ประกาศสำนักงานปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของสำนักงานปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี พ.ศ. ๒๕๕๙

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์ และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยีโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศดังต่อไปนี้

ข้อ ๑. ประกาศนี้เรียกว่า “ประกาศสำนักงานปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี พ.ศ. ๒๕๕๙”

ข้อ ๒. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓. คำนิยาม ประกอบด้วย

๓.๑ หน่วยงาน หมายถึง สำนักงานปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี ทั้งนี้ให้หมายรวมถึงสำนักงานรัฐมนตรี

๓.๒ ศูนย์ หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๓.๓ ผู้บริหาร หมายถึง ปลัดกระทรวง รองปลัดกระทรวง หัวหน้าผู้ตรวจราชการ ผู้ตรวจราชการที่ปรึกษาด้านวิทยาศาสตร์และเทคโนโลยี ผู้อำนวยการสำนัก/ศูนย์/กลุ่ม

๓.๔ ผู้ใช้งาน หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว ผู้รับจ้างตามสัญญาจ้างในหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

๓.๕ สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๓.๖ สินทรัพย์ หมายถึง สิ่งใดก็ตามที่มีคุณค่าสำหรับหน่วยงาน

๓.๗ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๓.๘ ความมั่นคงปลอดภัยด้านสารสนเทศ (information security) หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ไดแกความถูกตองแทจริง (authenticity) ความรับผิด (accountability) การหามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๓.๙ เหตุการณดานความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ สภาพของบริการหรือเครือขายที่แสดงใหเห็นความเปนไปไดที่จะเกิด การฝาฝนนโยบายดานความมั่นคงปลอดภัยหรือมาตรการปองกันที่ลมเหลว หรือเหตุการณอันไมอาจรูไดวาอาจเกี่ยวของกับความมั่นคงปลอดภัย

๓.๑๐ สถานการณ์ด้านความมั่นคงปลอดภัย (Information Security Incident) ที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๓.๑๑ ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

๓.๑๒ ระบบสารสนเทศ หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น

๓.๑๓ ผู้ดูแลระบบ (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

๓.๑๔ หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

๓.๑๕ ชื่อผู้ใช้งาน (Username) หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

๓.๑๖ รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวผู้ใช้ เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๓.๑๗ การเข้ารหัส (Encryption) หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๓.๑๘ อุปกรณ์จัดเส้นทาง (Router) หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

๓.๑๙ การพิสูจน์ยืนยันตัวตน (Authentication) หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ โดยทั่วไปจะใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ในการพิสูจน์ยืนยันตัวตน

๓.๒๐ แผนผังระบบเครือข่าย (Network Diagram) หมายถึง แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

๓.๒๑ เครื่องคอมพิวเตอร์ หมายถึง เครื่องคอมพิวเตอร์ของหน่วยงานซึ่งประกอบด้วยเครื่องคอมพิวเตอร์ตั้งโต๊ะ(Desktop Computer) และเครื่องคอมพิวเตอร์โน้ตบุ๊ก (Notebook) รวมถึงเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer)

๓.๒๒ อุปกรณ์คอมพิวเตอร์ หมายถึง เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่สามารถเชื่อมต่อกับระบบเครือข่ายของหน่วยงานได้ เช่น เครื่องพิมพ์ เครื่องโทรสาร เครื่องสแกนเนอร์ SmartTV เป็นต้น

๓.๒๓ อุปกรณ์สื่อสารเคลื่อนที่ หมายถึง โทรศัพท์เคลื่อนที่แบบสมาร์ทโฟนและอุปกรณ์ประเภทแท็บเล็ตที่สามารถเชื่อมต่อกับระบบเครือข่ายของหน่วยงานได้

ข้อ ๔. การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้มี ๒ ส่วน ดังนี้

๔.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๕

๔.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๖ – ๑๔

ข้อ ๕. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๕.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

๕.๑.๑ นโยบายได้ทำเป็นลายลักษณ์อักษร โดยเผยแพร่ผ่านทางเว็บไซต์ของหน่วยงาน และประกาศให้ผู้ใช้งานทราบและถือปฏิบัติอย่างเคร่งครัด

๕.๑.๒ กำหนดให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้รับผิดชอบติดตาม กำกับ ดูแล ควบคุม ตรวจสอบตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๕.๑.๓ ต้องทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๕.๑.๔ การปฏิบัติตามประกาศนโยบายฉบับนี้ให้เป็นไปตามเอกสารแนบท้ายประกาศ

๕.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

๕.๒.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

การให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานเป็นไปอย่างทั่วถึง โดยให้ผู้ใช้งานสามารถเข้าถึงและใช้งานสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย ซึ่งมีเนื้อหาครอบคลุม ๔ ด้าน ได้แก่ การเข้าถึงระบบสารสนเทศ การเข้าถึงระบบเครือข่าย การเข้าถึงระบบปฏิบัติการ และการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ โดยมีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

๕.๒.๒ การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

การบริหารจัดการสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองของระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

๕.๒.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

การตรวจสอบและประเมินความเสี่ยง รวมถึงการทบทวนมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ กำหนดให้มีการดำเนินการอย่างน้อยปีละ ๑ ครั้ง

๕.๒.๔ การสร้างความรู้ความเข้าใจและตระหนักในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

การสร้างความรู้ความเข้าใจและตระหนักในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก ต้องจัดทำในรูปแบบของการจัดทำคู่มือ หรือการจัดฝึกอบรม หรือการจัดทำเอกสารเผยแพร่

ข้อ ๖. มีข้อกำหนดการควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control) อย่างน้อยดังนี้

๖.๑ มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๖.๒ กฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน และเป็นไปตามเอกสารแนบท้ายประกาศ

๖.๓ ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๗. มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

๗.๑ การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๗.๒ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

๗.๓ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๗.๔ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review Of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๘. มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

๘.๑ การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๘.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๘.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk And Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

ข้อ ๙. มีการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๙.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๙.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication For External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๙.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification In Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๙.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic And Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๙.๕ การแบ่งแยกเครือข่าย (Segregation In Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๙.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

๙.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๐. มีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๑๐.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๑๐.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification And Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๑๐.๓ การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๑๐.๔ การใช้งานโปรแกรมยูทิลิตี้ (Use Of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๑๐.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out)

๑๐.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation Of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๑. มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application And Information Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

๑๑.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๑๑.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing And Teleworking)การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๑๑.๓ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๑๒. การจัดทำระบบสำรองของระบบสารสนเทศ ตามแนวทางต่อไปนี้

๑๒.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

๑๒.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๑๒.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๑๒.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๑๒.๕ ต้องทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๓. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

๑๓.๑ ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit And Assessment) อย่างน้อยปีละ ๑ ครั้ง

๑๓.๒ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๔. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยีในฐานะผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

ประกาศ ณ วันที่ ๑๕ กุมภาพันธ์ พ.ศ. ๒๕๕๙

(นายวีระพงษ์ แพสุวรรณ)

ปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี

เอกสารแนบท้ายประกาศ

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของสำนักงานปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี พ.ศ.๒๕๕๙

สารบัญ

หมวดที่ ๑

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงาน

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับหน่วยงาน ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

๑.๑ ผู้ใช้งานสามารถเข้าถึงข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ โดยได้รับอนุญาตจากผู้อำนวยการศูนย์หรือผู้ที่ได้รับมอบหมาย

๑.๒ ศูนย์ต้องจัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและผู้รับผิดชอบ

๑.๓ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ โดยกำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตและการกำหนดสิทธิ์ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์ในการใช้งานสารสนเทศ

(๒) กำหนดเกณฑ์การระงับสิทธิ์ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(๓) การเข้าใช้งานระบบสารสนเทศของหน่วยงานต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์หรือผู้ที่ได้รับมอบหมาย

๑.๔ การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสม ในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้

(๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี
- ข้อมูลสารสนเทศด้านวิทยาศาสตร์ เทคโนโลยีและนวัตกรรมที่ใช้สำหรับการให้บริการและเผยแพร่องค์ความรู้ ได้แก่ ข้อมูลสิ่งประดิษฐ์และนวัตกรรม บทความงานวิจัย สิ่งตีพิมพ์ทางด้านวิทยาศาสตร์ เทคโนโลยีและนวัตกรรม

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๒ ระดับ คือ

- ข้อมูลที่มีความสำคัญ หมายถึง ข้อมูลทางด้านบัญชี/การเงิน ข้อมูลที่มีชั้นความลับของข้อมูลตั้งแต่ข้อมูลลับขึ้นไป ข้อมูลส่วนบุคคล
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุดกับหน่วยงานและประเทศ
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงกับหน่วยงานและประเทศ
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายกับหน่วยงานหรือบุคลากร
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร หมายถึง ผู้บริหารหรือผู้ใช้งานที่ดำรงตำแหน่งในระดับผู้อำนวยการสำนัก/ศูนย/กลุ่ม หรือผู้ที่ทำหน้าที่รักษาราชการแทนผู้อำนวยการสำนัก/ศูนย์/กลุ่ม
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป หมายถึง ผู้ใช้งานที่ปฏิบัติหน้าที่ทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย หมายถึง เจ้าหน้าที่ของศูนย์ที่ทำหน้าที่เป็นผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

(๕) จัดแบ่งประเภทของขอบเขตในการเข้าถึง

- การเข้าถึงข้อมูลของหน่วยงานผ่านระบบเครือข่ายภายในหน่วยงาน (Intranet)
- การเข้าถึงข้อมูลของหน่วยงานผ่านระบบเครือข่ายภายนอกหน่วยงาน (Internet)

(๖) การกำหนดระยะเวลาในการเข้าถึงระบบสารสนเทศ

- สามารถเข้าถึงระบบสารสนเทศได้ตลอดเวลา

(๗) ช่องทางการเข้าถึงสำหรับสารสนเทศ

- การเข้าถึงข้อมูลของหน่วยงานผ่านเครื่องคอมพิวเตอร์
- การเข้าถึงข้อมูลของหน่วยงานผ่านอุปกรณ์สื่อสารเคลื่อนที่

๑.๕ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements For Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิ์ที่เกี่ยวข้องกับระบบสารสนเทศ

(๒) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑ การลงทะเบียนผู้ใช้งาน (User Registration) มีขั้นตอน ดังนี้

(๑) ผู้ดูแลระบบจัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน

(๒) ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม พร้อมจัดเก็บลายนิ้วมือและลายเซ็นเพื่อใช้ในระบบสารสนเทศของหน่วยงาน

(๓) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน พร้อมทั้งจัดทำทะเบียนการขออนุญาตเข้าใช้ระบบสารสนเทศ

(๔) ผู้ดูแลระบบกำหนดชื่อผู้ใช้งาน (Username) โดยกำหนดจากชื่อภาษาอังกฤษ ตามด้วยเครื่องหมายจุลภาค (.) และตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(๕) ผู้ดูแลระบบต้องตรวจสอบและมอบหมายสิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบที่ผู้ใช้งานได้รับมอบหมาย

(๖) ผู้ดูแลระบบจัดทำเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศ โดยผู้ใช้งานต้องลงนามรับทราบด้วย

๒.๒ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) เป็นการควบคุมและดูแลสิทธิ์ประเภทต่างๆ ในการเข้าใช้งานระบบสารสนเทศของผู้ใช้งาน โดยมีแนวทางการปฏิบัติดังนี้

(๑) ผู้ใช้งานต้องได้รับสิทธิ์ในการเข้าถึงระบบสารสนเทศอย่างเพียงพอต่อการปฏิบัติงานตามที่ได้รับมอบหมาย

(๒) กรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมให้ผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณาและควรได้รับการอนุมัติจากผู้อำนวยการสำนัก/ศูนย์/กลุ่ม นั้น

๒.๓ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

(๑) ชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๒) ต้องส่งมอบ/แจ้งรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นในการจัดส่งรหัสผ่าน และกำหนดให้ผู้ใช้งานตอบยืนยันกลับทันทีหลังจากได้รับรหัสผ่านทางจดหมายอิเล็กทรอนิกส์ (E-Mail)

(๓) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และต้องเปลี่ยนรหัสผ่านให้ยากต่อการเดา ตามข้อ ๓.๑

(๔) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน โดยถือว่าข้อมูลรหัสผ่านเป็นความลับเฉพาะบุคคล หากในกรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่น เพื่อให้สามารถปฏิบัติงานแทนตนเองได้ หลังจากที่ทำงานนั้นเสร็จเรียบร้อยแล้วให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง หากเกินกว่าที่กำหนด ระบบจะทำการ lock ไม่ให้ใช้งาน ผู้ใช้งานจะต้องติดต่อผู้ดูแลระบบ

(๖) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๗) ผู้ใช้งานต้องไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๔ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review Of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

(๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามสำนัก/ศูนย์/กลุ่ม

(๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของสำนัก/ศูนย์/กลุ่ม เพื่อดำเนินการทบทวนรายชื่อและสิทธิการเข้าใช้งานว่าถูกต้องหรือไม่

(๓) ดำเนินการแก้ไขข้อมูลและสิทธิของผู้ใช้งานให้ถูกต้องตามที่ได้รับแจ้งกลับจากสำนัก/ศูนย์/กลุ่ม

(๔) การยกเลิกสิทธิการเข้าถึงของผู้ใช้งาน

- เมื่อผู้ใช้งานลาออก ต้องดำเนินการภายใน ๓ วัน
- เมื่อผู้ใช้งานมีการเปลี่ยนตำแหน่งงาน ต้องดำเนินการภายใน ๗ วัน

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงระบบสารสนเทศหรืออุปกรณ์โดยไม่ได้รับอนุญาต รวมถึงการเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ โดยมีข้อปฏิบัติอย่างน้อย ดังนี้

๓.๑ การใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

(๑) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

(๒) ต้องเปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๓) กำหนดรหัสผ่านที่ยากต่อการคาดเดา ให้มีตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๔) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๕) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๗) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(๘) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

(๙) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๐) ควรมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑๑) หลีกเลี่ยงการใช้รหัสผ่านเดิม

(๑๒) ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป โดยทุกๆ ๓ เดือน สำหรับผู้ดูแลระบบ และทุกๆ ๖ เดือนสำหรับผู้ใช้งานหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๓.๒ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

๓.๓ ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๓.๔ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของหน่วยงาน และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

๓.๕ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

๓.๖ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่าแต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bit torrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการศูนย์หรือผู้ที่ได้รับมอบหมาย

๓.๗ ห้ามใช้ทรัพย์สินของหน่วยงาน ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของหน่วยงาน

๓.๘ ห้ามใช้ทรัพย์สินของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของหน่วยงาน

๓.๙ ห้ามใช้ทรัพย์สินของหน่วยงานเพื่อประโยชน์ทางการค้า

๓.๑๐ ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ในเครือข่ายระบบสารสนเทศของหน่วยงานโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

๓.๑๑ ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

๓.๑๒ ห้ามใช้ระบบสารสนเทศของหน่วยงาน เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๑๓ ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

๓.๑๔ ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๑๕ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ (Unattended User Equipment) ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

(๑) เครื่องคอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๒) กำหนดให้เครื่องคอมพิวเตอร์ล็อกหน้าจอ (Screen Saver) หลังจากที่ไม่ได้ใช้งานเป็นเวลา ๕ นาทีหรือตามความเหมาะสม และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอเพื่อเข้าถึงเครื่องคอมพิวเตอร์หรือระบบงานได้

(๓) การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

(๔) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน เช่น ออกจากระบบงาน เครื่องให้บริการ เครื่องคอมพิวเตอร์ทันทีเมื่อเสร็จสิ้นงาน เป็นต้น

(๕) ต้องล็อกอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราวเพื่อป้องกันการสูญหายหรือถูกขโมย

(๖) กำหนดให้มีการสร้างความตระหนักเพื่อให้เกิดความเข้าใจในมาตรการป้องกันที่ได้กำหนดไว้

๓.๑๖ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ในที่ที่ปลอดภัย (Clear Desk And Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล เครื่องคอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

(๑) การจัดการบริเวณล้อมรอบ (Physical security management)

- กำหนดระดับความสำคัญของพื้นที่หรือจำแนกพื้นที่ใช้งาน
- พื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในห้องคอมพิวเตอร์แม่ข่ายให้ติดตั้งสัญญาณเตือนภัย เพื่อแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น
- ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพเพื่อตรวจสอบยังใช้งานได้ตามปกติ
- บุคลากรของศูนย์ควรปิดประตูและหน้าต่างให้ล็อคอยู่เสมอ

(๒) การควบคุมการเข้า – ออกห้องคอมพิวเตอร์แม่ข่าย (MOST Data Center)

- ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้มาเยือน (Visitors)
- ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต
- มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอกและควรมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว ซึ่งต้องได้รับการอนุญาตจากผู้อำนวยการศูนย์หรือผู้ที่ได้รับมอบหมายเท่านั้น
- มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่
- ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต
- มีการพิสูจน์ตัวตนด้วยการใช้บัตรอิเล็กทรอนิกส์ประกอบกับการใช้ลายพิมพ์นิ้วมือเพื่อควบคุมการเข้า – ออกในพื้นที่ของห้องคอมพิวเตอร์แม่ข่าย
- จัดเก็บบันทึกการเข้า – ออกสำหรับพื้นที่ห้องคอมพิวเตอร์แม่ข่าย เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

- ผู้มาเยือนต้องติดบัตรอยู่ตลอดระยะเวลาที่อยู่ภายในหน่วยงานและจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของผู้มาเยือนหรือบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่ห้องคอมพิวเตอร์แม่ข่าย
- จัดให้มีการทบทวนหรือยกเลิกสิทธิ์การเข้าถึงพื้นที่ห้องคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอ

(๓) การจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access, Delivery and Loading Areas)

- จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณที่ส่งมอบนั้น
- จัดพื้นที่หรือบริเวณส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในหน่วยงาน
- ให้ตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน
- ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของหน่วยงาน

(๔) การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)

- จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในห้องคอมพิวเตอร์แม่ข่ายให้น้อยที่สุด
- อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัย
- ไม่ให้นำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในห้องคอมพิวเตอร์แม่ข่าย
- ดำเนินการตรวจสอบ สอดส่องและดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ใน

บริเวณดังกล่าว เช่น ตรวจสอบระดับอุณหภูมิ ความชื้น ให้อยู่ในระดับปกติหรือไม่

(๕) ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

- มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้
  - ระบบสำรองกระแสไฟฟ้า (UPS)
  - ระบบระบายอากาศ
  - ระบบปรับอากาศ และควบคุมความชื้น
- ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นทุกๆ ๓ เดือน เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ
- ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

(๖) การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)

- ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย
- ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน
- ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น
- จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง
- ตู้ Rack ที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

(๗) การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

- ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต
- ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

- จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง
- จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว
- ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน
- จัดให้มีการอนุญาตสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๘) การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)
- ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน
- กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน
- กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน
- เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย
- บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

(๙) การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises)
- กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์
- ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ
- เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

(๑๐) การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or re-use of Equipment)

- ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว
- มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

ส่วนที่ ๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๔.๑ มาตรการควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย (Server)

(๑) ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตร ผู้ติดต่อ (Visitor) แล้วทำการลงชื่อในสมุดบันทึกรายชื่อผู้ใช้งานห้องแม่ข่ายคอมพิวเตอร์

(๒) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องห้องคอมพิวเตอร์แม่ข่าย ต้องทำการขออนุญาตจากผู้อำนวยการศูนย์ หรือผู้ที่ได้รับมอบหมายให้ดูแลห้องคอมพิวเตอร์แม่ข่าย

๔.๒ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๔.๓ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน โดยผู้ดูแลระบบควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ดังนี้

- มีการตรวจสอบการเชื่อมต่อเครือข่าย
- จำกัดสิทธิ์ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

- ระบุอุปกรณ์เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย
- มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย
- ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่ายโดยไม่ได้รับอนุญาต

(๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้ โดยผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control) ดังนี้

- ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)
- กำหนดให้มีการแปลงหมายเลขเครือข่ายเพื่อแยกเครือข่ายย่อย
- กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านทางที่กำหนดไว้ หรือจำกัดสิทธิ์ในการใช้บริการเครือข่าย

(๔) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๕) การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดของเครื่องคอมพิวเตอร์ที่ขอใช้บริการ (IP Address MAC Address และระบบปฏิบัติการ) และสถานที่ติดตั้ง
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

๔.๔ ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

๔.๕ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

๔.๖ ต้องมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามที่กำหนดไว้ใน พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อย่างเคร่งครัด

๔.๗ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติ ดังต่อไปนี้

(๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร

(๒) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม โดยให้ผู้ดูแลระบบปิดพอร์ตที่ไม่ใช้งาน

(๓) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(๔) การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๔.๘ การแบ่งแยกเครือข่าย (Segregation In Networks) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็นเครือข่ายสำหรับผู้ใช้งานภายในหน่วยงาน (Staff) และเครือข่ายสำหรับผู้ใช้งานภายนอกหน่วยงาน (Guest)

๔.๙ กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๔.๑๐ ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๔.๑๑ ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคล ที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง IP Address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

๕.๑ ขั้นตอนปฏิบัติเพื่อการเข้าใช้งาน

(๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(๒) หลังจากระบบติดตั้งเสร็จ ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

(๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

(๔) ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง

(๕) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

(๖) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

(๗) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการศูนย์หรือผู้ที่ได้รับมอบหมาย

(๘) ซอฟต์แวร์ที่หน่วยงานใช้มีลิขสิทธ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใด ที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

(๙) ซอฟท์แวร์ที่หน่วยงานจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

(๑๐) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของหน่วยงาน เพื่อประโยชน์ทางการค้า

(๑๑) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมบนระบบเครือข่ายของหน่วยงาน

(๑๒) ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้อำนวยการศูนย์หรือผู้ที่ได้รับมอบหมาย

๕.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification And Authentication) ต้องกำหนดให้ผู้ใช้งานทุกคนมีบัญชีผู้ใช้งานแยกกันของแต่ละบุคคล โดยมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคหรือวิธีการพิสูจน์ตัวตนที่มีความเหมาะสมในการยืนยันตัวตน โดยมีแนวปฏิบัติ ดังนี้

(๑) ผู้ดูแลระบบมีหน้าที่บริหารจัดการทะเบียนบัญชีของผู้ใช้งาน ซึ่งประกอบไปด้วยข้อมูลชื่อ-นามสกุล ตำแหน่ง หน่วยงานที่สังกัด รหัสผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

(๒) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงานเพื่อพิสูจน์ตัวตน (User Authentication)

(๓) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกัน หรือบัญชีผู้ใช้งานแบบกลุ่ม ต้องขึ้นอยู่กับความจำเป็นตามภารกิจ (Business Requirements) และให้มีการอนุมัติการใช้งานเป็นลายลักษณ์อักษรเพื่อให้สามารถตรวจสอบได้ว่าใครคือผู้ใช้งานของบัญชีแบบกลุ่มนี้บ้างและกำหนดให้ผู้ใช้งานเหล่านี้ต้องรับผิดชอบร่วมกันกรณีที่มีปัญหาเกิดขึ้น

(๔) กำหนดให้ผู้ดูแลระบบหลีกเลี่ยงการใช้บัญชีผู้ใช้งานที่มีสิทธิ์ในระดับสูง เช่น ในฐานะ Root ฐานะ Administrator เพื่อปฏิบัติงานทั่วไป ซึ่งไม่มีความจำเป็นต้องใช้สิทธิ์ระดับสูงในการทำงานนั้น

๕.๓ การบริหารจัดการรหัสผ่าน (Password Management System) ผ่านระบบบริหารจัดการรหัสผ่านโดยกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านครั้งแรกที่เข้าใช้หรือกำหนดให้เปลี่ยนรหัสผ่านทุก ๓ เดือน โดยสามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ

๕.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use Of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการดังนี้

(๑) จำกัดสิทธิ์การเข้าถึง และกำหนดสิทธิ์อย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) โปรแกรมที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

(๓) ต้องจัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน

(๔) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๕) ผู้ใช้งานไม่ได้รับอนุญาตให้ติดตั้งโปรแกรมอรรถประโยชน์บนเครื่องคอมพิวเตอร์ของหน่วยงาน หากต้องการติดตั้งโปรแกรมดังกล่าว ต้องได้รับอนุญาตและติดตั้งโดยผู้ดูแลระบบ

๕.๕ การหมดเวลาการใช้งานระบบ (Session Time-Out) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น

(๑) กำหนดให้ระบบสารสนเทศยุติการให้บริการหรือใช้งาน เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลา ๑๕ นาทีตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๒) ถ้าไม่มีการใช้งานระบบ ต้องทำการปิดการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบ

(๓) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

(๔) กำหนดให้มีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบอีกครั้ง หลังจากที่ระบบได้หมดเวลาการใช้งานไปแล้ว

๕.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation Of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

(๑) กำหนดให้ระบบสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนด เช่น กำหนดให้ใช้งานได้ ๓ ช.ม. ต่อการเชื่อมต่อหนึ่งครั้ง หรือกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น

(๒) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

(๓) กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application And Information Access Control)

เพื่อป้องกันการเข้าถึงสารสนเทศของแอพพลิเคชั่นโดยไม่ได้รับอนุญาต โดยต้องมีการควบคุมอย่างน้อยดังนี้

๖.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรม

ประยุกต์หรือแอพพลิเคชั่น โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๑) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ (โดยปฏิบัติตามข้อ ๒.๑) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๒.๔) เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

(๒) ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้อำนวยการศูนย์หรือผู้ที่ได้รับมอบหมายเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

(๓) ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศเกิน ๑๕ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

(๔) ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากร (โดยปฏิบัติตามข้อ ๒.๓)

(๕) ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

- ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
- ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล
- กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

- การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น
- กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล
- กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

(๖) กรณีการจ้างเหมาดำเนินการพัฒนาระบบ ดูแล และบำรุงรักษาระบบ (Outsource)

- ก่อนการจ้าง ผู้ดูแลระบบต้องกำหนดสิทธิ์ในการเข้าถึงข้อมูลสารสนเทศและระบบเครือข่ายภายในตามความจำเป็น รวมถึงการทำสัญญารักษาความลับข้อมูลของหน่วยงาน
- ระหว่างการจ้าง ผู้ดูแลระบบต้องควบคุมสิทธิ์ในการเข้าถึงข้อมูลสารสนเทศระบบเครือข่ายภายในของหน่วยงานของผู้ที่ได้รับมอบหมายให้ดำเนินการตลอดระยะเวลาของสัญญาจ้าง
- หลังการจ้าง ผู้ดูแลระบบต้องยกเลิกสิทธิ์ทั้งหมดในการเข้าถึงข้อมูลสารสนเทศระบบเครือข่ายภายในของหน่วยงานของผู้ที่ได้รับมอบหมายให้ดำเนินการ

๖.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการดังนี้

(๑) ต้องแยกระบบซึ่งไวต่อการรบกวนออกจากระบบอื่นๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน โดยระบบซึ่งไวต่อการรบกวน ได้แก่

- ระบบ GFMIS

(๒) มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ ได้แก่ เครือข่ายที่แยกทางกายภาพต่างหากจากเครือข่ายอื่นๆ หรือเครือข่ายเสมือน (Virtual Local Area Network : VLAN) ที่แยกโดยใช้วิธีทางเทคนิค

(๓) อนุญาตให้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ (Mobile Computing) สามารถเข้าถึงระบบซึ่งไวต่อการรบกวนได้จากเครือข่ายภายในหน่วยงานเท่านั้น และไม่สามารถเข้าใช้งานระบบซึ่งไวต่อการรบกวนจากการปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ได้

๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ (Mobile Computing) ต้องมีมาตรการที่เหมาะสมในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ซึ่งต้องปฏิบัติดังนี้

(๑) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๒) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๔) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

(๕) หากปรากฏว่า ความเสียหายที่เกิดขึ้นนั้น เกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๖.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ศูนย์กำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวปฏิบัติ ดังนี้

(๑) ผู้ดูแลระบบตรวจสอบอุปกรณ์ที่ใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล ต้องมีโปรแกรมป้องกันไวรัสและเปิดใช้งานไฟร์วอลล์

(๒) ผู้ดูแลระบบต้องจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล อุปกรณ์การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ใช้งาน

(๓) ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

(๔) ไม่อนุญาตให้ใช้งานอุปกรณ์ที่ไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัย เข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล

(๕) หน่วยงานต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่างๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

(๖) หน่วยงานต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ส่วนที่ ๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๗.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงาน ต้องทำการลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์หรือผู้ที่ได้รับมอบหมาย

๗.๒ ผู้ดูแลระบบ (System Administrator) ต้องดำเนินการดังต่อไปนี้

(๑) ต้องลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

(๒) ต้องลงทะเบียนอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกเครื่องที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(๓) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๔) ต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่เป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน

(๕) ต้องเปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

(๖) ต้องกำหนดค่าใช้ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

(๗) เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้น ที่สามารถเข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

(๘) ต้องมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

(๙) ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการศูนย์ทราบโดยทันที

(๑๐) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

ส่วนที่ ๘ การบริหารจัดการการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๘.๑ การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

(๑) กำหนดให้มีรหัสผู้ใช้งาน/รหัสผ่าน (Username/Password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการ

(๒) กำหนดจำนวนครั้งที่สามารถพิมพ์รหัสผิดได้ไม่เกิน ๓ ครั้ง หากเกินกว่าที่กำหนดระบบต้องทำการ lock ไม่ให้ใช้งานเป็นระยะเวลาไม่น้อยกว่า ๓๐ นาที

(๓) ผู้ดูแลระบบต้องกำหนดรหัสผ่านให้มีคุณสมบัติอย่างน้อยตามที่ระบุไว้ในข้อ ๒.๓

(๔) ผู้ดูแลระบบควรตั้งระบบการล็อคหน้าจอเมื่อไม่มีการใช้งาน เมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

(๕) ผู้ดูแลระบบต้องทำการ log out ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๘.๒ ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ (Control of operational software)

(๑) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

(๒) ผู้ที่มีหน้าที่ดูแลเครื่องคอมพิวเตอร์แม่ข่าย ต้องเป็นผู้ที่ได้รับการอบรมหรือมีความชำนาญเท่านั้น

(๓) ให้มีการจัดเก็บซอร์สโค้ด (Source code) และไลบรารี่สำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๔) ระบบสารสนเทศต้องผ่านการทดสอบตามจุดประสงค์ที่กำหนดไว้ และผ่านการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งระบบสารสนเทศบนเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ปรับปรุงไลบารี่สำหรับซอฟต์แวร์ของระบบงานให้มีความทันสมัยและสอดคล้องกับไลบารี่ทั้งหมดที่ทำการติดตั้ง

(๖) ควรกำหนดรอบระยะเวลาในการจัดเก็บรหัสโปรแกรม / ข้อมูลที่เกี่ยวข้อง / ขั้นตอนปฏิบัติ ของระบบสารสนเทศ เพื่อใช้ในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่า

๘.๓ ทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications after Operating System Changes)

(๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๘.๔ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development)

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์ที่พัฒนาโดยหน่วยงานภายนอก รวมถึงการทำสัญญารักษาความลับข้อมูลของหน่วยงาน

(๒) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

(๓) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(๕) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านและยกเลิกสิทธิ์ต่างๆ ของหน่วยงานภายนอกทั้งหมด

๘.๕ มาตรการควบคุมช่องโหว่ทางเทคนิค

(๑) กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ โดยมีการบันทึกดังต่อไปนี้

- ชื่อซอฟต์แวร์และเวอร์ชั่นที่ใช้งาน
- สถานที่ที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้นๆ

(๒) กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

(๓) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบดำเนินการดังนี้

- มีการเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

- ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน
- กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

(๔) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๘.๖ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ข้อมูลชื่อบัญชีผู้ใช้งาน

(๒) ข้อมูลวันเวลาที่เข้าถึงระบบ

(๓) ข้อมูลวันเวลาที่ออกจากระบบ

(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้นระหว่างการใช้งานระบบสารสนเทศ

(๕) ข้อมูลแสดงการใช้งานแอพพลิเคชัน

(๖) ข้อมูลไอพีแอดเดรสที่เข้าถึง

(๗) ข้อมูลแสดงการสำรองข้อมูล

ส่วนที่ ๙ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer) และเครื่องคอมพิวเตอร์แบบพกพา (Computer Notebook)

๙.๑ การใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ของหน่วยงานที่อนุญาตให้ผู้ใช้งานใช้งาน ถือเป็นทรัพย์สินของหน่วยงาน ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพ

(๒) โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมายหรือเป็นโปรแกรมประเภทโอเพ่นซอร์สที่ไม่มีค่าใช้จ่าย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งานติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน

(๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการตามมาตรการการนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน และการกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

(๕) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่

(๖) ห้ามนำอาหารหรือเครื่องดื่มวางใกล้บริเวณการใช้งานของอุปกรณ์คอมพิวเตอร์

(๗) ห้ามวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

(๘) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

(๙) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๑๐) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๑๑) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๑๒) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

(๑๓) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(๑๔) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๑๕) ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในเครื่องคอมพิวเตอร์รวมถึงแบตเตอรี่

๙.๒ การใช้รหัสผ่านให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในข้อ ๒.๓

๙.๓ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(๑) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Flash Drive ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๒) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

(๓) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่ กำหนดไว้

๙.๔ การสำรองข้อมูลและการกู้คืนข้อมูล

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญที่เกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

ส่วนที่ ๑๐ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๑๐.๑ เจ้าของข้อมูลต้องกำหนดชั้นความลับของข้อมูลและนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ และทบทวนความเหมาะสมของของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๑๐.๒ ผู้ดูแลระบบต้องกำหนดวิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ โดยกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

๑๐.๓ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๑๐.๔ หน่วยงานควรมีวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับอย่างเหมาะสม

๑๐.๕ หน่วยงานควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๑๐.๖ ผู้ใช้งานต้องทำการเข้ารหัสกับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

ส่วนที่ ๑๑ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๑.๑ การใช้งานสำหรับผู้ใช้งาน

(๑) ผู้ใช้งานที่ต้องการใช้งาน E-Mail ของหน่วยงานต้องทำการกรอกข้อมูลคำขอเข้าใช้งานและยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิ์ชื่อผู้ใช้งานรายใหม่และรหัสผ่าน (Password)

(๒) เมื่อได้รับรหัสผ่าน (Password) จะต้องเปลี่ยนรหัสผ่าน (Password) โดยทันทีหลังจากการเข้าสู่ระบบเป็นครั้งแรก

(๓) ต้องใช้ E-Mail ของหน่วยงานเพื่อติดต่องานของราชการเท่านั้น

(๔) ไม่ควรใช้ E-Mail Address ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของ E-Mail และให้ถือว่าเจ้าของ E-Mail เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ใน E-Mail ของตน

(๕) หลังจากการใช้งาน ควรลงชื่อออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานระบบ

(๖) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

(๗) ควรตรวจสอบและลบ E-Mail ของตนเองทุกวัน เพื่อลดปริมาณการใช้พื้นที่ของระบบ E-Mail ให้เหลือจำนวนน้อยที่สุด

(๘) ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

(๙) ปฏิบัติตามวิธีการใช้งานรหัสผ่าน (Password Use) ที่ได้กำหนดไว้อย่างเคร่งครัด

(๑๐) ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

(๑๑) ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

(๑๒) ห้ามส่ง E-Mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิ์ของบุคคลอื่น

(๑๓) ห้ามส่ง E-Mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

(๑๔) ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

(๑๕) ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

(๑๖) ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงานผ่านทางจดหมายอิเล็กทรอนิกส์

๑๑.๒ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ (System Administrator)

(๑) กำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงานให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน

(๒) มีการทบทวนสิทธิ์การเข้าใช้งานและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น การลาออก โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

(๓) มีการควบคุมการเข้าถึงระบบตามแนวทางการบริหารจัดการเข้าถึงผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้อย่างเคร่งครัด

ส่วนที่ ๑๒ การใช้งานระบบอินเทอร์เน็ต (Internet)

๑๒.๑ ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-Up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและได้รับการอนุมัติจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมายเป็นลายลักษณ์อักษรแล้วเท่านั้น

๑๒.๒ การใช้งานเครื่องคอมพิวเตอร์ จะต้องมีการป้องกันโปรแกรมไม่พึงประสงค์และทำการอุดช่องโหว่ของระบบปฏิบัติการก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บบราวเซอร์

๑๒.๓ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของหน่วยงาน และต้องไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงานเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงแห่งชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับหน่วยงาน เป็นต้น

๑๒.๔ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๑๒.๕ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๑๒.๖ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

๑๒.๗ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

๑๒.๘ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๑๒.๙ ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่างเคร่งครัด

ส่วนที่ ๑๓ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๓.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

๑๓.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอและต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์

๑๓.๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับหน่วยงาน ผู้ใช้งานต้องแจ้งต่อศูนย์โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

ส่วนที่ ๑๔ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ ให้ปฏิบัติดังต่อไปนี้

๑๔.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง

๑๔.๒ ห้ามแก้ไขข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

๑๔.๓ กำหนดให้มีการบันทึกการทำงานของระบบสารสนเทศในการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น และต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน เพื่อประโยชน์ในการใช้ตรวจสอบ โดยปฏิบัติตามพ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑๔.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวดที่ ๒

การจัดทำระบบสำรองของระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงาน ให้บริการได้อย่างต่อเนื่อง

๒. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงาน และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

๑. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานตามแนวทางต่อไปนี้

๑.๑ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(๑) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

(๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

(๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง ผลการสำรองข้อมูลสำเร็จ/ไม่สำเร็จ เป็นต้น

(๔) ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกกูเรชัน ข้อมูลในฐานข้อมูล เป็นต้น

(๕) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

(๖) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น

(๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

(๘) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(๙) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(๑๐) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

(๑๑) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๒. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

๒.๑ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญและกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุม ประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่ายฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุฉุกเฉิน เป็นต้น

๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๔. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

๕. ต้องมีการทบทวนแนวทางการจัดทำสำรองของระบบสารสนเทศ และแผนเตรียมความพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๓

การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)

๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

๑.๑ จัดลำดับความสำคัญของความเสี่ยง

๑.๒ ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

๑.๓ ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

๑.๔ สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

๑.๕ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

๑.๖ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆ ได้ ๔ ประเภท ดังนี้

ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดทำงาน และส่งผลให้ ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

(๑) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human error ลดน้อยลง

(๒) จัดทำหนังสือแจ้งเวียนผู้ใช้งานทั้งส่วนกลางและส่วนภูมิภาค เรื่อง การใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

ประเภทที่ ๒ ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเตอร์เน็ต (Internet Worm), ม้าโทรจัน (Trojan Horse), และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

(๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก

(๒) ติดตั้งซอฟต์แวร์ Anti virus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

ประเภทที่ ๓ ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(๒) ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

ประเภทที่ ๔ ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

(๒) ถอดเทป Back up ข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย

(๓) ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเบรคเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า

(๔) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในที่สูง

(๕) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์ แม่ข่ายและอุปกรณ์เครือข่าย

(๖) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบเครือข่ายว่า สามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

(๗) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ

หมวดที่ ๔

การสร้างความรู้ความเข้าใจและตระหนักในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจและตระหนักในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของหน่วยงาน
๒. เพื่อเป็นการป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน
๓. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

๑. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงานอย่างสม่ำเสมอหรือ ทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ
๒. จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน
๓. จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน
๔. จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดให้ความรู้

๕. มีการประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะของเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงเนื้อหาความรู้ให้ทันสมัยอยู่เสมอ

แผนเตรียมความพร้อมกรณีฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

สป.วท. ได้ตระหนักถึงโอกาสที่จะประสบกับสถานการณ์ความไม่แน่นอน และความสูญเสียที่เกิดจากภัยพิบัติต่างๆ อาทิ กระแสไฟฟ้าขัดข้องอันเนื่องจากไฟฟ้าดับ ไฟฟ้าตก ไฟฟ้ากระชาก หรือมีสัญญาณรบกวนเกิดไฟไหม้ ระบบเครือข่ายขัดข้องใช้งานไม่ได้ เป็นต้น ซึ่งจะสร้างความเสียหายแกทรัพย์สินของทางราชการ รวมทั้งอุปกรณ์เทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของ สป.วท. จึงได้มีการวิเคราะห์และวางแผนการป้องกัน/แก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้น ดังต่อไปนี้

การกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

สป.วท. ได้จัดตั้งทีมงานและมอบหมายหน้าที่ความรับผิดชอบ เพื่อรองรับกับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

๑. ระดับนโยบาย

ทำหน้าที่รับผิดชอบในการกำหนดนโยบายและทิศทาง รวมทั้งให้ข้อเสนอแนะ/คำปรึกษา ตลอดจนการติดตาม กำกับ ดูแล ควบคุม และตรวจสอบการปฏิบัติงาน โดยมีผู้รับผิดชอบ ได้แก่

- ผู้บริหารระดับสูงสุด (CEO)
- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำกระทรวง (CIO)
- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ระดับปฏิบัติการ

๒.๑ ทีมบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร

มีหน้าที่หลักในการบริหารจัดการและประสานงานต่างๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีผู้รับผิดชอบ ได้แก่

นายพฤทธิ์ แกะกระโทก หมายเลขติดต่อ ๐-๒๓๓๓-๓๘๒๖
น.ส.สุพนิดา อารยเมธี หมายเลขติดต่อ ๐-๒๓๓๓-๓๘๒๐
น.ส.ศุภกร สาระวงศ์ หมายเลขติดต่อ ๐-๒๓๓๓-๓๗๐๐ ต่อ ๑๑๑๑
นายกิตติศักดิ์ วงศ์ธานุวัฒน์ หมายเลขติดต่อ ๐-๒๓๓๓-๓๗๐๐ ต่อ ๑๑๒๒

๒.๒ ทีมอาคารสถานที่

มีหน้าที่จัดเตรียมสถานที่สำรอง รวมถึงระบบไฟฟ้า ระบบสื่อสาร และบริหารจัดการอาคารและสถานที่ของ สป.วท. โดยมีผู้รับผิดชอบ ได้แก่

นายสมาน ยะก๊บ หมายเลขติดต่อ ๐-๒๓๓๓-๓๙๖๐

นายวิชา พลบุบผา หมายเลขติดต่อ ๐-๒๓๓๓-๓๗๐๐ ต่อ ๑๐๒๐

นายเหรียญ เกษไธสง หมายเลขติดต่อ ๐-๒๓๓๓-๓๗๐๐ ต่อ ๑๐๓๐

แผนการดำเนินการกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

เมื่อเกิดเหตุการณ์ที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้ดำเนินการดังต่อไปนี้

๑. แจ้งทีมบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุเหตุที่ไม่สามารถดำเนินการผ่านระบบได้

๒. ผู้ใช้งานดำเนินการด้วยวิธีการจดบันทึกข้อมูลลงกระดาษ เพื่อใช้สำหรับการบันทึกรายการเข้าสู่ระบบ

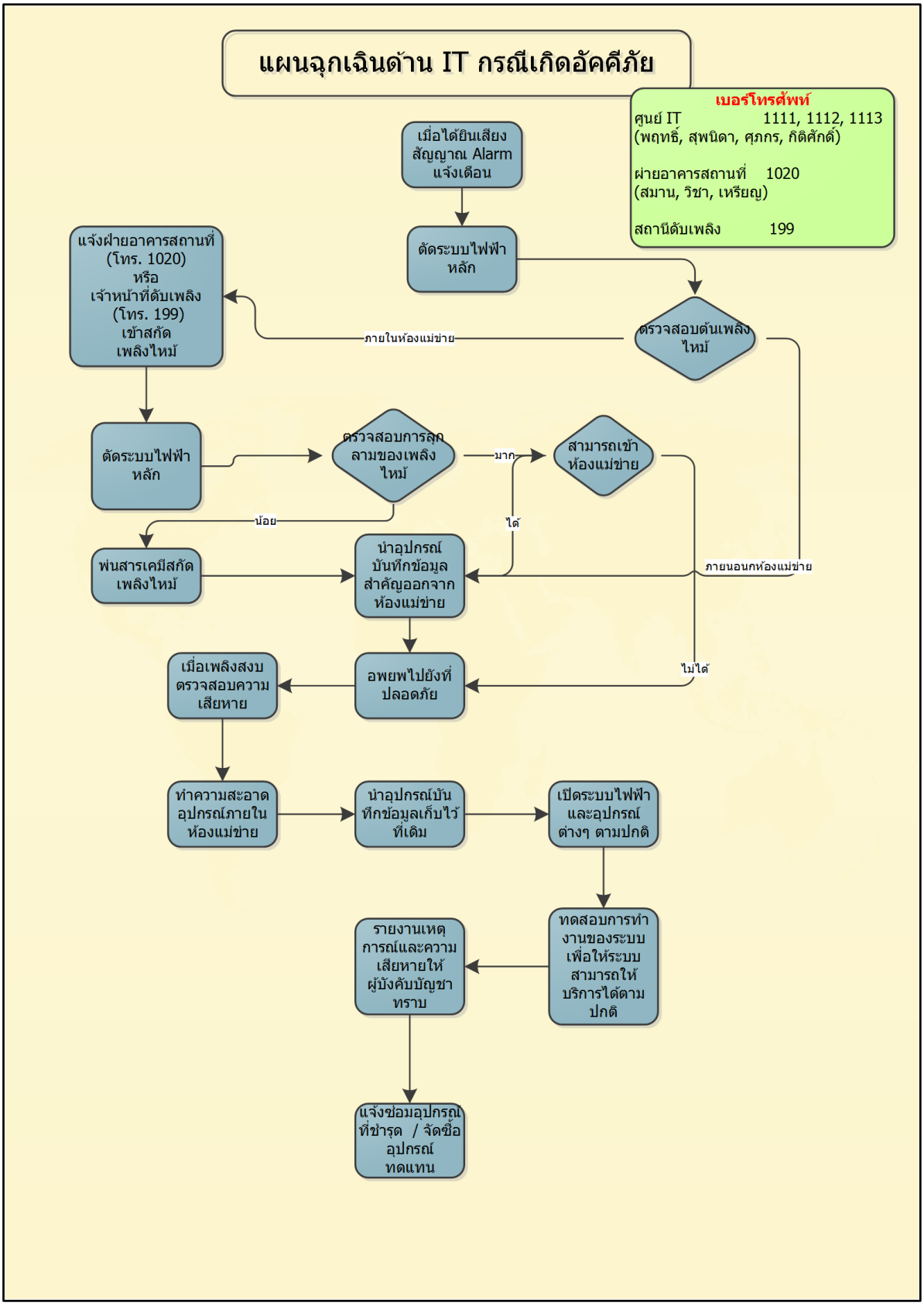
๓. ทีมบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการตรวจสอบและแก้ไขโดยด่วนหลังจากได้รับแจ้งเหตุ

เมื่อมีการกู้คืนระบบงาน

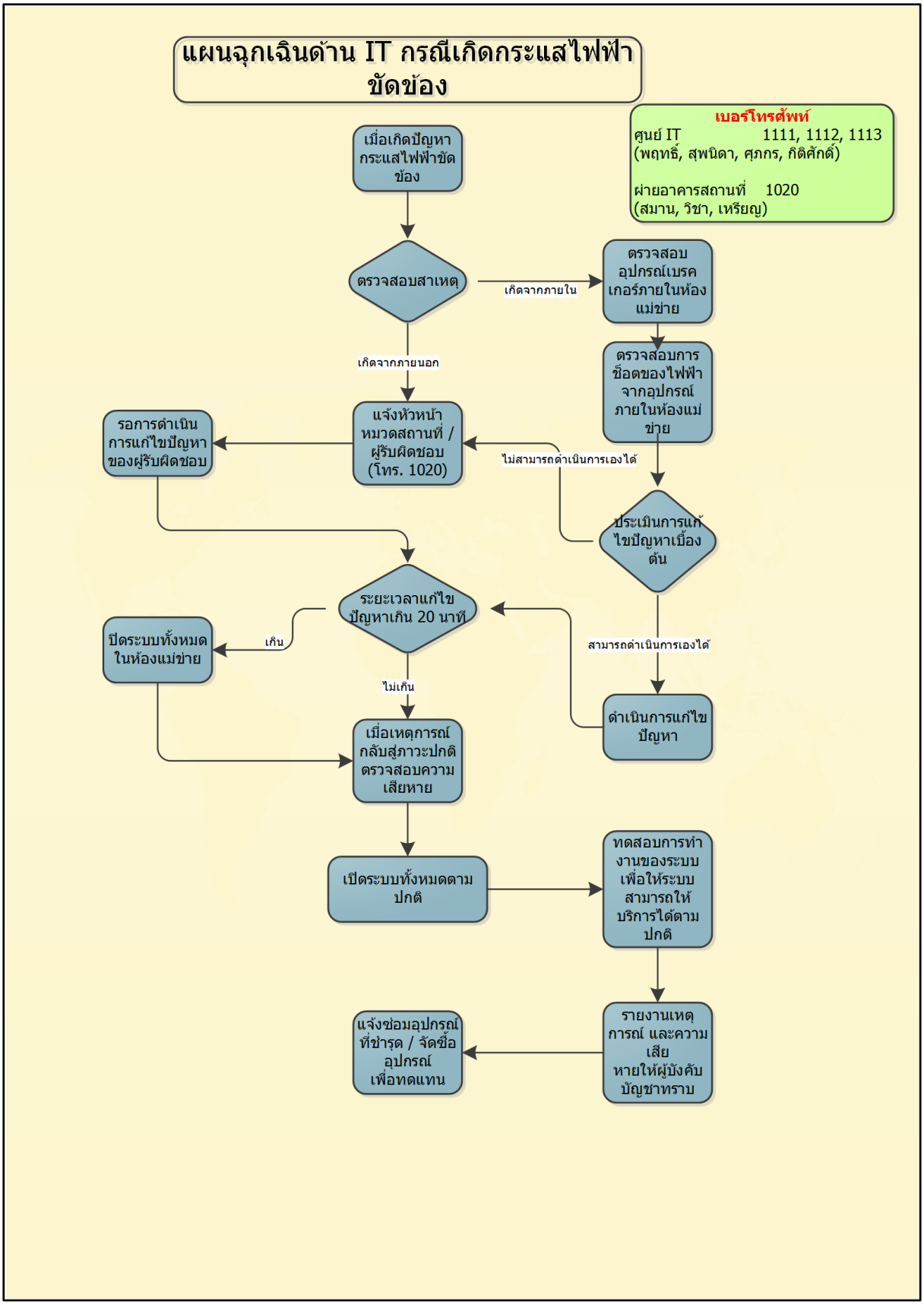
๑. ทีมบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารตรวจสอบสถานะของข้อมูลที่กู้คืนได้ และสร้างข้อมูลที่เสียหายขึ้นมาใหม่

๒. บันทึกรายการที่เกิดขึ้นระหว่างที่ระบบล้มเหลว และระมัดระวังไม่ให้มีการบันทึกรายการซ้ำหรือผิดพลาด

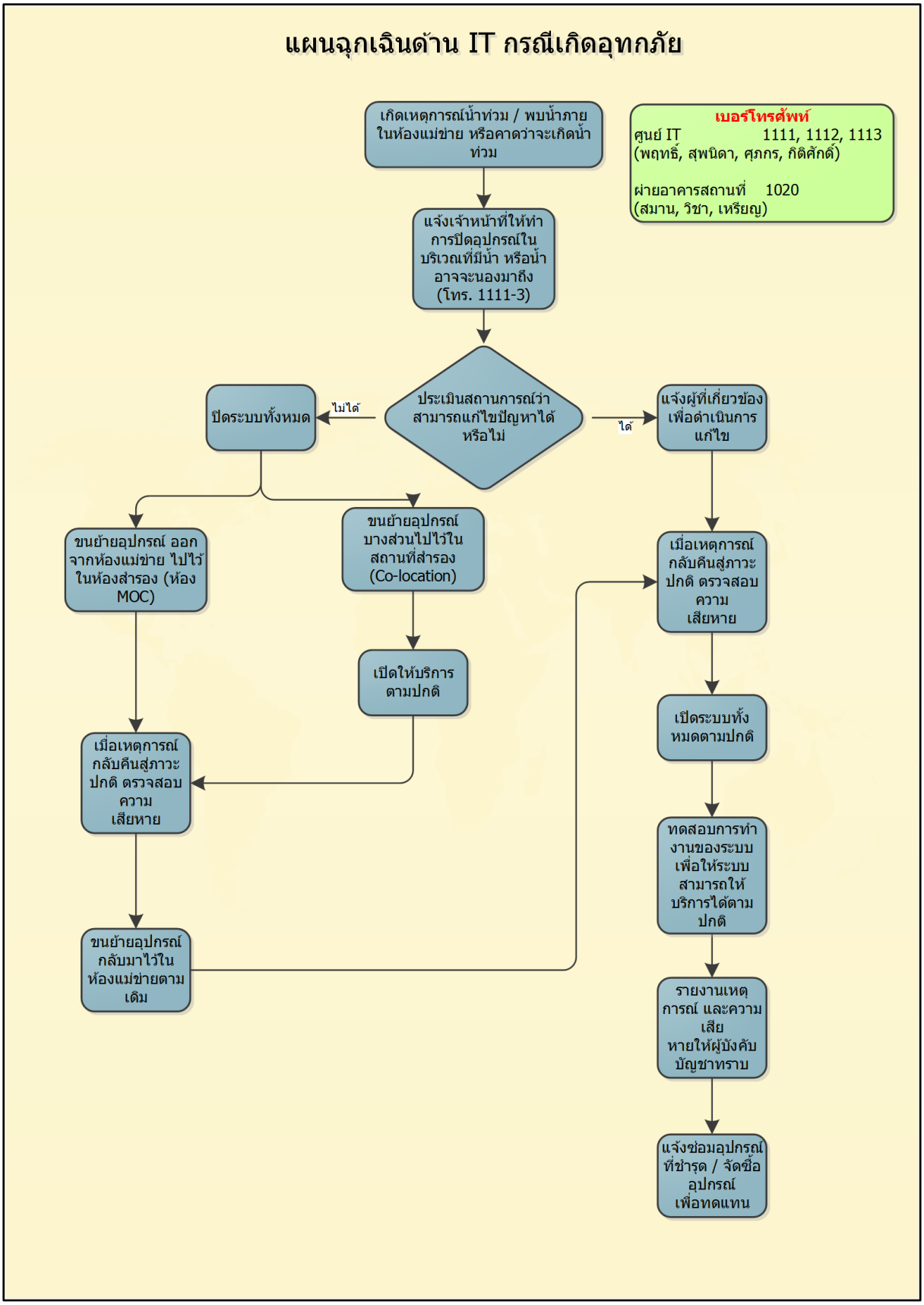
แผนการดำเนินการเมื่อเกิดอัคคีภัย



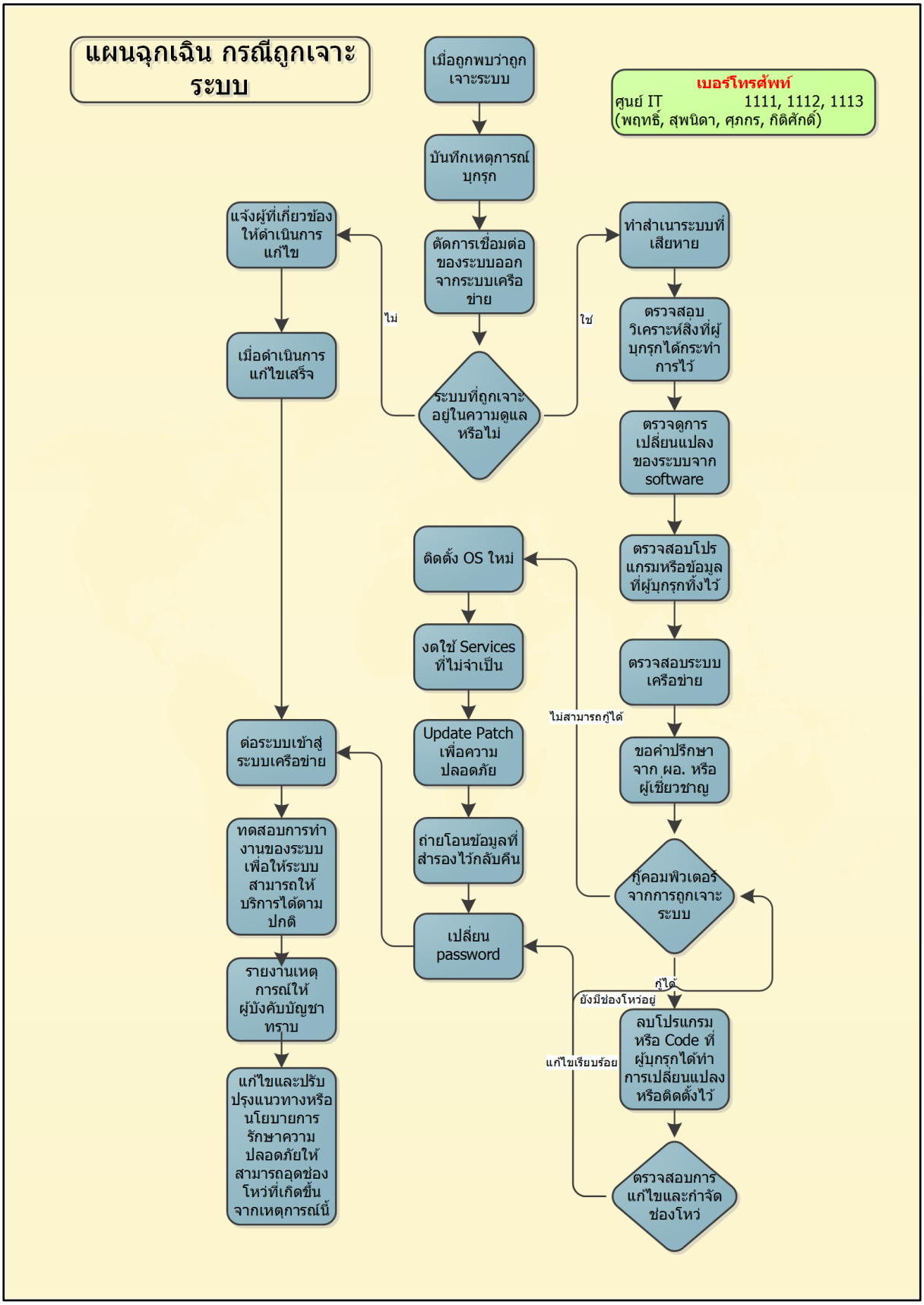
แผนการดำเนินการเมื่อเกิดเหตุไฟฟ้าขัดข้อง



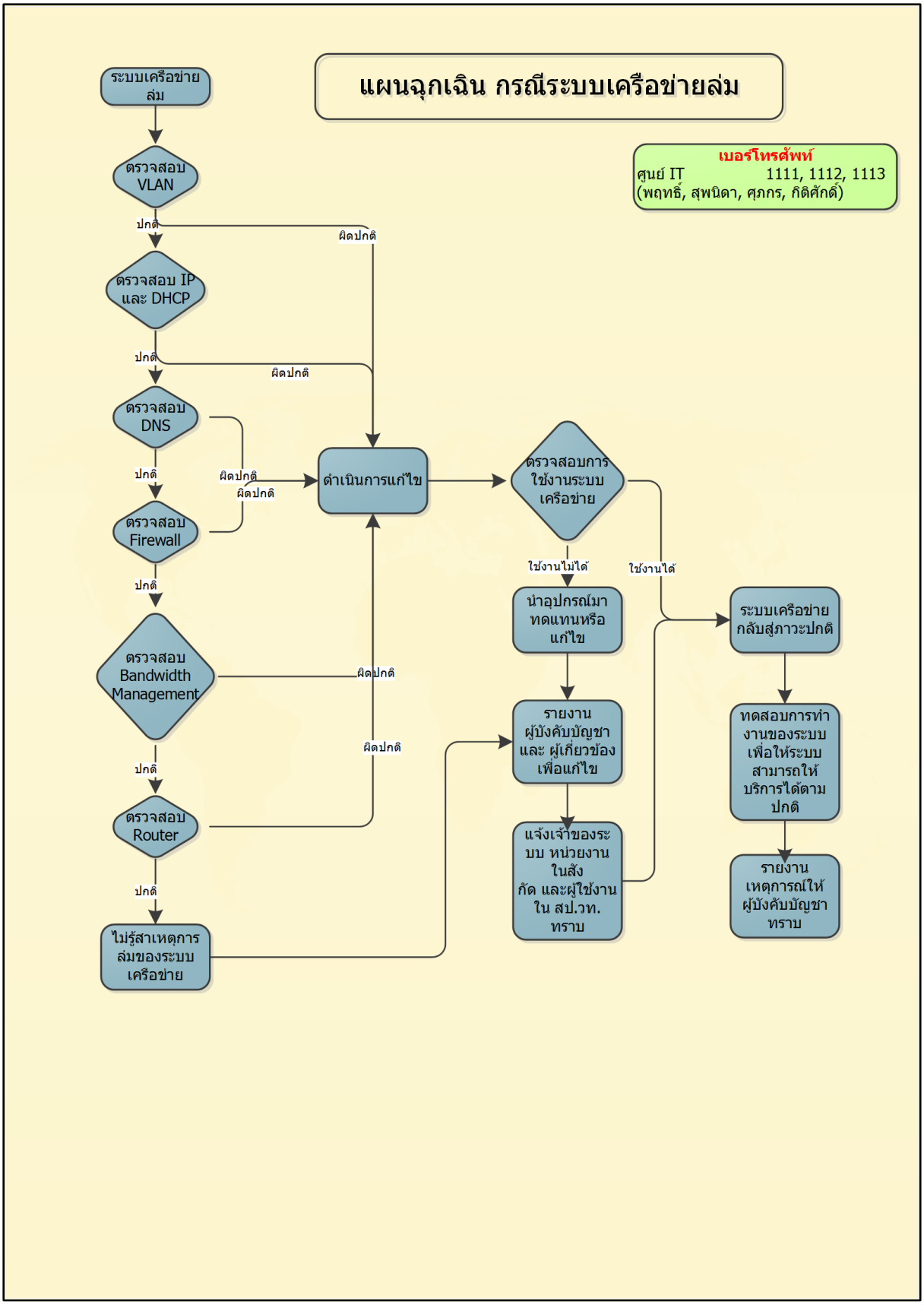
แผนการดำเนินการเมื่อเกิดน้ำท่วม



แผนการดำเนินการเมื่อถูกเจาะระบบ



แผนการดำเนินการเมื่อระบบเครือข่ายใช้งานไม่ได้



แผนการสำรองกู้คืนข้อมูล (Backup and Restore)

ศูนย์สารสนเทศและการสื่อสารได้ดำเนินการ backup เครื่องแม่ข่ายที่อยู่บนระบบ Virtualization ซึ่งมีเครื่องแม่ข่ายทั้งหมด 40 ระบบ ดังมีรายละเอียดดังนี้

: รายละเอียดเครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน (Virtual Machine) ของ สป.วท.

(HOST) VMWare ESXi
192.168.3.12
192.168.3.13
192.168.3.14
192.168.3.15

จะดำเนินการติดตั้ง ระบบป้องกันเครือข่ายคอมพิวเตอร์แบบเสมือน 4 โมดูล (ตามจำนวน ESXi ที่มีอยู่) ในส่วนนี้

	(GUEST) Web Application (Virtual Machine)		
1	ArcSightConnector CentOS 6.5	21	vm13.web-cloud.l
2	BlueCatAddressManager	22	vm14.app-dev.s
3	Cisco Sourcefire MGT POC	23	vm15.sarabun-dev.s
4	Mobile_STKC_Server	24	vm16.AD.Secondary
5	SolarWinds Virtualization Manager	25	vm17.Pentest
6	STKC_Server	26	vm18.Office
7	Vcenter	27	vm19.Anti Virus
8	vCenter Mobile Access	28	vm20.VidyoDashboard
9	vm01.ad1.s	29	vm21.db3.m
10	vm02.ad2.s	30	vm22.report.s
11	vm03.web.s.dmz	31	vm23.web.OPS
12	vm04.web-cms.s	32	vm24.Dell Enterprise Manager
13	vm05.web.s	33	vm25.Scimuseum.STKC
14	vm06.db1.m	34	vm26.DMS
15	vm07.db2.m	35	vm27.CAS
16	vm08.web.m.dmz	36	vm28.web.php55.m
17	vm09.web-cms.m	37	vm29.web2.php55
18	vm10.web.m	38	vm30.web.hr.m
19	vm11.app.l.dmz	39	vm31.db.mssql.m
20	vm12.db3.m	40	vm32.DocMoc.m

* HOST : คือ เครื่องคอมพิวเตอร์ตัวหลักที่เป็นเครื่องคอมพิวเตอร์จริงๆ จะทำหน้าที่คอยควบคุมเครื่องคอมพิวเตอร์แบบเสมือน หรือที่เรียกว่า GUEST ที่อยู่ในระบบเสมือนทั้งหมด
*GUEST : คือ เครื่องคอมพิวเตอร์แบบเสมือน ที่สร้างหรือจำลองไว้ใน HOST ซึ่งเราสามารถสร้างได้หลายๆ GUEST ตามประสิทธิภาพที่ HOST รองรับได้

การดำเนินการ Backup

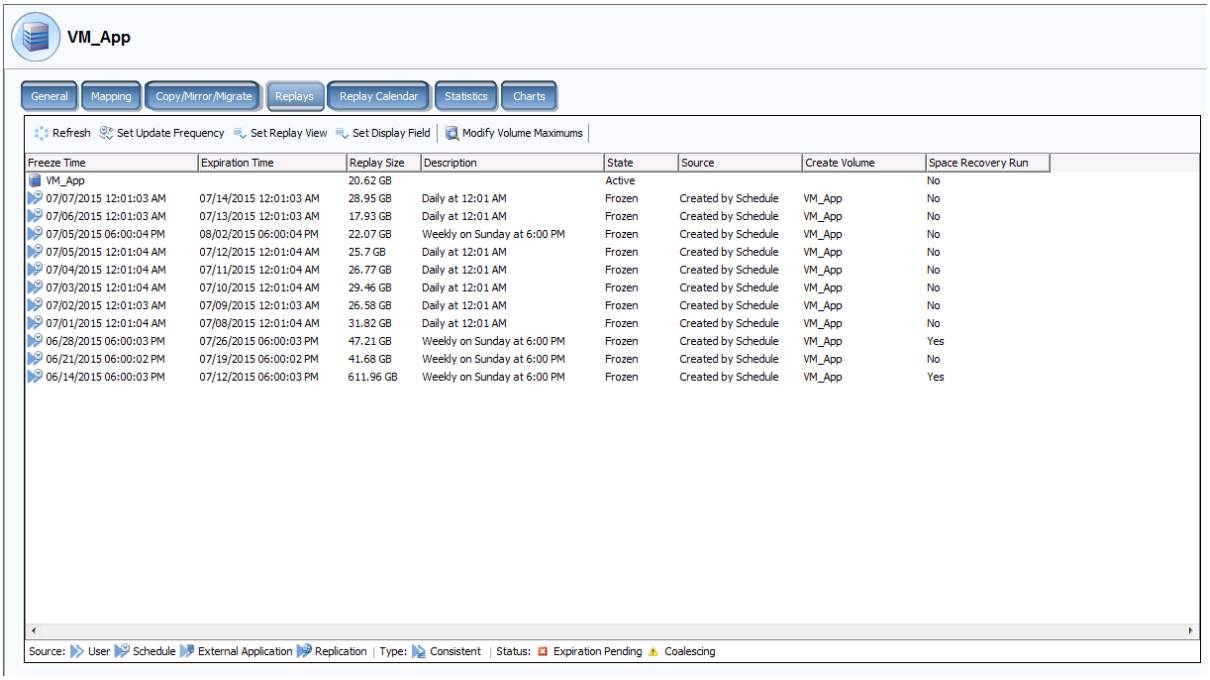
1. ดำเนินการ backup แบบ Full backup ทุกวันอาทิตย์ในแต่ละสัปดาห์

2. ดำเนินการ backup แบบ Incremental backup ทุกวัน จ-ส ในแต่ละสัปดาห์

3. ดำเนินการ backup แบบ Differential backup ทุกวันหากเกิดการเปลี่ยนแปลงของข้อมูล

4. ดำเนินการ backup ลงเทปทุกๆ 3 เดือน

ดังแสดงรายละเอียดตามแผนภาพดังนี้



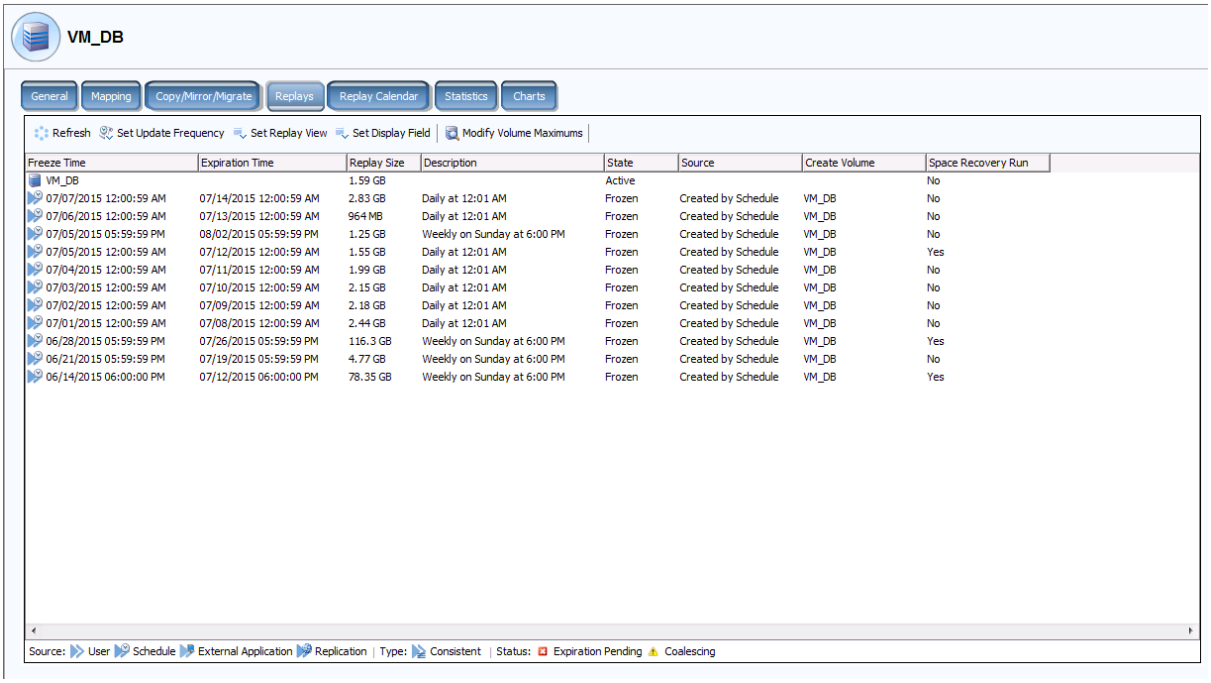
VM_App

General | Mapping | Copy/Mirror/Migrate | Replays | Replay Calendar | Statistics | Charts

Refresh | Set Update Frequency | Set Replay View | Set Display Field | Modify Volume Maximums

Freeze Time	Expiration Time	Replay Size	Description	State	Source	Create Volume	Space Recovery Run
VM_App		20.62 GB		Active			No
07/07/2015 12:01:03 AM	07/14/2015 12:01:03 AM	28.95 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_App	No
07/06/2015 12:01:03 AM	07/13/2015 12:01:03 AM	17.93 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_App	No
07/05/2015 06:00:04 PM	08/02/2015 06:00:04 PM	22.07 GB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_App	No
07/05/2015 12:01:04 AM	07/12/2015 12:01:04 AM	25.7 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_App	No
07/04/2015 12:01:04 AM	07/11/2015 12:01:04 AM	26.77 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_App	No
07/03/2015 12:01:04 AM	07/10/2015 12:01:04 AM	29.46 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_App	No
07/02/2015 12:01:03 AM	07/09/2015 12:01:03 AM	26.58 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_App	No
07/01/2015 12:01:04 AM	07/08/2015 12:01:04 AM	31.82 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_App	No
06/28/2015 06:00:03 PM	07/26/2015 06:00:03 PM	47.21 GB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_App	Yes
06/21/2015 06:00:02 PM	07/19/2015 06:00:02 PM	41.68 GB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_App	No
06/14/2015 06:00:03 PM	07/12/2015 06:00:03 PM	611.96 GB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_App	Yes

Source: User | Schedule | External Application | Replication | Type: Consistent | Status: Expiration Pending | Coalescing



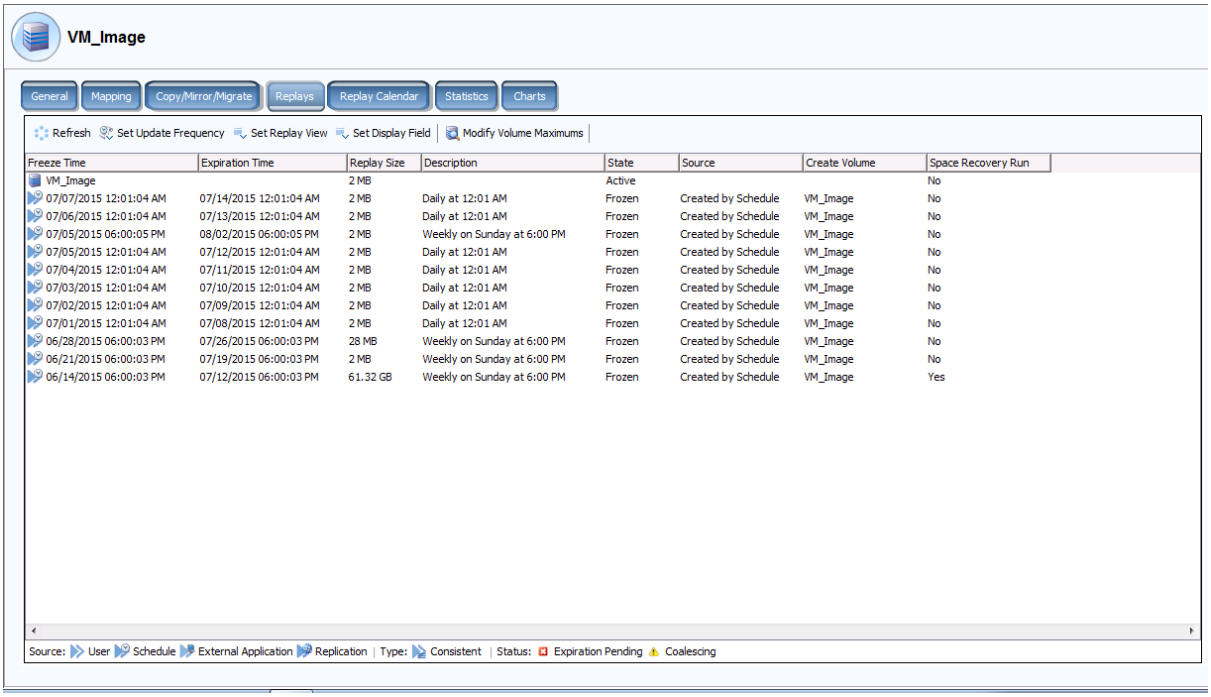
VM_DB

General | Mapping | Copy/Mirror/Migrate | Replays | Replay Calendar | Statistics | Charts

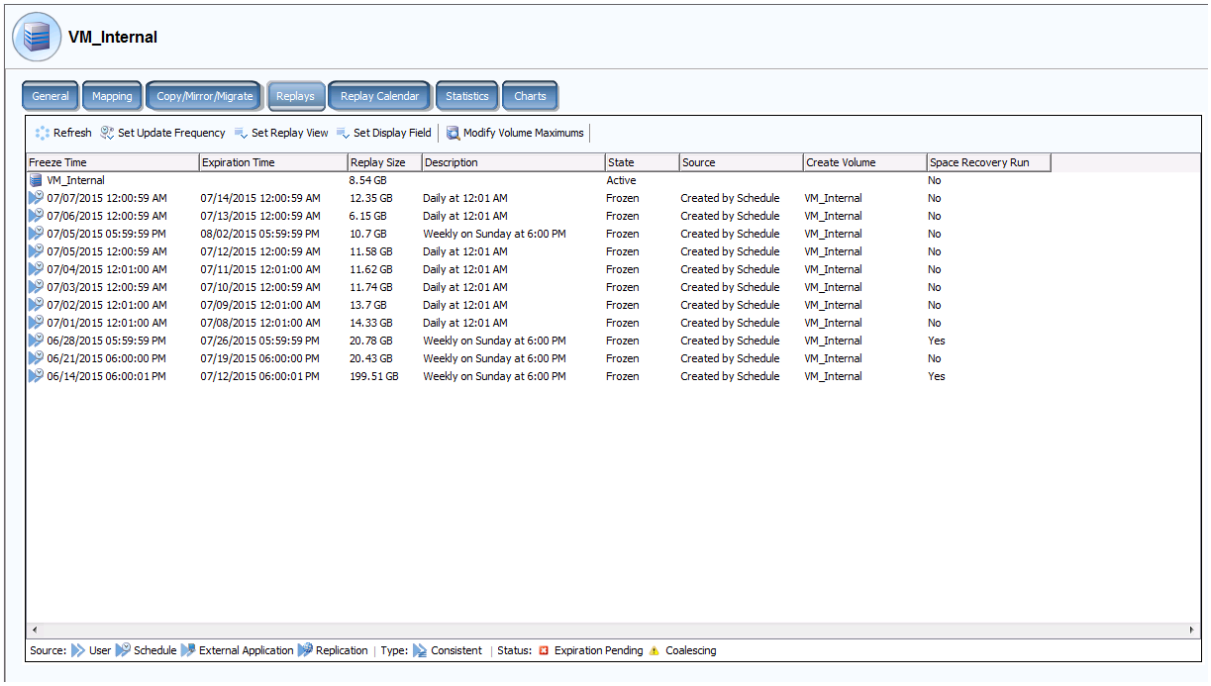
Refresh | Set Update Frequency | Set Replay View | Set Display Field | Modify Volume Maximums

Freeze Time	Expiration Time	Replay Size	Description	State	Source	Create Volume	Space Recovery Run
VM_DB		1.59 GB		Active			No
07/07/2015 12:00:59 AM	07/14/2015 12:00:59 AM	2.83 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_DB	No
07/06/2015 12:00:59 AM	07/13/2015 12:00:59 AM	964 MB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_DB	No
07/05/2015 05:59:59 PM	08/02/2015 05:59:59 PM	1.25 GB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_DB	No
07/05/2015 12:00:59 AM	07/12/2015 12:00:59 AM	1.55 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_DB	Yes
07/04/2015 12:00:59 AM	07/11/2015 12:00:59 AM	1.99 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_DB	No
07/03/2015 12:00:59 AM	07/10/2015 12:00:59 AM	2.15 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_DB	No
07/02/2015 12:00:59 AM	07/09/2015 12:00:59 AM	2.18 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_DB	No
07/01/2015 12:00:59 AM	07/08/2015 12:00:59 AM	2.44 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_DB	No
06/28/2015 05:59:59 PM	07/26/2015 05:59:59 PM	116.3 GB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_DB	Yes
06/21/2015 05:59:59 PM	07/19/2015 05:59:59 PM	4.77 GB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_DB	No
06/14/2015 06:00:00 PM	07/12/2015 06:00:00 PM	78.35 GB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_DB	Yes

Source: User | Schedule | External Application | Replication | Type: Consistent | Status: Expiration Pending | Coalescing

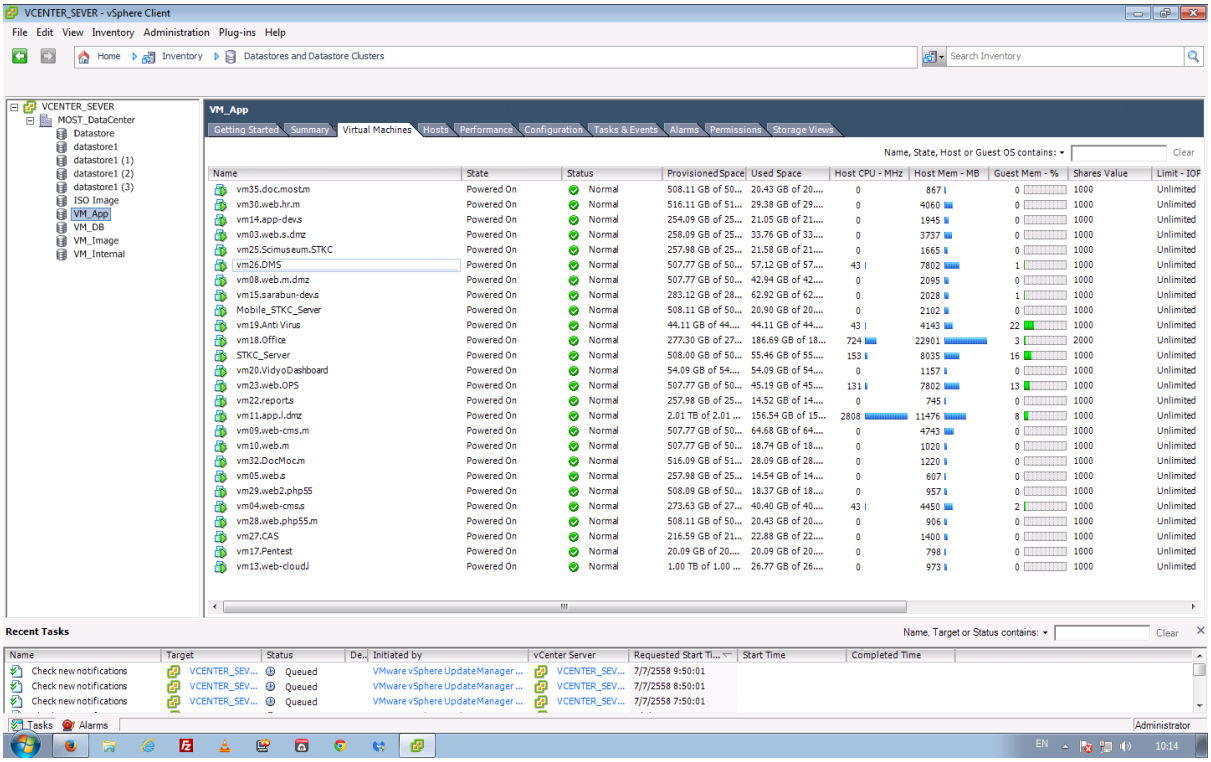


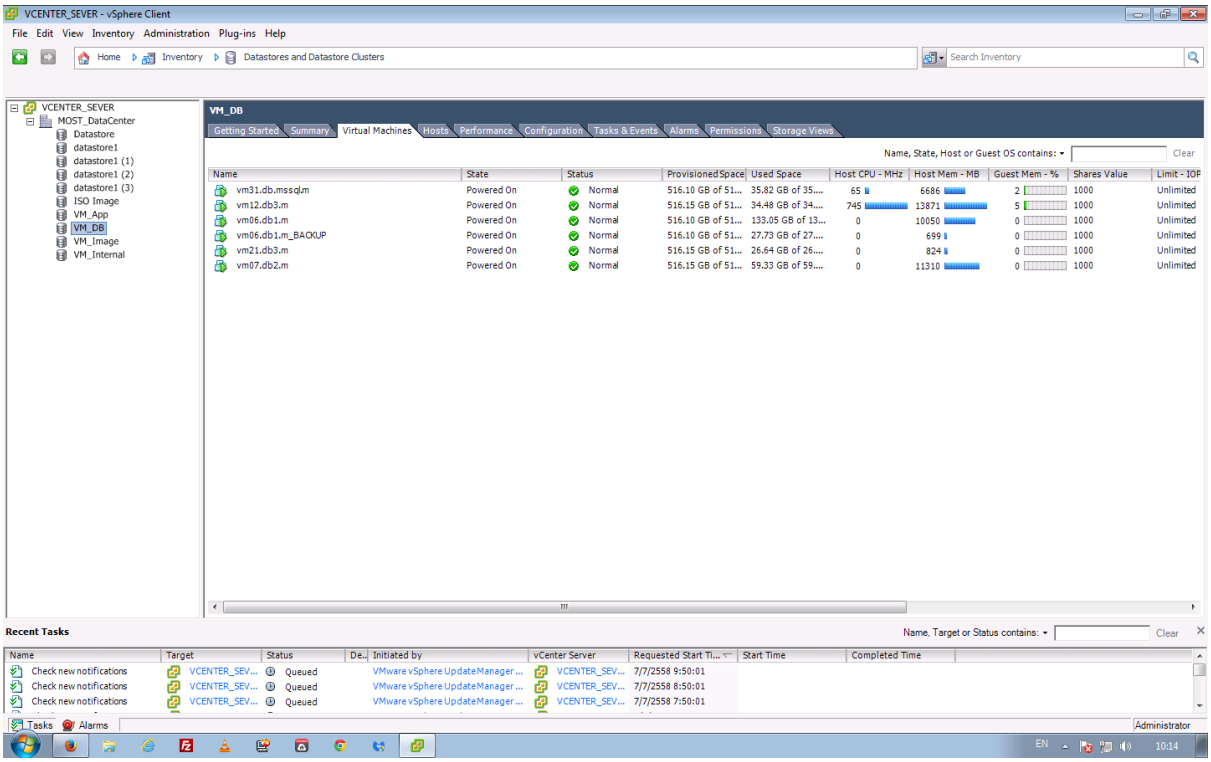
Freeze Time	Expiration Time	Replay Size	Description	State	Source	Create Volume	Space Recovery Run
VM_Image		2 MB		Active			No
07/07/2015 12:01:04 AM	07/14/2015 12:01:04 AM	2 MB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_Image	No
07/06/2015 12:01:04 AM	07/13/2015 12:01:04 AM	2 MB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_Image	No
07/05/2015 06:00:05 PM	08/02/2015 06:00:05 PM	2 MB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_Image	No
07/05/2015 12:01:04 AM	07/12/2015 12:01:04 AM	2 MB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_Image	No
07/04/2015 12:01:04 AM	07/11/2015 12:01:04 AM	2 MB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_Image	No
07/03/2015 12:01:04 AM	07/10/2015 12:01:04 AM	2 MB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_Image	No
07/02/2015 12:01:04 AM	07/09/2015 12:01:04 AM	2 MB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_Image	No
07/01/2015 12:01:04 AM	07/08/2015 12:01:04 AM	2 MB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_Image	No
06/28/2015 06:00:03 PM	07/26/2015 06:00:03 PM	28 MB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_Image	No
06/21/2015 06:00:03 PM	07/19/2015 06:00:03 PM	2 MB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_Image	No
06/14/2015 06:00:03 PM	07/12/2015 06:00:03 PM	61.32 GB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_Image	Yes

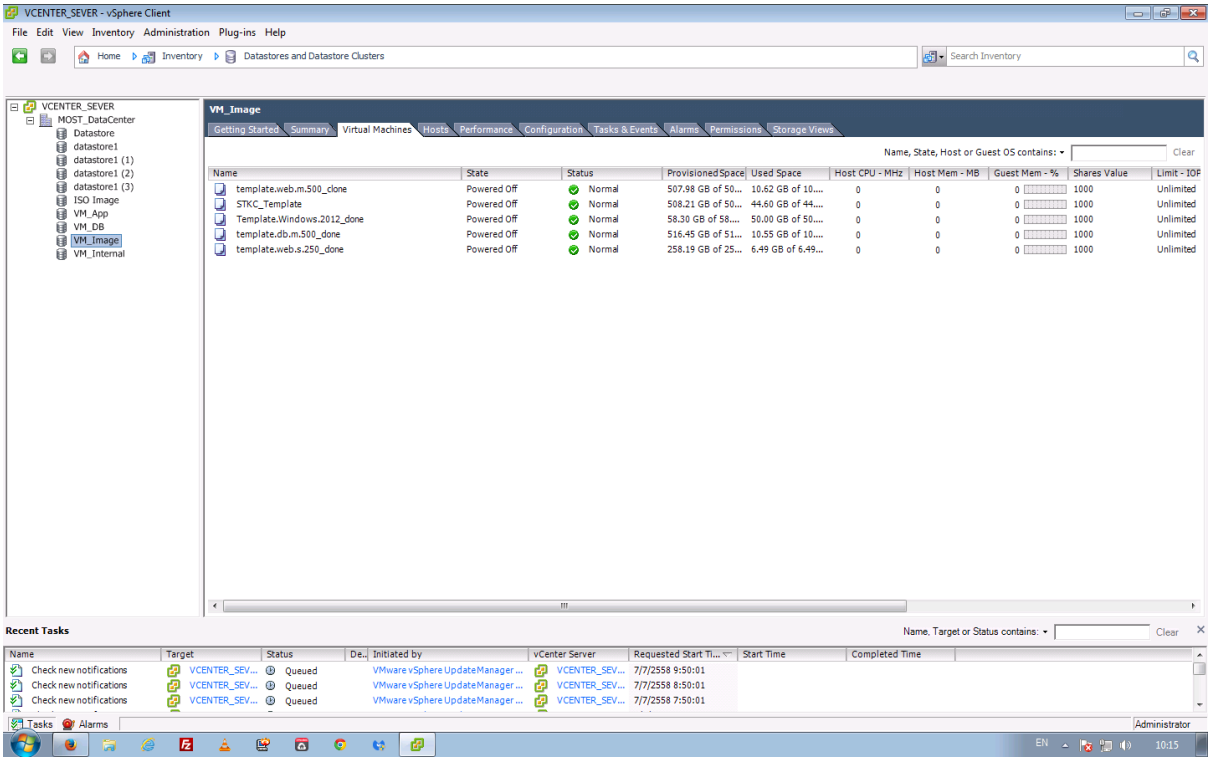


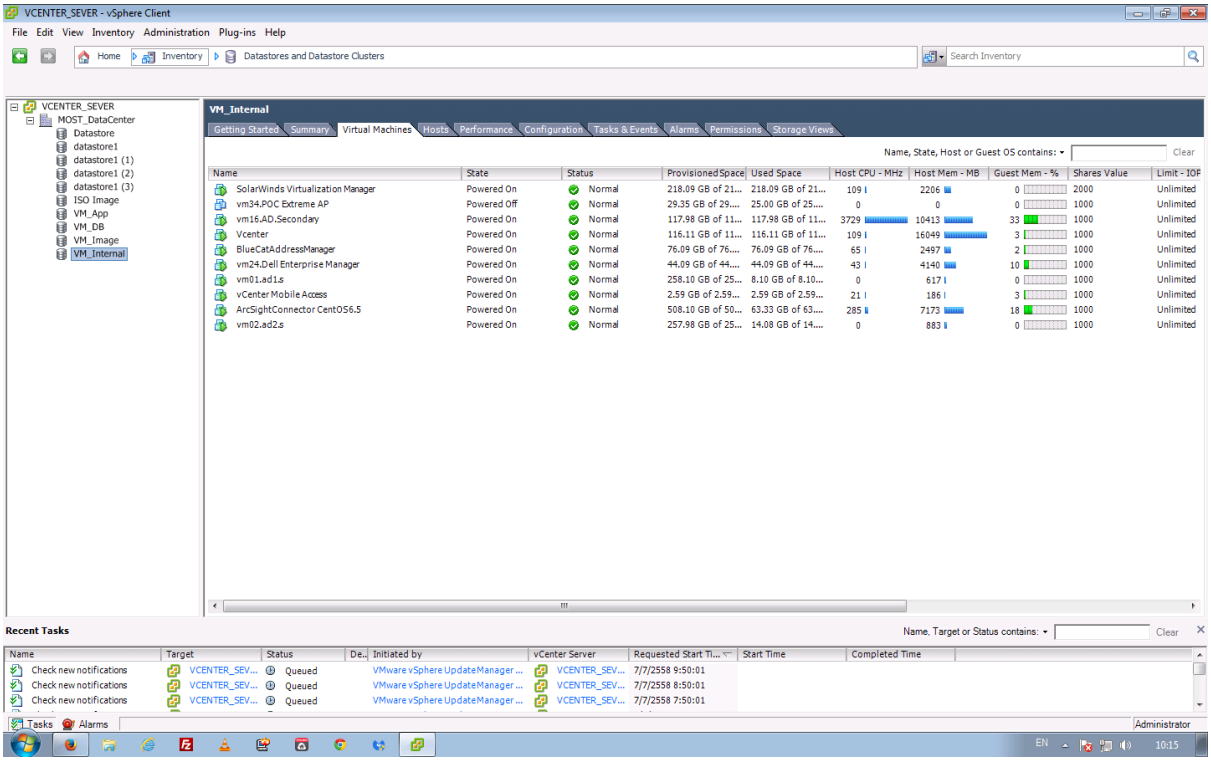
Freeze Time	Expiration Time	Replay Size	Description	State	Source	Create Volume	Space Recovery Run
VM_Internal		8.54 GB		Active			No
07/07/2015 12:00:59 AM	07/14/2015 12:00:59 AM	12.35 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_Internal	No
07/06/2015 12:00:59 AM	07/13/2015 12:00:59 AM	6.15 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_Internal	No
07/05/2015 05:59:59 PM	08/02/2015 05:59:59 PM	10.7 GB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_Internal	No
07/05/2015 12:00:59 AM	07/12/2015 12:00:59 AM	11.58 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_Internal	No
07/04/2015 12:01:00 AM	07/11/2015 12:01:00 AM	11.62 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_Internal	No
07/03/2015 12:00:59 AM	07/10/2015 12:00:59 AM	11.74 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_Internal	No
07/02/2015 12:01:00 AM	07/09/2015 12:01:00 AM	13.7 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_Internal	No
07/01/2015 12:01:00 AM	07/08/2015 12:01:00 AM	14.33 GB	Daily at 12:01 AM	Frozen	Created by Schedule	VM_Internal	No
06/28/2015 05:59:59 PM	07/26/2015 05:59:59 PM	20.78 GB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_Internal	Yes
06/21/2015 06:00:00 PM	07/19/2015 06:00:00 PM	20.43 GB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_Internal	No
06/14/2015 06:00:01 PM	07/12/2015 06:00:01 PM	199.51 GB	Weekly on Sunday at 6:00 PM	Frozen	Created by Schedule	VM_Internal	Yes

แผนภาพแสดงชื่อ Data Store ซึ่ง map เข้ากับเครื่องแม่ข่ายบริการซึ่งอยู่บนระบบ Virtualization มีรายละเอียดดังนี้






VCENTER_SEVER - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Datastores and Datastore Clusters
Search Inventory
VCENTER_SEVER
MOST_DataCenter
Datastore
datastore1
datastore1 (1)
datastore1 (2)
datastore1 (3)
ISO Image
VM_App
VM_DB
VM_Image
VM_Internal
VM_Image
Getting Started Summary Virtual Machines Hosts Performance Configuration Tasks & Events Alarms Permissions Storage Views
Name, State, Host or Guest OS contains: Clear
Name State Status Provisioned Space Used Space Host CPU - MHz Host Mem - MB Guest Mem - % Shares Value Limit - IOP
template.web.m.500_clone Powered Off Normal 507.98 GB of 50... 10.62 GB of 10.... 0 0 0 1000 Unlimited
STKC_Template Powered Off Normal 508.21 GB of 50... 44.60 GB of 44.... 0 0 0 1000 Unlimited
Template.Windows.2012_done Powered Off Normal 58.30 GB of 58.... 50.00 GB of 50.... 0 0 0 1000 Unlimited
template.db.m.500_done Powered Off Normal 516.45 GB of 51... 10.55 GB of 10.... 0 0 0 1000 Unlimited
template.web.s.250_done Powered Off Normal 258.19 GB of 25... 6.49 GB of 6.49... 0 0 0 1000 Unlimited
Recent Tasks
Name, Target or Status contains: Clear
Name Target Status De.. Initiated by vCenter Server Requested Start Ti... Start Time Completed Time
Check new notifications VCENTER_SEV... Queued VMware vSphere Update Manager ... VCENTER_SEV... 7/7/2558 9:50:01
Check new notifications VCENTER_SEV... Queued VMware vSphere Update Manager ... VCENTER_SEV... 7/7/2558 8:50:01
Check new notifications VCENTER_SEV... Queued VMware vSphere Update Manager ... VCENTER_SEV... 7/7/2558 7:50:01
Tasks Alarms
Administrator
EN 10:15


VCENTER_SEVER - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Datastores and Datastore Clusters
Search Inventory
VCENTER_SEVER
MOST_DataCenter
Datastore
datastore1
datastore1 (1)
datastore1 (2)
datastore1 (3)
ISO Image
VM_App
VM_DB
VM_Image
VM_Internal
VM_Internal
Getting Started Summary Virtual Machines Hosts Performance Configuration Tasks & Events Alarms Permissions Storage Views
Name, State, Host or Guest OS contains: Clear
Name State Status Provisioned Space Used Space Host CPU - MHz Host Mem - MB Guest Mem - % Shares Value Limit - IOP
SolarWinds Virtualization Manager Powered On Normal 218.09 GB of 21... 218.09 GB of 21... 109 2206 0 2000 Unlimited
vm34.POC Extreme AP Powered Off Normal 29.35 GB of 29.... 25.00 GB of 25.... 0 0 0 1000 Unlimited
vm16.AD.Secondary Powered On Normal 117.98 GB of 11... 117.98 GB of 11... 3729 10413 33 1000 Unlimited
Vcenter Powered On Normal 116.11 GB of 11... 116.11 GB of 11... 109 16049 3 1000 Unlimited
BlueCatAddressManager Powered On Normal 76.09 GB of 76.... 76.09 GB of 76.... 65 2497 2 1000 Unlimited
vm24.Dell Enterprise Manager Powered On Normal 44.09 GB of 44.... 44.09 GB of 44.... 43 4140 10 1000 Unlimited
vm01.ad1.s Powered On Normal 258.10 GB of 25... 8.10 GB of 8.10... 0 617 0 1000 Unlimited
vCenter Mobile Access Powered On Normal 2.59 GB of 2.59... 2.59 GB of 2.59... 21 186 3 1000 Unlimited
ArcSightConnector CentOS6.5 Powered On Normal 508.10 GB of 50... 63.33 GB of 63.... 285 7173 18 1000 Unlimited
vm02.ad2.s Powered On Normal 257.98 GB of 25... 14.08 GB of 14.... 0 883 0 1000 Unlimited
Recent Tasks
Name, Target or Status contains: Clear
Name Target Status De.. Initiated by vCenter Server Requested Start Ti... Start Time Completed Time
Check new notifications VCENTER_SEV... Queued VMware vSphere Update Manager ... VCENTER_SEV... 7/7/2558 9:50:01
Check new notifications VCENTER_SEV... Queued VMware vSphere Update Manager ... VCENTER_SEV... 7/7/2558 8:50:01
Check new notifications VCENTER_SEV... Queued VMware vSphere Update Manager ... VCENTER_SEV... 7/7/2558 7:50:01
Tasks Alarms
Administrator
EN 10:15