ข้อ 3 ประกอบด้วยอักขระภาษาอังกฤษ (Alphabet) ตัวเลข (Numeric character) และอักขระพิเศษ (Special character)เช่น !@#$ โดยจัดเรียงแบบไหนก็ได้

ข้อ 4 รหัสผ่านต้องไม่เป็นลักษณะตัวเลขหรืออักขระที่เรียงกันหรือซ้ำเกิน 3 ตัวอักษร หรือตัวอักขระ ที่เหมือนกับบัญชีชื่อผู้ใช้งาน เกิน 3 ตัวอักษร

ข้อ 5 ต้องไม่ใช้รหัสผ่านซ้ำกับรหัสผ่านที่เคยใช้มาแล้ว

ข้อ 6 ในกรณีมีความจำเป็นต้องใช้ User ที่มีสิทธิพิเศษ (บุคคลภายนอก) ต้องมีการควบคุมการใช้งานอย่างรัดกุม

6.1 ต้องได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่

6.2 มีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

ข้อ 7 Password age อายุหรือความถี่ในการเปลี่ยนรหัสผ่าน

7.1 ผู้ใช้งานทั่วไป ต้องเปลี่ยนรหัสผ่าน ทุกๆ หรือไม่เกิน 90 วัน

7.2 ผู้ใช้งานระดับผู้ใช้งานที่มีสิทธิพิเศษ เช่น ผู้บริการระบบ (system administrator) ต้องเปลี่ยนทุกๆ 60 วัน

7.3 ผู้ใช้งานที่เกี่ยวเนื่องกับ Out Source ต้องมีการเปลี่ยนทุกครั้งหลังใช้งาน

ข้อ 8 ห้ามส่งต่อ รหัสผ่านกับผู้ใช้งานโดยการส่ง E-mail เพื่อป้องการการรั่วไหลและความปลอดภัยในการเข้าใช้งาน

ข้อ 9 ผู้ใช้งานต้องยินยอมให้ทางเจ้าหน้าที่หรือตัวแทนบริษัทเข้าตรวจสอบการพิสูจน์ตัวตนโดยไม่ต้องบอกล่วงหน้า

หมวด 2

ว่าด้วยการบริหารจัดการทรัพย์สิน

(Assets Management)

ข้อ 1 ต้องมีระบบทะเบียนทรัพย์สิน เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์และผู้รับผิดชอบ มีการลงบันทึกรายละเอียด และ ปรับปรุงให้ทันสมัยอยู่เสมอ

1.1 เจ้าหน้าที่ฝ่ายบัญชี ดำเนินการจัดทำบันทึกอุปกรณ์ Computer server ลงในระบบบันทึกทรัพย์สินโปรแกรม D365BC

1.2 ฝ่ายจัดซื้อและโลจิสติกส์ ดำเนินการจัดซื้ออุปกรณ์ Hardware, Software ต่างๆ ที่จำเป็นสำหรับการดำเนินงานของบริษัทฯ

ข้อ 2 ผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใดๆ

ข้อ 3 ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน (เอกสารสำคัญของบริษัท) ก่อนได้รับอนุญาต

ข้อ 4 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่บริษัทมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง การรับ หรือคืนทรัพย์สินและโอรย้ายจะถูกบันทึกและตรวจสอบทุกครั้งโดยฝ่ายทรัพยากรบุคคล

ข้อ 5 ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจาก ความประมาทของผู้ใช้งาน

ข้อ 6 ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม Computer หรือ Notebook ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษร จากผู้มีอำนาจ

ข้อ 7 ทรัพย์สินและระบบสารสนเทศต่างๆ ที่บริษัท จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์ เพื่อการใช้งานของบริษัทเท่านั้น ห้ามมิให้ ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่บริษัทไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อบริษัท

ข้อ 8 ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ 7 ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ข้อ 9 บริษัทมีตารางเวลา รายละเอียดการบำรุงรักษาและการ Maintenance Checklist ของอุปกรณ์สารสนเทศแต่ละชิ้น

การดูแลอุปกรณ์ Hardware ต่างๆ ที่ใช้ในการดำเนินการของบริษัทฯ

(Maintenance and Management of Hardware Equipment Used in Company Operations)

ข้อ 1 เมื่อมีพนักงงานใหม่ พนักงานโอนย้ายตำแหน่ง หรือพนักงานมีการร้องขออุปกรณ์ Hardware เพิ่มเติม เจ้าหน้าที่ IT จะทำการจัดหาอุปกรณ์ตามที่ได้รับการร้องขอผ่านทาง E-mail หรือแจ้งผ่านทางช่องทางต่างๆ โดยทำการตรวจสอบในสต๊อค หรือดำเนินการจัดซื้ออุปกรณ์เพิ่มเติมผ่านทางเจ้าหน้าที่จัดซื้อและโลจิสติกส์

ข้อ 2 เมื่อเจ้าหน้าที่จัดซื้อและโลจิสติกส์ ดำเนินการจัดซื้ออุปกรณ์ และที่เจ้าหน้าที่ IT ทำการตรวจสอบแล้วเสร็จ จะมีการแจ้งไปยังเจ้าหน้าที่ฝ่ายบัญชีเพื่อดำเนินการจัดทำบันทึกอุปกรณ์ Hardware ลงในระบบบันทึกทรัพย์สิน D365BC User จะต้องใช้งานอุปกรณ์ Hardware อย่างระมัดระวังเพื่อไม่ให้เกิดความเสียหายต่อทรัพสินย์ของบริษัท

ข้อ 3 เมื่อพบปัญหาการใช้งาน User ทำการแจ้งปัญหาการใช้งานมายังเจ้าหน้าที่ IT ผ่านทาง E-mail หรือทำการแจ้งผ่านทางช่องทางติดต่อต่างๆ เพื่อดำเนินการแก้ไข

ข้อ 4 ในการดำเนินการซ่อมแซมอุปกรณ์ ดำเนินการโดยเจ้าหน้าที่ IT ในกรณีที่ไม่สามารถซ่อมเองได้ และต้องนำบริษัทภายนอก เข้ามาแก้ไขปัญหา จะต้องทำการแจ้งการประเมินราคา และรายละเอียดข้อตกลงเป็นรายลักษณ์อักษรช่องทางใดทางหนึ่ง เพื่อเป็นข้อมูลในการตัดสินใจการซ่อมอุปกรณ์ และในกรณีที่อุปกรณ์ไม่

สามารถซ่อมเพื่อใช้งานได้ เจ้าหน้าที่ IT ดำเนินการแจ้งลงใบแบบบันทึกการแจ้งปัญหาคอมพิวเตอร์และโปรแกรม และดำเนินการระบุรายละเอียดอุปกรณ์ เพื่อทำการจัดซื้อ

ข้อ 5 เมื่อเจ้าหน้าที่ IT ดำเนินการแก้ไขอุปกรณ์ที่เสียแล้วเสร็จ ให้ดำเนินการแจ้งไปยังผู้ใช้งาน และบันทึกรายละเอียดลงในเอกสารบันทึกการแจ้งปัญหาคอมพิวเตอร์และโปรแกรม

หมวด 3

ว่าด้วยการบริหารจัดการข้อมูลองค์กร

(Corporate Management)

ข้อ 1 ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของบริษัทหรือเป็นข้อมูลของบุคคลภายนอก

ข้อ 2 ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของบริษัทถือเป็นทรัพย์สินของบริษัท ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลงทำซ้ำ ทำลายโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา หรือเห็นชอบจากผู้บิหารหรือหน่วยงานรับผิดชอบข้อมูลนั้นๆ

ข้อ 3 ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของบริษัท หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วยเพียงผู้เดียว

ข้อ 4 ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ 5 ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร บริษัทจะให้การสนับสนุน และเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่บริษัท ต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับบริษัท ซึ่งบริษัทอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ DPO (Data Protection Officer) ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ 6 ผู้ใช้งานมีสิทธิ์ขอเพิ่ม/เปลี่ยนแปลง/ยกเลิก สิทธิ์ต่างๆในระบบข้อมูลโดยให้พนักงานเขียนแบบฟอร์มขอเพิ่ม/เปลี่ยนแปลง/ ยกเลิก (Memo แต่ละฝ่าย) พร้อมชี้แจงเหตุผลผล

หมวด 4

ว่าด้วยการบริหารจัดการระบบสารสนเทศ

(IT Infrastructure Management)

ข้อ 1 ห้ามผู้ใช้งานห้ามเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพ็จบนเครือข่ายคอมพิวเตอร์

ข้อ 2 ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เร้นท (Bittorrent), อีมูล (Emule) และอื่นๆที่ไม่ได้รับอนุญาติ

ข้อ 3 ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัทที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของบริษัท

ข้อ 4 ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัท เพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการ โจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของบริษัท

ข้อ 5 ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของบริษัทเพื่อประโยชน์ทางการค้าส่วนตัว

ข้อ 6 ห้ามกระทำาการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของบริษัท โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

ข้อ 7 ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของบริษัท ต้องหยุดชะงัก

ข้อ 8 ห้ามใช้ระบบสารสนเทศของบริษัท เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ 9 ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ 10 ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของบริษัท โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

หมวด 5

ว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ

(Law and Compliance)

ข้อ 1 บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของบริษัท ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัดและไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวด 6

ว่าด้วยซอฟต์แวร์ลิขสิทธิ์และการทวนสอบซอฟต์แวร์

(Software Licensing intellectual property and Software Validation)

ข้อ 1 บริษัท ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่บริษัทอนุญาตให้ใช้งานหรือที่บริษัท มีลิขสิทธิ์ผู้ใช้งาน สามารถขอใช้งานได้ตามหน้าที่ความจำเป็นและบริษัทห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์บริษัท ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ 2 ซอฟต์แวร์ ที่บริษัทได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

การทวนสอบซอฟต์แวร์ที่ดำเนินการใช้งาน

(Software Validation)

ข้อ 1 ทางฝ่าย IT จัดการสอบทวนซอฟต์แวร์ที่องค์กรใช้งานโดยผู้เชี่ยวชาญของแผนก

ข้อ 2 ความเสี่ยงของซอฟต์แวร์และฟังก์ชันแบ่งเป็น ความเสี่ยงสูงและความเสี่ยงต่ำ โดยเกณฑ์การแบ่งความเสี่ยงของซอฟต์แวร์และฟังก์ชัน จะพิจารณาว่าซอฟต์แวร์และฟังก์ชันมีส่วนเกี่ยวข้องโดยตรงกับคุณภาพของผลิตภัณฑ์ โดยกำหนดเกณฑ์ในการแบ่งดังต่อไปนี้

2.1 ความเสี่ยงสูง เกี่ยวข้องกับคุณภาพของผลิตภัณฑ์โดยตรง

2.2 ความเสี่ยงต่ำ ไม่เกี่ยวข้องกับผลิตภัณฑ์โดยตรง

ข้อ 3 ในกรณีฟังก์ชันในซอฟต์แวร์สามารถแบ่งความเสี่ยงได้ทั้งความเสี่ยงสูงและความเสี่ยงต่ำ ให้ถือว่าฟังก์ชันทั้งหมดในซอฟต์แวร์เป็นความเสี่ยงสูง

ข้อ 4 ซอฟต์แวร์/ฟังก์ชันที่มีความเสี่ยงสูงต้องจัดให้มีการสอบทวนอย่างน้อยปีละ 1 ครั้ง และซอฟต์แวร์/ฟังก์ชันที่มีความเสี่ยงต่ำต้องจัดให้มีการสอบทวนอย่างน้อย 2 ปีละ 1 ครั้ง

หมวด 7

ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี

(Preventing Malware)

ข้อ 1 คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-virus) ตามที่บริษัทได้ประกาศให้ใช้ เว้นแต่ คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษาพัฒนาระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ 2 บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรม ไม่ประสงค์ดีก่อนนำมาให้ใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ 3 ผู้ใช้งานต้องทำการปรับปรุงข้อมูลสำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการ ป้องกันความเสียหายที่อาจเกิดขึ้น (ทางเจ้าหน้าที่ IT เป็นผู้ดำเนินการให้)

ข้อ 4 ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ 5 เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ 6 ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆ ที่เป็นทรัพย์สินของบริษัท หรือของผู้อื่น โดย ไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ 7 ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของบริษัท

หมวด 8

ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์

(Electronic mail)

ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตาม “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550” หมวด 1 มาตรา 11 ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

กฎข้อห้าม

ข้อ 1. ผู้ใช้งานที่ต้องการใช้งาน E-Mail ของหน่วยงานต้องทำการกรอกข้อมูลคำขอเข้าใช้งาน และยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิ์ชื่อผู้ใช้งานรายใหม่และรหัสผ่าน (ฝ่ายทรัพยากรบุคล)

ข้อ 2. ต้องใช้ E-Mail ของหน่วยงานเพื่อติดต่องานของบริษัทเท่านั้น

ข้อ 3. ไม่ควรใช้ E-Mail Address ของผู้อื่นเพื่ออ่านรับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของ E-Mail และให้ถือว่า เจ้าของ E-Mail เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ใน E-Mailของตน

ข้อ 4. ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

ข้อ 5. ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ 6. ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ 7. ห้ามส่ง E-Mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิ์ของบุคคลอื่น

ข้อ 8. ห้ามส่ง E-Mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ 9. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็นExecutable file เช่น .exe .com เป็นต้น

ข้อ 10. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ 11. ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียง ของบริษัท ทำให้เกิดความแตกแยกระหว่างบริษัทผ่านทางจดหมายอิเล็กทรอนิกส์

หมวด 9

ว่าด้วยการควบคุมการใช้บริการงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น

(IT Outsourcing)

ข้อ 1 ต้องมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data Cnfidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) อย่างชัดเจน

ข้อ 2 ต้องให้เจ้าหน้าที่ IT ควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่บริษัทฯ (Onsite Service) และให้เจ้าหน้าที่ IT ตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ Remote Access และปิด VPN Service หรือ Remote Access Service ทันทีที่การให้บริการเสร็จสิ้น

ข้อ 3 ดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

ข้อ 4 ต้องกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไข

ข้อ 5 ต้องมีขั้นตอนในการตรวจรับงานของผู้ให้บริการ จากผู้ มีใช้งานที่เกี่ยวข้อง และมีการรองรับการตรวจรับงานจากผู้มีอำนาจหน้าที่

หมวด 10

ว่าด้วยการพัฒนาระบบเทคโนโลยีสารสนเทศ

(System development)

ข้อ 1 มีแผนในการพัฒนาระบบเทคโนโลยีสารสนเทศ และมีการทบทวนแผนอย่างน้อยปี ละ 1 ครั้ง

ข้อ 2 แผนต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่

ส่วนที่ 2

นโยบายความปลอดภัยของการควบคุมการเข้าถึง

(Access Control Policy)

หมวด 1

ว่าด้วยการควบคุมการเข้าถึงระบบสารสนเทศ

(Data Access Control And Management)

ข้อ 1 กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงาน ภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งาน ระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้มีอำนาจอนุมัติ ผู้บังคับบัญชา

ข้อ 2 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูล ให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ

ข้อ 3 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ 4 ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ มีหลักฐานการขอเข้าถึงระบบสารสนเทศอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงาน ภายในหน่วยงาน เป็นต้น

ข้อ 5 ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (email) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์ เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

ข้อ 6 เพื่อให้การใช้งานในระบบสารสนเทศเกิดความปลอดภัยสูงสุด ต้องจัดให้มีการอบรม อย่างน้อยปีละ 1 ครั้งเพื่อสร้างความรู้ความความเข้าใจกับผู้ใช้งาน และสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) อันจะเกิดจากความรู้เท่าไม่ถึงการณ์หรือความไม่ระมัดระวัง

หมวด 2

การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อมห้องแม่ข่าย

(Server Physical and Environment Security)

ข้อ 1 อาคาร สถานที่และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบ สารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ 2 ให้เจ้าหน้าที่ หรือผู้ดูแลระบบ ซึ่งเป็นผู้ที่ได้รับอนุญาตเท่านั้น เป็นผู้มีสิทธิ์เข้า-ออก และต้องได้รับความเห็นชอบจากผู้บังคับบัญชา เป็นลายลักษณ์อักษร

ข้อ 3 มีระบบกล้องวงจรปิดภายในห้องคอมพิวเตอร์แม่ข่าย และทางเข้าออก และมีการตรวจสอบสภาพให้พร้อมใช้งานเสมอ

ข้อ 4 มีระบบการพิสูจน์ตัวตนและจัดเก็บบันทึกการเข้าออก เช่น ระบบ Access Control เป็นต้น

ข้อ 5 ระบบสำรองไฟและระบบปรับอากาศ จะต้องมีความปลอดภัยและเหมาะสม โดยจัดให้มีระบบสำรองไฟและระบบปรับอากาศสำรอง เพื่อใช้งานเมื่อไฟฟ้าขัดข้องและรักษาอุณหภูมิในห้อง

ข้อ 6 ต้องมีมาตรการป้องกันอัคคีภัย ภายในห้องติดตั้งเครื่อง Server ต้องมีการติดตั้งอุปกรณ์ดับเพลิงสำหรับใช้กรณีฉุกเฉินเมื่อเกิดอัคคีภัย

ข้อ7 การเก็บรักษาสื่อหรืออุปกรณ์เก็บข้อมูลและสำรองข้อมูลจะต้องถูกจัดเก็บไว้อย่างปลอดภัยมีระบบสำรองข้อมูลที่มีประสิทธิภาพ

ข้อ 8 ต้องมีแผนและนโยบายเตรียมรับสถานการณ์ฉุกเฉิน เช่นแผนแก้ไขปัญหาจากความไม่แน่นอนและภัยพิบัติ (Contingency Plan)

หมวด 3

นโยบายความปลอดภัยของการสำรองข้อมูล

(Backup Policy)

ข้อ 1 ต้องมีการสำรองข้อมูลเก็บไว้ ครอบคลุมถึงข้อมูลทั้งบริษัท ทั้งที่เป็นข้อมูลดิบ (Raw Data) และฐานข้อมูล (Data base) โดย แบ่งการสำรองออกเป็นแต่ละหน่วยงานอย่างชัดเจน

ข้อ 2 มีขั้นตอนการจัดทำการสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้อง โดยแยกตามในแต่ละระบบสารสนเทศ และมีการติดตามความ สมบูรณ์ของการสำรองข้อมูลอย่างต่อเนื่อง

ข้อ 3 ต้องมีแผนเตรียมความพร้อมกรณีฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ในเวลาที่เหมาะสม

หมวดที่ 4

ความปลอดภัยของเครือข่ายและคอมพิวเตอร์แม่ข่าย

(Network and Server Policy)

ข้อ 1 กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมคอมพิวเตอร์แม่ข่าย (Server)

ข้อ 2 ห้ามผู้ใช้งาน นำเครื่องคอมพิวเตอร์หรืออุปกรณ์มาเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายของบริษัท เว้นแต่ได้รับอนุญาต จากทางผู้มีอำนาจดูแลระบบ

ข้อ 3 ห้ามผู้ใช้งาน ติดตั้งเพิ่มเติม เคลื่อนย้ายหรือทำการใดๆกับอุปกรณ์ส่วนกลางระบบเครือข่ายของบริษัท เว้นแต่ได้รับอนุญาตจากผู้มีอำนาจดูแลระบบ

ข้อ 4 ผู้ดูแลระบบต้องมีการควบคุมการเข้าถึงระบบเครือข่าย จำกัดสิทธิ์ให้ใช้งานในระบบเครือข่ายที่ได้รับอนุญาตเท่านั้นเพื่อบริหาร จัดการระบบเครือข่ายอย่างมีประสิทธิภาพ

ข้อ 5 การเข้าสู่ระบบเครือข่ายภายในบริษัท โดยผ่าน Internet จำเป็นต้องมีการลงชื่อเข้าใช้ และมีการพิสูจน์ยืนยันตัวตน (Login and Authentication)

ข้อ 6 ต้องจัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดครอบคลุม เครือข่ายภายใน เครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

ข้อ 7 ต้องมีการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ของระบบเครือข่าย (Log) อย่างน้อย 90 วัน

ข้อ 8 ควรตรวจสอบบันทึกของผู้ใช้งานระบบสม่ำเสมอ

ข้อ 9 บุคคลจากภายนอกต้องการใช้งานเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย ต้องทำเรื่องขออนุญาต เป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้มีอำนาจดูแลระบบ

ข้อ 10 มีการควบคุมช่องทาง (Port) ใช้ในการเข้าสู่ระบบอย่างรัดกุม

ข้อ 11 การเข้าสู่ระบบจากระยะไกล ต้องได้รับอนุญาตจากประธานเจ้าหน้าที่บริหารเท่านั้น และต้องมีการควบคุม Port ในการใช้งาน อย่างรัดกุม ยกเว้นผู้ดูแลระบบ (เฉพาะบุคคลภายในบริษัทเท่านั้น)

ข้อ 12 ระบบเครือข่ายของบริษัท ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ นอกบริษัท ต้องเชื่อมต่อผ่านอุปกรณ์ ที่ป้องกันจากการบุกรุกต่างๆ เช่น Firewall , Proxy เท่านั้น

บทลงโทษและการบังคับใช้

ความผิด

ข้อ 1 ผู้ใช้งานที่มีเจตนาฝ่าฝืนนโยบาย เกี่ยวกับความปลอดภัยระบบสารสนเทศของบริษัท แม้ว่าการฝ่าฝืนนั้นจะกระทำไม่บรรลุผลโดยสมบูรณ์ก็ให้ถือว่ามีความผิดโดยสมบูรณ์

การลงโทษ

ข้อ 1 วิธีดำเนินการความผิดเกี่ยวกับนโยบายและข้อบังคับของบริษัท ให้ลงโทษผู้กระทำผิดตามกฎหมายและระเบียบของบริษัท

การบังคับใช้

ข้อ 1 ประธานเจ้าหน้าที่บริหาร ผู้อำนวยการ ผู้จัดการฝ่าย มีหน้าที่ควบคุมผู้ใต้บังคับบัญชา ให้ปฏิบัติตามนโยบายและข้อบังคับอย่างเคร่งครัด หากพบว่าผู้ใต้บังคับบัญชากระทำความผิด ให้ผู้บังคับบัญชารายงานตามลำดับชั้นเพื่อเอาโทษต่อ ผู้กระทำความผิดอย่างเคร่งครัด การละเว้นการปฏิบัติหน้าที่ถือเป็นความผิดเช่นเดียวกับผู้กระทำผิด

ภาคผนวก

ระเบียบปฏิบัติในการเข้าถึงข้อมูลที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

ปัจจุบันระบบสารสนเทศเป็นสิ่งสำคัญที่เข้ามาอำนวยความสะดวก และสนับสนุนการปฏิบัติงานของบริษัท ส่งผลให้การเข้าถึงข้อมูล ข่าวสารมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพสูงขึ้น อย่างไรก็ตาม แม้ว่าระบบ เครือข่ายดังกล่าวจะมีประโยชน์ และอำนวยความสะดวกในการปฏิบัติงาน แต่ในขณะเดียวกันก็มีความเสี่ยงสูงและก่อให้เกิดภัยอันตราย หรือสร้างความเสียหายต่อการปฏิบัติงานของบริษัทได้เช่นกัน เพราะการใช้งานระบบสารสนเทศเปรียบเสมือนการเปิดประตูเพื่อติดต่อกับโลกภายนอก ทำให้มีโอกาสถูกบุกรุกได้มากขึ้น ซึ่งก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้ รวมถึงการขโมยข้อมูลส่วนบุคลหรือความลับทางบริษัท

ดังนั้นผู้ใช้งาน และผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท จำเป็นต้องตระหนักรู้ และให้ความสำคัญในการรักษาความมั่นคงปลอดภัยด้านข้อมูล เพื่อให้ระบบสารสนเทศของบริษัทสามารถดำเนินการหรือให้บริการต่าง ๆ ได้อย่างต่อเนื่อง มีความมั่นคงปลอดภัยและเชื่อถือได้ ทางบริษัทได้จัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฉบับนี้ขึ้น เพื่อให้ ผู้ใช้งาน และผู้ดูแลระบบสารสนเทศในบริษัทรับทราบ เพื่อยึดถือปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนดอย่างเคร่งครัด และให้เป็นไปตามระเบียบปฏิบัติที่เกี่ยวข้องต่อไป

การทบทวน

บริษัทตั้งเป้าหมายในการทบทวนนโยบายระบบสารสนเทศเพื่อให้ทันสมัย และมีความสอดคล้องกับบริษัท โดยกำหนดให้มีการทบทวนทุก ๆ 1-2 ปีหรือหากมีกรณีเร่งด่วนจะนำมาทบทวน ปรับปรุงก่อนครบกำหนดระยะเวลาดังกล่าว โดยผู้มีอำนาจ