ประกาศกรมการค้าภายใน

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมการค้าภายใน

พ.ศ. ๒๕๕๕

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ อธิบดีกรมการค้าภายใน จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมการค้าภายใน เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมการค้าภายใน พ.ศ. ๒๕๕๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“ระบบสารสนเทศ” หมายความว่า ระบบข้อมูลข่าวสารที่นำเอาเทคโนโลยีสารสนเทศและการสื่อสารมาใช้ในการสร้างสารสนเทศของหน่วยงาน

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” หมายความว่า ระบบการสื่อสารที่เป็นการเชื่อมต่อคอมพิวเตอร์ ตั้งแต่ ๒ เครื่องขึ้นไปเข้าด้วยกัน เพื่อสะดวกต่อการร่วมใช้ข้อมูล โปรแกรม หรือเครื่องพิมพ์ และอำนวยความสะดวกในการติดต่อแลกเปลี่ยนข้อมูลระหว่างคอมพิวเตอร์ได้ตลอดเวลา

“ระบบเทคโนโลยีสารสนเทศและการสื่อสาร” หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างระบบสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผนบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร เช่น คอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลสารสนเทศ เป็นต้น

“คอมพิวเตอร์” หมายความว่า คอมพิวเตอร์แบบตั้งโต๊ะ คอมพิวเตอร์แบบพกพา และให้หมายความรวมถึงอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้องด้วย

“ทรัพย์สินสารสนเทศ” หมายความว่า ข้อมูล ระบบข้อมูล และระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) ระบบเทคโนโลยีสารสนเทศ (Information Technology System) เครื่องคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ สารสนเทศ (Information) สื่อบันทึกพกพา

“หน่วยงาน” หมายความว่า กรมการค้าภายใน

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

“ผู้ใช้งาน” หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว ผู้รับจ้างของหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

“ผู้บริหารสูงสุด” หมายถึง อธิบดี กรมการค้าภายใน

“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” หมายถึง รองอธิบดี กรมการค้าภายใน ผู้ควบคุมดูแลและรับผิดชอบด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมการค้าภายใน

ข้อ ๔ การใช้และการบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมการค้าภายใน ให้คำนึงถึงประโยชน์ในการดำเนินงานของกรมการค้าภายในเป็นสำคัญ

ข้อ ๕ การดำเนินการที่เกี่ยวข้องกับการใช้และการบริหารจัดการระบบคอมพิวเตอร์สารสนเทศของกรมการค้าภายใน ที่มิได้กำหนดไว้ในประกาศนี้ ต้องได้รับความเห็นชอบจากอธิบดีกรมการค้าภายใน หรือผู้ที่อธิบดีกรมการค้าภายในมอบหมาย

ข้อ ๖ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๖.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

หน่วยงานมีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานเทคโนโลยีสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

๖.๒ มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

หน่วยงานมีนโยบายในการบริหารจัดการเทคโนโลยีสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บระบบเทคโนโลยีสารสนเทศและการสื่อสารเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งาน เพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

๖.๓ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

หน่วยงานมีนโยบายให้มีการตรวจสอบ ประเมินความเสี่ยง และกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละหนึ่งครั้ง

๖.๔ การสร้างความรู้ความเข้าใจในการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร

หน่วยงานมีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ ๗ กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ดังต่อไปนี้

๗.๑ จัดทำแนวปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

๗.๒ ประกาศนโยบายและแนวปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจและสามารถปฏิบัติได้

๗.๓ กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

๗.๔ ทบทวนปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ข้อ ๘ ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ดังต่อไปนี้

๘.๑ มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๘.๒ ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบาย ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือหน้าที่ หรือการมอบอำนาจของหน่วยงาน

๘.๓ ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๙ ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยมีการจัดทำแนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศและการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๑๐ ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศของผู้ใช้งาน ที่ผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักในเรื่องของความมั่นคงปลอดภัยด้านสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังต่อไปนี้

๑๐.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๑๐.๒ การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๑๐.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

๑๐.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๑๐.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๑๑ กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศหรือการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ดังต่อไปนี้

๑๑.๑ การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๑๑.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๑๑.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๑๑.๔ อาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๑๒ ให้ควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ดังต่อไปนี้

๑๒.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๑๒.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๑๒.๓ การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๑๒.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๑๒.๕ การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๑๒.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

๑๒.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๓ ให้ควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ดังต่อไปนี้

๑๓.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๑๓.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๑๓.๓ การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๑๓.๔ การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๑๓.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

๑๓.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๔ ให้ควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นหรือระบบสารสนเทศ (information access restriction) ดังต่อไปนี้

๑๔.๑ การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๑๔.๒ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๑๔.๓ การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๑๕ ให้มีการจัดทำระบบสำรอง ดังต่อไปนี้

๑๕.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

๑๕.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๑๕.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๑๕.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

๑๕.๕ ความถี่ของการปฏิบัติในแต่ละข้อ ต้องมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้

ข้อ ๑๖ ให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังต่อไปนี้

๑๖.๑ ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละหนึ่งครั้ง

๑๖.๒ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑๗ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ประกาศ ณ วันที่ ๔ กันยายน พ.ศ. ๒๕๕๕

(นางวัชรี วิมุกตายน)
อธิบดีกรมการค้าภายใน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมการค้าภายใน

ปัจจุบันระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ (Computer Network) เป็นสิ่งสำคัญสำหรับหน่วยงานที่เข้ามาช่วยอำนวยความสะดวกในการปฏิบัติงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็วการติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่างๆ ของหน่วยงานที่เชื่อมต่อระบบอินเทอร์เน็ต ทั้งนี้ระบบเครือข่ายดังกล่าว แม้จะมีประโยชน์และอำนวยความสะดวกก็ตามแต่ในขณะเดียวกันก็มีความเสี่ยงสูง และอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติงาน ได้เช่นกัน เพราะการใช้งานระบบเครือข่ายคอมพิวเตอร์เปรียบเสมือนการเปิดประตูเพื่อติดต่อกับโลกภายนอก ทำให้มีโอกาสถูกบุกรุกได้มากขึ้น ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมไม่พึงประสงค์ หรือการโจมตีทางระบบเครือข่ายเพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศ และทำให้สูญเสียชื่อเสียงหรือภาพพจน์ของหน่วยงาน ดังนั้นผู้ใช้งานและผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความจำเป็นต้องตระหนักถึงการให้การดูแลบำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง

กรมการค้าภายใน ได้ดำเนินการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการค้าภายในขึ้น เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยเป็นที่ยอมรับและเชื่อมั่นในข้อมูลด้านสารสนเทศและเป็นไปตามบทบัญญัติกฎหมาย กฎระเบียบที่เกี่ยวข้อง

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นภารกิจที่ต้องได้รับความร่วมมือจากทุกหน่วยและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว โดยนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องยึดถือในการปฏิบัติงานของกรมการค้าภายในให้เกิดประสิทธิภาพสูงสุดต่อไป

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมการค้าภายใน

๑. หลักการและเหตุผล

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัย และเชื่อถือได้ กรมการค้าภายใน จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของกรมการค้าภายในขึ้น เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งเป็นเครื่องมือที่สำคัญในการปฏิบัติงานและการบริหารราชการ

๒. วัตถุประสงค์

๒.๑ เพื่อให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการค้าภายในเป็นไปตามกฎหมาย กฎ ระเบียบที่เกี่ยวข้อง

๒.๒ เพื่อกำหนดแนวทางและวิธีการปฏิบัติให้บุคลากรและผู้ใช้งานที่ปฏิบัติงานให้กับหน่วยงาน รวมทั้งการยืนยันตัวบุคคล การเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศ

๒.๓ เพื่อให้มีการสำรองข้อมูลสารสนเทศ อย่างสม่ำเสมอ เพื่อรักษาความถูกต้องสมบูรณ์ความพร้อมใช้อยู่เสมอของระบบสารสนเทศและการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน ให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

๒.๔ เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศอย่างสม่ำเสมอ

๒.๕ เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ ความเข้าใจและการให้การอบรมทางด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้แก่บุคลากรและผู้ใช้งานที่เกี่ยวข้อง

๓. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการค้าภายใน

กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการค้าภายในเพื่อเป็นแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยแบ่งแนวปฏิบัติออกเป็นส่วนๆ ดังต่อไปนี้

ส่วนที่ ๑ คำนิยาม

ส่วนที่ ๒ นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร

ส่วนที่ ๓ นโยบายการใช้งานคอมพิวเตอร์และเครือข่ายสำหรับผู้ใช้งาน ผู้ดูแลระบบและผู้พัฒนาระบบ

ส่วนที่ ๔ นโยบายการจัดการคอมพิวเตอร์และเครือข่ายสำหรับเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ

ส่วนที่ ๕ นโยบายการจัดการด้านบุคลากรสำหรับศูนย์เทคโนโลยีสารสนเทศ

ส่วนที่ ๖ นโยบายการเผยแพร่ข้อมูลสู่สาธารณะสำหรับผู้เป็นเจ้าของหรือรับผิดชอบต่อข้อมูลที่ต้องทำการเผยแพร่สู่สาธารณะ

ส่วนที่ ๑
คำนิยาม

คำนิยามที่ใช้ในประกาศประกอบด้วย

“หน่วยงาน” หมายถึง กรมการค้าภายใน

“ผู้บริหารสูงสุด” หมายถึง อธิบดี กรมการค้าภายใน

“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)” หมายถึง รองอธิบดี กรมการค้าภายใน ผู้ควบคุมดูแลและรับผิดชอบด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมการค้าภายใน

“ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของหน่วยงาน หรือผู้ที่ได้รับมอบหมายให้มีอำนาจสั่งการ

“การรักษาความมั่นคงปลอดภัย” หมายถึง การรักษาความมั่นคงปลอดภัย สำหรับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมการค้าภายใน

“ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)” หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน (Integrity) และสภาพความพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

“มาตรฐาน” หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

“ขั้นตอนปฏิบัติ” หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

“แนวทางปฏิบัติ” หมายถึง แนวทางที่ควรปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายได้ง่ายขึ้น

“ข้อปฏิบัติ” หมายถึง การปฏิบัติเพื่อให้บรรลุวัตถุประสงค์ของนโยบาย

“ระบบเทคโนโลยีสารสนเทศ (Information Technology System)” หมายถึง ระบบงานของกรมการค้าภายในที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่กรมการค้าภายใน สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

“ผู้ใช้งาน” หมายถึง บุคคลที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศของกรมการค้าภายใน ดังนี้

- ข้าราชการ เจ้าหน้าที่ราชการ ลูกจ้างประจำ ลูกจ้างตามสัญญาจ้างในสังกัดหน่วยงาน
- บุคคลที่กรมการค้าภายใน อนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศของกรมการค้าภายในได้ชั่วคราว เพื่อประโยชน์ในการดำเนินงานของกรมการค้าภายใน เช่น เจ้าหน้าที่หรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับกรมการค้าภายใน หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง หรือนิสิตนักศึกษาฝึกงาน

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของกรมการค้าภายในที่กำหนดโดยผู้ดูแลระบบ

“เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ” หมายถึง บุคลากรของศูนย์เทคโนโลยีสารสนเทศที่ได้รับมอบหมายให้สามารถเข้าใช้งานดูแลระบบเทคโนโลยีสารสนเทศของกรมการค้าภายใน ดังนี้

- **“ผู้ดูแลระบบ (System Administrator)”** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์
- **“ผู้พัฒนาระบบ (System Developer)”** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่ในการพัฒนาและดูแลรักษาระบบงานสารสนเทศของหน่วยงาน

“หน่วยงานภายนอก” หมายถึง ส่วนราชการ องค์การ หรือหน่วยงานอื่นที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบสารสนเทศตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

“ผู้ให้บริการภายนอก (External service provider)” หมายถึง หน่วยงานภายนอกที่รับจ้างปฏิบัติงานด้านเทคโนโลยีสารสนเทศตามความต้องการของกรมการค้าภายใน

“ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

“ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Log)” หมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสาร ของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ข้อมูลล็อก (Event Log)” หมายถึง ข้อมูลที่เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่บันทึกไว้ซึ่งแสดงถึงเหตุการณ์หรือกิจกรรมต่าง ๆ ที่เกิดขึ้น โดยทั่วไปข้อมูลที่บันทึกไว้นี้จะมีหรือแสดงวันเวลาที่เหตุการณ์หรือกิจกรรมหนึ่งเกิดขึ้นด้วย เพื่อใช้ในการวิเคราะห์ว่าเหตุการณ์หรือกิจกรรมนั้นเกิดขึ้นเมื่อไร

“สารสนเทศ (Information)” หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิกให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย แบะสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

“ระบบคอมพิวเตอร์ (Computer System)” หมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย (Network System)” หมายถึง ระบบที่ใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของกรมการค้าภายใน เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

“ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet)” หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานของกรมการค้าภายใน เข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

“ระบบอินเทอร์เน็ต (Internet)” หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของกรมการค้าภายในเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

“ห้อง Data Center” หมายถึง ห้องที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายหรือคอมพิวเตอร์หลักและอุปกรณ์เครือข่ายหลักที่ใช้งานในหน่วยงาน

“สินทรัพย์” หมายถึง ทรัพย์สินด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมการค้าภายใน เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีค่าลิขสิทธิ์ เป็นต้น

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตที่ว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจจะทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

“กระบวนการทางธุรกิจ (Business Process)” หมายถึง งานตามภารกิจของกรมการค้าภายใน ซึ่งประกอบด้วยกิจกรรมต่าง ๆ ที่เกี่ยวข้องที่ต้องดำเนินการจนกระทั่งแล้วเสร็จ ปกติกระบวนการ ๆ หนึ่ง จะมีปัจจัยนำเข้า (input) ที่ใช้ในกระบวนการ และมีผลลัพธ์ (output) ของกระบวนการนั้นเกิดขึ้น

“กระบวนการทางธุรกิจสำคัญ (Critical Business Process)” หมายถึง งานตามภารกิจสำคัญของกรมการค้าภายใน ซึ่งหากงานเหล่านี้เกิดการหยุดชะงักหรือไม่สามารถปฏิบัติต่อไปได้ จะก่อให้เกิดความเสียหายต่อหน่วยงานเป็นอย่างมาก เช่น ความเสียหายด้านการเงิน ด้านชื่อเสียงภาพลักษณ์ ด้านความเชื่อมั่นของลูกค้า ประชาชน หรือผู้ใช้บริการ ด้านการละเมิดกฎหมาย เป็นต้น

“จดหมายอิเล็กทรอนิกส์ (E-mail)” หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อความที่ส่งจะเป็นได้ทั้งตัวอักษร ตัวเลข ภาพ เสียง ภาพกราฟฟิก ภาพเคลื่อนไหว หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ ที่ผู้ส่งสามารถส่งข้อความไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ ในการรับส่งข้อความชนิดนี้ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น

“รหัสผ่าน (Password)” หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

“โปรแกรมไม่พึงประสงค์” หมายถึง โปรแกรมคอมพิวเตอร์ ชุดคำสั่ง และหรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหาย ไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิ่ง (Phishing) หรือจดหมายขยะ (Spam mail) เป็นต้น

“ข้อมูลที่เกี่ยวข้องกับภารกิจของหน่วยงาน” หมายถึง ข้อมูลที่กรมการค้าภายใน เป็นผู้สร้าง เปลี่ยนแปลง หรือ แก้ไขตามภารกิจหรือหน้าที่ความรับผิดชอบของหน่วยงานนั้น ข้อมูลที่ได้รับจากหน่วยงานภายนอก ไม่ถือว่ากรมการค้าภายในเป็นเจ้าของ เป็นแต่เพียงผู้ใช้งานข้อมูลเท่านั้น

“เจ้าของข้อมูล” หมายถึง เจ้าหน้าที่ของกรมการค้าภายใน ซึ่งได้รับมอบหมายให้เป็นผู้รับผิดชอบและสามารถสร้าง เปลี่ยนแปลง หรือแก้ไขข้อมูลที่เกี่ยวกับภารกิจของหน่วยงานนั้น รวมทั้งการให้

สิทธิในการเข้าถึงข้อมูลนั้นแก่ผู้อื่น

“ชั้นความลับของข้อมูล” หมายถึง การจำแนกข้อมูลสำคัญของกรมการค้าภายใน ออกเป็นแต่ละระดับ เพื่อให้มีการจัดการกับข้อมูลเหล่านั้นอย่างมั่นคงปลอดภัยเพียงพอ ดังนี้

- **“ข้อมูลลับ”** หมายถึง เอกสาร/ข้อมูลต่าง ๆ รวมทั้งข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่าง ๆ ซึ่งจำกัดการเข้าถึงโดยผู้ที่เกี่ยวข้องเท่านั้น ห้ามไม่ให้เปิดเผยกับผู้อื่น การเปิดเผยโดยไม่ได้รับอนุญาตอาจทำให้เกิดความเสียหายอย่างร้ายแรงได้ กำหนดชั้นความลับเป็น ๓ ชั้น คือ ลับที่สุด (Top secret) ลับมาก (Secret) และลับ (Confidential)
- **“ข้อมูลใช้ภายในเท่านั้น”** (Internal Data) หมายถึง เอกสาร/ข้อมูลต่าง ๆ รวมทั้งข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่าง ๆ ซึ่งทางกรมการค้าภายในสร้างขึ้นมาเพื่อใช้งานในกรมการค้าภายในเท่านั้น ห้ามไม่ให้เปิดเผยกับบุคคลภายนอกโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลในกรณีต้องส่งมอบให้กับกระทรวงหรือหน่วยงานของรัฐอื่น ซึ่งมีอำนาจในการกำกับดูแลกรมการค้าภายใน
- **“ข้อมูลส่วนบุคคล”** (Personal Data) หมายถึง เอกสาร/ข้อมูลต่าง ๆ รวมทั้งข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่าง ๆ ซึ่งทางกรมการค้าภายในสร้างขึ้นมาเอง หรือได้รับจากภายนอก โดยที่ข้อมูลเหล่านี้สามารถบ่งชี้ตัวบุคคลผู้เป็นเจ้าของข้อมูลได้ เช่น ข้อมูลการศึกษา ฐานะการเงิน ประวัติสุขภาพ หรือ ประวัติการทำงาน ข้อมูลที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัส หรือสิ่งที่สามารถบ่งบอกลักษณะอื่น ๆ ที่ทำให้รู้ตัวผู้นั้นได้ ข้อมูลส่วนบุคคลในเอกสารนี้จะหมายถึงเฉพาะข้อมูลของประชาชน ผู้ใช้บริการต่าง ๆ ของกรมการค้าภายในซึ่งถูกสร้างขึ้นมาเพื่อใช้งานตามภารกิจของกรมการค้าภายใน
- **“ข้อมูลที่เปิดเผยได้”** (Public Data) หมายถึง เอกสาร/ข้อมูลต่าง ๆ รวมทั้งข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่าง ๆ ซึ่งทางกรมการค้าภายในสร้างขึ้นมาเอง หรือได้รับจากภายนอก และมีจุดประสงค์เพื่อให้สามารถเผยแพร่ข้อมูลได้ในวงกว้าง เช่น เผยแพร่ให้ประชาชน หรือผู้ใช้บริการได้รับทราบ

“สื่อบันทึกข้อมูล” หมายถึง กระดาษ เทป Harddisk, Flash Drive และแผ่น CD/DVD หรือสื่อชนิดอื่น ๆ ที่ใช้ในการบันทึกข้อมูล

“คณะกรรมการทำลายข้อมูล” หมายถึง กลุ่มเจ้าหน้าที่ของกรมการค้าภายใน ที่ได้รับแต่งตั้งเพื่อทำหน้าที่ทำลายข้อมูลที่สิ้นสุดหรือหมดอายุการจัดเก็บ ข้อมูลที่ต้องการทำลายสามารถอยู่บนสื่อบันทึกข้อมูลได้ในหลากหลายรูปแบบ

“การเข้ารหัสข้อมูล” หมายถึง การใช้ซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ซึ่งมีความสามารถในการซ่อนข้อมูลสำคัญจากการมองเห็น หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต โดยใช้วิธีการแปลงข้อมูลเดิมไปสู่ข้อมูลอีกรูปแบบหนึ่ง ที่ไม่สามารถอ่านทำความเข้าใจได้ (แม้ว่าจะสามารถเข้าถึงได้ก็ตาม)

“ช่องโหว่ (Software/Hardware vulnerabilites)” หมายถึง จุดอ่อนที่พบในซอฟต์แวร์หรือฮาร์ดแวร์ ที่กรมการค้าภายในใช้งาน (ซอฟต์แวร์หรือฮาร์ดแวร์นั้น ถูกพัฒนาหรือจัดทำโดยผู้ผลิตซอฟต์แวร์หรือฮาร์ดแวร์) จุดอ่อนที่พบอาจทำให้ซอฟต์แวร์หรือฮาร์ดแวร์ทำงานผิดพลาดในลักษณะต่าง ๆ ซึ่งรวมถึงความผิดพลาดในตัวข้อมูลด้วย

“โปรแกรมแก้ไขช่องโหว่ (Patch for Software/Hardware vulnerabilities)” หมายถึง โปรแกรมสำหรับแก้ไขที่ผู้ผลิตซอฟต์แวร์หรือฮาร์ดแวร์จัดทำขึ้นมาเพื่อแก้ไขปัญหาช่องโหว่ ที่ผู้ใช้งานค้นพบและรายงานเข้ามาให้ผู้ผลิตได้รับทราบ

“ซอร์สโค้ด (Source code)” หมายถึง ชุดคำสั่งที่สามารถสั่งการให้เครื่องคอมพิวเตอร์ทำงานตามที่ต้องการได้ ชุดคำสั่งนี้จะถูกแปลงโดยโปรแกรมแปลงภาษา เช่น Compliler, Interpreter หรือ Assembler ไปเป็นโค้ดที่เครื่องคอมพิวเตอร์ สามารถตีความและสั่งการให้เครื่องทำงานตามที่ตีความ

“เอกสารลับ” หมายถึง ข้อมูลลับที่อยู่ในรูปของเอกสาร

“ไฟล์ข้อมูลลับอิเล็กทรอนิกส์ (ไฟล์ข้อมูลลับ)” หมายถึง ไฟล์ที่ถูกสร้างจากเครื่องคอมพิวเตอร์และมีข้อมูลลับอยู่ในไฟล์ เช่น ไฟล์.doc ของ Microsoft Office เป็นต้น

“ทะเบียนข้อมูลลับ” หมายถึง เอกสารแสดงรายการของข้อมูลลับของหน่วยงานภายในว่าประกอบไปด้วยข้อมูลลับอะไรบ้าง ใครเป็นเจ้าของข้อมูล หน่วยงานใดบ้างที่อนุญาตให้เข้าถึง สถานที่ใดที่ใช้ในการจัดเก็บข้อมูล เป็นต้น

“เจ้าของข้อมูลลับ” หมายถึง เจ้าหน้าที่ของกรมการค้าภายในที่ทำหน้าที่เป็นผู้สร้างข้อมูลลับขึ้นมา เป็นผู้ที่สามารถเปลี่ยงแปลงหรือแก้ไขข้อมูลได้ สามารถกำหนดสิทธิการเข้าถึงข้อมูลลับ คือการกำหนดว่าจะอนุญาตให้ใครบ้างที่สามารถเข้าถึงข้อมูลนี้ได้

“ข้อมูลชั่วคราว” หมายถึง ข้อมูลที่เกี่ยวข้องกับภารกิจของหน่วยงานซึ่งอยู่บนสื่อบันทึกข้อมูล แต่ไม่ได้เป็นข้อมูลสำเนาชุดสุดท้ายที่เจ้าของข้อมูลมีอยู่ ข้อมูลดังกล่าวถือเป็น “ข้อมูลชั่วคราว” ที่เจ้าของข้อมูลสามารถทำลายได้

“พอร์ต (Ports)” หมายถึง บริการต่าง ๆ บนเครื่องเซิร์ฟเวอร์ให้บริการ โดยทั่วไปบริการเหล่านี้จะได้รับการบริการหมายเลขเป็นหมายเลขมาตรฐาน เช่น พอร์ต ๘๐ หมายถึงบริการเว็บซึ่งบริการข้อมูลต่าง ๆ บนเว็บหนึ่ง หรือพอร์ต ๒๕ หมายถึงบริการรับส่งอีเมล์บนอินเทอร์เน็ต เป็นต้น

“ซอฟต์แวร์ยูทิลิตี้ (Utility Software)” หมายถึง ซอฟต์แวร์ที่มีการติดตั้งเพิ่มเติมลงไปในเครื่องคอมพิวเตอร์เพื่อประโยชน์การใช้งานในลักษณะใดลักษณะหนึ่ง

“สภาพความพร้อมใช้ของระบบ (IT system availability)” หมายถึง ความสามารถของระบบที่จะให้บริการตามหน้าที่ของตัวเองหรือตามที่ได้ถูกพัฒนาได้อย่างต่อเนื่องมากที่สุด หรือมีช่วงระยะเวลาที่ไม่สามารถให้บริการได้น้อยที่สุด

“ร้อยละของสภาพความพร้อมใช้ของระบบ (Percent IT system availability)” หมายถึง ภายในช่วงระยะเวลาหนึ่งที่ได้กำหนดไว้ ระบบงานหนึ่งสามารถให้บริการได้อย่างต่อเนื่อง คิดรวมเป็นระยะเวลาทั้งหมดเท่าไร เช่น กำหนดช่วงไว้ ๑ ปี ระบบงานสามารถให้บริการรวมทั้งหมดได้กี่ชั่วโมงภายใน ๑ ปี เมื่อคำนวณเป็นร้อยละหรือสัดส่วน วิธีการคำนวณคือ (ระยะเวลาที่ระบบงานสามารถให้บริการได้ภายใน ๑ ปี/ระยะเวลา ๑ ปี) × ๑๐๐

“ระยะเวลาการหยุดชะงักโดยเฉลี่ยต่อครั้ง (Mean time to repair - MTTR)” หมายถึง ค่าเฉลี่ยของระยะเวลาที่ระบบงานหนึ่งเกิดการหยุดชะงักต่อหนึ่งครั้ง ค่าเฉลี่ยนี้เกิดจากการนำระยะเวลารวมทั้งหมดที่ระบบเกิดการหยุดชะงักหารด้วยจำนวนครั้งที่เกิดการหยุดชะงัก

“การประเมินผลกระทบทางธุรกิจ (Business Import Analysis - BIA)” หมายถึง การประเมินผลในเชิงลบที่เกิดขึ้นกับธุรกิจ หากระบบงานหนึ่งซึ่งสนับสนุนกระบวนการทางธุรกิจเกิดการหยุดชะงักหรือไม่สามารถให้บริการได้ เช่น ผลในเชิงลบด้านมูลค่าความเสียหายทางธุรกิจ การให้บริการลูกค้า สัญญาจ้าง กฎหมาย ระเบียบ ข้อบังคับอื่น ๆ ที่หน่วยงานต้องปฏิบัติตาม

“RTO (Recovery Time Objective)” หมายถึง ระยะที่จะใช้ในการกู้คืนระบบงานที่มีการหยุดชะงัก เพื่อให้ระบบกลับคืนมาทำให้หน่วยงานสามารถดำเนินงานหรือให้บริการต่อไปได้

“MTD (Maximum Tolerable Downtime)” หมายถึง ระยะเวลานานที่สุดที่หน่วยงานยอมให้การดำเนินงานหยุดชะงักได้

“RPO (Recovery Point Objective)” หมายถึง ระยะเวลาที่ให้ข้อมูลสูญหายได้นานที่สุดโดยไม่ส่งผลเสียหายต่อการดำเนินงาน หรือทำให้การปฏิบัติงานขาดความความต่อเนื่อง

ส่วนที่ ๒
นโยบายการบริหารจัดการความมั่นคงปลอดภัย
สำหรับผู้บริหาร

วัตถุประสงค์

- เพื่อให้มีการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศของหน่วยงาน เพื่อให้สอดคล้องมาตรฐานสากล ISO/IEC ๒๗๐๐๑

ผู้รับผิดชอบ

- ผู้บริหารสูงสุด และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

อ้างอิงมาตรฐาน

- หมวดที่ ๑ นโยบายความมั่นคงปลอดภัย
- หมวดที่ ๒ โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร
- หมวดที่ ๓ การบริหารจัดการสินทรัพย์ขององค์กร
- หมวดที่ ๔ ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร
- หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร
- หมวดที่ ๗ การควบคุมการเข้าถึง
- หมวดที่ ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ
- หมวดที่ ๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร
- หมวดที่ ๑๐ การบริหารความต่อเนื่องในการดำเนินงานขององค์กร
- หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

ข้อปฏิบัติ

๑) จัดการให้มีการทำและทบทวนหรือปรับปรุงนโยบายความมั่นคงปลอดภัยและนโยบายสนับสนุนต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง โดยมีขั้นตอนปฏิบัติสำหรับการทบทวนและปรับปรุงนโยบายความมั่นคงปลอดภัย ดังนี้

๑.๑) ศึกษาผลของการประเมินความเสี่ยงหรือผลการตรวจสอบในรอบปีที่ผ่านมาเพื่อกำหนดนโยบายเชิงป้องกันเพิ่มเติม

๑.๒) ศึกษาจากแหล่งข้อมูลอ้างอิงต่าง ๆ ในการจัดทำนโยบาย

๑.๓) กำหนดหัวข้อนโยบายเชิงป้องกันเพิ่มเติมเพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้น

๑.๔) ดำเนินการเพื่อสร้างความตระหนักหรือเพื่อให้เกิดการเรียนรู้ ในหัวข้อนโยบายใหม่ที่กำหนดขึ้นมา

๑.๕) จัดหาซอฟต์แวร์ตามความจำเป็นเพื่อใช้ในการตรวจสอบความสอดคล้องในการปฏิบัติตามนโยบายนั้น

๑.๖) นำนโยบายที่ทบทวนหรือปรับปรุงเสนอคณะทำงานเทคโนโลยีสารสนเทศเพื่อขอคำแนะนำในการปรับปรุง และขอความเห็นชอบเพื่อประกาศใช้งานต่อไป

๑.๗) นำเสนอผู้บริหารลงนามและประกาศใช้

๒) มีการทำหนังสือเวียนปีละ ๑ ครั้ง เพื่อแจ้งให้เจ้าหน้าที่ทั้งหมดของหน่วยงานได้รับทราบเกี่ยวกับประเภทของเหตุการณ์ด้านความมั่นคงปลอดภัยที่ต้องทำการรายงาน และข้อมูลที่ต้องทำการรายงาน รวมทั้งให้ปรับปรุงข้อมูลการรายงานดังกล่าวตามความจำเป็น ประเภทของเหตุการณ์ที่ต้องรายงาน ได้แก่

๒.๑) การกระทำที่ขัดต่อ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๒.๒) การกระทำที่ขัดต่อความมั่นคงของชาติ

๒.๓) การใช้ทรัพยากรสารสนเทศของหน่วยงานผิดวัตถุประสงค์

๒.๔) หน้าเว็บไซต์หลักถูกเปลี่ยนแปลง

๒.๕) ข้อมูลในหน้าเว็บไซต์หลักไม่ถูกต้อง หรือคลาดเคลื่อนจากความเป็นจริง

๒.๖) ข้อมูลสำคัญถูกเปลี่ยนแปลง ถูกลบ หรือสูญหาย

๒.๗) การเปิดเผยข้อมูลสำคัญ หรือข้อมูลส่วนบบุคคลโดยไม่ได้รับอนุญาต

๒.๘) การนำข้อมูลสำคัญไปใช้ผิดวัตถุประสงค์

๒.๙) ทรัพยากรสารสนเทศถูกขโมย

๒.๑๐) การอนุญาตให้บุคคลภายนอกเข้าใช้ระบบของหน่วยงาน

๒.๑๑) การแอบติดตั้งอุปกรณ์ หรือโปรแกรมเพื่อดักขโมยข้อมูล หรือดักดูข้อมูลในเครือข่าย

๒.๑๒) การใช้อำนาจของสิทธิการเป็นผู้ดูแลระบบอย่างไม่เหมาะสม

๒.๑๓) การบุกรุกห้อง Data Center

๒.๑๔) โปรแกรมไม่พึงประสงค์

๒.๑๕) เหตุการณ์อื่น ๆ ที่เป็นการละเมิดนโยบายด้านความมั่นคงปลอดภัย

๓) มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่พอเพียงต่อการบริหารจัดการด้านความมั่นคงปลอดภัยในแต่ละปีงบประมาณ ซึ่งรวมถึงแผนความมั่นคงปลอดภัยสารสนเทศที่จะดำเนินการในปีงบประมาณนั้นด้วย

๔) มีการประเมินความรู้ ความสามารถ หรือทักษะที่ต้องการเพิ่มเติม เป็นระยะ ๆ สำหรับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ เพื่อใช้ในการวางแผนการอบรมเพิ่มพูนความรู้ความสามารถของเจ้าหน้าที่ต่อไป

๕) มีการอบรมเจ้าหน้าที่เพื่อสร้างความตระหนักที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๖) มีการเก็บข้อมูลการฝึกอบรมของเจ้าหน้าที่สารสนเทศ รวมทั้งการสร้างความตระหนักที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศ

๗) มีการตรวจสอบแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมการค้าภายในโดยผู้ตรวจสอบภายใน ปีละ ๑ ครั้ง และจัดการให้มีการทำแผนเพื่อปรับปรุงหรือแก้ไขปัญหาที่พบ

๘) มีการซ้อมแผนกู้คืนระบบอย่างน้อยปีละ ๑ ครั้ง และปรับปรุงแผนฯ ตามความเหมาะสม รวมทั้งการทำแผนเพื่อปรับปรุงหรือแก้ไขปัญหาที่พบ

๙) กำหนดเจ้าหน้าที่ดำเนินงานด้านความมั่นคงปลอดภัยสำหรับสารสนเทศและกำหนดหน้าที่ความรับผิดชอบ รวมทั้งปรับปรุงโครงสร้างดังกล่าวตามความจำเป็น

๑๐) มีการทำแผนความมั่นคงปลอดภัย โดยให้พิจารณาจากปัจจัยนำเข้าดังต่อไปนี้

๑๐.๑) การปรับปรุงนโยบายความมั่นคงปลอดภัยสำหรับปีถัดไป

๑๐.๒) ผลการประเมินความเสี่ยงและแผนลดความเสี่ยง

๑๐.๓) ผลการแจ้งเตือนโดยระบบป้องกันการบุกรุกในปีที่ผ่านมา

๑๐.๔) ผลของการตรวจสอบและแก้ไขช่องโหว่สำหรับระบบต่าง ๆ ในปีที่ผ่านมา

๑๐.๕) ผลการทบทวนการบริหารจัดการด้านความมั่นคงปลอดภัยโดยผู้บริหาร

๑๐.๖) การจัดทำและต่อสัญญาบำรุงรักษาระบบและอุปกรณ์ต่าง ๆ

๑๐.๗) แผนการอบรมทางด้านความมั่นคงปลอดภัยประจำปีซึ่งรวมถึงการสร้างความตระหนัก

๑๐.๘) ผลการทดสอบแผนกู้คืนในปีที่ผ่านมา

๑๐.๙) ข้อมูลภัยคุกคามต่าง ๆ ที่ได้รับจากหน่วยงานภายนอก

๑๐.๑๐) การปรับปรุงสัญญาการให้บริการโดยหน่วยงานภายนอก

๑๐.๑๑) ข้อมูลกฎหมาย ระเบียบ ข้อบังคับต่าง ๆ ที่ต้องปฏิบัติตาม

๑๐.๑๒) ผลการตรวจสอบการแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมการค้าภายใน โดยผู้ตรวจสอบภายใน

๑๑) แสดงเจตนารมณ์หรือสื่อสารอย่างสม่ำเสมอเพื่อให้เจ้าหน้าที่ทั้งหมดได้เห็นถึงความสำคัญของการปฏิบัติตามนโยบายความมั่นคงปลอดภัยและนโยบายสนับสนุนต่าง ๆ โดยเคร่งครัด

๑๒) กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ **ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง** ต้องเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ส่วนที่ ๓
นโยบายการใช้งานคอมพิวเตอร์และเครือข่าย
สำหรับผู้ใช้งาน ผู้ดูแลระบบและผู้พัฒนาระบบ

ผู้ใช้งาน ผู้ดูแลระบบและผู้พัฒนาระบบมีหน้าที่ความรับผิดชอบต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงาน ดังนี้

- ประพฤติและปฏิบัติตามนโยบายความมั่นคงปลอดภัยโดยเคร่งครัด
- ปฏิบัติตามกิจกรรมหรือกระบวนการด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้
- ไม่เข้าถึง เปิดเผย เปลี่ยงแปลง แก้ไข ทำลาย หรือทำให้เสียหายต่อสินทรัพย์สารสนเทศของหน่วยงานโดยไม่ได้รับอนุญาต
- ไม่รบกวนหรือแทรกแซงการสื่อสารของผู้อื่นจนทำให้ไม่สามารถดำเนินต่อไปได้
- ปฏิบัติงานตามหน้าที่ความรับผิดชอบของตนเองที่ได้กำหนดไว้
- รายงานเหตุการณ์ความเสี่ยง จุดอ่อน หรือเหตุการณ์ความมั่นคงปลอดภัยที่พบไปยังหน่วยรับแจ้ง
- ในกรณีที่มีการละเลยต่อหน้าที่หรือนโยบายที่ได้กำหนดไว้ จะมีการสอบสวนและดำเนินการทั้งทางวินัยและกฎหมายตามความเหมาะสม

นโยบายการใช้งานคอมพิวเตอร์และเครือข่ายประกอบด้วย

๑. นโยบายการป้องกันสินทรัพย์ของหน่วยงาน

วัตถุประสงค์

- เพื่อป้องกันสินทรัพย์ของหน่วยงานจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต สูญหาย เสียหาย หรือถูกขโมย

ผู้รับผิดชอบ

- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- หมวดที่ ๗ การควบคุมการเข้าถึง

ข้อปฏิบัติ

๑) ออกจากระบบงานโดนทันทีที่ใช้งานเสร็จ
๒) ปิดเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งานอยู่ เมื่อใช้งานประจำวันเสร็จสิ้น เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ให้บริการที่ต้องใช้บริการตลอด ๒๔ ชั่วโมง
๓) ควรมีการตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพหลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที เมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน
๔) เมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์ (Personal Computer) หรือไม่ได้อยู่ที่หน้าเครื่องคอมพิวเตอร์เกินกว่า ๓๐ นาที ให้ทำการล็อกเครื่องคอมพิวเตอร์ โดยกดปุ่ม windows+L พร้อมกันที่คีย์บอร์ด
๕) ให้ขออนุมัติจากผู้บังคับบัญชา ในกรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกสำนักงาน
๖) ระมัดระวังและดูแลสินทรัพย์ของหน่วยงานที่ตนเองใช้งานหรือถือครองเสมือนเป็นสินทรัพย์ของตนเอง หากเกิดความสูญหายหรือเสียหายโดยประมาทเลินเล่อ ต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

๒. นโยบายการป้องกันไวรัสบนเครื่องคอมพิวเตอร์

วัตถุประสงค์

- เพื่อป้องกันข้อมูลในเครื่องคอมพิวเตอร์ไม่ให้เกิดความเสียหาย
- เพื่อให้เครื่องคอมพิวเตอร์ทำงานอย่างถูกต้อง มีความเสถียรภาพ เชื่อถือได้ และปลอดภัยจากการถูกบุกรุกหรือโจมตี

ผู้รับผิดชอบ

- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ข้อปฏิบัติ

๑) ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัสว่ายังทำงานตามปกติหรือไม่ และมีการปรับปรุงฐานข้อมูลไวรัสอย่างสม่ำเสมอหรือไม่ โดยให้การทำการตรวจสอบอย่างน้อยวันละ ๑ ครั้ง หากพบว่าทำงานผิดปกติ ให้รีบแจ้งผู้ดูแลระบบที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยทันที

๓. นโยบายการห้ามติดตั้งระบบหรืออุปกรณ์ต่าง ๆ เพิ่มเติม

วัตถุประสงค์

- เพื่อป้องกันผลข้างเคียงจากการติดตั้งเครื่องคอมพิวเตอร์ ซอฟต์แวร์หรืออุปกรณ์อื่น ๆ ที่นอกเหนือจากที่หน่วยงานได้ติดตั้งไว้ให้ใช้งาน เช่น เป็นแหล่งที่มาของไวรัส โทรจัน หรือโปรแกรมไม่พึงประสงค์อื่น ๆ หรือใช้เป็นทางเข้าสู่เครือข่ายภายในหน่วยงานโดยผู้ไม่พึงประสงค์
- เพื่อป้องกันการเข้าถึงระบบเครือข่าย หรือข้อมูลของหน่วยงานโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ ๓ การบริหารจัดการสินทรัพย์ขององค์กร
- หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ข้อปฏิบัติ

๑) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกเหนือจากที่หน่วยงานได้ติดตั้งไว้ให้ใช้งาน

๒) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้งานการตรวจสอบข้อมูลบนระบบเครือข่าย ยกเว้นการติดตั้งเพื่อการปฏิบัติงานของผู้ดูแลระบบที่เกี่ยวข้อง

๓) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครือข่ายของหน่วยงาน เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์นั้น หรือเครือข่ายของหน่วยงานได้

๔) ห้ามนำเครื่องคอมพิวเตอร์ที่ผู้ใช้งานเป็นเจ้าของมาใช้กับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบที่เกี่ยวข้องก่อนการใช้งาน

๔. นโยบายการใช้งานอินเทอร์เน็ต

วัตถุประสงค์

- เพื่อให้มีการใช้งานอินเทอร์เน็ตที่หน่วยงานจัดไว้ให้อย่างเหมาะสมตามภารกิจงานของผู้ใช้งาน โดยไม่นำไปใช้ในกิจกรรมอื่น ๆ ที่เป็นการสูญเสียเวลาทำงานโดยไม่มีประโยชน์ ที่มีลักษณะเป็นอบายมุข ที่อาจก่อให้เกิดความเสียหายต่อภาพลักษณ์และชื่อเสียงของหน่วยงาน หรือที่ขัดต่อศีลธรรม จริยธรรม ชาติ ศาสนา พระมหากษัตริย์ หรือสิ่งที่บุคคลทั่วไปพึงประพฤติปฏิบัติ

ผู้รับผิดชอบ

- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ ๓ การบริหารจัดการสินทรัพย์ขององค์กร
- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ข้อปฏิบัติ

๑) ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น และห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและได้รับอนุญาตแล้ว

๒) ห้ามทำการดาวน์โหลด (Download) หรือส่งไฟล์ประเภทสื่อลามกอนาจาร

๓) ห้ามเล่นเกมส์ ดูภาพยนตร์ หรือฟังเพลง ผ่านทางอินเทอร์เน็ตในเวลาทำงาน

๔) ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้

๔.๑) การพนัน

๔.๒) การวิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และพระมหากษัตริย์

๔.๓) การลามก อนาจาร

๔.๔) อื่น ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือผิดศีลธรรม จริยธรรม

๕) ห้ามเข้าไปสนทนาในห้องสนทนาบนเครือข่ายอินเทอร์เน็ต

๖) ห้ามใช้อินเทอร์เน็ตเพื่อดาวน์โหลด ส่ง กระจาย หรือแจกจ่าย สื่อหรือข้อมูลดังต่อไปนี้

๖.๑) สื่อสิ่งพิมพ์อิเล็กทรอนิกส์ที่เป็นการละเมิดลิขสิทธิ์ทางปัญญา

๖.๒) ข้อมูลส่วนบุคคลที่ไม่ได้รับอนุญาตจากผู้เป็นเจ้าของ

๗) ห้ามใช้อินเทอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่อาจก่อให้เกิดความเสียหายต่อภาพลักษณ์และชื่อเสียงของหน่วยงาน

๘) หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๕. นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

- เพื่อให้มีการใช้งาน E-mail ที่หน่วยงานจัดไว้ให้อย่างเหมาะสมตามภารกิจงานของเจ้าหน้าที่และลูกจ้าง และไม่ใช้ในกิจกรรมอื่น ๆ ที่อาจก่อให้เกิดความเสียหายต่อผู้อื่นหรือต่อหน่วยงาน

ผู้รับผิดชอบ

- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ ๓ การบริหารจัดการสินทรัพย์ขององค์กร
- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร
- หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

ข้อปฏิบัติ

๑) ผู้ใช้งานที่ต้องการขอลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) ของหน่วยงาน โดยยื่นคำขอกับเจ้าหน้าที่ผู้ดูแลระบบเพื่อดำเนินการกำหนดสิทธิบัญชีผู้ใช้งาน และรหัสผ่าน (Password)

๒) ผู้ใช้งานไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๓) ผู้ใช้งานควรมีการเปลี่ยนรหัสผ่าน (Password) ทุก ๖ เดือน

๔) ห้ามใช้ที่อยู่ E-mail (E-mail Address) อื่น ๆ นอกเหนือจากที่หน่วยงานได้จัดสรรไว้ให้ เพื่อใช้ในการติดต่องานตามภารกิจหรือหน้าที่ความรับผิดชอบของตนกับหน่วยงานทั้งภายในและภายนอก

๕) ห้ามผู้ใช้งานเข้าถึงข้อมูล E-mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต

๖) ห้ามลงทะเบียนด้วยที่อยู่ E-mail (E-mail Address) ที่หน่วยงานมอบให้ไว้ตามที่อยู่เว็บไซต์ต่าง ๆ ที่ไม่มีความเกี่ยวข้องกับงานของหน่วยงาน

๗) ห้ามส่ง E-mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

๘) ห้ามส่ง E-mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

๙) ห้ามส่ง E-mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมายสินทรัพย์ทางปัญญา หรือสิทธิของบุคคลอื่น

๑๐)ห้ามส่งต่อ หรือเผยแพร่ E-mail ที่มีลักษณะดังต่อไปนี้

- ๑๐.๑) การพนัน
- ๑๐.๒) การวิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และพระมหากษัตริย์
- ๑๐.๓) การลามก อนาจาร
- ๑๐.๔) อื่น ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือผิดศีลธรรม จริยธรรม

๑๑)ห้ามส่ง E-mail ที่มีโปรแกรมไม่พึงประสงค์ไปให้กับบุคคลอื่นโดยเจตนา

๑๒)ห้ามปลอมแปลง E-mail ของบุคคลอื่น

๑๓)ห้ามรับ หรือส่ง E-mail แทนบุคคลอื่นโดยไม่ได้รับอนุญาต

๑๔)ห้ามใช้คำที่ไม่สุภาพในการส่ง E-mail

๑๕)ห้ามส่ง E-mail ที่มีข้อมูลความลับของหน่วยงาน เว้นเสียแต่ว่าจะใช้วิธีการที่มีความปลอดภัยที่หน่วยงานกำหนดไว้

๑๖)ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ E-mail ของผู้รับให้ถูกต้อง เพื่อป้องกันการส่งข้อมูลผิดพลาด

๑๗)ให้ระบุชื่อของผู้ส่งใน E-mail ทุกฉบับที่ส่งไป

๑๘)ให้จำกัดกลุ่มผู้รับ E-mail เท่าที่มีความจำเป็นต้องรับทราบในข้อมูลที่ส่งไปนั้น

๑๙)ควรลบข้อมูล E-mail ที่ไม่มีความจำเป็นอย่างสม่ำเสมอ

๒๐)หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นผู้ใช้งานควรทำการลงบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

๒๑)ผู้ใช้งานมีหน้าที่ต้องรักษาชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๖. นโยบายการป้องกันการใช้ทรัพยากรผิดวัตถุประสงค์

วัตถุประสงค์

- เพื่อป้องกันการใช้ทรัพยากรของหน่วยงานผิดวัตถุประสงค์

ผู้รับผิดชอบ

- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

ข้อปฏิบัติ

ผู้ใช้งานจะต้องไม่ใช้ระบบเครือข่ายของหน่วยงานโดยมีวัตถุประสงค์ดังต่อไปนี้

๑) เพื่อกระทำการผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น
๒) เพื่อกระทำการที่ขัดต่อ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๓) เพื่อกระทำการที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
๔) เพื่อค้าขายส่วนตัว
๕) เพื่อกระทำการอันมีลักษณะเป็นการละเมิดสินทรัพย์ทางปัญญาของหน่วยงาน หรือของบุคคลอื่น
๖) เพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว
๗) เพื่อรับหรือส่งข้อมูลซึ่งอาจก่อให้เกิดความเสียหายต่อหน่วยงาน เช่น การส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ การส่งข้อมูลอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น เป็นต้น
๘) เพื่อขัดขวางหรือทำให้ไม่สามารถใช้งานได้ตามปกติ การใช้งานเครือข่ายคอมพิวเตอร์ของหน่วยงานของผู้ใช้งานอื่น หรือของหน่วยงานภายนอกอื่น
๙) เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของหน่วยงาน ไปยังที่อยู่เว็บใดๆ ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง
๑๐) เพื่อกระทำการอื่นใดที่อาจขัดต่อผลประโยชน์ของหน่วยงาน หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายต่อหน่วยงาน

๗. นโยบายการใช้งานเครื่องคอมพิวเตอร์พกพา

วัตถุประสงค์

- เพื่อให้มีการใช้งานเครื่องคอมพิวเตอร์คอมพิวเตอร์พกพาที่หน่วยงานจัดไว้ให้อย่างเหมาะสม และป้องกันการสูญหาย เสียหาย หรือถูกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ ๓ การบริหารจัดการสินทรัพย์ขององค์กร

ข้อปฏิบัติ

๑) กรอกแบบคำขอยืม – คืนสำหรับเครื่องคอมพิวเตอร์คอมพิวเตอร์พกพาที่จัดสรรไว้เป็นเครื่องกลางเพื่อขออนุมัติก่อนนำไปใช้งาน
๒) ตรวจสอบว่าเครื่องคอมพิวเตอร์คอมพิวเตอร์พกพาของหน่วยงานได้รับการติดตั้งโปรแกรมที่มีลิขสิทธิ์ตามรายชื่อโปรแกรมมาตรฐานที่กำหนดให้ติดตั้งหรือไม่ (โปรแกรมดังกล่าว ได้แก่ โปรแกรมออฟฟิศ โปรแกรมป้องกันไวรัส หรือโปรแกรมอื่น ๆ เป็นต้น) หากพบว่ายังไม่ได้ติดตั้ง ให้ติดต่อผู้ดูแลระบบที่เกี่ยวข้องเพื่อขอรับการติดตั้งก่อนการใช้งาน

๓) ระมัดระวังและรักษาเครื่องคอมพิวเตอร์คอมพิวเตอร์พกพาเมื่อมีการนำไปใช้งานนอกสถานที่ เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
๔) ควรมีการตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพ เมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน
๕) ห้ามปล่อยเครื่องทิ้งไว้โดยไม่มีผู้ดูแลเมื่ออยู่ในที่สาธารณะ

๘. นโยบายการกำหนดและป้องกันรหัสผ่าน

วัตถุประสงค์

- เพื่อป้องกันการเข้าถึงข้อมูล ระบบ อุปกรณ์ หรือทรัพยากรสารสนเทศอื่น ๆ ของหน่วยงานโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ ๗ การควบคุมการเข้าถึง

ข้อปฏิบัติ (ด้านการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน)

๑) เก็บรักษารหัสผ่านของตนเองไว้เป็นความลับ ห้ามเปิดเผยต่อผู้อื่น
๒) กำหนดรหัสผ่านให้มีคุณสมบัติตาม**นโยบายการตั้งรหัสผ่าน**
๓) กำหนดรหัสผ่านสำหรับการใช้ไฟล์ข้อมูลร่วมกันกับบุคคลอื่น โดยผ่านทางระบบเครือข่าย
๔) ห้ามบันทึกรหัสผ่านไว้ในโปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำรหัสผ่านของตน
๕) ต้องไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่น
๖) ในกรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเพื่อให้สามารถปฏิบัติงานแทนตนเองได้ หลังจากที่ทำงานนั้นเสร็จเรียบร้อยแล้ว ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

ข้อปฏิบัติ (ด้านการใช้งานรหัสผ่าน)

๑) ห้ามใช้รหัสผ่านของผู้อื่นโดยไม่ได้รับอนุญาตโดยเด็ดขาด
๒) ให้ทำการออกจากระบบ (Log Out) ทุกครั้ง หลังจากใช้งานระบบสารสนเทศหรือระบบอื่นๆ ที่ต้องใช้รหัสผ่านเสร็จแล้ว
๓) ในกรณีลืมรัหสผ่านหรือไม่สามารถเข้าใช้งานระบบได้ ให้ติดต่อผู้ดูแลระบบ หรือผู้พัฒนาระบบนั้น เพื่อแก้ไขปัญหา ไม่ควรพยายามเดารหัสผ่านด้วยตัวเอง

๙. นโยบายการบริหารจัดการรหัสผ่าน

วัตถุประสงค์

- เพื่อป้องกันการเข้าถึงข้อมูล ระบบ อุปกรณ์ หรือทรัพยากรสารสนเทศอื่น ๆ ของหน่วยงานโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ ๗ การควบคุมการเข้าถึง

ข้อปฏิบัติ

๑) กำหนดรหัสผ่านให้มีความยาวไม่น้อยกว่า ๘ ตัวอักษร

๒) ตั้งรหัสผ่านโดยคำนึงถึงความยากต่อการคาดเดา ตามแนวทางปฏิบัติดังนี้
   ๒.๑) มีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ และตัวอักขระพิเศษหรือสัญลักษณ์ต่างๆ ด้วยก็ได้
   ๒.๒) ไม่กำหนดรหัสผ่านจากชื่อ หรือชื่อสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน
   ๒.๓) ไม่กำหนดรหัสผ่านจากคำศัพท์ที่ปรากฏในพจนานุกรม หรือจากหมายเลขโทรศัพท์
๓) ทำการเปลี่ยนรหัสผ่านเพื่อใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานทุก ๖ เดือน หรือเปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหล
๔) ไม่บันทึกหรือเปิดเผยรหัสผ่านให้บุคคลอื่นที่ไม่ใช่เจ้าของรหัสผ่านโดยเด็ดขาด ยกเว้นกรณี

๑๐.นโยบายการเข้าปฏิบัติงานในห้อง Data Center

วัตถุประสงค์

- เพื่อควบคุมการเข้าถึงทางกายภาพโดยอนุญาตให้เฉพาะผู้ที่มีภารกิจเท่านั้น จึงจะสามารถเข้าถึงห้อง Data Centerได้ และป้องกันการสูญหาย เสียหาย การถูกขโมยของสินทรัพย์ต่าง ๆ ในห้อง Data Center รวมทั้งการเข้าถึงระบบโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ดูแลระบบและผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ข้อปฏิบัติ

๑) ห้ามเข้าไปในบริเวณห้อง Data Center โดยไม่มีภารกิจที่เกี่ยวข้องหรือจำเป็น
๒) ห้ามใส่รองเท้าเข้าไปในห้อง Data Center
๓) ห้ามนำอาหาร และเครื่องดื่มเข้าไปในบริเวณห้อง Data Center
๔) ลงบันทึกการเข้าห้อง Data Centerในสมุดบันทึกการเข้า – ออกห้อง Data Center
๕) หากพบเห็นความผิดปกติในห้อง Data Center เช่น มีสินทรัพย์หาย มีร่องรอยการบุกรุก เป็นต้น ให้รีบแจ้งเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง
๖) ปฏิบัติตามคำแนะนำของเจ้าหน้าที่ที่ดูแลห้อง Data Center อย่างเคร่งครัด

๑๑.นโยบายการจัดชั้นความลับของข้อมูล

วัตถุประสงค์

- เพื่อควบคุมการจัดชั้นความลับของข้อมูลของ กรมการค้าภายใน ให้มีความถูกต้องตามลักษณะข้อมูล ซึ่งจะมีผลต่อการบริหารจัดการและความมั่นคงปลอดภัยของข้อมูล

ผู้รับผิดชอบ

- ผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๓ การบริหารจัดการสินทรัพย์ขององค์กร

ข้อปฏิบัติ

๑) กำหนดชั้นความลับของข้อมูลเป็น ข้อมูลลับ ข้อมูลใช้ภายในเท่านั้น ข้อมูลส่วนบุคคล หรือข้อมูลเปิดเผยได้ โดยพิจารณาจากองค์ประกอบต่อไปนี้ เพื่อกำหนดชั้นความลับของข้อมูล

๑.๑) ความสำคัญของเนื้อหา เช่น เนื้อหาของข้อมูลนั้นมีความสำคัญต่อความสำเร็จของงานตามภารกิจของ กรมการค้าภายใน มากน้อยเพียงใด หากมีความสำคัญสูง ข้อมูลนั้นจะสามารถจัดอยู่ในชั้นความลับประเภทใช้ภายในเท่านั้น หรือ ลับ เป็นต้น

๑.๒) แหล่งที่มาของข้อมูล เช่น หากข้อมูลนั้นมาจากภายนอกและเป็นข้อมูลลับ ชั้นความลับก็จะต้องคงไว้เช่นเดิม หรือหากข้อมูลนั้นมาจากอินเทอร์เน็ต ชั้นความลับก็จะเป็นประเภทเปิดเผยได้ เป็นต้น

๑.๓) วิธีการนำไปใช้ประโยชน์ เช่น หากข้อมูลนั้นสามารถนำไปใช้ประโยชน์ในเชิงพาณิชย์ได้ หากถูกเปิดเผยจะส่งผลกระทบด้านการเงินของ กรมการค้าภายใน ข้อมูลนี้จะอยู่ในประเภท ลับ เป็นต้น

๑.๔) จำนวนบุคคลที่ควรทราบ เช่น หากข้อมูลนั้นสามารถเปิดเผยต่อผู้ใช้งานข้อมูลเป็นจำนวนมาก ชั้นความลับจะเป็นข้อมูลเปิดเผยได้ เป็นต้น

๑.๕) ผลกระทบหากมีการเปิดเผย เช่น หากข้อมูลนั้นถูกเปิดเผย จะมีผลระทบด้านชื่อเสียงและภาพลักษณ์ ด้านการเงิน ด้านการปฏิบัติตามกฎระเบียบข้อบังคับที่หน่วยงานต้องปฏิบัติตาม หรือด้านการมีส่วนได้ส่วนเสียของผู้ที่เกี่ยวข้อง ดังนั้น ข้อมูลจะสามารถจัดอยู่ในชั้นความลับประเภทใช้ภายในเท่านั้น หรือ ลับ เป็นต้น

๑.๖) หน่วงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่อง เช่น ข้อมูลสำคัญ หรือข้อมูลลับที่มาจากเจ้าของเรื่องใด จะต้องคงชั้นความลับไว้เช่นเดิม การนำไปใช้งานควรขออนุญาตจากผู้ที่เป็นเจ้าของเรื่องก่อน เป็นต้น

๒) สำหรับข้อมูลในชั้นความลับ “ลับ” ได้แก่ ลับ ลับมาก หรือ ลับที่สุด เจ้าของข้อมูล ต้องพิจารณาเกณฑ์ต่อไปนี้เพิ่มเติมเพื่อกำหนดชั้นความลับที่ถูกต้อง

๒.๑) **ลับที่สุด** หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐและเจ้าของข้อมูลอย่างร้ายแรงที่สุด

๒.๒) **ลับมาก** หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐและเจ้าของข้อมูลอย่างร้ายแรง

๒.๓) **ลับ** หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐและเจ้าของข้อมูล

๑๒.นโยบายการจัดการกับข้อมูลลับ

วัตถุประสงค์

- เพื่อป้องกันการเข้าถึงข้อมูลลับของ กรมการค้าภายใน โดยไม่ได้รับอนุญาต
- เพื่อกำหนดวิธีการจัดการข้อมูลลับของ กรมการค้าภายใน อย่างเป็นรูปธรรม มีมาตรฐาน และมีความมั่นคงปลอดภัยเพียงพอ
- เพื่อควบคุมการใช้งานหรือการเข้าถึงข้อมูลลับของ กรมการค้าภายใน ให้เป็นไปอย่างมั่นคงปลอดภัย

ผู้รับผิดชอบ

- ผู้พัฒนาระบบ (ที่เป็นเจ้าของข้อมูลลับ)

อ้างอิงมาตรฐาน

- หมวดที่ ๓ การบริหารจัดการสินทรัพย์ขององค์กร
- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ข้อปฏิบัติ

๑) ในการกำหนดชั้นความลับ ให้ปฏิบัติดังนี้

๑.๑) กำหนดชั้นความลับของข้อมูลลับที่ตนเองรับผิดชอบตาม**นโยบายการจัดชั้นความลับของข้อมูล**

๑.๒) พิจารณาปรับชั้นความลับ (ปรับลด เพิ่ม หรือยกเลิกชั้นความลับ) ตามความจำเป็นให้ถูกต้องและทันสมัย และต้องแจ้งให้หน่วยงานที่สามารถเข้าถึงข้อมูลหรือที่ได้รับการแจกจ่ายทราบด้วยทุกครั้ง เพื่อแก้ไขชั้นความลับให้ถูกต้อง

๒) ในการจัดทำหรือจัดเตรียมข้อมูลลับ ให้ปฏิบัติดังนี้

๒.๑) จัดทำหรือจัดเตรียมข้อมูลในสถานที่ที่ปลอดภัย เช่น จัดทำในสำนักงาน ไม่ทำในสถานที่ที่เป็นสาธารณะซึ่งบุคคลภายนอกสามารถเห็นข้อมูลที่จัดทำได้ และจำกัดผู้ที่เป็นผู้ดำเนินการจัดทำ

๒.๒) ในการจัดทำข้อมูลลับซึ่งใช้กระดาษหรือวัสดุชั่วคราว เช่น กระดาษร่าง กระดาษคาร์บอน ต้องทำลายกระดาษหรือวัสดุนั้นทันทีที่จัดทำเสร็จเรียบร้อย ถ้าเป็นการจัดทำโดยใช้เครื่องคอมพิวเตอร์ จะต้องทำการลบ หรือทำลายสื่อบันทึกข้อมูลจนไม่สามารถนำไปใช้ประโยชน์ได้ (ดูวิธีการทำลายใน **นโยบายการทำลายข้อมูลบนสื่อบันทึกข้อมูล**) หากไม่ทำลาย ต้องเก็บรักษาไว้ในสถานที่ที่ปลอดภัย

๒.๓) จัดทำข้อมูลโดยแสดงเลขที่หน้าของจำนวนหน้าทั้งหมดไว้ในทุกหน้าของข้อมูลลับ และแสดงไว้ในส่วนที่สามารถเห็นได้ชัดเจน เช่น มุมขวาด้านบนของเอกสาร

๓) ในการแสดงชั้นความลับบนข้อมูลลับ ให้ปฏิบัติดังนี้

๓.๑) แสดงชั้นความลับของข้อมูล (ซึ่งประกอบด้วย “ลับ” “ลับมาก” หรือ “ลับที่สุด”) ให้ปรากฏเห็นอย่างเด่นชัดทั้งข้อมูลที่มีสภาพเป็นกระดาษ ไฟล์อิเล็กทรอนิกส์ เทป External Harddisk, Flash Drive แผ่น CD/DVD หรือข้อมูลลับที่อยู่ในรูปแบบอื่น ๆ

๓.๒) แสดงชั้นความลับบนเอกสารลับในทุกหน้าของเอกสารให้ปรากฏเห็นอย่างเด่นชัด

๔) ในการทำสำเนาหรือแจกจ่ายข้อมูลลับ ให้ปฏิบัติดังนี้

๔.๑) ทำสำเนาหรือแจกจ่ายข้อมูลลับให้แก่ผู้รับปลายทาง ซึ่งเป็นผู้ที่มีสิทธิในการเข้าถึงข้อมูลตามที่ระบุไว้ในทะเบียนข้อมูลลับ หรือสามารถแจกจ่ายให้ได้ตามความจำเป็นในการเข้าถึงข้อมูลนั้น

๔.๒) แจ้งให้หน่วยงานภายนอกที่อนุญาตให้เข้าถึงข้อมูลลับนั้นได้ ว่าไม่อนุญาตให้ทำสำเนาเพิ่มเติม เว้นเสียแต่ได้รับอนุญาตจาก กรมการค้าภายใน ก่อน

๕) ในการเก็บรักษาเอกสารลับ ให้ปฏิบัติดังนี้

๕.๑) จัดเก็บเอกสารลับไว้ในแฟ้มข้อมูลลับ และนำไปเก็บในตู้เก็บเอกสารลับโดยแยกเก็บเป็นแต่ละเรื่องหรือแต่ละหัวข้อ

๕.๒) ไม่จัดเก็บเอกสารลับร่วมกับเอกสารที่อยู่ในชั้นความลับอื่น ๆ เช่น ข้อมูลใช้ภายในเท่านั้น ข้อมูลส่วนบุคคล หรือข้อมูลที่เปิดเผยได้

๕.๓) จัดเก็บแฟ้มข้อมูลลับ และสื่อบันทึกข้อมูล ไว้ในตู้และปิดล็อกด้วยกุญแจที่มั่นคง

๖) ในการยืมหรือขอเข้าถึงข้อมูลลับ ให้ปฏิบัติดังนี้

๖.๑) เมื่อมีการขอยืมหรือขอเข้าถึงข้อมูลลับ โดยผู้อื่นที่ไม่ได้เป็นผู้มีสิทธิในการเข้าถึงข้อมูลตามทะเบียนข้อมูลลับ ให้หัวหน้าหน่วยงานภายใน เป็นผู้พิจารณาตารวจสอบคุณสมบัติของผู้ยืมหรือขอเข้าถึงก่อน ว่าเป็นผู้มีอำนาจหน้าที่ที่เกี่ยวข้องหรือไม่ หรือมีความจำเป็นในการเข้าถึงข้อมูลนั้นหรือไม่ พร้อมทั้งต้องทำบันทึกหลักฐานการยืมหรือการขอเข้าถึงข้อมูลนั้นด้วย แจ้งให้ผู้ยืมหรือขอเข้าถึงทราบว่า ห้ามทำการสำเนาเพิ่มเติม

๖.๒) เมื่อหมดความจำเป็นในการใช้งานแล้ว หัวหน้าหน่วยงานภายใน กำหนดให้ผู้ขอยืมจัดส่งข้อมูลนั้นกลับคืนมาโดยทันที สำหรับกรณีการเข้าถึงระบบเทคโนโลยีสารสนเทศ ให้ทำการยกเลิกบัญชีผู้ใช้งานที่ขอเข้าถึงข้อมูลลับโดยทันที

๗) ในการส่งเอกสารลับ ให้ปฏิบัติดังนี้

๗.๑) ปฏิบัติตามระเบียบการส่งเอกสารลับของ กรมการค้าภายใน

๗.๒) ตรวจสอบที่อยู่อีเมล์ของผู้รับปลายทางให้ถูกต้อง ก่อนจัดส่งไฟล์นั้นไปยังผู้รับ เพื่อป้องกันการส่งผิดตัวบุคคล

๘) ในการทำลายข้อมูลลับ ให้ปฏิบัติตาม **นโยบายการทำลายข้อมูลบนสื่อบันทึกข้อมูล**

๙) ในการจัดการกับไฟล์ข้อมูลลับ ให้ปฏิบัติดังนี้

๙.๑) แสดงชั้นความลับบนไฟล์ข้อมูลลับ เช่น การทำลายน้ำและแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว

๙.๒) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ด้วยการใช้การเข้ารหัสข้อมูลตามมาตรฐานของระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๙.๓) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยการใช้รหัสผ่านที่มีความมั่นคงปลอดภัย

๙.๔) ห้าม Share ไฟล์ข้อมูลลับบนเครือข่ายของ กรมการค้าภายใน เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้

๙.๕) ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลลับ ว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

๙.๖) ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ เพื่อแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่

๙.๗) ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

๑๓.นโยบายการจัดการกับข้อมูลใช้ภายใน

วัตถุประสงค์

- เพื่อป้องกันการเข้าถึงข้อมูลใช้ภายในหน่วยงานเท่านั้น โดยไม่ได้รับอนุญาต
- เพื่อกำหนดวิธีการจัดการกับข้อมูลใช้ภายในเท่านั้นอย่างเป็นรูปธรรม มีมาตรฐาน และมีความมั่นคงปลอดภัยเพียงพอ

ผู้รับผิดชอบ

- ผู้ใช้งาน (ที่เป็นเจ้าของข้อมูลใช้ภายใน)

อ้างอิงมาตรฐาน

- หมวดที่ ๓ การบริหารจัดการสินทรัพย์ขององค์กร
- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ข้อปฏิบัติ

๑) ในการระบุชนิดของข้อมูลใช้ภายในเท่านั้น ให้ปฏิบัติตาม **นโยบายการจัดชั้นความลับของข้อมูล** เพื่อระบุชนิดของข้อมูลใช้ภายในเท่านั้นที่ตนเองรับผิดชอบ

๒) ในการสร้างและแสดงชั้นความลับบนข้อมูลใช้ภายในเท่านั้น ให้สร้างและแสดงชั้นความลับบนข้อมูล กล่าวคือ “ข้อมูลใช้ภายในเท่านั้น” ให้ปรากฏเห็นอย่างเด่นชัดทั้งข้อมูลที่มีสภาพเป็นกระดาษ ไฟล์อิเล็กทรอนิกส์ เทป External Harddisk, Flash Drive แผ่น CD/DVD หรือข้อมูลลับที่อยู่ในรูปแบบอื่น ๆ

๓) ในการเก็บรักษาเอกสารที่เป็นข้อมูลใช้ภายในเท่านั้น ให้ปฏิบัติดังนี้

๓.๑) จัดเก็บเอกสารที่เป็นข้อมูลใช้ภายในเท่านั้นไว้ในแฟ้มข้อมูลและสื่อบันทึกข้อมูล แล้วนำไปเก็บในตู้เก็บเอกสารลับโดยแยกเก็บเป็นแต่ละเรื่องหรือแต่ละหัวข้อ

๓.๒) จัดเก็บแฟ้มข้อมูลและสื่อบันทึกข้อมูลที่เป็นข้อมูลใช้ภายในเท่านั้น ไว้ในตู้และปิดล็อกด้วยกุญแจที่มั่นคง

๔) ในการส่ง การสำเนา หรือการให้ยืมเอกสารที่เป็นข้อมูลใช้ภายในเท่านั้น ให้จำกัดการส่ง การสำเนาหรือการให้ยืมเอกสารที่เป็นข้อมูลใช้ภายในเท่านั้นให้แก่หน่วยงานหรือบุคคลทั้งภายในและภายนอกหน่วยงานที่มีความจำเป็นต้องใช้งานหรือเข้าถึงข้อมูลนั้นเท่านั้น หากไม่ต้องการให้ผู้รับเอกสารเปิดเผยข้อมูลนั้นต่อผู้อื่น ให้แจ้งให้ผู้รับเอกสารได้รับทราบด้วย และเมื่อหมดความจำเป็นในการใช้งานแล้ว หัวหน้าหน่วยงานภายใน กำหนดให้ผู้ขอยืมจัดส่งข้อมูลนั้นกลับคืนมาโดยทันที สำหรับกรณีการเข้าถึงระบบเทคโนโลยีสารสนเทศ ให้ทำการยกเลิกบัญชีผู้ใช้งานที่ขอเข้าถึงข้อมูลลับโดยทันที

๕) ในการทำลายข้อมูลใช้ภายในเท่านั้น ให้ปฏิบัติตาม **นโยบายการทำลายข้อมูลบนสื่อบันทึกข้อมูล**

๖) ในการจัดการกับไฟล์ข้อมูลใช้ภายในเท่านั้น ให้ปฏิบัติดังนี้

๖.๑) ป้องกันไฟล์ข้อมูลใช้ภายในเท่านั้นซึ่งจัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยการใช้รหัสผ่านที่มีความมั่นคงปลอดภัย

๖.๒) สามารถ Share ไฟล์ข้อมูลใช้ภายในเท่านั้นบนเครือข่ายของ กรมการค้าภายใน ให้แก่หน่วยงานหรือผู้ใช้งานข้อมูลภายใน กรมการค้าภายใน ได้ โดยพิจารณาจากหน้าที่หรือความจำเป็นในการเข้าถึงข้อมูลนั้น แต่ต้องใช้รหัสผ่านที่มีความมั่นคงปลอดภัยเพื่อป้องกันข้อมูลที่ Share นั้น

๖.๓) ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลใช้ภายในเท่านั้น ว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

๖.๔) ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ เพื่อแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่

๖.๕) ดำเนินการสำรองไฟล์ข้อมูลใช้ภายในเท่านั้นในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

๗) ในการส่งไฟล์ข้อมูลใช้ภายในเท่านั้นทางอีเมล์ ให้ตรวจสอบที่อยู่อีเมล์ของผู้รับปลายทางให้ถูกต้อง ก่อนจัดส่งไฟล์ข้อมูลใช้ภายในเท่านั้นไปยังผู้รับ เพื่อป้องกันการส่งผิดตัวบุคคลและทำให้ข้อมูลเกิดการรั่วไหล

๑๔.นโยบายการทำลายข้อมูลบนสื่อบันทึกข้อมูล

วัตถุประสงค์

- เพื่อให้มีวิธีการปฏิบัติที่ปลอดภัยในการทำลายข้อมูลบนสื่อบันทึกข้อมูลโดยไม่สามารถเข้าถึงเนื้อหาภายในสื่อบันทึกข้อมูลได้อีกต่อไป
- เพื่อป้องกันการเข้าถึงข้อมูลบนสื่อบันทึกข้อมูลโดยไม่ได้รับอนุญาต รวมทั้งป้องกันการรั่วไหลของข้อมูล

ผู้รับผิดชอบ

- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ข้อปฏิบัติ

๑) ในการทำลายสื่อบันทึกข้อมูล เจ้าของข้อมูลพิจารณาทำลายสื่อบันทึกข้อมูลด้วยวิธีการทำลายแยกตามประเภทของสื่อบันทึกข้อมูลในตาราง

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลายข้อมูล	วิธีการทำลายสื่อบันทึกข้อมูล (กรณีไม่ต้องการนำกลับมาใช้ใหม่)
Flash Drive/การ์ดบันทึกข้อมูล	ให้ทำลายข้อมูลบน Flash Drive/การ์ดบันทึกข้อมูลด้วยวิธีการฟอร์แม็ต (Format) ตาม **มาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหม สหรัฐอเมริกา DOD ๕๒๒๐.๓๓-M** (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ทำลายด้วยเครื่องทำลายเอกสารหรือฉีกให้ละเอียด	
แผ่น CD/DVD	ให้บันทึกข้อมูลเปล่าลงแผ่น CD/DVD ทับข้อมูลเดิมเป็นจำนวนหลายรอบ (กรณีเป็นชนิด CD/DVD-RW เท่านั้น)	ใช้วิธีการหักแผ่น CD/DVD หรือขูดให้เสียหาย
เทป/วิดีโอ	ให้อัดเทป/วิดีโอเปล่าทับข้อมูลเดิมเป็นจำนวนหลายรอบ	ใช้วิธีการทุบหรือบดให้เสียหาย
ฮาร์ดดิสก์	ให้ทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แม็ต (Format) ตาม **มาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหม สหรัฐอเมริกา DOD ๕๒๒๐.๓๓-M** (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)	ใช้วิธีการทุบหรือบดให้เสียหาย
อุปกรณ์สื่อสารที่มีหน่วยความจำ	ให้ใช้เมนู ตั้งค่าข้อมูลจากโรงงาน (Factory Data Reset) เพื่อให้อุปกรณ์ล้างข้อมูลออก	ใช้วิธีการทุบหรือบดให้เสียหาย

๒) ในการทำลายสื่อบันทึกข้อมูลลับในทะเบียนข้อมูลลับที่สิ้นสุดหรือหมดอายุการจัดเก็บ คณะกรรมการทำลายข้อมูล ตรวจสอบและปฏิบัติตามระเบียบเรื่องการทำลายข้อมูลลับในระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

๑๕.นโยบายการลงทะเบียนการใช้งาน

วัตถุประสงค์

- เพื่อควบคุมการเข้าถึงระบบโดยอนุญาตให้เข้าถึงได้ตามความจำเป็นในการใช้งาน
- เพื่อให้มีการลงทะเบียนและจัดทำบัญชีผู้ใช้งานแยกเป็นผู้ใช้งานรายบุคคลและผู้ใช้งานร่วมกัน

ผู้รับผิดชอบ

- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ ๗ การควบคุมการเข้าถึง

ข้อปฏิบัติ

๑) ห้ามผู้ใช้งานใช้ระบบงานของหน่วยงาน จนกว่าจะได้รับการอนุมัติให้ใช้งานโดยผ่านการลงทะเบียนก่อน รวมทั้งต้องไม่พยายามเข้าถึงระบบงานใด ๆ ก็ตามที่ตนยังไม่ได้รับอนุญาตให้ใช้งาน

๒) กรอกแบบคำขอเพื่อขออนุมัติใช้งานระบบงานตาม **แบบคำขอสำหรับลงทะเบียนผู้ใช้งานรายบุคคล** และนำเสนอต่อผู้บังคับบัญชาเพื่อขออนุมัติการใช้งาน เมื่อได้รับการอนุมัติแล้วให้ส่งผู้บังคับบัญชาของผู้ดูแลระบบและ/หรือผู้พัฒนาระบบเพื่อดำเนินการต่อไป

๓) ในกรณีที่มีความจำเป็นต้องมีการใช้งานบัญชีผู้ใช้งานร่วมกัน ให้ขออนุมัติผู้บังคับบัญชาระดับฝ่ายตาม **แบบคำขอสำหรับลงทะเบียนผู้ใช้งานร่วมกัน** หากมีความเสียหายเกิดขึ้น ผู้ใช้งานบัญชีร่วมกันนั้นจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นร่วมกัน เมื่อได้รับการอนุมัติแล้วให้ส่งผู้บังคับบัญชาของผู้ดูแลระบบและ/หรือผู้พัฒนาระบบเพื่อดำเนินการต่อไป

๑๖.นโยบายการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัย

วัตถุประสงค์

- เพื่อให้การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อนำผลที่ได้ไปสู่การบริหารจัดการ รวมทั้งดำเนินการแก้ไขได้อย่างเหมาะสม ได้ผล และทันการณ์

ผู้รับผิดชอบ

- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ ๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

ข้อปฏิบัติ

๑) แจ้งไปยังเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ โดยทันที เมื่อพบเห็น เหตุการณ์ด้านความมั่นคงปลอดภัย ได้แก่

- ๑.๑) การกระทำที่ขัดต่อ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- ๑.๒) การกระทำที่ขัดต่อความมั่นคงของชาติ
- ๑.๓) การใช้ทรัพยากรสารสนเทศของหน่วยงานผิดวัตถุประสงค์
- ๑.๔) หน้าเว็บไซต์หลักถูกเปลี่ยนแปลง
- ๑.๕) ข้อมูลในหน้าเว็บไซต์หลักไม่ถูกต้อง หรือคลาดเคลื่อนจากความเป็นจริง
- ๑.๖) ข้อมูลสำคัญถูกเปลี่ยนแปลง ถูกลบ หรือสูญหาย
- ๑.๗) การเปิดเผยข้อมูลสำคัญ หรือข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
- ๑.๘) การนำข้อมูลสำคัญไปใช้ผิดวัตถุประสงค์
- ๑.๙) ทรัพยากรสารสนเทศถูกขโมย
- ๑.๑๐) การอนุญาตให้บุคคลภายนอกเข้าใช้ระบบของหน่วยงาน
- ๑.๑๑) การแอบติดตั้งอุปกรณ์ หรือโปรแกรมเพื่อดักขโมยข้อมูล หรือดักดูข้อมูลในเครือข่าย
- ๑.๑๒) การใช้อำนาจของสิทธิการเป็นผู้ดูแลระบบอย่างไม่เหมาะสม
- ๑.๑๓) การบุกรุกห้อง Data Center
- ๑.๑๔) โปรแกรมไม่พึงประสงค์
- ๑.๑๕) เหตุการณ์อื่น ๆ ที่เป็นการละเมิดนโยบายด้านความมั่นคงปลอดภัยของหน่วยงาน

๒) ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลระบบที่เกี่ยวข้องในการตรวจสอบเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้น รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชาและผู้ดูแลระบบที่เกี่ยวข้องด้วย

ส่วนที่ ๔
นโยบายการจัดการคอมพิวเตอร์และเครือข่าย
สำหรับเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ

นโยบายการจัดการคอมพิวเตอร์และเครือข่ายประกอบด้วย

๑. นโยบายการจัดทำคู่มือการปฏิบัติงาน

วัตถุประสงค์

- เพื่อให้การปฏิบัติงานด้านสารสนเทศเป็นไปอย่างถูกต้อง ลดความผิดพลาดที่อาจจะเกิดขึ้น ซึ่งอาจส่งผลกระทบให้ระบบเกิดการหยุดชะงักการทำงาน

ผู้รับผิดชอบ

- ผู้ดูแลระบบและผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ข้อปฏิบัติ

๑) ให้จัดทำและปรับปรุงคู่มือการปฏิบัติงานให้มีความทันสมัย อย่างน้อยให้ครอบคลุมในรายการคู่มือการปฏิบัติงานของหน่วยงาน รวมทั้งให้จัดเก็บไว้ในสถานที่ที่มีความปลอดภัย

๒. นโยบายการตรวจสอบข้อมูลความรู้ที่เกี่ยวข้องกับผลิตภัณฑ์ที่หน่วยงานใช้งาน และความรู้ที่เกี่ยวกับความมั่นคงปลอดภัย

วัตถุประสงค์

- เพื่อให้เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ ได้ติดตามข้อมูล ข่าวสาร หรือความรู้ที่เกี่ยวข้องกับผลิตภัณฑ์ต่าง ๆ ที่หน่วยงานใช้งาน หรือที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยและนำมาปรับปรุงระบบให้ดีหรือปลอดภัยยิ่งขึ้น

ผู้รับผิดชอบ

- ผู้ดูแลระบบและผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๒ โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร

ข้อปฏิบัติ

๑) ให้จัดทำ และปรับปรุงที่อยู่ URL สำหรับเว็บไซต์ของผู้ผลิตทางด้านฮาร์ดแวร์และซอฟต์แวร์ที่หน่วยงานใช้งาน เพื่อใช้ในการศึกษา และติดตามแนวโน้มทางด้านเทคโนโลยีสารสนเทศต่าง ๆ และแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบ

๒) ให้จัดทำและปรับปรุงที่อยู่ URL สำหรับเว็บไซต์ของแหล่งความรู้ที่สำคัญที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย เพื่อใช้ในการศึกษา และติดตามแนวโน้มทางด้านความมั่นคงปลอดภัยต่าง ๆ

๓. นโยบายการพัฒนาระบบงาน

วัตถุประสงค์

- เพื่อลดความผิดพลาดในการพิจารณาปรับปรุงระบบงานเพิ่มเติม
- เพื่อให้ระบบงานได้รับการพัฒนา เพื่อให้ประมวลผลหรือคำนวณได้อย่างถูกต้อง และเพื่อให้ข้อมูลนำเข้าและนำออกจากระบบมีความถูกต้องและเชื่อถือได้ รวมทั้งปลอดภัยจากการถูกบุกรุกหรือเจาะระบบโดยผู้ไม่พึงประสงค์
- เพื่อให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อกำหนดหรือคุณลักษณะของระบบที่กำหนดไว้
- เพื่อให้สามารถตรวจสอบกิจกรรมสำคัญต่าง ๆ ที่เกิดกับระบบงานได้ในภายหลัง
- เพื่อลดความผิดพลาดในการติดตั้งระบบงานและอาจส่งผลให้ระบบหยุดชะงักการทำงาน

ผู้รับผิดชอบ

- ผู้พัฒนาระบบและ/หรือ ผู้ให้บริการภายนอก

อ้างอิงมาตรฐาน

- หมวดที่ ๒ โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร
- หมวดที่ ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

ข้อปฏิบัติ

๑) กรอกแบบคำขอเพื่อขออนุมัติพัฒนาระบบงานใหม่หรือปรับปรุงระบบงานเดิม และปฏิบัติตาม **ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบงาน** ที่ได้กำหนดไว้

๒) วิเคราะห์และประเมินทางเลือกในการพัฒนาระบบงานซึ่งแบ่งเป็น ๕ ทางเลือก ดังนี้

๒.๑) การจัดหาซอฟต์แวร์สำเร็จรูปซึ่งเป็นซอฟต์แวร์ขนาดใหญ่หรือมีความซับซ้อน

๒.๒) การจัดหาซอฟต์แวร์สำเร็จรูปซึ่งเป็นซอฟต์แวร์ขนาดเล็กและไม่มีความซับซ้อน

๒.๓) การจ้างพัฒนาระบบที่มีขนาดเล็กและไม่มีความซับซ้อน

๒.๔) การพัฒนาระบบที่มีขนาดเล็กและไม่มีความซับซ้อนด้วยตนเอง

๒.๕) การจ้างพัฒนาระบบที่มีขนาดใหญ่หรือมีความซับซ้อน

๓) จัดทำสัญญาการจัดซื้อจัดจ้างระบบงานดังนี้

๓.๑) ระบุข้อกำหนดการไม่เปิดเผยความลับหรือข้อมูลสำคัญของหน่วยงานแก่ผู้อื่น

๓.๒) จัดทำเอกสารข้อกำหนดการจ้างงาน (Term of Reference) โดยระบุคุณลักษณะของระบบงานที่ต้องการจัดหาไว้ในเอกสารดังกล่าว

๓.๓) อ้างอิงตามข้อกำหนดต่าง ๆ ที่ระบุไว้ใน

- **ข้อกำหนดที่ควรจัดทำในสัญญาการพัฒนาระบบงาน**
- **ข้อกำหนดที่ควรจัดทำในสัญญาดูแลรักษาฮาร์ดแวร์**
- **ข้อกำหนดที่ควรจัดทำในสัญญาการให้บริการเครือข่าย**

๔) บริหารจัดการโครงการการจ้างพัฒนาระบบงาน ดังนี้

๔.๑) กำหนดให้ผู้ให้บริการภายนอกจัดทำข้อเสนอโครงการเพื่อประกอบการพิจารณาจัดจ้าง หัวข้อที่ควรปรากฏในข้อเสนอโครงการอย่างน้อย ประกอบด้วย

- หลักการและเหตุผล
- วัตถุประสงค์
- เป้าหมายของโครงการ
- ผลสัมฤทธิ์ของโครงการ

- แผนการดำเนินงาน
- ระยะเวลาการดำเนินงาน
- กระบวนการพัฒนาระบบที่ใช้สำหรับโครงการ
- เงื่อนไขทั่วไป
- ทีมผู้พัฒนาระบบและบุคลากรที่มีส่วนร่วมในโครงการและหน้าที่ความรับผิดชอบ
- วิธีการติดตามการดำเนินงานโครงการและความถี่ในการรายงานความคืบหน้า
- ข้อเสนอด้านราคา

๔.๒) กำหนดให้มีการติดตาม ประเมิน และบันทึกความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับโครงการพัฒนาระบบงาน (เช่น บุคลากรในทีมผู้พัฒนาระบบมีการลาออก มีการขอเพิ่มความต้องการการใช้งานระบบ เริ่มมีการใช้งบประมาณมากกว่าที่กำหนดไว้) กำหนดมาตรการลดความเสี่ยงที่พบและประสานงานให้ผู้ที่เกี่ยวข้องไปดำเนินการตามมาตรการลดความเสี่ยงนั้น จนกระทั่งแล้วเสร็จ

๔.๓) ประสานงานกับผู้ใช้งานเพื่อขอให้ยืนยันและรับรองความถูกต้องของระบบงานที่การพัฒนาแล้วเสร็จ

๔.๔) กำหนดให้ผู้ให้บริการภายนอกส่งมอบงานตามรายการสิ่งที่ส่งมอบที่ได้กำหนดไว้ในข้อเสนอโครงการ (เช่น เอกสารความต้องการของระบบ เอกสารการวิเคราะห์และออกแบบระบบ ซอร์สโค้ด แผนการทดสอบ คู่มือการใช้งาน เอกสารฝึกอบรม เอกสารลงนามรับทราบการทดสอบระบบจากผู้ใช้งาน เป็นต้น)

๕) กำหนดความต้องการด้านความมั่นคงปลอดภัยของระบบงาน โดยพิจารณาจากความเสี่ยงที่มีต่อระบบงานและกำหนดมาตรการรองรับหรือลดความเสี่ยงเหล่านั้น (มาตรการรองรับหรือลดความเสี่ยงคือความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบงาน) ความต้องการด้านความมั่นคงปลอดภัยควรครอบคลุมหัวข้อต่อไปนี้

๕.๑) ด้านการตรวจสอบข้อมูลนำเข้าระบบ (Input Data Validation and Verification)

๕.๒) ด้านการบันทึกกิจกรรมต่าง ๆ ที่สำคัญและอาจจำเป็นต้องตรวจสอบในภายหลัง

๕.๓) ด้านกลุ่มผู้ใช้งาน บทบาท และสิทธิการเข้าถึงระบบงาน

๕.๔) ด้านการลงทะเบียนสำหรับการเข้าถึงระบบงาน

๕.๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

๕.๖) ด้านการตัดหรือหมดเวลาการใช้งาน

๕.๗) ด้านการระบุและพิสูจน์ตัวตน

๕.๘) ด้านหน้าจอการล็อกอินที่มีความมั่นคงปลอดภัย

๕.๙) ด้านการป้องกันข้อมูลรหัสผ่านของผู้ใช้งาน

๕.๑๐) ด้านการป้องกันข้อมูลสำคัญที่จัดเก็บไว้ในระบบ

๕.๑๑) ด้านการป้องกันข้อมูลสำคัญที่มีการส่งผ่านเครือข่าย

๕.๑๒) ด้านการสนับสนุนการบริหารจัดการการเข้ารหัสข้อมูล

๖) พัฒนาระบบงานตามที่ได้วิเคราะห์และออกแบบด้านความมั่นคงปลอดภัยไว้

๗) ทดสอบระบบดังนี้

๗.๑) ควบคุมการนำข้อมูลสำคัญมาใช้ในการทดสอบกับระบบทดสอบ

- กรณีข้อมูลส่วนบุคคล ลบข้อมูลส่วนที่สามารถบ่งชี้ตัวบุคคลทิ้งไปก่อนนำข้อมูลนั้นไปใช้ในการทดสอบ เช่น ลบชื่อ-นามสกุลทิ้งไป เป็นต้น

- กรณีข้อมูลลับ ลบข้อมูลส่วนที่เป็นความลับทิ้งไปก่อนนำข้อมูลนั้นไปใช้ในการทดสอบ

๗.๒) จัดทำแผนการทดสอบระบบอย่างน้อยดังนี้
- แผนการทดสอบ Unit Test
- แผนการทดสอบ UAT (User Acceptance Test)
- แผนการทดสอบ System Integration Test

และดำเนินการทดสอบตามแผนที่ได้กำหนดไว้นั้น

๗.๓) ทดสอบข้อมูลนำเข้าระบบให้ครอบคลุมตาม
- รูปแบบของข้อมูลในพจนานุกรมข้อมูล (Data dictionary)
- **แนวทางปฏิบัติในการทดสอบข้อมูลนำเข้า**

๗.๔) จัดทำแผนการทดสอบด้านความมั่นคงปลอดภัยโดยอย่างน้อยให้ครอบคลุมความต้องการด้านความมั่นคงปลอดภัยที่ได้วิเคราะห์และออกแบบไว้ และดำเนินการทดสอบระบบตามแผนที่ได้กำหนดนั้น

๗.๕) ตรวจสอบความถูกต้องของข้อมูลและรายงานต่าง ๆ ในระหว่างที่ทำการทดสอบ และหากพบข้อผิดพลาดให้ตรวจสอบหาสาเหตุและดำเนินการแก้ไข

๘) ปฏิบัติตาม **นโยบายควบคุมการติดตั้งบนระบบให้บริการจริง** ในการติดตั้งระบบงาน

<u>ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบงาน</u>

วัตถุประสงค์

- เพื่อลดความผิดพลาดในการดำเนินการเปลี่ยนแปลงต่อระบบงาน ซึ่งอาจส่งผลให้ระบบเสียหาย ทำงานผิดปกติ หยุดชะงักการทำงาน หรือไม่สามารถให้บริการได้

ผู้รับผิดชอบ

- ผู้บังคับบัญชาของผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

ขั้นตอนปฏิบัติ

๑) เมื่อผู้ใช้งานต้องการพัฒนาระบบงานใหม่ ปรับปรุง เปลี่ยนแปลง หรือแก้ไขระบบงานเดิม ให้มีการทำบันทึกภายในแจ้งเพื่อขอดำเนินการเปลี่ยนแปลงระบบงาน

๒) ประเมินผลกระทบของการเปลี่ยนแปลงนั้นว่ามีผลกระทบมาก (Major) หรือน้อย (Minor) โดยใช้เกณฑ์ดังนี้

๒.๑) ในกรณีที่เป็นการพัฒนาระบบงานใหม่ ให้พิจารณาว่ามีผลกระทบมาก

๒.๒) ในกรณีที่เป็นการปรับปรุงระบบงานเดิมที่ต้องพัฒนาเพิ่มเติม
- ไม่เกินร้อยละ ๑๐ ให้พิจารณาว่ามีผลกระทบน้อย
- เกินกว่าร้อยละ ๑๐ ให้พิจารณาว่ามีผลกระทบมาก

๒.๓) ในกรณีที่เป็นการแก้ไขข้อผิดพลาดในระบบงาน และ
- การแก้ไขค่อนข้างซับซ้อนและมีปริมาณงานมาก ให้พิจารณาว่ามีผลกระทบมาก
- กรณีอื่น ๆ ให้พิจารณาว่ามีผลกระทบน้อย

สำหรับการเปลี่ยนแปลงที่มีผลกระทบมาก (ยกเว้นการพัฒนาระบบงานใหม่) ให้จัดเตรียมแผนถอยหลังกลับด้วย (ในกรณีที่ทำไม่สำเร็จ จะได้กลับไปใช้เวอร์ชั่น (Version) ก่อนการเปลี่ยนแปลงได้)

๓) ประเมินความเร่งด่วนว่ามีความเร่งด่วน (Urgent) หรือปกติ (Normal) โดยใช้เกณฑ์ ดังนี้

๓.๑) ในกรณีที่เป็นการพัฒนาระบบงานใหม่ ให้พิจารณาว่าปกติ

๓.๒) ในกรณีที่เป็นการปรับปรุงระบบงานเดิม และ

- ระบบงานนั้นสอดคล้องกับโครงการตามแผนวิสาหกิจหรือแผนแม่บทเทคโนโลยีสารสนเทศสำหรับปีงบประมาณนั้น ให้พิจารณาว่าปกติว่ามีความเร่งด่วน
- กรณีอื่น ๆ ให้พิจารณาว่าปกติ

๓.๓) ในกรณีที่เป็นการแก้ไขข้อผิดพลาดในระบบงาน และ

- หากไม่ดำเนินการโดยทันที ระบบจะทำงานผิดพลาดหรือไม่สามารถทำงานได้ ให้พิจารณาว่ามีความเร่งด่วน
- กรณีอื่น ๆ ให้พิจารณาว่าปกติ

๔) อนุมัติการขอดำเนินการนั้น

๕) จัดลำดับความสำคัญว่าการขออนุมัติใดที่ต้องทำก่อนหลังเรียงตามลำดับ

๖) จัดให้ทีมผู้พัฒนาระบบวางแผนดำเนินการพัฒนาหรือปรับปรุงระบบงาน

๗) เมื่อทีมผู้พัฒนาระบบได้ดำเนินการแล้วเสร็จ จะต้องบันทึกข้อมูลต่อท้ายลงในบันทึกภายในขอเปลี่ยนแปลง ดังกล่าวในส่วนการปฏิบัติด้วย

๘) การพัฒนา/แก้ไขระบบงาน ในกรณีที่ผู้พัฒนาระบบมีความจำเป็นต้องใช้รหัสผ่านร่วมกันในการเข้าถึงฐานข้อมูล ให้แจ้งเหตุผลความจำเป็นพร้อมขออนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาระดับสำนัก/กอง ขึ้นไป

<u>แนวทางปฏิบัติในการทดสอบข้อมูลนำเข้า</u>

วัตถุประสงค์

- เพื่อให้ข้อมูลนำเข้าและนำออกจากระบบมีความถูกต้องและเชื่อถือได้
- เพื่อให้ระบบงานทำการประมวลผลหรือคำนวณได้อย่างถูกต้อง

ผู้รับผิดชอบ

- ผู้พัฒนาระบบและ/หรือผู้ให้บริการภายนอก

อ้างอิงมาตรฐาน

- หมวดที่ ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

แนวทางปฏิบัติ

๑) ทดสอบข้อมูลนำเข้าระบบงานดังนี้

๑.๑) ข้อมูลนำเข้าตรงหรือสอดคล้องกับชนิดของข้อมูลตามที่ต้องการหรือไม่

๑.๒) ข้อมูลนำเข้าอยู่ภายในค่าขอบเขตบนและล่างตามที่ต้องการหรือไม่

๑.๓) ข้อมูลนำเข้ามีการขาดหายบางส่วนหรือไม่ครบถ้วนหรือไม่

๑.๔) ข้อมูลนำเข้ามีการใส่ตัวอักษรหรืออักขระที่ไม่ถูกต้องหรือไม่

๑.๕) ข้อมูลนำเข้าไม่ได้มีการระบุค่าคีย์ (Key) หรือไม่

๑.๖) ข้อมูลนำเข้ามีการซ้ำซ้อนกันหรือไม่

<u>มาตรฐานทางด้านความมั่นคงปลอดภัยในการพัฒนาระบบงาน</u>

วัตถุประสงค์

- เพื่อกำหนดมาตรฐานขั้นต่ำของการพัฒนาระบบงานเพื่อให้ระบบงานมีความมั่นคงปลอดภัยจากการถูกเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต หรือจากการถูกบุกรุกระบบ

ผู้รับผิดชอบ

- ผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๗ การควบคุมการเข้าถึง
- หมวดที่ ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

ข้อปฏิบัติ

๑) ให้ระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Requirement) ในการพัฒนาระบบงาน เช่น การเข้ารหัสข้อมูลที่มีการรับส่งระหว่างเครื่องลูกข่ายกับเครื่องคอมพิวเตอร์แม่ข่าย การกำหนดสิทธิในการใช้งานตามความจำเป็น การกำหนดผู้ใช้งานมีการตั้งรหัสผ่านที่ความเข้มแข็ง เป็นต้น โดยอ้างอิงระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๒) ให้พัฒนาระบบงานเพื่อให้มีหน้าจอสำหรับผู้ดูแลระบบงาน ให้สามารถบันทึกและปรับปรุงสิทธิของผู้ใช้งานได้ รวมทั้งต้องสามารถบันทึกสิทธิดังกล่าวลงเก็บไว้ในฐานข้อมูลได้ด้วย

๓) ให้พัฒนาระบบงานเพื่อให้ผู้ใช้งานสามารถกำหนดรหัสผ่านที่มีความปลอดภัยตาม **นโยบายการตั้งรหัสผ่าน** ได้แก่ การกำหนดความยาว และระยะเวลาการเปลี่ยนรหัสผ่าน

๔) ให้พัฒนาระบบงาน ให้การล็อกอิน (Log in) ของผู้ใช้งานเข้าสู่ระบบงานมีความปลอดภัย โดยปฏิบัติตามแนวทางดังนี้

๔.๑) ไม่แสดงรายละเอียดของระบบจนกว่าจะล็อกอิน (Log in) สำเร็จ

๔.๒) ไม่มีหรือไม่แสดงฟังก์ชั่น (Function) ให้การช่วยเหลือในระหว่างที่ทำการล็อกอิน (Log in)

๔.๓) บันทึกความพยายามในการล็อกอิน (Log in) ทั้งที่สำเร็จและไม่สำเร็จ และแสดงประวัติการล็อกอิน (Log in) ๓ ครั้งล่าสุด

๔.๔) ตัดการเชื่อมต่อหลังจากที่ทำการล็อกอิน (Log in) ไม่สำเร็จเกินกว่า ๓ ครั้ง

๔.๕) เมื่อมีการใส่ข้อมูลบัญชีผู้ใช้งานและรหัสผ่านที่ไม่ถูกต้อง ให้แสดงข้อความรวม ๆ เช่น “ข้อมูลการล็อกอิน (Log in) ไม่ถูกต้อง”

๔.๖) ให้แสดงข้อความเตือนที่หน้าจอ ภายหลังจากการล็อกอิน (Log in) เสร็จสิ้น ข้อความเตือนดังกล่าว ได้แก่ “ระบบนี้เป็นระบบที่เป็นสินทรัพย์ของ กรมการค้าภายใน การใช้งานจะต้องได้รับการอนุมัติก่อนเท่านั้น จึงจะสามารถใช้งานได้ ผู้ที่ไม่ได้รับสิทธิและเข้ามาใช้ระบบงานหากมีการตรวจพบ อาจมีการลงโทษทางวินัย หรือดำเนินการทางกฎหมายตามความเหมาะสม หน่วยงานมีสิทธิในการตรวจสอบพฤติกรรมการใช้งานในระหว่างที่ผู้ใช้งานใช้ระบบงานนี้”

๕) ให้พัฒนาระบบงานเพื่อให้มีการป้องกันข้อมูลโดยการเข้ารหัส ระหว่างเครื่องลูกข่ายกับเครื่องคอมพิวเตอร์แม่ข่าย สำหรับระบบงานที่มีข้อมูลที่มีความสำคัญ เช่น โดยใช้ โปรโตคอล HTTPS โดยอ้างอิงระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๖) สำหรับระบบงานที่มีความสำคัญสูง ให้พัฒนาระบบงานเพื่อให้มีการตัดการเชื่อมต่อทางเครือข่าย เมื่อผู้ใช้งานไม่ได้ใช้งานนานเกินกว่าระยะเวลาหนึ่ง เช่น ๓๐ นาที รวมทั้งแจ้งให้ผู้ใช้งานได้รับทราบว่าระบบงานจะมีการตัดการเชื่อมต่อ เมื่อผู้ใช้งานไม่ได้ใช้งานนานเกินกว่าระยะเวลาดังกล่าว

๔. นโยบายควบคุมการติดตั้งบนระบบให้บริการจริง

วัตถุประสงค์

- เพื่อลดความผิดพลาดในการติดตั้งระบบงาน และอาจส่งผลให้ระบบหยุดชะงักการทำงานหรือไม่สามารถให้บริการได้
- เพื่อให้ระบบที่ติดตั้งมีความมั่นคงปลอดภัย และเสถียรภาพในการทำงานสูง
- เพื่อป้องกันการละเมิดลิขสิทธิ์ของซอฟต์แวร์ที่จะทำการติดตั้ง
- เพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขระบบงานดดยไม่ได้รับอนุญาตและทำให้ระบบงานทำงานไม่ถูกต้อง และอาจเกิดความเสียหายต่อหน่วยงาน

ผู้รับผิดชอบ

- ผู้ดูแลระบบและ/หรือผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร
- หมวดที่ ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

ข้อปฏิบัติ

๑) ปฏิบัติตาม **ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศ** เพื่อขออนุมัติติดตั้งระบบงาน

๒) ในกรณีที่เป็นการติดตั้งระบบเพื่อทดแทนระบบงานเดิม ให้ทำการสำรองข้อมูลที่จำเป็น เช่น ฐานข้อมูล ซอฟต์แวร์ ค่าคอนฟิกกูเรชั่นหรืออื่น ๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งทำไม่สำเร็จ จะได้สามารถถอยหลังกลับไปใช้งานระบบงานเดิมได้

๓) ในกรณีที่มีความจำเป็นต้องเปลี่ยนแปลงข้อมูลในระบบงานเดิมไปสู่ในระบบที่จะทำการติดตั้ง ให้กำหนดแผนการถ่ายโอนหรือแปลงข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ ถ่ายโอนข้อมูลตามแผน ฯ และร่วมกับผู้ใช้งานตรวจสอบว่า ข้อมูลที่มีการถ่ายโอนไปนั้น มีความถูกต้องและครบถ้วนหรือไม่

๔) กำหนดแผนการติดตั้งสำหรับระบบงาน ซึ่งรวมถึงระยะเวลาที่จะดำเนินการ รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า เช่น การติดตั้ง ฮาร์ดแวร์ ซอฟต์แวร์ และอื่น ๆ

๕) สำหรับซอฟต์แวร์ที่จะทำการติดตั้ง

๕.๑) ถ้าเป็นซอฟต์แวร์ที่ขายเชิงพาณิชย์ ต้องเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้อง

๕.๒) ถ้าเป็นซอฟต์แวร์ประเภทฟรีแวร์ (Freeware) หรือแชร์แวร์ (Shareware) ต้องตรวจสอบก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ผู้ผลิตซอฟต์แวร์นั้น

๖) อ่านและปฏิบัติตามเงื่อนไขหรือข้อตกลงการใช้งานซอฟต์แวร์ที่จะทำการติดตั้งอย่างเคร่งครัด

๗) สำหรับการติดตั้งซอฟต์แวร์ยูทิลิตี้ (Utility Software) ต้องตรวจสอบก่อนว่าเป็นซอฟต์แวร์ที่มีการทำงานที่ถูกต้องและเชื่อถือได้

๘) ไม่ติดตั้งโปรแกรมคอมไพเลอร์สำหรับระบบงานบนเครื่องให้บริการ ยกเว้นในกรณีที่ระบบงานต้องเรียกใช้โปรแกรมคอมไพเลอร์ในขณะที่ทำงาน

๙) ไม่ติดตั้งซอร์สโค้ดของระบบงานบนเครื่องให้บริการ ยกเว้นในกรณีที่ระบบงานต้องเรียกใช้ซอร์สโค้ดโดยตรงในขณะที่ทำงาน

๑๐) ติดตั้งโปรแกรมแก้ไขช่องโหว่ต่าง ๆ ที่เกี่ยวข้องกับระบบงานตามความจำเป็น เช่น โปรแกรมแก้ไขช่องโหว่สำหรับระบบปฏิบัติการ โปรแกรมแก้ไขช่องโหว่สำหรับระบบบริหารจัดการฐานข้อมูล เป็นต้น

๑๑)กำหนดค่าพารามิเตอร์ต่าง ๆ มีมีผลต่อความมั่นคงปลอดภัยของระบบงานตาม Sequrity Baseline ที่เกี่ยวข้องกับระบบงานนั้น โดยดำเนินการตาม Sequrity Baseline สำหรับ

๑๑.๑) ระบบปฏิบัติการ Windows

๑๑.๒) ระบบปฏิบัติการ Unit

๑๑.๓) ระบบบริหารจัดการฐานข้อมูล

๑๑.๔) เว็บเซิร์ฟเวอร์

๑๑.๕) อุปกรณ์เครือข่าย

๑๒)ตรวจสอบและปิดบริการ (Service) บนระบบที่ไม่มีความจำเป็นในการใช้งานก่อนเปิดระบบให้บริการ

๑๓)บันทึกและตรวจสอบข้อมูลล็อกของระบบงาน ดังนี้

๑๓.๑) เปิดให้ระบบงานทำการบันทึกข้อมูลล็อกที่จำเป็น สำหรับการตรวจสอบในภายหลัง เช่น ข้อมูลล็อกของระบบปฏิบัติของระบบบริหารจัดการฐานข้อมูล เป็นต้น

๑๓.๒) กำหนดแผนการตรวจสอบข้อมูลล็อกบนระบบงานที่ทำการติดตั้ง โดยปฏิบัติตาม **นโยบายการตรวจสอบข้อมูลล็อกและการดำเนินการแก้ไข** และดำเนินการตรวจสอบข้อมูลล็อกตามแผนที่ได้กำหนดไว้

๑๔)มีการป้องกันไวรัสคอมพิวเตอร์บนระบบงานที่ทำการติดตั้ง

๑๕)จำกัดการเชื่อมต่อทางเครือข่ายเพื่อเข้าสู่ระบบงานที่ทำการติดตั้ง ดังนี้

๑๕.๑) จำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งานในการเข้าถึง หรือใช้งานระบบที่ทำงานติดตั้งให้เป็นไปตาม **นโยบายการควบคุมการเข้าถึง** ของหน่วยงาน

๑๕.๒) กำหนด Routing ที่เหมาะสมบนเครือข่าย เพื่อจำกัดการเข้าถึงระบบงานโดยผู้ใช้งาน

๑๖)จัดเก็บซอร์สโค้ดของระบบงานไว้ในสถานที่ที่มีความปลอดภัย ถ้าจัดเก็บในเครื่องคอมพิวเตอร์ ต้องมีการควบคุมการเข้าถึง เช่น การให้สิทธิเฉพาะผู้เกี่ยวข้องเท่านั้น การใช้รหัสผ่านสำหรับการเข้าถึง เป็นต้น และจัดเก็บไว้อย่างน้อย ๒ เวอร์ชั่นล่าสุด

๕. นโยบายการควบคุมการเข้าถึง

วัตถุประสงค์

- เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายของกรมการค้าภายใน ให้สามารถเข้าถึงเฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- เพื่อป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก
- เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมได้อย่างถูกต้อง

ผู้รับผิดชอบ

- ศูนย์เทคโนโลยีสารสนเทศ
- ผู้ดูแลระบบ/ผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- หมวดที่ ๗ การควบคุมการเข้าถึง
- หมวดที่ ๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

ข้อปฏิบัติ

๑) ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๒) กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๓) ผู้ใช้งานต้องลงนามรับทราบสิทธิ์ และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

๔) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจสอบการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

๕) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๖) ต้องควบคุมการเข้าถึงระบบเครือข่าย โดยแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามลักษณะของการใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น โดยกำหนดเลขที่อยู่ไอพี (IP Address) แบ่งเป็นสัดส่วนตามหน่วยงานภายใน

๗) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน โดยจัดเส้นทางบนเครือข่าย คือ อินเทอร์เน็ต ระบบงานภายในกระทรวง และระบบเครือข่าย GIN

๘) ยุติการใช้งานระบบสารสนเทศนั้น เมื่อว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง (Session Time-out) โดยให้ทุกระบบสารสนเทศหรือแอพพลิเคชั่น มีระยะเวลาว่างเว้นจากการใช้งานไม่เกิน ๓๐ นาที

๙) จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) โดยให้ทุกระบบสารสนเทศหรือแอพพลิเคชั่น มีระยะเวลาสิ้นสุดการเชื่อมต่อไม่เกิน ๑๘๐ นาที

๑๐) กำหนด routing table เพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้

๑๑) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยัง ระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานมีการเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall) รวมทั้งต้องสามารถใช้ในการตรวจจับโปรแกรมไม่พึงประสงค์ได้

๑๒) มีระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบข้อมูลที่มีการเข้าใช้งานผ่านระบบระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๑๓) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการล็อกอิน (Log in) เพื่อตรวจสอบความถูกต้องของผู้ใช้งาน โดยการตรวจสอบกับชื่อผู้ใช้งานที่มีอยู่ในระบบ ว่าเป็นผู้ใช้งานใด และมีสิทธิในการเข้าถึงหรือไม่

๑๔) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๑๕) การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๖. นโยบายการวางแผนเตรียมการสภาพความพร้อมใช้ของระบบงาน

วัตถุประสงค์

- เพื่อกำหนดให้มีการวางแผนเตรียมการสภาพความพร้อมใช้ของระบบงาน
- เพื่อให้ระบบงานมีสภาพความพร้อมใช้ของระบบงาน หรือเกิดการหยุดชะงักในระยะเวลาที่หน่วยงานยอมรับได้

ผู้รับผิดชอบ

- เจ้าของกระบวนการทางธุรกิจ (Business Process Owner)
- ศูนย์เทคโนโลยีสารสนเทศ
- ผู้ดูแลระบบ
- ผู้พัฒนาระบบ
- ผู้ให้บริการภายนอก

อ้างอิงมาตรฐาน

- หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร
- หมวดที่ ๑๐ การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

ข้อปฏิบัติ

๑) ประเมินผลกระทบต่อ Business Process กรณีที่ระบบงานเกิดการหยุดชะงัก และกำหนดระดับความสำคัญของระบบงาน ดังนี้

๑.๑) เจ้าของกระบวนการทางธุรกิจและศูนย์เทคโนโลยีสารสนเทศ ร่วมกันประเมินผลกระทบ หากระบบงานนั้นเกิดการหยุดชะงัก

๑.๒) เมื่อพิจารณาผลกระทบที่เกิดขึ้น เจ้าของกระบวนการทางธุรกิจและศูนย์เทคโนโลยีสารสนเทศร่วมกันกำหนด RTO, RPO และ MTD ของระบบงานนั้น

๑.๓) จากผลการประเมินผลกระทบ ค่า RTO, RPO และ MTD ที่กำหนดไว้ เจ้าของกระบวนการทางธุรกิจและศูนย์เทคโนโลยีสารสนเทศร่วมกันกำหนด

- ระดับความสำคัญของระบบ (ซึ่งแบ่งเป็น ๓ ระดับ คือ ระบบมีความสำคัญมาก/ปานกลาง/น้อย)
- ร้อยละของสภาพความพร้อมใช้ของระบบ
- ระยะเวลาการหยุดชะงักโดยเฉลี่ยต่อครั้ง

๒) ผู้ดูแลระบบออกแบบฮาร์ดแวร์ของระบบงาน โดยคำนึงถึงความทนทาน และความเชื่อถือได้ของฮาร์ดแวร์ ซึ่งจะต้องมีความเหมาะสมกับร้อยละของสภาพความพร้อมใช้ของระบบงานและระยะเวลาการหยุดชะงักโดยเฉลี่ยต่อครั้งตามที่ได้กำหนดไว้

๓) ผู้ดูแลระบบออกแบบฮาร์ดแวร์ของระบบงาน โดยคำนึงการมีทรัพยากรและความรวดเร็วของระบบอย่างเพียงพอ ได้แก่ การมีซีพียู หน่วยความจำ และฮาร์ดดิสก์ในปริมาณและความรวดเร็วที่มากพอต่อการให้บริการ

๔) ผู้ดูแลระบบกำหนดแผนการบำรุงรักษาฮาร์ดแวร์ของระบบงาน โดยพิจารณาประเด็น ดังนี้

- การรับประกันความเสียหายของฮาร์ดแวร์ใหม่
- การตรวจสอบและปรับปรุงสภาพของฮาร์ดแวร์ตามรอบระยะเวลาหนึ่งที่กำหนดไว้

- การกำหนดให้ผู้บริการด้านฮาร์ดแวร์เข้ามาดำเนินการแก้ไขปัญหาตามที่ได้รับแจ้งจากศูนย์เทคโนโลยีสารสนเทศ และ/หรือ
- การทำสัญญาการบำรุงรักษากับผู้ให้บริการด้านฮาร์ดแวร์

๕) ผู้พัฒนาระบบ กำหนดแผนการบำรุงรักษาซอฟต์แวร์/แอพพลิเคชั่น ของระบบงานที่มีความสำคัญอย่างน้อย ๖ เดือนภายหลังการติดตั้งเสร็จ

๖) ผู้ดูแลระบบกำหนดแผนการสำรองข้อมูลของระบบงาน โดยปฏิบัติตาม**นโยบายการสำรองและทดสอบกู้คืนข้อมูล** และดำเนินการสำรองข้อมูลตามแผนที่ได้กำหนดไว้

๗) ผู้พัฒนาระบบ กำหนดแผนการตรวจสอบและติดตามสภาพความพร้อมใช้ของระบบงานและดำเนินการตรวจสอบ และติดตามสภาพความพร้อมใช้ตามแผนที่ได้กำหนดไว้ สำหรับระบบงานที่มีความสำคัญจากมากไปน้อย ให้กำหนดแผนการตรวจสอบและติดตามสภาพความพร้อมใช้ด้วยความถี่ในการตรวจสอบจากสูงไปต่ำ เช่น ระบบงานที่มีความสำคัญมาก ควรมีความถี่ในการตรวจสอบสูงกว่าระบบงานที่มีความสำคัญปานลางและน้อย เป็นต้น

๘) ผู้ดูแลระบบ กำหนดแผนการตรวจสอบและติดตามทรัพยากรของระบบงาน โดยปฏิบัติตาม **นโยบายการจัดการทรัพยากรของระบบ** และดำเนินการตรวจสอบ และติดตามทรัพยากรของระบบงานตามแผนที่ได้กำหนดไว้

๗. นโยบายการลงทะเบียนผู้ใช้งาน

วัตถุประสงค์

- เพื่อควบคุมการเข้าถึงระบบโดยอนุญาตให้เข้าถึงตามความจำเป็นในการใช้งาน
- เพื่อกำหนดมาตรฐานการลงทะเบียนผู้ใช้งานและการบริหารจัดการบัญชีผู้ใช้งาน
- เพื่อกำหนดและทบทวนสิทธิการใช้งานเพื่อให้ได้รับสิทธิตามความจำเป็นในการใช้งาน

ผู้รับผิดชอบ

- ผู้ดูแลระบบและ/หรือผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๗ การควบคุมการเข้าถึง

ข้อปฏิบัติ

๑) ลงทะเบียนผู้ใช้งานก่อนอนุญาตให้เข้าใช้ระบบงานต่าง ๆ ของหน่วยงานโดยให้ขออนุมัติผ่านทาง **แบบคำขอสำหรับลงทะเบียนผู้ใช้งาน**

๒) ตั้งชื่อบัญชีผู้ใช้งานตามมาตรฐานการตั้งชื่อของหน่วยงาน เช่น “รหัสประจำตัวของผู้ขอ”

๓) จัดส่งบัญชีผู้ใช้งานและรหัสผ่านโดยใส่ซองปิดผนึก และประทับตรา “ลับ” ให้ผู้ขอใช้งาน

๔) สร้างบัญชีผู้ใช้งานแยกเป็นรายบุคคล ในกรณีที่มีความจำเป็นต้องมีการใช้งานผู้ใช้งานร่วมกัน ให้ขออนุมัติเป็นกรณี ๆ ไป

๕) กำหนดสิทธิการเข้าใช้ระบบงานให้แก่ผู้ใช้งาน ตามหน้าที่และความรับผิดชอบของผู้ใช้งานนั้น หรือตามความจำเป็นในการเข้าถึง (ทั้งเจ้าหน้าที่และบุคคลภายนอกที่หน่วยงานอนุญาตให้ใช้งาน)

๖) ทบทวนสิทธิการเข้าใช้งานระบบของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

๗) ยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งานกรณีที่ผู้ใช้งานลาออก ปรับเปลี่ยนตำแหน่ง หมดความจำเป็นในการใช้งาน

๘. นโยบายการบริหารจัดการช่องโหว่ของระบบ

วัตถุประสงค์

- เพื่อให้ระบบทำงานอย่างถูกต้อง มีเสถียรภาพเชื่อถือได้ และปลอดภัยจากการถูกบุกรุกหรือโจมตี

ผู้รับผิดชอบ

- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

ข้อปฏิบัติ

๑) ติดตั้งโปรแกรมแก้ไขช่องโหว่ตามความจำเป็นสำหรับช่องโหว่ที่มีผลกระทบต่อการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบงานของหน่วยงาน

๒) จัดให้เครื่องคอมพิวเตอร์ (Personal Computer) และคอมพิวเตอร์พกพา (Notebook computer) ทั้งหมดของผู้ใช้งานติดตั้งโปรแกรมแก้ไขช่องโหว่ให้ครบถ้วน (เช่น โดยการตั้งให้เครื่องดำเนินการเองโดยอัตโนมัติ)

๙. นโยบายการจัดการกับโปรแกรมไม่พึงประสงค์

วัตถุประสงค์

- เพื่อป้องกันข้อมูลในระบบไม่ให้เกิดความเสียหาย
- เพื่อให้มีการจัดการกับปัญหาไวรัสได้อย่างเหมาะสม ได้ผลและทันการณ์
- เพื่อให้ระบบทำงานอย่างถูกต้อง มีเสถียรภาพเชื่อถือได้ และปลอดภัยจากการถูกบุกรุกหรือโจมตี

ผู้รับผิดชอบ

- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ข้อปฏิบัติ

๑) ให้ผู้ใช้งานแจ้งปัญหาการติดไวรัสไปยังผู้ดูแลระบบโดยทันทีที่พบ

๒) ตรวจสอบว่าเครื่องคอมพิวเตอร์แม่ข่ายป้องกันไวรัสยังทำงานตามปกติและมีการปรับปรุงฐานข้อมูลไวรัสหรือไม่ ตรวจสอบอย่างน้อยวันละ ๑ ครั้ง หากพบว่าทำงานผิดปกติ ให้รีบดำเนินการแก้ไข

๓) ตรวจสอบและติดตั้งโปรแกรมป้องกันไวรัสอย่างน้อยสำหรับเครื่องลูกข่ายทั้งหมด เครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบงานที่มีความสำคัญ และเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการจดหมายอิเล็กทรอนิกส์ (Mail Server)

๔) ตรวจสอบโปรแกรมป้องกันไวรัส เพื่อให้ทำงานในลักษณะ Real time scan เมื่อมีการเปิดไฟล์ขึ้นมาใช้งาน โปรแกรมป้องกันไวรัสจะทำการสแกนทันที

๑๐. นโยบายการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัย

วัตถุประสงค์

- เพื่อให้มีการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยและบริหารจัดการรวมทั้งดำเนินการแก้ไขได้อย่างเหมาะสม ได้ผลและทันการณ์
- เพื่อนำผลที่ได้ไปปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยให้ดียิ่งขึ้น

ผู้รับผิดชอบ

- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร
- หมวดที่ ๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

ข้อปฏิบัติ

๑) เมื่อได้รับรายงานเหตุการณ์เกี่ยวกับโปรแกรมไม่พึงประสงค์จากผู้ใช้งาน ให้ปฏิบัติตาม **ขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่พึงประสงค์** เพื่อดำเนินการแก้ไขเหตุการณ์ดังกล่าว

๒) เมื่อได้รับรายงานเหตุการณ์ความมั่นคงปลอดภัยอื่น ๆ ให้ปฏิบัติตาม **ขั้นตอนปฏิบัติสำหรับการจัดการกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย** เพื่อดำเนินการแก้ไขเหตุการณ์ดังกล่าว

<u>ขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่พึงประสงค์</u>

วัตถุประสงค์

- เพื่อให้มีการบริหารจัดการปัญหาไวรัสและดำเนินการแก้ไขได้อย่างเหมาะสม ได้ผล และทันการณ์

ผู้รับผิดชอบ

- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร
- หมวดที่ ๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

ขั้นตอนปฏิบัติ

เมื่อผู้รับผิดชอบได้รับแจ้งจากผู้ใช้งานเกี่ยวกับปัญหาไวรัส ให้ปฏิบัติตามขั้นตอนดังต่อไปนี้

๑) ดำเนินการตรวจสอบเครื่องคอมพิวเตอร์ในเบื้องต้น ด้วยโปรแกรมป้องกันไวรัส ว่าเครื่องคอมพิวเตอร์นั้นติดไวรัสหรือไม่

๒) หากพบว่ามีไวรัสให้ตัดการเชื่อมต่อเครื่องดังกล่าวออกจากระบบเครือข่าย เช่น ถอนสาย LAN ออก เป็นต้น

๓) หากทราบชื่อของไวรัสนั้น ให้เข้าไปที่เว็บไซต์ของผู้ผลิตซอฟต์แวร์ป้องกันไวรัส ที่หน่วยงานใช้งาน เพื่อศึกษาข้อมูลวิธีการแก้ไข หรือดูข้อมูลเพิ่มเติมจากแหล่งข้อมูลที่น่าเชื่อถือรวมทั้งให้ทำการ Download เครื่องมือหรือทูล (Tool) ต่าง ๆ ที่จำเป็นสำหรับการแก้ไข

๔) ศึกษาและวิเคราะห์การทำงานของไวรัสนั้น เช่นมีโปรเซส (Process) แปลกปลอมอะไรบ้างที่ทำงานอยู่ หรือมีไฟล์แปลกปลอมอะไรเพิ่มเติมบ้าง เป็นต้น

๕) ตรวจสอบว่ามีไฟล์ใดบ้างในเครื่องที่ได้รับความเสียหาย เพื่อเตรียมการติดตั้งและกู้คืนไฟล์ดังกล่าว

๖) ในกรณีที่มี Process แปลกปลอมทำงานอยู่ให้หยุดการทำงาน Process นั้น

๗) ติดตั้งโปรแกรมแก้ไขช่องโหว่ตามคำแนะนำของผู้ผลิตซอฟต์แวร์ป้องกันไวรัส

๘) ใช้เครื่องมือฟิกทูล (Fix Tool) ตามคำแนะนำของผู้ผลิตซอฟต์แวร์ป้องกันไวรัส เพื่อทำการแก้ไขเครื่อง

๙) สำหรับไฟล์ที่เสียหาย ให้นำข้อมูลที่สำรองไว้มาติดตั้งกลับคืน

๑๐) หาก Process ที่ได้หยุดการทำงานไว้นั้น มีความจำเป็นต้องใช้งาน ให้เปิดการทำงาน Process นั้นมาอีกครั้ง เมื่อได้รับการแก้ไขปัญหา

๑๑)เชื่อมโยงเครื่องคอมพิวเตอร์ที่ได้รับการแก้ไขแล้ว กลับคืนสู่เครือข่ายเพื่อให้ใช้งานได้ตามปกติ
๑๒)แจ้งให้ผู้ที่เกี่ยวข้องทราบถึงการแก้ไขปัญหาที่ได้ดำเนินการไป รวมทั้งให้คำแนะนำในการระมัดระวังและป้องกันไวรัส

<u>ขั้นตอนปฏิบัติสำหรับการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัย</u>

วัตถุประสงค์

- เพื่อให้มีการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงาน

ผู้รับผิดชอบ

- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

ขั้นตอนปฏิบัติ

เมื่อได้รับแจ้งจากผู้ใช้งานเกี่ยวกับเหตุการณ์ทางด้านความมั่นคงปลอดภัย ให้ปฏิบัติตามขั้นตอนดังนี้

๑) ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้น โดยอ้างอิงตามเกณฑ์ของแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมการค้าภายใน
๒) แจ้งให้ผู้บังคับบัญชาตามลำดับชั้นได้รับทราบ เฉพาะกรณีที่เหตุการณ์นั้นมีผลกระทบตั้งแต่ระดับปานกลาง (Medium) ขึ้นไป
๓) ดำเนินการตามความจำเป็น ตามประเภทของเหตุการณ์ดังนี้
   ๓.๑) สำหรับเหตุการณ์ด้านระบบถูกบุกรุกหรือโจมตี ให้ปรึกษากับผู้ให้บริการภายนอก เพื่อวิเคราะห์เหตุการณ์และดำเนินการแก้ไข
   ๓.๒) สำหรับเหตุการณ์หน้าเว็บไซต์หลักของหน่วยงานถูกเปลี่ยน ให้รายงานผู้บังคับบัญชาของผู้ดูแลระบบ เพื่อขอความเห็นในการดำเนินการ รวมทั้งอาจปรึกษากับผู้ให้บริการภายนอก เพื่อวิเคราะห์และดำเนินการแก้ไข
   ๓.๓) สำหรับเหตุการณ์บุกรุกทางกายภาพของห้อง Data Center ให้รายงานผู้บังคับบัญชาของผู้ดูแลระบบ เพื่อขอความเห็นในการดำเนินการแก้ไข
   ๓.๔) สำหรับซอฟต์แวร์มีจุดอ่อนทำงานผิดปกติ ให้รายงานผู้บังคับบัญชาของผู้พัฒนาระบบและ/หรือผู้ดูแลระบบ เพื่อขอความเห็นในการดำเนินการแก้ไข
   ๓.๕) สำหรับเหตุการณ์การไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัย ให้รายงานผู้บังคับบัญชา เพื่อขอความเห็นในการดำเนินการแก้ไข
   ๓.๖) สำหรับเหตุการณ์อื่น ๆ ให้รายงานผู้บังคับบัญชา เพื่อขอความเห็นในการดำเนินการแก้ไข
๔) บันทึกข้อมูลที่เกี่ยวข้องกับเหตุการณ์ดังกล่าวใน**แบบรายงานเหตุการณ์ทางด้านความมั่นคงปลอดภัย**
๕) ทำรายงานสรุปสำหรับเหตุการณ์ที่มีผลกระทบตั้งแต่ระดบปานกลาง (Medium) ขึ้นไปและแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ

๑๑. นโยบายการจัดการความมั่นคงปลอดภัยสำหรับระบบและเครือข่าย

วัตถุประสงค์

- เพื่อให้ระบบและเครือข่ายมีความมั่นคงปลอดภัย มีเสถียรภาพและความน่าเชื่อถือสูง และมีความปลอดภัยจากการถูกเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต
- เพื่อควบคุมการเข้าถึงระบบบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง
- เพื่อลดความผิดพลาดในการเปลี่ยนแปลงระบบซึ่งอาจส่งผลให้ระบบหยุดชะงักการทำงานหรือไม่สามารถให้บริการได้
- เพื่อให้การปฏิบัติที่มีการสอดคล้องกับกฎหมาย พ.ร.บ. หรือข้อบังคับภายนอกอื่น ๆ ที่ได้กำหนดไว้

ผู้รับผิดชอบ

- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร
- หมวดที่ ๗ การควบคุมการเข้าถึง
- หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

ข้อปฏิบัติ

๑) จัดทำและปรับปรุงเครื่องคอมพิวเตอร์แม่ข่ายพร็อกซี่ (Proxy) เพื่อช่วยลดปริมาณข้อมูลในเครือข่าย

๒) จำกัดการเข้าถึงระบบและอุปกรณ์เครือข่ายสำคัญเพื่อให้การเข้าถึงนั้นจะต้องมาจากอุปกรณ์ ระบบหรือสถานที่ที่ได้รับอนุญาตแล้วเท่านั้น

๓) ตรวจสอบและปิดพอร์ต (Port) ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ

๔) ปรับปรุงผังเครือข่ายและการระบุอุปกรณ์บนระบบเครือข่ายให้มีความทันสมัยอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง โดยใช้เลขที่อยู่ไอพี และชื่อโฮสต์ (Hostname) ในการระบุอุปกรณ์บนระบบเครือข่าย (equipment identification in networks)

๕) จัดทำและปรับปรุงระบบสำหรับการพิสูจน์ตัวตนก่อนเข้าใช้ระบบสำคัญต่าง ๆ เพื่อให้มีความมั่นคงปลอดภัยมากขึ้น โดยมีข้อมูลของชื่อผู้ใช้งาน ชื่อ-สกุลของผู้ใช้งาน หน่วยงานหรือบริษัทที่สังกัด และสิทธิการใช้งาน และมีการบันทึกลงข้อมูลล็อก (Event Log) เพื่อให้สามารถตรวจสอบย้อนหลังได้

๖) ตรวจสอบและจัดแบ่งเครือข่ายของหน่วยงานให้มีความมั่นคงปลอดภัยโดยแบ่งเครือข่ายแยกตามสำนัก/กองของกรมการค้าภายใน

๗) ตรวจสอบและจำกัดการเชื่อมต่อทางเครือข่ายโดยผ่านทางอุปกรณ์เครือข่ายเพื่อให้เป็นไปตาม**นโยบายการควบคุมการเข้าถึง**ของหน่วยงาน

๘) ตรวจสอบและกำหนดเส้นทางบนเครือข่ายให้เหมาะสมโดยอุปกรณ์ทางเครือข่าย เพื่อควบคุมการเชื่อมต่อทางเครือข่ายให้เป็นไปตาม**นโยบายควบคุมการเข้าถึง**

๙) เฝ้าระวัง ติดตาม และตรวจสอบการทำงานของระบบหรืออุปกรณ์ต่าง ๆ อย่างสม่ำเสมอ เพื่อป้องกันกิจกรรมที่ไม่ได้รับอนุญาตหรือการเข้าถึงโดยไม่ได้รับอนุญาต

๑๐) ตรวจสอบและตั้งเวลาของระบบหรืออุปกรณ์ต่าง ๆ ให้ถูกต้องตามเวลามาตรฐานสากล (Stratum ๐)

๑๑) กรอกแบบคำขอเพื่อขออนุมัติดำเนินการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศต่าง ๆ และปฏิบัติตาม**ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศ**ที่ได้กำหนดไว้

๑๒)ห้ามเปิดช่องทางการเชื่อมต่อทางเครือข่ายจากภายนอกเข้าสู่เครือข่ายภายในหน่วยงาน เพื่อให้สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบงานได้จากระยะไกล ยกเว้นในกรณีที่มีความจำเป็น หรือมีความเร่งด่วนสูง ซึ่งจะต้องได้รับอนุมัติจากผู้มีบังคับบัญชาก่อนการดำเนินการ รวมทั้งต้องใช้วิธีการที่มีความปลอดภัยที่เป็นมาตรฐานสำหรับการเชื่อมต่อจากระยะไกลที่หน่วยงานกำหนดไว้ หลังจากที่สิ้นสุดการใช้งาน ให้ทำการปิดช่องทางการเชื่อมต่อนั้นโดยทันที

๑๓)การเชื่อมต่อทางเครือข่ายจากภายนอกเข้าสู่เครือข่ายภายในหน่วยงาน เพื่อให้สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบงานได้จากระยะไกล จำเป็นต้องมีการล็อกอิน (Log in) เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อน โดยระบบจะตรวจสอบชื่อผู้ใช้งานกับข้อมูลที่มีอยู่ในระบบ ว่าเป็นผู้ใช้งานใด และมีสิทธิในการเข้าถึงหรือไม่ จึงจะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้ และทำการบันทึกลงข้อมูลล็อก (Event Log)

<u>ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศ</u>

วัตถุประสงค์

- เพื่อลดความผิดพลาดในการดำเนินการเปลี่ยนแปลงต่อโครงสร้างพื้นฐานสารสนเทศ ซึ่งอาจส่งผลให้ระบบเสียหาย ทำงานผิดปกติ หยุดชะงักการทำงาน หรือไม่สามารถให้บริการได้

ผู้รับผิดชอบ

- ผู้บังคับบัญชาของผู้ดูแลระบบและ/หรือผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ขั้นตอนปฏิบัติ

๑) หารือกับผู้ดูแลระบบและ/หรือผู้พัฒนาระบบ เกี่ยวกับการติดตั้งหรือปรับปรุงโครงสร้างพื้นฐานดังกล่าว

๒) จัดหมวดหมู่ของการเปลี่ยนแปลงนั้นว่าเป็นการเปลี่ยนแปลงชนิดใด ซึ่งประกอบด้วย

๒.๑) การเปลี่ยนแปลงที่เกี่ยวข้องกับระบบงาน

๒.๒) การเปลี่ยนแปลงกับอุปกรณ์เครือข่าย (เช่น กำแพงไฟ (Firewall) เราท์เตอร์ (Router) ระบบป้องกันการบุกรุก เป็นต้น)

๓) ประเมินผลกระทบของการเปลี่ยนแปลงนั้นว่ามีผลกระทบมาก (Major) หรือน้อย (Minor) ในกรณีที่เป็นการเปลี่ยนแปลงดังนี้ ให้พิจารณาว่ามีผลกระทบมาก

๓.๑) ติดตั้ง/ปรับปรุงฮาร์ดแวร์ของระบบงานสำคัญ

๓.๒) ติดตั้ง/ปรับปรุงซอฟต์แวร์ต่าง ๆ บนระบบงานสำคัญ ซึ่งรวมถึงระบบปฏิบัติการ ระบบบริหารจัดการฐานข้อมูล การติดตั้งโปรแกรมแก้ไขช่องโหว่

๓.๓) ติดตั้งระบบงานสำคัญ

๓.๔) ปรับปรุงโครงสร้างของฐานข้อมูลของระบบงานสำคัญ

๓.๕) ติดตั้ง/ปรับปรุงกำแพงไฟ (Firewall) เราท์เตอร์ (Router) หรือระบบป้องกันการบุกรุก

สำหรับการเปลี่ยนแปลงอื่น ๆ ให้พิจารณาผลกระทบเป็นกรณีไป โดยใช้เกณฑ์ดังนี้

๓.๖) การเปลี่ยนแปลงที่มีขั้นตอนการดำเนินการที่มากหรือซับซ้อน หรือใช้เวลาเกินกว่า ๓ ชั่วโมง หรือมีผลกระทบกับผู้ใช้งานเป็นจำนวนมาก ให้พิจารณาว่ามีผลกระทบมาก

๓.๗) กรณีอื่น ๆ ให้พิจารณาว่ามีผลกระทบน้อย

สำหรับการเปลี่ยนแปลงที่มีผลกระทบมากต้องให้ผู้ขอเปลี่ยนแปลงจัดทำแผนการถอยหลังกลับ (ในกรณี

ที่ทำไม่สำเร็จ จะได้กลับไปใช้เวอร์ชั่น (Version) ก่อนการเปลี่ยนแปลงได้)

๔) ประเมินความเร่งด่วนว่ามีความเร่งด่วน (Urgent) หรือปกติ (Normal) โดยใช้เกณฑ์ดังนี้

๔.๑) หากเป็นการเปลี่ยนแปลงที่ต้องดำเนินการภายใน ๒ วันทำการ ซึ่งรวมถึงการเปลี่ยนแปลงที่ต้องทำอย่างฉุกเฉิน เช่น อุปกรณ์/เครื่องคอมพิวเตอร์แม่ข่ายสำคัญเสีย ให้พิจารณาว่ามีความเร่งด่วน

๔.๒) หากสามารถดำเนินการได้หลังจาก ๒ วันทำการ ให้พิจารณาว่าปกติ

๕) ในกรณีที่เป็นการเปลี่ยนแปลงเร่งด่วน ให้ผู้ขอเปลี่ยนแปลงแจ้งผู้บังคับบัญชาของผู้ดูแลระบบก่อนเข้าไปทำการเปลี่ยนแปลง หลังจากนั้นจึงทำเอกสารขออนุมัติทำการเปลี่ยนแปลงเข้ามาในภายหลัง

๖) อนุมัติการขอดำเนินการนั้น

๗) จัดลำดับความสำคัญว่าการขออนุมัติใดที่ต้องทำก่อนหลังเรียงตามลำดับ

๘) จัดให้ผู้ขอเปลี่ยนแปลงวางแผนดำเนินการเปลี่ยนแปลงนั้น

๙) บันทึกข้อมูลข้างต้นทั้งหมดลงในแบบคำขออนุมัติเปลี่ยนแปลง

โครงสร้างพื้นฐานสารสนเทศที่ควบคุม

โครงสร้างพื้นฐานสารสนเทศที่ต้องควบคุมเมื่อจะดำเนินการติดตั้ง เปลี่ยนแปลง แก้ไข หรือปรับปรุง ประกอบด้วย

๑) ระบบงานสำคัญทั้งหมด

๒) ฮาร์ดแวร์ (Hardware) ของระบบงานสำคัญ

๓) ซอฟต์แวร์ (Software) ต่าง ๆ บนระบบงานสำคัญ ซึ่งรวมถึงระบบปฏิบัติการ ระบบบริหารจัดการฐานข้อมูล การติดตั้งโปรแกรมแก้ไขช่องโหว่

๔) ฐานข้อมูลของระบบงานสำคัญ

๕) ระบบเครือข่าย (Network)

๖) กำแพงไฟ (Firewall) เราท์เตอร์ (Router)

๗) ระบบป้องกันการบุกรุก

๑๒. นโยบายการจัดการทรัพยากรของระบบ

วัตถุประสงค์

- เพื่อให้ระบบงานหรืออุปกรณ์มีทรัพยากรที่เพียงพอต่อการให้บริการอย่างต่อเนื่อง
- เพื่อให้ระบบงานหรืออุปกรณ์ทำงานอย่างรวดเร็วและมีประสิทธิภาพเพียงพอ

ผู้รับผิดชอบ

- ผู้บังคับบัญชาของผู้ดูแลระบบและ/หรือผู้พัฒนาระบบ
- ผู้ดูแลระบบและ/หรือผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ข้อปฏิบัติ

๑) จัดทำแผนการตรวจสอบและติดตามทรัพยากรของระบบ ดังนี้

๑.๑) กำหนดประเภทของข้อมูลที่ใช้ในการตรวจสอบและติดตามการใช้ทรัพยากรของระบบ เช่น ร้อยละของการใช้ซีพียู ร้อยละของการใช้หน่วยความจำ ร้อยละของการใช้พื้นที่ฮาร์ดดิสก์ และร้อยละของปริมาณการใช้เครือข่าย เป็นต้น

๑.๒) กำหนดค่าปริมาณการใช้ทรัพยากรสูงสุดบนระบบที่ยอมรับได้

๑.๓) กำหนดความถี่ในการเข้าตรวจสอบปริมาณการใช้ทรัพยากรของระบบ (สำหรับระบบที่มีความถี่ในการตรวจสอบจากสูงไปต่ำ เช่น ระบบที่มีความสำคัญมากควรมีความถี่ในการตรวจสอบสูงกว่าระบบที่มีความสำคัญปานกลางและน้อย เป็นต้น)

๒) ติดตามและตรวจสอบทรัพยากรของระบบตามแผนฯ ที่ได้กำหนดไว้เพื่อดูว่ายังมีทรัพยากรเพียงพอต่อการให้บริการหรือไม่ รวมทั้งบันทึกข้อมูลผลการติดตามนั้นไว้ด้วย

๓) รายงานข้อมูลผลการติดตามการใช้ทรัพยากรของระบบ (เช่น สถิติปริมาณการใช้ซีพียู หน่วยความจำ ฮาร์ดดิสก์ และปริมาณเครือข่าย) ให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ

๔) ประเมินความต้องการทรัพยากรของระบบที่ต้องการเพิ่มเติมเพื่อนำไปใช้ในการวางแผนปรับปรุงประสิทธิภาพและขีดความสามารถของระบบต่อไป

๑๓. นโยบายการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงาน

วัตถุประสงค์

- เพื่อให้ข้อมูลที่แลกเปลี่ยนกันมีความมั่นคงปลอดภัย ถูกต้อง เชื่อถือได้ รวมทั้งป้องกันความเสียหายและการเข้าถึงโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้บริหารสูงสุด

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ข้อปฏิบัติ

๑) จัดทำมาตรการป้องกันข้อมูลสำคัญที่มีการแลกเปลี่ยนกันระหว่างหน่วยงานอย่างเป็นทางการโดยกล่าวถึงประเด็นสำคัญดังนี้

๑.๑) ขอบเขตของการป้องกัน

๑.๒) วัตถุประสงค์ในการป้องกัน

๑.๓) ความจำเป็นในการป้องกัน

๑.๔) ชนิดของข้อมูลที่แลกเปลี่ยนกันและชั้นความลับ เป็นต้น

๑๔. นโยบายการสำรองและทดสอบกู้คืนข้อมูล

วัตถุประสงค์

- เพื่อให้มีข้อมูลสำรองไว้ใช้สำหรับระบบต่าง ๆ ในกรณีข้อมูลหลักเกิดความเสียหายหรือไม่สามารถใช้งานหรือเข้าถึงได้
- เพื่อให้มั่นใจได้ว่าข้อมูลที่สำรองไว้สำหรับระบบเหล่านั้นสามารถใช้งานได้จริง

ผู้รับผิดชอบ

- ผู้บังคับบัญชาของผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ข้อปฏิบัติ

๑) กำหนดระบบที่มีความสำคัญ

๒) กำหนดผู้รับผิดชอบในการสำรองข้อมูล

๓) กำหนดชนิดของข้อมูลของระบบเหล่านั้นที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อยต้องประกอบด้วย
   ๓.๑) ข้อมูลการตั้งค่า (Configuration) สำหรับระบบ
   ๓.๒) ข้อมูลคู่มือการปฏิบัติงานสำหรับระบบ
   ๓.๓) ข้อมูลในฐานข้อมูลของระบบงาน (กรณีที่เป็นระบบงาน)
   ๓.๔) ข้อมูลซอฟต์แวร์ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงานและซอฟต์แวร์อื่น ๆ เป็นต้น
๔) กำหนดความถี่ในการสำรองข้อมูลสำหรับระบบเหล่านั้น (ระบบที่มีการเปลี่ยนแปลงข้อมูลบ่อยควรมีความถี่ในการสำรองข้อมูลสูง)
๕) จัดทำหรือปรับปรุงขั้นตอนปฏิบัติในการสำรองและกู้คืนข้อมูล โดยให้มีการปฏิบัติตาม**แนวทางปฏิบัติสำหรับการสำรองและทดสอบกู้คืนข้อมูล**

<u>แนวทางปฏิบัติสำหรับการสำรองและทดสอบกู้คืนข้อมูล</u>

วัตถุประสงค์

- เพื่อให้มีการปฏิบัติเพื่อสำรองข้อมูลของระบบต่าง ๆ รวมทั้งทดสอบข้อมูลที่สำรองไว้นั้นอย่างสม่ำเสมอ

ผู้รับผิดชอบ

- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

แนวทางปฏิบัติ

๑) สำรองข้อมูลตามความถี่ที่กำหนดไว้
๒) ตรวจสอบว่าการสำรองที่เกิดขึ้นนั้นสำเร็จครบถ้วนหรือไม่ หากไม่สำเร็จ ให้หาสาเหตุ ดำเนินการแก้ไขและดำเนินการใหม่อีกครั้งหนึ่ง
๓) นำข้อมูลที่สำรองไว้นั้นไปเก็บไว้ทั้งในและนอกสถานที่อย่างน้อยอย่างละ ๑ ชุด
๔) ทดสอบกู้คืนข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมออย่างน้อยปีละ ๒ ครั้ง เพื่อดูว่าข้อมูลยังคงสามารถใช้งานได้ตามปกติหรือไม่

๑๕. นโยบายการสร้างความมั่นคงปลอดภัยทางกายภาพสำหรับพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย

วัตถุประสงค์

- เพื่อควบคุมและจำกัดการเข้าถึงทางกายภาพสำหรับพื้นที่ที่มีความสำคัญ
- เพื่อป้องกันสินทรัพย์ในพื้นที่ที่มีความสำคัญไม่ให้เกิดความเสียหาย ถูกเข้าถึงโดยไม่ได้รับอนุญาตหรือถูกขโมย

ผู้รับผิดชอบ

- ผู้ดูแลระบบและ/หรือผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ข้อปฏิบัติ

๑) ห้ามนำบุคคลภายนอกเข้าไปในห้อง Data Center โดยไม่มีกิจที่จำเป็น
๒) ให้เปลี่ยนรองเท้าที่เตรียมไว้หน้าห้องก่องเข้าห้อง Data Center

๓) ห้ามนำอาหาร และเครื่องดื่มเข้าไปในบริเวณห้อง Data Center
๔) สำรวจและติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) เพิ่มเติมความจำเป็น เช่น ในกรณีที่เป็นมุมอับรวมทั้งตรวจสอบการทำงานของกล้องให้มีการทำงานอย่างถูกต้อง ต่อเนื่องและให้สามารถเก็บภาพได้ในมุมกว้าง และไม่มีสิ่งกีดขวาง
๕) บันทึกและจัดเก็บภาพของกล้องโทรทัศน์วงจรปิดตามความจำเป็น (เช่น เก็บไว้อย่างน้อย ๑ เดือน) เพื่อใช้ในการตรวจสอบในภายหลัง
๖) ตรวจสอบประตูทางเข้า-ออกและหน้าต่างของห้อง Data Center ให้ปิดล็อก (Lock) อยู่เสมอ
๗) ผู้ให้บริการภายนอกจะต้องระมัดระวัง สอดส่องและดูแลสินทรัพย์สารสนเทศที่ได้รับมอบ เพื่อใช้งานจนกระทั้งเสร็จสิ้นงาน
๘) ตรวจสอบ และปรับปรุงข้อมูลรายชื่อผู้มีสิทธิเข้า-ออกห้อง Data Center ให้มีความถูกต้อง และทันสมัยอย่างน้อยปีละ ๑ ครั้ง
๙) ตรวจสอบห้องตู้ Data Center สายสัญญาณสื่อสารให้มีการปิดล็อก (Lock) อยู่เสมอ
๑๐)ตรวจสอบตู้ Rack คอมพิวเตอร์ให้มีการล็อก (Lock) อยู่เสมอ
๑๑)ให้ดูแลความสะอาด และความเป็นระเบียบเรียบร้อยของห้อง Data Centerอย่างสม่ำเสมอ
๑๒)จัดทำและปรับปรุงผังพื้นที่ห้อง Data Center ให้ทันสมัย อย่างน้อยปีละ ๑ ครั้ง

๑๖.นโยบายการป้องกันภัยคุกคามทางด้านสิ่งแวดล้อม

วัตถุประสงค์

- เพื่อป้องกันภัยคุกคามทางด้านสิ่งแวดล้อม เช่น ไฟไหม้ น้ำท่วม หรืออื่น ๆ ซึ่งอาจเป็นผลให้เกิดความเสียหายต่อสินทรัพย์สารสนเทศของหน่วยงาน

ผู้รับผิดชอบ

- ผู้บังคับบัญชา

อ้างอิงมาตรฐาน

- หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ข้อปฏิบัติ

๑) ตรวจสอบการทำงานของอุปกรณ์ดับเพลิงอย่างน้อยปีละ ๑ ครั้ง ว่ายังใช้งานได้เป็นปกติหรือไม่
๒) ตรวจสอบการทำงานของอุปกรณ์ตรวจน้ำรั่วซึมอย่างน้อยปีละ ๑ ครั้ง ว่ายังใช้งานได้เป็นปกติหรือไม่
๓) ประเมินสภาพแวดล้อมของห้อง Data Centerอย่างน้อยปีละ ๑ ครั้ง และปรับปรุงตามความจำเป็น

๑๗.นโยบายการป้องกันระบบ อุปกรณ์และสายสัญญาณต่าง ๆ

วัตถุประสงค์

- เพื่อป้องกันระบบอุปกรณ์ และสายสัญญาณต่าง ๆ ให้มีความปลอดภัยและสามารถทำงานได้อย่างต่อเนื่องไม่ติดขัด

ผู้รับผิดชอบ

- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ข้อปฏิบัติ

๑) การจัดวางเครื่องคอมพิวเตอร์ อุปกรณ์สื่อสาร หรือสินทรัพย์อื่น ๆ ไว้ในบริเวณที่มีความปลอดภัย ระมัดระวังการจัดตั้งอุปกรณ์ให้อยู่ในสภาพที่มั่นคง และไม่ล้ม หรือโอนเอียงได้โดยง่าย

๒) ตรวจสอบและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย หรือสินทรัพย์อื่น ๆ ที่มีความสำคัญอย่างสม่ำเสมอ

๓) จัดทำหรือต่อสัญญาการบำรุงรักษาห้อง Data Center เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์สำรองไฟฟ้า (UPS) เครื่องปรับอากาศและอุปกรณ์เครือข่ายที่มีความสำคัญให้ครบถ้วน

๔) จัดให้ระบบงาน เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่มีความสำคัญต้องมีระบบกระแสไฟฟ้าสำรองสนับสนุนการทำงานอย่างครบถ้วน

๕) ในการเดินสายสัญญาณสื่อสารแบบถาวร ต้องเดินสายอย่างเป็นระเบียบเรียบร้อยไม่เกะกะ ขวางทาง และมีการร้อยสายเข้าไปในท่อเพื่อป้องกันความเสียหาย

๖) ตรวจสอบและจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย พร้อมทั้งจัดทำป้ายกำกับ (Label) ของสายสัญญาณเหล่านั้นให้ครบถ้วน

๗) ตรวจสอบสภาพการทำงานของอุปกรณ์สนับสนุนการทำงานของระบบคอมพิวเตอร์ ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ ได้แก่

๗.๑) ระบบกระแสไฟฟ้า

๗.๒) ระบบการควบคุมความชื้น

๗.๓) ระบบการระบายอากาศ

๗.๔) ระบบการปรับอุณหภูมิ

๗.๕) ระบบกระแสไฟฟ้าสำรอง

๗.๖) ระบบสำรองไฟฟ้า (UPS) เป็นต้น

๑๘. นโยบายการตรวจสอบข้อมูลล็อกและการดำเนินการแก้ไข

วัตถุประสงค์

- เพื่อตรวจจับ ป้องกัน และแก้ไขกิจกรรมการประมวลผลของระบบที่ทำงานผิดปกติหรือไม่ถูกต้อง เกิดความผิดพลาดในระหว่างที่ทำงาน มีลักษณะเป็นการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือมีลักษณะเป็นการโจมตีหรือบุกรุกระบบ ซึ่งอาจทำให้ระบบเกิดความเสียหายหรือไม่สามารถให้บริการได้
- เพื่อให้มีการดำเนินการจัดการ แก้ไข หรือป้องกันที่เกี่ยวข้องกับเหตุการณ์ที่เกิดขึ้นนั้นอย่างทันการณ์และได้ผล

ผู้รับผิดชอบ

- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ข้อปฏิบัติ

๑) กำหนดแผนการตรวจสอบข้อมูลล็อกบนระบบ เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายที่มีความสำคัญ ประกอบด้วย

- เหตุการณ์ที่ต้องตรวจสอบ

- ความถี่ในการตรวจสอบ เช่น รายวัน สัปดาห์
- ชื่อไฟล์ที่มีข้อมูลล็อกที่เกี่ยวข้องกับเหตุการณ์
- ระยะเวลาในการจัดเก็บไฟล์ที่มีข้อมูลล็อก
- ผู้รับผิดชอบดำเนินการตรวจสอบ

๒) ดำเนินการตรวจสอบเหตุการณ์ต่าง ๆ ในข้อมูลล็อกตามแผนและความถี่ที่กำหนดไว้

๓) ดำเนินการจัดการหรือแก้ไขเหตุการณ์ที่พบนั้นตามความเหมาะสม บันทึกเหตุการณ์และวิธีการจัดการหรือแก้ไข และรายงานให้ผู้บังคับบัญชาได้รับทราบสำหรับกรณีที่เหตุการณ์ที่พบมีผลกระทบสูง

๔) ทบทวนและปรับปรุงแผนการตรวจสอบข้อมูลล็อกตามความจำเป็นอย่างน้อยปีละ ๑ ครั้ง

๑๙.นโยบายการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Log) ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี ๒๕๕๐

วัตถุประสงค์

- เพื่อให้มีการปฏิบัติที่สอดคล้องกับกฎหมาย พ.ร.บ. หรือข้อบังคับภายนอกอื่น ๆ ที่ได้กำหนดไว้
- เพื่อจำกัดการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Log) โดยผู้ที่รับผิดชอบเท่านั้น

ผู้รับผิดชอบ

- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร
- หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

ข้อปฏิบัติ

๑) จัดเก็บและสำรองข้อมูลจราจรทางคอมพิวเตอร์ ของระบบดังต่อไปนี้อย่างน้อยเป็นระยะเวลา ๙๐ วัน

ชนิดของระบบ	ข้อมูลจราจรฯ ที่ต้องเก็บ
FTP Server	ข้อมูลจราจรฯ ที่เกิดจากการโอนย้ายไฟล์
Mail Server	ข้อมูลจราจรฯ ที่เกิดจากการรับส่งอี-เมล์
Firewall/ Proxy/ Gateway	ข้อมูลเลขที่อยู่ไอพีของเครื่องทั้งภายในและภายนอกที่มีการเชื่อมต่อกับเครือข่ายของหน่วยงาน
Active Directory	ข้อมูลจราจรฯ การพิสูจน์ตัวตนของผู้ใช้งาน
Web Server	ข้อมูลจราจรฯ การเข้าถึงเว็บเซิร์ฟเวอร์
Web Application ซึ่งรวมถึง webboard	ข้อมูลจราจรฯ การพิสูจน์ตัวตนของผู้ใช้งาน

๒) จำกัดการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวโดยกำหนดสิทธิให้เฉพาะผู้ดูแลระบบที่เกี่ยวข้องเท่านั้นที่สามารถเข้าถึงได้

๒๐.นโยบายการสร้างความต่อเนื่องในการดำเนินงานสำหรับกระบวนการทางธุรกิจสำคัญ

วัตถุประสงค์

- เพื่อให้มีการบริหารจัดการเพื่อสร้างความต่อเนื่องให้กับกระบวนการทางธุรกิจสำคัญของหน่วยงาน เมื่อมีเหตุการณ์ที่ทำให้เกิดการหยุดชะงักหรือติดขัดต่อกระบวนการดังกล่าว

ผู้รับผิดชอบ

- เจ้าของกระบวนการทางธุรกิจสำคัญและ/หรือ ผู้บังคับบัญชา

อ้างอิงมาตรฐาน

- หมวดที่ ๑๐ การบริหารความต่อเนื่องในการดำเนินงานขององค์กร
- หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

ข้อปฏิบัติ

๑) กำหนดกระบวนการทางธุรกิจสำคัญและระบบซึ่งสนับสนุนกระบวนการดังกล่าว

๒) ประเมินผลกระทบกรณีกระบวนการทางธุรกิจสำคัญและ/หรือ ระบบสนับสนุนเกิดการหยุดชะงักหรือไม่สามารถให้บริการได้ (ดูการประเมินผลกระทบใน **นโยบายการวางแผนเตรียมการสภาพความพร้อมใช้**ของระบบงาน)

๓) ประเมินความเสี่ยงกำหนดแผนการลดความเสี่ยงสำหรับกระบวนการทางธุรกิจสำคัญและ/หรือระบบสนับสนุน

๔) ดำเนินการเตรียมการล่วงหน้าที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับกระบวนการทางธุรกิจสำคัญ (โดยปฏิบัติตาม **นโยบายการเตรียมการล่วงหน้าที่จำเป็นสำหรับการสร้างความต่อเนื่องในการดำเนินงาน**)

๕) ดำเนินการเตรียมการล่วงหน้าที่จำเป็นสำหรับการกู้คืนระบบสนับสนุน (โดยปฏิบัติตาม **นโยบายการเตรียมการล่วงหน้าที่จำเป็นสำหรับการกู้คืนระบบเทคโนโลยีสารสนเทศ**)

๖) จัดทำแผนสร้างความต่อเนื่องในการดำเนินงานสำหรับกระบวนการทางธุรกิจสำคัญ (โดยปฏิบัติตาม **แนวทางปฏิบัติในการจัดทำแผนสร้างความต่อเนื่องในการดำเนินงาน**)

๗) จัดทำแผนกู้คืนระบบสนับสนุน (โดยปฏิบัติตาม**แนวทางปฏิบัติในการจัดทำแผนกู้คืนระบบเทคโนโลยีสารสนเทศ**)

๘) ให้ความรู้แก่ผู้ที่เกี่ยวข้องทั้งหมด (ซึ่งรวมถึงทีมสร้างความต่อเนื่องในการดำเนินงาน ทีมกู้คืนระบบ และผู้ให้บริการภายนอก) และสร้างความตระหนักแก่ผู้ใช้งานเพื่อให้คุ้นเคยกับการสร้างความต่อเนื่องในการดำเนินงานเข้าใจในบทบาทและหน้าที่ความรับผิดชอบของตนเอง รวมทั้งสามารถปฏิบัติได้อย่างถูกต้อง

๙) ทบทวนและตรวจสอบรายละเอียดของแผนสร้างความต่อเนื่องในการดำเนินงาน และแผนกู้คืนระบบสนับสนุนโดยผู้ตรวจสอบภายใน เพื่อนำไปสู่การปรับปรุงให้ดียิ่งขึ้นอย่างน้อยปีละ ๑ ครั้ง

๑๐)จัดทำแผนการทดสอบ (การสร้างความต่อเนื่องในการดำเนินงานและการกู้คืนระบบ) กำหนดสถานการณ์การทดสอบ ดำเนินการทดสอบตามแผนการทดสอบ บันทึกผลการทดสอบ สรุปผลและข้อเสนอแนะและนำเสนอต่อผู้บริหารระดับสูงเพื่อพิจารณาและให้ข้อคิดเห็นในการปรับปรุงตามความจำเป็น

๑๑)ทบทวนการดำเนินการในทุกรายการข้างต้นอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๒๑. นโยบายการเตรียมการล่วงหน้าที่จำเป็นสำหรับการสร้างความต่อเนื่องในการดำเนินงาน

วัตถุประสงค์

- เพื่อให้มีการเตรียมการล่วงหน้าต่างๆ ที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับกระบวนการทางธุรกิจสำคัญของ กรมการค้าภายใน คือเมื่อมีเหตุการณ์ที่ทำให้เกิดการหยุดชะงักหรือติดขัดต่อกระบวนการดังกล่าว กระบวนการสามารถฟื้นกลับคืนมาให้บริการได้ภายในระยะเวลาที่เหมาะสม

ผู้รับผิดชอบ

- เจ้าของกระบวนการทางธุรกิจสำคัญและ/หรือ ผู้บังคับบัญชา

อ้างอิงมาตรฐาน

- หมวดที่ ๑๐ การบริหารความต่อเนื่องในการดำเนินงานขององค์กร
- หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

ข้อปฏิบัติ

สำหรับกระบวนการทางธุรกิจสำคัญกระบวนการหนึ่ง ผู้รับผิดชอบ ปฏิบัติดังนี้

๑) กำหนดรายละเอียดพื้นฐานของกระบวนการทางธุรกิจสำคัญ
๒) กำหนดสถานที่สำรองที่ใช้ในการปฏิบัติงานของผู้ปฏิบัติงานสำหรับกระบวนการทางธุรกิจสำคัญ (กรณีสำนักงานปัจจุบันไม่สามารถใช้งานได้)
๓) กำหนดขั้นตอนของกระบวนการทางธุรกิจสำคัญ
๔) กำหนดเอกสารหรือคู่มือที่จำเป็นสำหรับกระบวนการทางธุรกิจสำคัญ
๕) กำหนดบุคลากรผู้เป็นเจ้าของ ผู้ปฏิบัติงาน และผู้ที่เกี่ยวข้องกับกระบวนการทางธุรกิจสำคัญ
๖) กำหนดระบบเทคโนโลยีสารสนเทศที่สนับสนุนกระบวนการทางธุรกิจสำคัญ
๗) กำหนดข้อมูลสำคัญสำหรับกระบวนการทางธุรกิจสำคัญและการสำรองหรือสำเนาข้อมูล
๘) กำหนดสถานที่สำหรับจัดเก็บซอฟต์แวร์/เฟิร์มแวร์นอกสถานที่
๙) จัดทำสัญญาการให้บริการกับผู้ให้บริการภายนอกเพื่อให้สามารถให้บริการระบบเทคโนโลยีสารสนเทศสนับสนุนกระบวนการทางธุรกิจสำคัญ
๑๐)บันทึกข้อมูลของแต่ละประเด็นในข้างต้นให้ครบถ้วนสมบูรณ์มากที่สุด
๑๑)ทบทวนประเด็นทั้งหมดในข้างต้นอย่างน้อยปีละ ๑ ครั้งและปรับเปลี่ยนให้เหมาะสมตามความจำเป็น

แนวทางปฏิบัติในการจัดทำแผนสร้างความต่อเนื่องในการดำเนินงาน

วัตถุประสงค์

- เพื่อกำหนดแนวทางสำหรับการจัดทำแผนสร้างความต่อเนื่องให้กับกระบวนการทางธุรกิจสำคัญของกรมการค้าภายใน

ผู้รับผิดชอบ

- เจ้าของกระบวนการทางธุรกิจสำคัญและ/หรือ ผู้บังคับบัญชา

อ้างอิงมาตรฐาน

- หมวดที่ ๑๐ การบริหารความต่อเนื่องในการดำเนินงานขององค์กร
- หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

ข้อปฏิบัติ

ในการจัดทำแผนสร้างความต่อเนื่องสำหรับกระบวรการทางธุรกิจสำคัญของ กรมการค้าภายใน อย่างน้อยผู้รับผิดชอบ ต้องกำหนดรายละเอียดลงในแต่ละหัวข้อดังนี้

๑) ลำดับของผู้มีอำนาจในการสั่งการใช้แผน
๒) โครงสร้างของทีมสร้างความต่อเนื่องในการดำเนินงาน
๓) รายชื่อและข้อมูลติดต่อของทีมสร้างความต่อเนื่องในการดำเนินงาน
๔) การสั่งการใช้แผนสร้างความต่อเนื่องในการดำเนินงาน
๕) การสั่งย้ายสถานที่ปฏิบัติงานไปยังสถานที่ปฏิบัติงานสำรอง
๖) การเก็บรวบรวมเอกสารและอุปกรณ์ที่จำเป็นเพื่อนำไปใช้งานยังสถานที่ปฏิบัติงานสำรอง
๗) การเตรียมความพร้อมสำหรับการเริ่มปฏิบัติงาน ณ สถานที่สำรอง
๘) การแจ้งข้อมูลเกี่ยวกับเหตุการณ์ฉุกเฉินให้ผู้ที่เกี่ยวข้องกับกระบวนการทางธุรกิจสำคัญได้รับทราบ

๙) การเริ่มต้นปฏิบติงาน ณ สถานที่สำรอง
๑๐)การกลับคืนสู่สภาวะการทำงานตามปกติ (ภายหลังจากที่ได้แก้ไขสถานการณ์แล้ว)

๒๒. นโยบายการเตรียมการล่วงหน้าที่จำเป็นสำหรับการกู้คืนระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

- เพื่อให้มีการเตรียมการล่วงหน้าต่าง ๆ ที่จำเป็นสำหรับการกู้คืนระบบเทคโนโลยีสารสนเทศ ซึ่งสนับสนุนกระบวนการทางธุรกิจสำคัญของ กรมการค้าภายใน คือเมื่อมีเหตุการณ์ที่ทำให้เกิดการหยุดชะงักหรือติดขัดต่อระบบดังกล่าว ระบบสามารถกู้คืนกลับมาให้บริการได้ภายในระยะเวลาที่เหมาะสม

ผู้รับผิดชอบ

- ผู้บังคับบัญชา

อ้างอิงมาตรฐาน

- หมวดที่ ๑๐ การบริหารความต่อเนื่องในการดำเนินงานขององค์กร
- หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

ข้อปฏิบัติ

๑) กำหนดรายชื่อของระบบเทคโนโลยีสารสนเทศ (ซึ่งสนับสนุนกระบวนการทางธุรกิจสำคัญของกรมการค้าภายใน) ที่จำเป็นต้องเตรียมการการกู้คืนและระยะเวลาเป้าหมายในการกู้คืน
๒) กำหนดสถานที่ตั้งและความต้องการพื้นฐานของศูนยคอมพิวเตอร์สำรอง (เพื่อรองรับระบบเทคโนโลยีสารสนเทศสำรอง)
๓) กำหนดบุคลากรผู้รับผิดชอบการกู้คืนระบบเทคโนโลยีสารสนเทศและผู้ให้บริการภายนอกที่เกี่ยวข้อง
๔) กำหนดรายละเอียดของระบบเทคโนโลยีสารสนเทศที่จำเป็นต้องเตรียมการกู้คืน
   ๔.๑) ที่ศูนย์คอมพิวเตอร์หลัก
      ๔.๑.๑) ด้านฮาร์ดแวร์และซอฟต์แวร์ของระบบงาน
      ๔.๑.๒) ด้านฮาร์ดแวร์และเฟิร์มแวร์ของระบบเครือข่าย
   ๔.๒) ที่ศูนย์คอมพิวเตอร์สำรอง
      ๔.๒.๑) ด้านฮาร์ดแวร์และซอฟต์แวร์ของระบบงาน
      ๔.๒.๒) ด้านฮาร์ดแวร์และเฟิร์มแวร์ของระบบเครือข่าย
๕) กำหนดข้อมูลสำคัญที่จำเป็นสำหรับการกู้คืนระบบเทคโนโลยีสารสนเทศและการสำรองหรือสำเนาข้อมูล
   ๕.๑) ข้อมูลที่อยู่ในรูปกระดาษ
   ๕.๒) ข้อมูลที่เกี่ยวข้องกับแต่ละระบบเทคโนโลยีสารเทศ (ในรูปแบบอิเล็กทรอนิกส์)
๖) กำหนดสถานที่สำหรับจัดเก็บซอฟต์แวร์/เฟิร์มแวร์นอกสถานที่
๗) จัดทำสัญญาการให้บริการกับผู้ให้บริการภายนอกเพื่อให้สามารถบริการระบบเทคโนโลยีสารสนเทศได้อย่างต่อเนื่องทั้งศูนย์คอมพิวเตอร์หลักและสำรอง
๘) บันทึกข้อมูลของแต่ละประเด็นในข้างต้นให้ครบถ้วนสมบูรณ์มากที่สุด
๙) ทบทวนประเด็นทั้งหมดในข้างต้นอย่างน้อยปีละ ๑ ครั้งและปรับเปลี่ยนให้เหมาะสมตามความจำเป็น

แนวทางปฏิบัติในการจัดทำแผนกู้คืนระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

- เพื่อกำหนดแนวทางสำหรับการจัดทำแผนกู้คืนระบบเทคโนโลยีสารสนเทศซึ่งสนับสนุนกระบวนการทางธุรกิจสำคัญของ กรมการค้าภายใน

ผู้รับผิดชอบ

- ผู้บังคับบัญชา

อ้างอิงมาตรฐาน

- หมวดที่ ๑๐ การบริหารความต่อเนื่องในการดำเนินงานขององค์กร
- หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

ข้อปฏิบัติ

ในการจัดทำแผนกู้คืนระบบเทคโนโลยีสารสนเทศซึ่งสนับสนุนกระบวนการทางธุรกิจสำคัญของกรมการค้าภายใน อย่างน้อยให้ผู้รับผิดชอบ กำหนดรายละเอียดลงในแต่ละหัวข้อดังนี้

๑) ลำดับของผู้มีอำนาจในการสั่งการใช้แผนกู้คืนระบบเทคโนโลยีสารสนเทศ
๒) โครงสร้างของทีมกู้คืนระบบเทคโนโลยีสารสนเทศ
๓) รายชื่อและข้อมูลติดต่อของทีมกู้คืนระบบเทคโนโลยีสารสนเทศ
๔) การสั่งการใช้แผนกู้คืนระบบเทคโนโลยีสารสนเทศ
๕) การสั่งย้ายสถานที่ปฏิบัติงานไปยังศูนย์คอมพิวเตอร์สำรอง
๖) การเก็บรวบรวมเอกสารและอุปกรณ์ที่จำเป็นเพื่อนำไปใช้งานยังศูนย์คอมพิวเตอร์สำรอง
๗) การเตรียมความพร้อมของศูนย์คอมพิวเตอร์สำรอง
๘) การแจ้งข้อมูลเกี่ยวกับเหตุการณ์ฉุกเฉินให้ผู้ให้บริการภายนอกได้รับทราบ
๙) การเริ่มต้นปฏิบติงาน ณ ศูนย์คอมพิวเตอร์สำรอง
๑๐)การกลับคืนสู่สภาวะการทำงานตามปกติ ภายหลังจากที่ได้แก้ไขสถานการณ์แล้ว

ส่วนที่ ๕
นโยบายการจัดการด้านบุคลากร
สำหรับศูนย์เทคโนโลยีสารสนเทศ

๑. นโยบายการจัดการด้านบุคลากร

วัตถุประสงค์

- เพื่อให้มีการกำหนดหน้าที่ความรับผิดชอบที่ชัดเจนสำหรับบุคลากรที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ
- เพื่อให้มีการคัดเลือกบุคลากรด้านสารสนเทศที่มีคุณสมบัติเหมาะสมเพื่อมาปฏิบัติหน้าที่ให้กับหน่วยงาน
- เพื่อให้มีการกำหนดเงื่อนไขการจ้างงานบุคลากรที่รัดกุมและเป็นผลประโยชน์ต่อหน่วยงาน
- เพื่อให้มีการถอดถอนสิทธิของบุคลากรที่ลาออกหรือย้ายไปอยู่แผนกอื่น รวมทั้งตรวจสอบสินทรัพย์ของหน่วยงานที่ใช้งานโดยเจ้าหน้าที่นั้นก่อนลาออกไป

ผู้รับผิดชอบ

- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

อ้างอิงมาตรฐาน

- หมวดที่ ๔ ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

ข้อปฏิบัติ

๑) จัดทำและปรับปรุงหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ

๒) จัดตั้งคณะกรรมการเพื่อคัดเลือกบุคลากรด้านสารสนเทศ

๓) มีการทำสัญญาการจ้างหรือข้อตกลงการจ้าง สำหรับบุคลากรที่ผ่านการคัดเลือก โดยให้รวมเงื่อนไขการไม่เปิดเผยความลับของหน่วยงานเป็นส่วนหนึ่งของสัญญาจ้างหรือข้อตกลงการจ้าง

๔) เมื่อมีการลาออกหรือย้ายแผนกของเจ้าหน้าที่ ให้ฝ่ายบริหารทั่วไปแจ้งให้ผู้ดูแลระบบและ/หรือผู้พัฒนาระบบได้รับทราบภายใน ๑ สัปดาห์ นับจากมีคำสั่งให้ลาออกหรือย้ายแผนก เพื่อให้ดำเนินการปรับปรุงหรือถอดถอนสิทธิตามความจำเป็น

ส่วนที่ ๖
นโยบายการเผยแพร่ข้อมูลสู่สาธารณะ
สำหรับผู้เป็นเจ้าของหรือรับผิดชอบต่อข้อมูลที่ต้องทำการเผยแพร่สู่สาธารณะ

๑. นโยบายการนำข้อมูลเผยแพร่สู่สาธารณะ

วัตถุประสงค์

- เพื่อป้องกันความผิดพลาดของข้อมูลที่จะมีการเผยแพร่สู่สาธารณะ ซึ่งอาจจะก่อให้เกิดความเสียหายต่อชื่อเสียงและภาพลักษณ์ของหน่วยงาน

ผู้รับผิดชอบ

- เจ้าของข้อมูลที่ต้องทำการเผยแพร่สู่สาธารณะ

อ้างอิงมาตรฐาน

- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ข้อปฏิบัติ

๑) ให้ผู้ที่เป็นเจ้าของข้อมูลซึ่งต้องการนำข้อมูลนั้นขึ้นเผยแพร่สู่สาธารณะและผู้ที่มีหน้าที่รับผิดชอบในการนำข้อมูลขึ้นเผยแพร่สู่สาธารณะ เช่น โดยผ่านทางเว็บไซต์ของหน่วยงานจะต้องทำการตรวจสอบความถูกต้องและเหมาะสมของเนื้อหาก่อน หากมีความผิดพลาดเกิดขึ้นกับเนื้อหา จะต้องรับผิดชอบต่อความผิดพลาดนั้น

๒) ให้ผู้ที่มีหน้าที่รับผิดชอบในการนำข้อมูลขึ้นเผยแพร่สู่สาธารณะ เช่น โดยผ่านทางเว็บไซต์ของหน่วยงานจะต้องดำเนินการด้วยตนเอง หากมีการมอบหมายให้ผู้อื่นดำเนินการแทนต้องทำการตรวจสอบความถูกต้องและเหมาะสมของเนื้อหาโดยทันที เมื่อเผยแพร่ข้อมูลแล้วเสร็จ
