ประกาศกรมตรวจบัญชีสหกรณ์
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมตรวจบัญชีสหกรณ์ พ.ศ. ๒๕๖๐

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ตามมาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัย และเชื่อถือได้ โดยหน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยเป็นลายลักษณ์อักษร นั้น

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหาย จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) และขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมตรวจบัญชีสหกรณ์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมตรวจบัญชีสหกรณ์ พ.ศ. ๒๕๖๐”

ข้อ ๒ วัตถุประสงค์

๒.๑ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหารระดับสูงสุด ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้บังคับบัญชา ผู้ดูแลระบบและผู้ใช้งานของกรมตรวจบัญชีสหกรณ์ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๒ เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์ ให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๓ เพื่อเผยแพร่ให้ผู้บริหารระดับสูงสุด ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้บังคับบัญชา ผู้ดูแลระบบ และผู้ใช้งานของกรมตรวจบัญชีสหกรณ์ได้รับทราบ และต้องถือปฏิบัติตามนโยบายอย่างเคร่งครัด

ข้อ ๓ ขอบเขตการดำเนินงาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมตรวจบัญชีสหกรณ์ มีขอบเขตครอบคลุม ดังนี้

๓.๑ การควบคุมการเข้าถึงและการใช้งานสารสนเทศ

๓.๑.๑ การควบคุมการเข้าถึงห้องควบคุมระบบเครือข่าย

๓.๑.๒ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและระบบสารสนเทศ

๓.๑.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๑.๔ การควบคุมการเข้าถึงระบบเครือข่าย

๓.๒ การจัดทำระบบสำรองของระบบสารสนเทศ และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๔ สร้างความรู้ความเข้าใจให้กับผู้ใช้งานของกรมตรวจบัญชีสหกรณ์ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ ด้วยวิธีการดังนี้

๔.๑ เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศทางเว็บไซต์กรมตรวจบัญชีสหกรณ์ ให้แก่ผู้ใช้งาน

๔.๒ จัดอบรมให้ความรู้ความเข้าใจแก่ผู้ใช้งานในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

ข้อ ๕ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

ข้อ ๖ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และต้องทำการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๗ องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์ โดยอ้างอิงจากรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมตรวจบัญชีสหกรณ์ พ.ศ. ๒๕๖๐ เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง ซึ่งผู้บริหารระดับสูงสุด ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้บังคับบัญชา ผู้ดูแลระบบและผู้ใช้งาน ต้องถือปฏิบัติตามอย่างเคร่งครัด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๖ ตุลาคม พ.ศ. ๒๕๖๐

(นายโอภาส ทองยงค์)
อธิบดีกรมตรวจบัญชีสหกรณ์

เอกสารแนบท้ายประกาศ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมตรวจบัญชีสหกรณ์ พ.ศ. ๒๕๖๐

คำนิยาม

“หน่วยงาน” หมายถึง กรมตรวจบัญชีสหกรณ์

“ผู้บริหารระดับสูงสุด” (Chief Executive Officer : CEO) หมายถึง อธิบดีกรมตรวจบัญชีสหกรณ์

“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” (Chief Information Officer : CIO) หมายถึง ผู้มีอำนาจหน้าที่ดูแลรับผิดชอบในการบริหารงานเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์

“ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมตรวจบัญชีสหกรณ์

“ผู้ดูแลระบบ” หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลระบบเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์

“ผู้ใช้งาน” หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ พนักงานจ้างเหมา ที่ปรึกษาโครงการ ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ และระบบเครือข่ายของกรมตรวจบัญชีสหกรณ์

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของกรมตรวจบัญชีสหกรณ์

“สินทรัพย์” หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมตรวจบัญชีสหกรณ์ ได้แก่ เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพา อุปกรณ์ระบบเครือข่าย และซอฟต์แวร์ที่มีลิขสิทธิ์

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

“ความมั่นคงปลอดภัยด้านสารสนเทศ”หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่เป็นไปได้ว่าจะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการที่ล้มเหลว หรือเหตุการณ์อันไม่สามารถรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

“สารสนเทศ” (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลที่นำมาประมวลผลการจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“อุปกรณ์คอมพิวเตอร์” หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อหรือทำงานเป็นส่วนหนึ่งของระบบคอมพิวเตอร์ โดยอาจใช้ทำหน้าที่เป็นอุปกรณ์สื่อสาร หรือใช้บันทึกข้อมูล

“โปรแกรมพื้นฐาน” หมายถึง โปรแกรมระบบปฏิบัติการ (Operating System) โปรแกรมสำนักงาน โปรแกรมจัดการไฟล์ PDF โปรแกรมป้องกันไวรัส โปรแกรมบีบอัดไฟล์ และโปรแกรม Web Browser

“โปรแกรมกรมตรวจบัญชีสหกรณ์” หมายถึง โปรแกรมที่พัฒนาขึ้นเพื่อสนับสนุนงานตามภารกิจของกรมตรวจบัญชีสหกรณ์ รวมถึงโปรแกรมกรมตรวจบัญชีสหกรณ์ ที่อนุญาตให้สหกรณ์นำไปพัฒนาต่อยอด

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือส่งข้อมูล และสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเตอร์เน็ต (Internet) เป็นต้น

“ระบบเครือข่ายไร้สาย (Wireless LAN)” หมายถึง เทคโนโลยีที่ช่วยให้การติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ ๒ เครื่อง หรือกลุ่มของเครื่องคอมพิวเตอร์สามารถสื่อสารกันได้ รวมถึงการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่ายด้วยกัน โดยปราศจากการใช้สายสัญญาณในการเชื่อมต่อ

“ระบบเครือข่ายส่วนตัวเสมือน (VPN)” หมายถึง การนำโครงข่ายสาธารณะมาใช้เป็นสื่อในการส่งข้อมูลระหว่างหน่วยงานภายในองค์กร โดยใช้การเข้ารหัสข้อมูลสร้างเป็นระบบเครือข่ายเสมือนขึ้นเพื่อให้ข้อมูลที่ส่งผ่านมีความปลอดภัย

“ระบบเทคโนโลยีสารสนเทศ” หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุน การให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูล และสารสนเทศ เป็นต้น

“โปรแกรมประยุกต์และโปรแกรมอรรถประโยชน์” หมายถึง โปรแกรมที่มีความสามารถจัดการกับงานเฉพาะด้าน โดยตัวโปรแกรมจะเหมาะสมและใช้งานได้ดีกับงานเฉพาะนั้นๆ เท่านั้น เช่น โปรแกรม Microsoft Word โปรแกรม Microsoft Excel และโปรแกรม Microsoft PowerPoint เป็นต้น

“ระบบสารสนเทศ” หมายถึง ระบบของการจัดเก็บ ประมวลผลข้อมูล โดยอาศัยบุคคลและเทคโนโลยีสารสนเทศในการดำเนินการ เพื่อให้ได้สารสนเทศที่เหมาะสมกับงานหรือภารกิจ

“ระบบสำรอง” หมายถึง เครื่องมือที่ทำหน้าที่ในการสำรองข้อมูลไปยังที่ปลอดภัย

“ระบบสารสนเทศซึ่งไวต่อการรบกวน” หมายถึง ระบบสารสนเทศที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ได้แก่ ระบบ GFMIS หรือระบบการบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ เป็นระบบที่ใช้ในการปฏิบัติงานด้านการงบประมาณ การบัญชี การจัดซื้อจัดจ้าง การเบิกจ่าย และการบริหารทรัพยากร ซึ่งดูแลรับผิดชอบโดยกรมบัญชีกลาง

หมวด ๑
แนวปฏิบัติในการควบคุมการเข้าถึงห้องควบคุมระบบเครือข่าย

ข้อ ๑ การควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่าย ผู้รับผิดชอบด้านเครือข่ายของหน่วยงาน ต้องปฏิบัติตามข้อกำหนดดังนี้

(๑) ต้องกำหนดสิทธิบุคคลในการเข้า-ออกห้องควบคุมระบบเครือข่าย มีการบันทึก “ทะเบียนผู้มีสิทธิเข้า-ออกพื้นที่”

(๒) การเข้าถึงห้องควบคุมระบบเครือข่าย ต้องทำการสแกนลายนิ้วมือรวมทั้งมีการเก็บบันทึกการเข้า-ออกห้องควบคุมระบบเครือข่ายจากเครื่องสแกนลายนิ้วมือ

(๓) ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่” และต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้า-ออกทุกคนต้องกรอกแบบฟอร์มดังกล่าวทุกครั้ง

(๔) เมื่อมีบุคคลภายนอกต้องการเข้ามายังห้องควบคุมระบบเครือข่าย ต้องมีการขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นลายลักษณ์อักษร

(๕) เจ้าหน้าที่ที่รับผิดชอบด้านเครือข่ายของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องอยู่ภายในห้องควบคุมระบบเครือข่ายเมื่อมีบุคคลภายนอกเข้ามายังห้องควบคุมระบบเครือข่าย

(๖) ต้องทำการทบทวนสิทธิการเข้า-ออกห้องควบคุมระบบเครือข่าย อย่างน้อยปีละ ๑ ครั้ง

หมวด ๒
แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและระบบสารสนเทศ

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงาน ต้องจัดการควบคุมการเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ตนต้องใช้งานได้ก็ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบข้อมูล และ/หรือผู้รับผิดชอบระบบงานตามความจำเป็นต่อการใช้งานแล้วเท่านั้น

(๒) ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบ การอนุมัติ และกำหนดสิทธิในการผ่านเข้าสู่ระบบ กล่าวคือ ในการขออนุญาตเข้าถึงระบบนั้น ผู้ใช้งานจะต้องมีการจัดทำเป็นบันทึกและกรอกแบบเอกสารที่หน่วยงานกำหนด เพื่อขออนุญาตเข้าถึงระบบ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้บังคับบัญชาหรือผู้ได้รับมอบหมายจากผู้บังคับบัญชาเพื่อการจัดเก็บไว้เป็นหลักฐาน จากนั้นผู้ดูแลระบบจะสร้างบัญชีสำหรับการเข้าถึงโดยอนุญาตเฉพาะในส่วนที่จำเป็น โดยคำนึงถึงประเภทข้อมูลและชั้นความลับ

(๓) ผู้ดูแลระบบ ต้องกำหนดไม่ให้ผู้ใช้งานเข้าถึงระบบได้ หากผู้ใช้งานใส่รหัสผ่านผิด ๓ ครั้ง ให้ยื่นแบบฟอร์มเพื่อขอรหัสใหม่อีกครั้ง

(๔) ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่ใช้ในการปฏิบัติงาน เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศเกินกว่า ๓๐ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการ Log in เข้าระบบสารสนเทศอีกครั้ง และให้จำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน โดยให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลา ๘ ชั่วโมง ต่อการเชื่อมต่อ ๑ ครั้ง

(๕) ผู้รับผิดชอบข้อมูลและผู้รับผิดชอบระบบงาน ต้องอนุญาตให้ผู้ใช้งานเข้าถึงระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น

ข้อ ๒ การจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

(๑.๑) ข้อมูลสารสนเทศด้านการบริหาร

(๑.๒) ข้อมูลสารสนเทศด้านการให้บริการ

(๑.๓) ข้อมูลสารสนเทศเพื่อการบริหาร

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๔ ระดับ คือ

(๒.๑) ลับ (Top Secret/Secret/Confidential)

(๒.๒) ใช้ภายในเท่านั้น (Internal Use)

(๒.๓) ส่วนบุคคล (Personal)

(๒.๔) เปิดเผยได้ (Public)

ข้อ ๓ การเข้าถึงสารสนเทศ สามารถเข้าถึงระบบต่างๆ ได้ตลอด ๒๔ ชั่วโมง โดยผ่านช่องทางอินเตอร์เน็ต

ข้อ ๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงาน ต้องบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน ดังนี้

(๑) การลงทะเบียนผู้ใช้งาน ต้องปฏิบัติตามขั้นตอนลงทะเบียนที่หน่วยงานกำหนดขึ้นเพื่อให้มีสิทธิในการใช้งานระบบสารสนเทศตามความจำเป็น รวมทั้งปฏิบัติตามขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน ดังนี้

(๑.๑) การลงทะเบียนผู้ใช้งานที่บรรจุใหม่

(๑.๑.๑) เจ้าหน้าที่ที่ได้รับมอบหมายจากสำนักบริหารกลาง ทำการบันทึกข้อมูลรายละเอียดที่เกี่ยวข้องตามเอกสารและตามคำสั่งกรมตรวจบัญชีสหกรณ์ ลงในระบบ

(๑.๑.๒) ผู้ดูแลระบบกำหนดการเข้าถึงตามสิทธิที่ได้รับมอบหมาย

(๑.๒) การถอนสิทธิการใช้งาน

(๑.๒.๑) เจ้าหน้าที่ที่ได้รับมอบหมายจากสำนักบริหารกลาง ทำการถอนสิทธิผู้ใช้งานออกจากระบบ ตามคำสั่งกรมตรวจบัญชีสหกรณ์

(๑.๒.๒) ผู้ดูแลระบบถอนสิทธิผู้ใช้งานออกจากระบบ

(๒) กำหนดสิทธิการใช้ระบบสารสนเทศที่ให้บริการแก่บุคคลภายนอก ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

(๓) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้งานที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้สิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณาเพื่อขอความเห็นชอบ และอนุมัติจากผู้บังคับบัญชา

(๓.๑) ควบคุมการใช้งานอย่างเข้มงวด ได้แก่ กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(๓.๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓.๓) มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๖ เดือน

ข้อ ๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงาน ต้องบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของผู้ใช้งาน ดังนี้

(๑) กำหนดบัญชีรายชื่อผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน

(๒) ไม่อนุญาตให้ผู้ร้องขอใช้ระบบงานเข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้น

(๓) จัดเก็บข้อมูลการลงทะเบียนของผู้ที่ร้องขอใช้ระบบไว้เพื่อเอาไว้ใช้อ้างอิงหรือตรวจสอบในภายหลัง

(๔) ทบทวนบัญชีและสิทธิผู้ใช้งานทั้งหมด พร้อมทั้งปรับปรุงอย่างสม่ำเสมอทุก ๖ เดือน เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

ข้อ ๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงาน ต้องจัดให้มีการพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบสำคัญสำหรับผู้ใช้ที่อยู่ภายนอก ดังนี้

(๑) การแสดงตัวตนด้วยชื่อบัญชีผู้ใช้งาน

(๒) การพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน

(๓) การเข้าถึงระบบงานสำคัญของหน่วยงานผ่านเครือข่ายอินเทอร์เน็ตนั้น จะมีการตรวจสอบผู้ใช้งานด้วย

(๔) การเข้าถึงระบบงานสำคัญของหน่วยงานจากระยะไกลเพื่อเพิ่มความปลอดภัย จะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน ได้แก่ รหัสผ่าน หรือวิธีการเข้ารหัส

ข้อ ๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงาน ต้องกำหนดวิธีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานให้มีความมั่นคงปลอดภัย ดังนี้

(๑) การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย โดยใส่ซองปิดผนึกและประทับตรา “ลับ” และส่งไปยังผู้ใช้งาน และแนบเอกสารการได้รับอนุญาตจากผู้บังคับบัญชา รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติเก็บรักษารหัสผ่านเป็นความลับ และเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

(๒) การตั้งรหัสผ่านชั่วคราวให้กับผู้ใช้งาน ต้องกำหนดรหัสผ่านชั่วคราวให้มีความยากต่อการเดา และกำหนดรหัสผ่านให้มีความแตกต่างกัน

(๓) กำหนดรหัสผ่านที่มีความยาวไม่น้อยกว่า ๘ ตัวอักษร และต้องมีการผสมกันระหว่างตัวเลขและตัวอักษร

(๔) ต้องเก็บรหัสผ่านสำหรับการใช้งานระบบเทคโนโลยีสารสนเทศของผู้ใช้งานทั้งระบบไว้เป็นความลับ และต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบ

(๕) กำหนดให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านได้ และกำหนดให้เปลี่ยนรหัสผ่านอย่างน้อยทุก ๖ เดือน และไม่ใช้รหัสผ่านเดิมที่เคยใช้แล้ว

(๖) หลีกเลี่ยงการใช้ E-mail ในการจัดส่งรหัสผ่าน และผู้ใช้งานต้องตอบกลับทันทีหลังจากได้รับรหัสผ่าน

(๗) กำหนดให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(๘) เปลี่ยนรหัสผ่านทันทีภายหลังจากติดตั้งซอฟต์แวร์ที่ซื้อจากผู้ผลิต

(๙) มีการแจ้งเตือนโดยหนังสือหรือทางเว็บไซต์ในครั้งแรกที่ได้รับรหัสผ่าน โดยทำการเปลี่ยนรหัสผ่านทันที และเก็บรหัสผ่านไว้เป็นความลับ

(๑๐) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๑๑) กำหนดให้ผู้ดูแลระบบจัดทำระบบให้สามารถทำงานอัตโนมัติ เพื่อการกำหนดรหัสที่มีคุณภาพ

ข้อ ๘ การจ้างพัฒนาระบบสารสนเทศ หรือจ้างเหมาดำเนินงาน (Outsource) ให้บุคคลหรือนิติบุคคลหรือพนักงานลูกจ้างที่เป็นคู่สัญญา ต้องมีการลงนามในการรักษาความลับ ห้ามเปิดเผยข้อมูลขององค์กรก่อนปฏิบัติหน้าที่

ข้อ ๙ การจัดการกับข้อมูลลับ ให้ปฏิบัติดังนี้

(๑) การอนุญาตให้เข้าถึงข้อมูลลับผ่านเครือข่ายต้องเข้ารหัสด้วยรหัสผ่าน กำหนดวันหมดอายุของการเข้าถึง และระบุให้เข้าถึงได้เฉพาะผู้มีสิทธิ

(๒) การสำเนาข้อมูลชั้นความลับ ต้องจดบันทึกจำนวนชุดที่สำเนา รายละเอียดผู้ดำเนินการทุกครั้ง

ข้อ ๑๐ ในการทำลายข้อมูลลับ ให้ปฏิบัติดังนี้

(๑) เมื่อต้องทำลายข้อมูลอิเล็กทรอนิกส์ ผู้รับผิดชอบข้อมูลอิเล็กทรอนิกส์ต้องเป็นผู้ทำลายข้อมูล

(๒) กำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์บนสื่อบันทึกข้อมูล ดังนี้ หรือใช้มาตรฐาน DoD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา

ประเภทสื่อบันทึกข้อมูล	**วิธีการทำลายใช้ใหม่ได้**	**วิธีทำลาย**	**ระยะเวลาทำลาย**
กระดาษ	-	- ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร	เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด
Flash Drive	ใช้วิธีการ Format	- ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DoD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย	เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด
แผ่น CD/DVD	ใช้วิธีการ Format	- ใช้การหั่น ตัด เผา ให้สิ้นสภาพการใช้งาน	เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด
เทป	-	- ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย	เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด
ฮาร์ดดิสก์	ใช้วิธีการ Format	- ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DoD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย	เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด

ข้อ ๑๑ การจัดการระบบสารสนเทศซึ่งไวต่อการรบกวน ให้ปฏิบัติดังนี้

(๑) ต้องแยกระบบสารสนเทศซึ่งไวต่อการรบกวนออกจากระบบสารสนเทศอื่นๆ

(๒) ต้องมีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

(๓) แยกสภาพการติดตั้งทางเครือข่าย โดยใช้วิธีการทางเทคนิค ได้แก่ VLAN (Virtual Local Area Network)

(๔) แบ่งแยกเครือข่ายสำหรับระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญต่อหน่วยงานสูงออกจากระบบสารสนเทศอื่น โดยให้จัดทำเป็นเครือข่าย DMZ (DeMilitalized Zone)

(๕) ทำการควบคุมการเข้ามาใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกตามข้อกำหนดที่ตั้งค่าไว้ใน Firewall

ข้อ ๑๒ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ดังนี้

(๑) มีการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงระบบงานของหน่วยงานจากระยะไกล โดยผ่านทางอุปกรณ์คอมพิวเตอร์ประเภทพกพาของหน่วยงาน

(๒) ควบคุมการติดตั้งโปรแกรมไม่พึงประสงค์ในอุปกรณ์คอมพิวเตอร์ประเภทพกพาของหน่วยงาน

(๓) ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในหน่วยงานมาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้า-ออกพื้นที่ให้ถูกต้องชัดเจน และต้องได้รับอนุญาตจากเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาด้วยการลงนามอย่างเป็นลายลักษณ์อักษร

ข้อ ๑๓ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ให้ปฏิบัติดังนี้

(๑) ผู้ดูแลระบบ ต้องให้สิทธิตามที่ได้รับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน

(๒) ผู้ใช้งานระบบจากระยะไกล ต้องได้รับอนุมัติจากผู้บังคับบัญชาหรือเจ้าของระบบงานและต้องใช้งานตามระยะเวลาการเข้าถึงที่กำหนดไว้

(๓) ผู้ใช้งานระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

หมวด ๓
แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

ข้อ ๑ ผู้ใช้งาน ต้องยืนยันตัวตนด้วยชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนเองก่อนเข้าใช้งานระบบปฏิบัติการเครื่องคอมพิวเตอร์ทุกครั้ง

ข้อ ๒ ผู้ใช้งาน ต้องไม่อนุญาตให้บุคคลอื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนเองในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

ข้อ ๓ ผู้ดูแลระบบ ต้องตั้งค่าระบบให้มีการแจ้งเตือนแก่ผู้ใช้งาน เมื่อผู้ใช้งานใส่รหัสผ่านผิดเกิน ๓ ครั้ง โดยระบบจะล็อคสิทธิการเข้าถึงของผู้ใช้งาน ทำให้ผู้ใช้งานรายนั้นไม่สามารถเข้าถึงระบบปฏิบัติการได้อีก จนกว่าผู้ดูแลระบบจะดำเนินการปลดล็อคให้

ข้อ ๔ การจำกัดการใช้งานโปรแกรมประเภทอรรถประโยชน์

ให้ผู้ดูแลระบบทำบัญชีรายชื่อโปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้งานได้เท่านั้น เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

หมวด ๔
แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย

ข้อ ๑ การควบคุมการเข้าถึงระบบเครือข่าย ต้องปฏิบัติตามข้อกำหนดดังนี้

(๑) ผู้ดูแลระบบ ต้องออกแบบระบบเครือข่ายแบบแบ่งโซน โดยแยกกลุ่มเครือข่ายเป็นระบบเครือข่ายภายใน ระบบเครือข่ายภายนอก และ DMZ Zone (DeMilitalized Zone) เพื่อการควบคุมและป้องกันการบุกรุก และต้องกำหนดเส้นทางการเชื่อมต่อระบบเครือข่ายทั้งหมดในองค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงาน โดยต้องผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall, IPS/IDS และ Proxy System

(๒) ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๓) ผู้ใช้งาน ต้องรับผิดชอบระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งผู้ใช้งานต้องไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่ายจากบัญชีผู้ใช้ของตนเอง

(๔) การเข้าสู่ระบบเครือข่ายด้วยวิธีการ Remote Access VPN ผู้ใช้งานจะต้องมีการพิสูจน์ตัวตน (Authentication) ด้วยการป้อนชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อยืนยันตัวตนของผู้ใช้งาน

(๕) การเข้าสู่ระบบเครือข่ายภายในหน่วยงานผ่านทางระบบอินเตอร์เน็ต ต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

(๖) ทบทวนบัญชีและสิทธิผู้ใช้งานทั้งหมด พร้อมทั้งปรับปรุงอย่างสม่ำเสมอทุก ๑ ปี เพื่อป้องกันการเข้าถึงระบบโดยมิได้รับอนุญาต

(๗) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของคอมพิวเตอร์ (IP Address) ของระบบงานเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของหน่วยงานได้โดยง่าย

(๘) ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์เครือข่ายส่วนกลาง ได้แก่ อุปกรณ์จัดหาเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ WiFi หรืออุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

(๙) บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายของหน่วยงาน ต้องทำหนังสือขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ที่ได้รับมอบหมาย เพื่อขอรับชื่อผู้ใช้และรหัสผ่านในการเข้าใช้งานระบบ

(๑๐) ผู้ใช้งาน ต้องใช้เครือข่ายสารสนเทศอย่างมีประสิทธิภาพ ได้แก่ ห้ามดาวน์โหลดไฟล์หรืออัพโหลดไฟล์ที่มีขนาดใหญ่เกินไป หรือดูหนังฟังเพลงออนไลน์ในระหว่างเวลาปฏิบัติงาน ซึ่งมีผลกระทบต่อการใช้งานเครือข่ายของหน่วยงาน

(๑๑) ผู้ใช้งาน กรณีนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้ดูแลระบบ

(๑๒) ผู้ดูแลระบบ มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

(๑๓) ผู้ดูแลระบบ ต้องตรวจสอบเหตุการณ์ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวัน หากเกิดเหตุการณ์ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จหรือไม่ประสบความสำเร็จ จะต้องรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

(๑๔) ผู้ดูแลระบบ ต้องมีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก ได้แก่ บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง และควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

(๑๕) ผู้ดูแลระบบ ต้องจัดทำผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๑๖) ผู้ดูแลระบบ ต้องมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ตั้ง

(๑๗) ผู้ดูแลระบบ ต้องทำการตรวจสอบอุปกรณ์บนเครือข่าย โดยใช้หมายเลขเทอร์มินัล หมายเลข MAC Address และหมายเลข IP Address เพื่อเป็นการยืนยัน

(๑๘) ผู้ดูแลระบบ ต้องทำการเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน

(๑๙) ผู้ดูแลระบบ ต้องกำหนดการเปิด-ปิดพอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่าย โดยปิดพอร์ตที่มีความเสี่ยงอันจะก่อให้เกิดความเสียหายต่อระบบเครือข่าย

(๒๐) ผู้ดูแลระบบ ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๒๑) ผู้ดูแลระบบ ต้องแบ่งแยกเครือข่ายเป็นเครือข่ายย่อยๆ ตามอาคารต่างๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

(๒๒) ผู้ดูแลระบบ ต้องจัดแบ่งเครือข่ายภายในหน่วยงานออกเป็นเครือข่ายภายในและเครือข่ายภายนอก

(๒๓) ผู้ดูแลระบบ ต้องใช้ Firewall กั้น หรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อยๆ

(๒๔) ผู้ดูแลระบบ ต้องใช้ Gateway เพื่อควบคุมการเข้าถึงเครือข่ายทั้งจากภายในและภายนอกหน่วยงาน ซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของหน่วยงาน

(๒๕) ผู้ดูแลระบบ ต้องทำการตรวจสอบ Gateway หรืออุปกรณ์เครือข่าย IP Address ของทั้งต้นทางและปลายทางและควบคุมการไหลของข้อมูลผ่านเครือข่ายต่างๆ จากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง โดยให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

(๒๖) ผู้ดูแลระบบ จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่อนุญาตให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้ นอกจากเส้นทางที่ได้กำหนดไว้ให้เท่านั้น

(๒๗) ผู้ดูแลระบบ ตรวจสอบและกำหนดเส้นทางบนเครือข่ายให้เหมาะสม โดยผ่านทางอุปกรณ์เครือข่าย เพื่อควบคุมการเชื่อมต่อทางเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึงของหน่วยงาน

ข้อ ๒ การควบคุมการเข้าใช้งานระบบจากภายนอก ต้องปฏิบัติตามข้อกำหนดดังนี้

(๑) การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายของหน่วยงาน ซึ่งก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของหน่วยงาน การควบคุมบุคคลที่เข้าสู่ระบบของหน่วยงานจากระยะไกลจึงต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๒) ผู้ใช้งาน ต้องทำหนังสือระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอในการขอสิทธิการเข้าสู่ระบบจากระยะไกล และต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๓) ผู้ดูแลระบบ ต้องไม่เปิดพอร์ตในการเข้าสู่ระบบข้อมูลจากระยะไกล (Remote Access) ทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

หมวด ๕
แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

ข้อ ๑ การใช้คอมพิวเตอร์ของหน่วยงาน ให้ปฏิบัติดังนี้

(๑) ต้องตรวจสอบว่าโปรแกรมป้องกันไวรัส มีการทำงานตามปกติและมีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ หากพบว่าโปรแกรมดังกล่าวทำงานผิดปกติ ให้รีบแจ้งศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อดำเนินการแก้ไขโดยเร็ว

(๒) คอมพิวเตอร์ที่ใช้ในหน่วยงาน ให้ติดตั้งเฉพาะโปรแกรมพื้นฐาน หากมีการติดตั้งโปรแกรมเพิ่มเติม ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมาย

(๓) ต้องลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครือคอมพิวเตอร์เพื่อประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

(๔) ต้องออกจากระบบ (Log off) ทุกครั้งที่มิได้ปฏิบัติงานอยู่หน้าคอมพิวเตอร์ หรือปิดคอมพิวเตอร์เมื่อใช้งานประจำวันเสร็จสิ้น

(๕) ผู้ใช้งาน ต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพโดยอัตโนมัติเมื่อไม่มีการใช้งานเกินกว่า ๑๕ นาที

(๖) ให้ผู้ใช้งานล็อคอุปกรณ์คอมพิวเตอร์สำคัญเมื่อไม่ได้ถูกใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว เพื่อป้องกันการสูญหายหรือถูกขโมย

(๗) การยืมคอมพิวเตอร์ต้องได้รับอนุญาตจากผู้ดูแลรับผิดชอบหรือผู้ที่ได้รับมอบหมาย

(๘) การนำคอมพิวเตอร์ส่วนตัวมาใช้กับระบบเครือข่ายของหน่วยงาน ต้องได้รับการตรวจสอบและอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารโดยผ่านการลงทะเบียน

ข้อ ๒ การใช้คอมพิวเตอร์แบบตั้งโต๊ะและคอมพิวเตอร์พกพา ให้ปฏิบัติดังนี้

(๑) กำหนดให้ใช้งานเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของหน่วยงานอย่างมีประสิทธิภาพ และโปรแกรมที่ติดตั้งต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย

(๒) ไม่ทำการปิดหรือยกเลิก หรือเปลี่ยนระบบโปรแกรมป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

(๓) หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดไวรัส ห้ามเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของไวรัสไปยังเครื่องคอมพิวเตอร์อื่นๆ และแจ้งผู้ดูและระบบทราบ

(๔) ผู้ใช้งาน ต้องรับผิดชอบในการตรวจหาไวรัสจากสื่อต่างๆ ได้แก่ Flash Drive และ External Hard Disk อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ ตรวจสอบหาไวรัสจากเครื่องคอมพิวเตอร์ที่ใช้งาน รวมทั้งตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต

ข้อ ๓ การใช้งานอินเตอร์เน็ต ผู้ใช้งานต้องปฏิบัติดังนี้

(๑) ต้องไม่ใช้ระบบอินเตอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคลและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

(๒) ต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

(๓) การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Webboard) ของหน่วยงาน ต้องไม่เสนอความคิดเห็นหรือใช้ข้อความยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน

(๔) หลังจากการใช้งานเสร็จแล้ว ให้ปิดโปรแกรม Web Browser เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ข้อ ๔ การใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ผู้ใช้งานต้องปฏิบัติดังนี้

(๑) ต้องใช้จดหมายอิเล็กทรอนิกส์ (E-mail) เพื่อใช้ในราชการ ตามที่หน่วยงานกำหนดเท่านั้น

(๒) เมื่อได้รับรหัสผ่าน (Password) ต้องทำการเปลี่ยนรหัสผ่านโดยทันทีเมื่อมีการเข้าสู่ระบบในครั้งแรก

(๓) ห้ามใช้จดหมายอิเล็กทรอนิกส์ (E-mail) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (E-mail) ของตน

(๔) ต้องไม่ส่งข้อมูลหรือเผยแพร่ข้อมูลอันเป็นข้อมูลที่ผิดหรือขัดต่อกฎหมาย หรือข้อมูลที่เป็นในรูปแบบของ Junk Mail หรือ Spam Mail หรือการโฆษณา หรือชี้นำ หรือให้มีการซื้อขายสิ่งของหรือบริการ

(๕) ห้ามเปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ (E-mail) หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

(๖) ควรลบจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่

(๗) หลังจากการใช้งานเสร็จสิ้น ควรทำการบันทึกออก (Log out) จากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)

ข้อ ๕ การใช้งานรหัสผ่าน (Password Use) ผู้ใช้งานต้องใช้งานรหัสผ่าน และเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

(๑) ไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานร่วมกัน

(๒) กำหนดรหัสผ่านที่มีความยาวไม่น้อยกว่า ๘ ตัวอักษร มีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ต่างๆ

(๓) เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับครั้งแรกทันทีที่ทำการ Login เข้าสู่ระบบงาน

(๔) ไม่ตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน ได้แก่ ๑๒๓๔, abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน ได้แก่ ๙๙๙, aaa

(๕) ไม่กำหนดรหัสผ่านจากชื่อ หรือชื่อสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว หรือจากหมายเลขโทรศัพท์

(๖) ตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำตนเอง แต่ควรเป็นรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

(๗) ไม่ใช้รหัสผ่านเดียวกันกับระบบงานต่างๆ ที่มีสิทธิใช้งาน

(๘) ไม่กำหนดให้ระบบงานทำการบันทึกหรือบันทึกไว้ในหน้าจอ Log in

(๙) เก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย และต้องไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่น

(๑๐) เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

ข้อ ๖ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ ผู้ใช้งานต้องปฏิบัติดังนี้

(๑) ต้องควบคุมเอกสาร ข้อมูล หรือสื่อต่างๆ ที่มีข้อมูลสำคัญจัดเก็บ หรือบันทึกอยู่ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน

(๒) ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์สารสนเทศต่างๆ โดยไม่ได้รับอนุญาต

(๓) สินทรัพย์ที่ใช้งานอยู่ภายนอกหน่วยงานต้องมีการรักษาความมั่นคงปลอดภัยตามความเสี่ยง

หมวด ๖
แนวปฏิบัติในการสำรองข้อมูล

ข้อ ๑ ด้านการสำรองข้อมูล

(๑) ผู้ดูแลระบบ ต้องจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ดังนี้

ระบบสารสนเทศทุกระบบ ให้สำรองข้อมูลแบบ Full System Backup, Full Data Backup และมีการสำรองข้อมูลแบบ Incremental Backup (เฉพาะส่วนที่มีการเปลี่ยนแปลงแต่ละวัน)

(๒) จัดเก็บข้อมูลที่สำรอง ต้องกำหนดวันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

(๓) ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องสมบูรณ์ในการ Backup

(๔) การจัดทำบันทึกการสำรองข้อมูล (Operator Logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก และรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ

(๕) การรายงานข้อผิดพลาด (Fault Logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไข

(๖) ในกรณีพบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการสำรองข้อมูลอย่างสมบูรณ์ได้ ให้ผู้ดูแลระบบดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหา และรายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๗) ต้องจัดเก็บข้อมูลที่สำรองไว้ในสถานที่เก็บข้อมูลสำรอง ซึ่งติดตั้งแยกสถานที่กับห้องควบคุมระบบเครือข่าย เพื่อป้องกันไม่ให้ข้อมูลสูญหายเมื่อเกิดภัยพิบัติ และสามารถใช้งานได้อย่างต่อเนื่อง

(๘) ผู้ดูแลระบบ ดำเนินการตามกระบวนการสำรองข้อมูลสำหรับแต่ละระบบสารสนเทศโดยเคร่งครัด

(๙) ผู้ดูแลระบบ ทำการทบทวนข้อมูลที่มีการสำรองอย่างน้อยทุก ๖ เดือน

(๑๐) ผู้ดูแลระบบ ทำการทดสอบข้อมูลระบบสารสนเทศที่สำรองไว้อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ ด้านการกู้คืนระบบ

(๑) ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่าย จนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไข และรายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ

(๒) หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งให้ผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

หมวด ๗
แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยง

ข้อ ๑ กระบวนการในการบริหารจัดการกับความเสี่ยงของระบบฐานข้อมูลสารสนเทศให้ปฏิบัติตามวงจรบริหารงานคุณภาพ PDCA (Plan-Do-Check-Act) ดังต่อไปนี้

(๑) การกำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan)

(๑.๑) กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย โดยพิจารณาจากลักษณะการดำเนินงานของหน่วยงาน สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยีที่หน่วยงานใช้งาน

(๑.๒) กำหนดนโยบายความมั่นคงปลอดภัยเพื่อให้ครอบคลุมตามขอบเขตที่กำหนดไว้

(๑.๓) กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศของหน่วยงาน

(๑.๔) ประเมินความเสี่ยง กำหนดทางเลือกในการจัดการกับความเสี่ยงและกำหนดมาตรการลดความเสี่ยง (ซึ่งสามารถนำมาตรการต่างๆ ในมาตรฐาน ISO/IEC ๒๗๐๐๑ มาใช้ในการลดความเสี่ยง)

(๑.๕) นำเสนอภาพความเสี่ยงโดยรวม และขออนุมัติสำหรับความเสี่ยงที่ยังหลงเหลืออยู่

(๒) การดำเนินการกับระบบบริหารจัดการความมั่นคงปลอดภัย (Do)

(๒.๑) จัดทำแผนการลดความเสี่ยง

(๒.๒) ปฏิบัติตามแผนการลดความเสี่ยงที่ได้กำหนดไว้

(๒.๓) กำหนดแผนการวัดความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัย เพื่อใช้ในการติดตามภาพรวมของการบริหารจัดการ

(๒.๔) จัดทำและดำเนินการตามแผนการอบรม และสร้างความตระหนักเพื่อให้ความรู้และสร้างความตระหนักแก่บุคลากรทั้งหมดที่อยู่ในขอบเขต เพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพ ประสิทธิผล รวมทั้งมีความมั่นคงปลอดภัย

(๒.๕) บริหารจัดการการดำเนินงานและการใช้ทรัพยากรต่างๆ ภายในขอบเขตเพื่อให้เป็นไปตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

(๒.๖) จัดทำขั้นตอนปฏิบัติ และ/หรือกำหนดมาตรการที่จำเป็นสำหรับการติดตามและบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident Management Procedures and Controls) รวมทั้งกำหนดให้ผู้ที่เกี่ยวข้องให้ปฏิบัติตามโดยเคร่งครัด

(๓) การเฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย (Check)

(๓.๑) ดำเนินการตามขั้นตอนปฏิบัติและมาตรการในการเฝ้าระวังและติดตาม (ที่กำหนดไว้ในนโยบายความมั่นคงปลอดภัย) เพื่อตรวจหาข้อผิดพลาดจากการประมวลผล ตรวจหาการละเมิดหรือความพยายามในการละเมิดความมั่นคงปลอดภัย ตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น ตรวจสอบว่าการดำเนินการจัดการกับเหตุการณ์การละเมิดความมั่นคงปลอดภัยที่ได้ดำเนินการไปแล้วได้ผลหรือไม่

(๓.๒) ดำเนินการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ โดยอย่างน้อยนำสิ่งต่างๆ ดังนี้มาทบทวนด้วย ได้แก่ ผลการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย เหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น ผลจากการวัดความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัย คำแนะนำและผลตอบกลับ (Feedback) จากผู้ที่เกี่ยวข้อง

(๓.๓) ดำเนินการทบทวนความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ โดยดูว่าแผนการวัดความสัมฤทธิ์ผลฯ เป็นไปตามเป้าหมายหรือตัวชี้วัดที่กำหนดไว้ในแผนหรือไม่

(๓.๔) ทบทวนผลการประเมินความเสี่ยงอย่างเป็นระยะๆ ทบทวนระดับความเสี่ยงที่ยังเหลืออยู่ และระดับความเสี่ยงที่ยอมรับได้ ตามการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นกับหน่วยงาน เทคโนโลยีที่หน่วยงานใช้งาน วัตถุประสงค์และกระบวนการทางธุรกิจของหน่วยงาน ภัยคุกคามที่มีการระบุเพิ่มเติมหรือเปลี่ยนแปลง ความสัมฤทธิ์ผลของมาตรการต่างๆ ที่หน่วยงานใช้งาน เหตุการณ์ภายนอกต่างๆ ได้แก่ การเปลี่ยนแปลงด้านกฎหมาย ระเบียบ ข้อบังคับหรือสิ่งที่อยู่ในสัญญาจ้าง และการเปลี่ยนแปลงด้านสังคม

(๓.๕) ดำเนินการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบระยะเวลาที่ได้กำหนดไว้

(๓.๖) บันทึกข้อมูลการดำเนินการและเหตุการณ์ต่างๆ ซึ่งอาจมีผลกระทบต่อความสัมฤทธิ์ผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย ซึ่งประกอบด้วย การประชุมทบทวนด้านความมั่นคงปลอดภัยโดยผู้บริหาร ให้จัดทำรายงานการประชุมและแจ้งเวียนมติให้ผู้ที่เกี่ยวข้องได้รับทราบและปฏิบัติตาม การปฏิบัติตามนโยบายและขั้นตอนปฏิบัติต่างๆ ในในโยบายความมั่นคงปลอดภัยของหน่วยงาน ให้ผู้รับผิดชอบบันทึกหลักฐานการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเหล่านั้นไว้เพื่อให้สามารถตรวจสอบได้ในภายหลัง

(๔) การทบทวนและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย (Act)

(๔.๑) ปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามผลของการเฝ้าระวังติดตามและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย ได้แก่ การปฏิบัติตามมติการประชุม ทบทวนโดยผู้บริหาร การปรับปรุงนโยบายความมั่นคงปลอดภัย การจัดการหรือแก้ไขความไม่สอดคล้องกับนโยบายความมั่นคงปลอดภัย การกำหนดมาตรการเพิ่มเติมเพื่อลดการเกิดขึ้นของเหตุการณ์ด้านความมั่นคงปลอดภัยที่เคยเกิดขึ้นแล้ว การปฏิบัติตามแผนการลดความเสี่ยง การปฏิบัติตามแผนด้านความมั่นคงปลอดภัย การปฏิบัติตามคำแนะนำและผลตอบกลับจากผู้ที่เกี่ยวข้อง

(๔.๒) แจ้งการปรับปรุงและการดำเนินการให้แก่ทุกหน่วยที่เกี่ยวข้องทราบ โดยให้รายละเอียดที่เพียงพอและเหมาะสม ตรวจสอบว่าการปรับปรุงที่ได้ดำเนินการไปแล้วนั้นบรรลุผลตามที่ต้องการหรือไม่

ข้อ ๒ การวางแผนระบบบริหารความเสี่ยงของระบบฐานข้อมูลสารสนเทศ ต้องดำเนินการดังต่อไปนี้

(๑) มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่างๆ โดยสามารถฟื้นฟูระบบสารสนเทศ และการสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)

(๒) มีการจัดทำแผนแก้ไขปัญหาจากความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan)

(๓) มีระบบการรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล ได้แก่ ระบบ Antivirus และระบบไฟฟ้าสำรอง

(๔) มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access Rights)

ข้อ ๓ ต้องมีการทบทวนระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศเป็นประจำทุกปี อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๔ ต้องมีการตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) ดังนี้

(๑) แสดงรายชื่อฐานข้อมูลที่ครอบคลุมที่ใช้สนับสนุนการปฏิบัติงาน

(๒) แสดงผลการกำหนดผู้รับผิดชอบในการตรวจสอบข้อมูลและการจัดเก็บข้อมูล รวมถึงการดำเนินการตามแผนการจัดเก็บและตรวจสอบข้อมูลแต่ละประเภทในระบบฐานข้อมูล ในระยะเวลาที่เหมาะสม

(๓) แสดงระบบการตรวจสอบสิทธิการเข้าถึง (Log in) ที่สามารถ Verify Username และ Password

(๔) แสดงวิธีการ/ข้อกำหนดเกี่ยวกับรอบของการจัดเก็บข้อมูล

(๕) แสดงการอัพเดทข้อมูลที่จำเป็นอย่างสม่ำเสมอและทันท่วงที

(๖) แสดงเอกสารแนวทาง/มาตรการป องกันความเสียหาย และมีการสำรองข อมูลสารสนเทศ (Backup)

(๗) แสดงระบบรักษาความมั่นคงและปลอดภัยของระบบฐานข อมูลและสารสนเทศ ได้แก่ ระบบการตรวจสอบการบุกรุก การติดตั้งระบบบันทึกและติดตามการใช งานระบบสารสนเทศของสวนราชการ และตรวจตราการละเมิดความปลอดภัยที่มีตอระบบข อมูล ที่เปนไปตาม พ.ร.บ.วาด วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร พ.ศ. ๒๕๕๐

(๘) แสดงการจัดทำแผนบริหารความเสี่ยงดานคอมพิวเตอรและสารสนเทศ

(๙) แสดงระบบ Access Right ที่ถูกต องและทันสมัย ได้แก่ มีการกำหนดสิทธิการเขาถึงข อมูลและระบบข อมูลให เหมาะสมกับการเข าใช งานของผู ใช งาน ระบบและหนาที่ความรับผิดชอบของเจ าหนาที่ในการปฏิบัติงานก อนเข าใช ระบบสารสนเทศ รวมถึงการเปลี่ยนแปลงหรือยกเลิกรหัสผ าน (Password) เมื่อผู ใช งานระบบลาออก พ นจากตำแหนงหรือยกเลิกการใช งาน และมีการทบทวนสิทธิการเข าถึงอยางสม่ำเสมอ
