แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมตรวจบัญชีสหกรณ์
พ.ศ. ๒๕๕๗

คำนิยาม

"กรมฯ" หมายความว่า กรมตรวจบัญชีสหกรณ์

"ผู้ใช้งาน" หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ พนักงานจ้างเหมาที่ปรึกษาโครงการ ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

"สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

"สินทรัพย์" หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

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

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่เป็นไปได้ว่าจะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการที่ล้มเหลว หรือเหตุการณ์อันไม่สามารถรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"อุปกรณ์คอมพิวเตอร์" หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อหรือทำงานเป็นส่วนหนึ่งของระบบคอมพิวเตอร์ โดยอาจใช้ทำหน้าที่เป็นอุปกรณ์สื่อสาร หรือใช้บันทึกข้อมูล

"โปรแกรมพื้นฐาน" หมายความว่า โปรแกรมระบบปฏิบัติการ (Operating System), โปรแกรมสำนักงาน, โปรแกรมจัดการไฟล์ PDF, โปรแกรมป้องกันไวรัส, โปรแกรมบีบอัดไฟล์ และโปรแกรม Web Browser

"โปรแกรมกรมตรวจบัญชีสหกรณ์" หมายความว่า โปรแกรมที่พัฒนาขึ้นด้วยงบประมาณกรมตรวจบัญชีสหกรณ์ เพื่อสนับสนุนงานตามภารกิจของกรมฯ รวมถึงโปรแกรมกรมตรวจบัญชีสหกรณ์ที่อนุญาตให้สหกรณ์นำไปพัฒนาต่อยอด

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

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

“ระบบเครือข่ายส่วนตัวเสมือน (VPN)” หมายความว่า การนำโครงข่ายสาธารณะมาใช้เป็นสื่อในการส่งข้อมูลระหว่างหน่วยงานภายในองค์กร โดยใช้การเข้ารหัสข้อมูลสร้างเป็นระบบเครือข่ายเสมือนขึ้นเพื่อให้ข้อมูลที่ส่งผ่านมีความปลอดภัย

“ระบบเทคโนโลยีสารสนเทศ” หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผนบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูล และสารสนเทศ เป็นต้น

หมวด ๑
แนวปฏิบัติในการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องจัดการควบคุมการเข้าถึงระบบสารสนเทศของกรมฯ ดังนี้

(๑) ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ตนต้องใช้งานได้ก็ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบข้อมูล และ/หรือผู้รับผิดชอบระบบงานตามความจำเป็นต่อการใช้งานแล้วเท่านั้น

(๒) ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบกล่าวคือ ในการขออนุญาตเข้าระบบนั้น ผู้ใช้จะต้องมีการทำเป็นบันทึกและกรอกแบบเอกสารที่กรมฯ กำหนดเพื่อขออนุญาตเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้บังคับบัญชาหรือผู้รับมอบอำนาจจากผู้บังคับบัญชาเพื่อการจัดเก็บไว้เป็นหลักฐาน จากนั้น ผู้ดูแลระบบจะสร้างบัญชีสำหรับการเข้าถึงโดยอนุญาตเฉพาะในส่วนที่จำเป็น และโดยคำนึงถึงประเภทข้อมูลและชั้นความลับ

(๓) ผู้ดูแลระบบ ต้องกำหนดไม่ให้ผู้ใช้งานเข้าสู่ระบบได้ หากผู้ใช้งานใส่รหัสผ่านเข้าระบบผิด ๓ ครั้ง ให้ยื่นแบบฟอร์มเพื่อขอรหัสใหม่อีกครั้ง

(๔) ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่างๆ เมื่อผู้ใช้ไม่มีการใช้งานระบบสารสนเทศเกินกว่า ๓๐ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการ Log in เข้าระบบสารสนเทศอีกครั้ง และให้จำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานโดยให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลา ๓ ชั่วโมง ต่อการเชื่อมต่อ ๑ ครั้ง

(๕) ผู้รับผิดชอบข้อมูลและผู้รับผิดชอบระบบงาน ต้องอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น

ข้อ ๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน ดังนี้

(๑) การลงทะเบียนผู้ใช้งาน ต้องปฏิบัติตามขั้นตอนลงทะเบียนที่กรมฯ กำหนดขึ้นเพื่อให้มีสิทธิในการใช้งานระบบสารสนเทศตามความจำเป็น รวมทั้งปฏิบัติตามขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน ดังนี้

(๑.๑) การลงทะเบียนผู้ใช้งานที่บรรจุใหม่

(๑.๑.๑) เจ้าหน้าที่ที่ได้รับมอบหมายจากสำนักบริหารกลาง ทำการบันทึกข้อมูลรายละเอียดที่เกี่ยวข้องตามเอกสารและตามคำสั่งกรมฯ ลงในระบบ

(๑.๑.๒) ผู้ดูแลระบบกำหนดการเข้าถึงตามสิทธิที่ได้รับมอบ

(๑.๒) การถอนสิทธิการใช้งาน

(๑.๒.๑) เจ้าหน้าที่ที่ได้รับมอบหมายจากสำนักบริหารกลาง ทำการถอนสิทธิผู้ใช้งานออกจากระบบ ตามคำสั่งกรมฯ

(๑.๒.๒) ผู้ดูแลระบบถอนสิทธิผู้ใช้งานออกจากระบบ

(๒) กำหนดสิทธิการใช้ระบบสารสนเทศที่ให้บริการประชาชนภายนอก ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

(๓) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้สิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณาเพื่อขอความเห็นชอบและอนุมัติจากผู้บังคับบัญชา

(๓.๑) ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(๓.๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓.๓) มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

ข้อ ๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของผู้ใช้งาน ดังนี้

(๑) กำหนดบัญชีรายชื่อผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน

(๒) ไม่อนุญาตให้ผู้ร้องขอใช้ระบบงานเข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้น

(๓) จัดเก็บข้อมูลการลงทะเบียนของผู้ที่ร้องขอใช้ระบบไว้เพื่อเอาไว้ใช้อ้างอิงหรือตรวจสอบในภายหลัง

(๔) ทบทวนบัญชีและสิทธิผู้ใช้งานทั้งหมด พร้อมทั้งปรับปรุงอย่างสม่ำเสมอทุก ๖ เดือน เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

ข้อ ๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องจัดให้มีการพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบสำคัญสำหรับผู้ใช้ที่อยู่ภายนอก ดังนี้

(๑) การแสดงตัวตนด้วยชื่อบัญชีผู้ใช้งาน

(๒) การพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน

(๓) การเข้าสู่ระบบงานสำคัญของกรมฯ ผ่านเครือข่ายอินเตอร์เน็ตนั้น จะมีการตรวจสอบผู้ใช้งานด้วย

(๔) การเข้าสู่ระบบงานสำคัญของกรมฯ จากระยะไกลเพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ข้อ ๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในกรมฯ 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) เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์ที่ซื้อจากผู้ผลิต

(๙) มีการแจ้งเตือนโดยหนังสือหรือทางเว็บไซต์ในครั้งแรกที่ได้รับรหัสผ่าน โดยทำการเปลี่ยนรหัสผ่านทันที และเก็บรหัสผ่านไว้เป็นความลับ

(๑๐)การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๑๑)กำหนดให้ผู้ดูแลระบบจัดทำระบบให้สามารถทำงานอัตโนมัติ เพื่อการกำหนดรหัสที่มีคุณภาพ

ข้อ ๖ การจ้างพัฒนาระบบสารสนเทศ หรือจ้างเหมาดำเนินงาน (outsource) ให้ปฏิบัติดังนี้

(๑) บุคคลหรือนิติบุคคล หรือพนักงานลูกจ้างที่เป็นคู่สัญญา ต้องมีการลงนามในการรักษาความลับ ห้ามเปิดเผยข้อมูลขององค์กรก่อนปฏิบัติหน้าที่

ข้อ ๗ การจัดการระบบซึ่งไวต่อการรบกวน ให้ปฏิบัติดังนี้

(๑) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อกรมฯ ได้แก่ ระบบ GFMIS หรือระบบการบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ เป็นระบบที่ใช้ในการปฏิบัติงานด้านการงบประมาณ การบัญชี การจัดซื้อจัดจ้าง การเบิกจ่าย และการบริหารทรัพยากร ซึ่งดูแลรับผิดชอบโดยกรมบัญชีกลาง จะได้รับการแยกออกจากระบบงานอื่นๆ ของกรมฯ

(๒) ระบบซึ่งไวต่อการรบกวน ต้องมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องมีการกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้นเข้าไปปฏิบัติงาน

(๓) แยกสภาพการติดตั้งทางเครือข่ายโดยใช้วิธีการทางเทคนิค เช่น VLAN (Virtual Local Area Network)

(๔) แบ่งแยกเครือข่ายสำหรับระบบที่ไวต่อการรบกวน มีผลกระทบและมีความสำคัญต่อหน่วยงานสูงออกจากระบบอื่น โดยให้จัดทำเป็นเครือข่าย DMZ (Dermilitarize Zone)

(๕) ทำการควบคุมการเข้ามาใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกตามข้อกำหนดที่ตั้งค่าไว้ใน Firewall

ข้อ ๘ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ดังนี้

(๑) มีการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงระบบงานของหน่วยงานจากระยะไกลโดยผ่านทางอุปกรณ์คอมพิวเตอร์ประเภทพกพาของหน่วยงาน

(๒) ควบคุมการติดตั้งโปรแกรมไม่พึงประสงค์ในอุปกรณ์คอมพิวเตอร์ประเภทพกพาของหน่วยงาน

(๓) ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในหน่วยงานมาปฏิบัติงานที่ห้องระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้า-ออกพื้นที่ให้ถูกต้องชัดเจน และต้องได้รับอนุญาตจากเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ด้วยการลงนามอย่างเป็นลายลักษณ์อักษร

ข้อ ๙ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ให้ปฏิบัติดังนี้

(๑) ผู้ดูแลระบบ ต้องให้สิทธิตามที่ได้รับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

(๒) ผู้ใช้งานระบบจากระยะไกล ต้องได้รับอนุมัติจากผู้บังคับบัญชาหรือเจ้าของระบบงานอย่างเป็นทางการ และต้องใช้งานตามระยะเวลาการเข้าถึงที่กำหนดไว้

(๓) ผู้ใช้งานระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

(๔) มีการควบคุมทางกายภาพที่จำเป็นสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกลเพื่อป้องกันการขโมยอุปกรณ์ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี

หมวด ๒
แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

ผู้บังคับบัญชาหน่วยงานภายในกรมฯ ต้องจัดให้มีวิธีการจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ ซึ่งเบื้องต้นกรมฯ ใช้แนวทางตาม พ.ร.บ.ข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐ และระเบียบที่เกี่ยวข้องในการกำหนดชั้นความลับของข้อมูล ดังนี้

ข้อ ๑ การจัดแบ่งประเภทของข้อมูล

- ข้อมูลสารสนเทศด้านการบริหาร
- ข้อมูลสารสนเทศด้านการให้บริการ

ข้อ ๒ ผู้ใช้งาน ต้องจัดการกับข้อมูลตามชั้นความลับของข้อมูล ศูนย์เทคโนโลยีสารสนเทศได้กำหนดชั้นความลับของข้อมูลเป็น ๔ ระดับ ดังนี้

- ลับ (Top secret/Secret/Confidential)
- ใช้ภายในเท่านั้น (Internal use)
- ส่วนบุคคล (Personal)
- เปิดเผยได้ (Public)

ข้อ ๓ ผู้ใช้งาน พิจารณาจากองค์ประกอบต่อไปนี้เพื่อเป็นแนวทางกำหนดชั้นความลับของข้อมูล

- ความสำคัญของเนื้อหา เช่น เนื้อหาของข้อมูลนั้นมีความสำคัญต่อความสำเร็จของงานตามภารกิจของกรมฯ มากน้อยเพียงใด หากมีความสำคัญสูง ข้อมูลนั้นจะสามารถจัดอยู่ในชั้นความลับประเภทใช้ภายในเท่านั้น หรือลับ เป็นต้น
- แหล่งที่มาของข้อมูล เช่น หากข้อมูลนั้นมาจากภายนอกและเป็นข้อมูลลับ ชั้นความลับก็จะต้องคงไว้เช่นเดิม หรือหากข้อมูลนั้นมาจากอินเตอร์เน็ต ชั้นความลับก็จะเป็นประเภทเปิดเผยได้ เป็นต้น

- วิธีการนำไปใช้ประโยชน์ เช่น หากข้อมูลนั้นสามารถนำไปใช้ประโยชน์ในเชิงพาณิชย์ได้ หากถูกเปิดเผยจะส่งผลกระทบด้านการเงินของกรมฯ ดังนั้นข้อมูลนี้จะอยู่ในประเภทลับ เป็นต้น
- จำนวนบุคลากรที่ควรรับทราบ เช่น หากข้อมูลนั้นสามารถเปิดเผยต่อผู้ใช้งานข้อมูลเป็นจำนวนมาก ชั้นความลับจะเป็นข้อมูลเปิดเผยได้ เป็นต้น
- ผลกระทบหากมีการเปิดเผย เช่น หากข้อมูลนั้นถูกเปิดเผยจะมีผลกระทบด้านชื่อเสียงและภาพลักษณ์ ด้านการเงิน ด้านการปฏิบัติตามระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม หรือด้านการมีส่วนได้ส่วนเสียของผู้ที่เกี่ยวข้อง ดังนั้นข้อมูลจะสามารถจัดอยู่ในชั้นความลับประเภทใช้ภายในเท่านั้น หรือลับ เป็นต้น
- หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่อง เช่น ข้อมูลสำคัญหรือข้อมูลลับที่มาจากเจ้าของเรื่องใด จะต้องคงชั้นความลับไว้เช่นเดิม การนำไปใช้งานควรขออนุญาตจากผู้ที่เป็นเจ้าของเรื่องก่อน เป็นต้น

ข้อ ๔ ลำดับชั้นความลับของข้อมูล “ลับ” ได้แก่ ลับ ลับมาก หรือลับที่สุด เจ้าของข้อมูลพิจารณาเกณฑ์ต่อไปนี้เพิ่มเติมเพื่อกำหนดชั้นความลับที่ถูกต้อง

- ลับที่สุด หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด
- ลับมาก หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง
- ลับ หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

ข้อ ๕ การเข้าถึงสารสนเทศ สามารถเข้าถึงระบบงานต่างๆ ได้ตลอด ๒๔ ชั่วโมง โดยผ่านช่องทางอินเตอร์เน็ต

ข้อ ๖ การดำเนินการกับข้อมูลลับ (ถ้ามี) เจ้าของข้อมูลลับฯ ดำเนินการจัดทำทะเบียนข้อมูลกับที่ตนเองดูแลหรือรับผิดชอบ ซึ่งมีรายละเอียดประกอบด้วย

- ชื่อของข้อมูล
- ชั้นความลับ
- ชื่อเจ้าของข้อมูลลับ
- เหตุผลประกอบการกำหนดชั้นความลับ
- หน่วยงานภายในที่สามารถเข้าถึงได้
- สถานที่จัดเก็บข้อมูล
- ระบบงานที่ใช้จัดเก็บข้อมูล
- ระยะเวลาการเก็บรักษาข้อมูล
- ระยะเวลาการเข้าถึง

ข้อมูลความลับทั้งหมดให้ผู้รับผิดชอบในการจัดทำทะเบียนครุภัณฑ์ของศูนย์เทคโนโลยีสารสนเทศ เป็นผู้เก็บรักษา

ข้อ ๗ พิจารณาปรับชั้นความลับ (ปรับลด เพิ่ม หรือยกเลิกชั้นความลับ) ตามความจำเป็น ปรับปรุงทะเบียนข้อมูลลับให้ถูกต้องและทันสมัย และต้องแจ้งให้หน่วยงานที่สามารถเข้าถึงข้อมูลหรือที่ได้รับการแจกจ่ายทราบด้วยทุกครั้ง เพื่อแก้ไขชั้นความลับให้ถูกต้อง

ข้อ ๘ ในการจัดทำหรือจัดเตรียมข้อมูลลับ ให้ผู้ใช้งานปฏิบัติดังนี้

(๑) จัดทำหรือจัดเตรียมข้อมูลในสถานที่ที่ปลอดภัย เช่น จัดทำในสำนักงาน ไม่ทำในสถานที่ที่เป็นสาธารณะ ซึ่งบุคคลภายนอกสามารถมองเห็นข้อมูลที่จัดทำได้ และจำกัดผู้ที่เป็นผู้ดำเนินการจัดทำ

(๒) ในการจัดทำข้อมูลลับซึ่งใช้กระดาษหรือวัสดุชั่วคราว เช่น กระดาษร่าง กระดาษคาร์บอน ต้องทำลายกระดาษหรือวัสดุนั้นทันทีที่จัดทำเสร็จเรียบร้อย ถ้าเป็นการจัดทำโดยใช้เครื่องคอมพิวเตอร์ จะต้องทำการลบ หรือทำลายสื่อบันทึกข้อมูลจนไม่สามารถนำไปใช้ประโยชน์ได้ (ดูวิธีการทำลายในตารางแสดงแนวทางปฏิบัติในการทำลายข้อมูลบนสื่อบันทึกข้อมูล) หากไม่ทำลาย ต้องเก็บรักษาไว้ในสถานที่ที่ปลอดภัย

(๓) จัดทำข้อมูลโดยแสดงเลขที่หน้าของจำนวนหน้าทั้งหมดไว้ในทุกหน้าของข้อมูลลับ และแสดงไว้ในส่วนที่สามารถเห็นได้ชัดเจน เช่น มุมขวาด้านบนของเอกสาร (การบันทึกเลขหน้า มีจุดประสงค์เพื่อให้ทราบว่าข้อมูลลับนั้นเป็นหน้าใดของจำนวนทั้งหมดกี่หน้า หากมีการสูญหายไปหน้าใดหน้าหนึ่งจะได้ทราบและสามารถติดตามหาผู้ละเมิดและหาทางลดหรือแก้ไขความเสียหายที่เกิดขึ้นได้)

(๔) โปรแกรมกรมตรวจบัญชีสหกรณ์ที่พัฒนาแล้วเสร็จ ให้ผู้ดูแลระบบส่งมอบข้อมูล source code ให้กับผู้รับผิดชอบในการจัดทำทะเบียนครุภัณฑ์ของศูนย์เทคโนโลยีสารสนเทศ

ข้อ ๙ ในการแสดงชั้นความลับบนข้อมูลลับ ให้ปฏิบัติดังนี้

(๑) แสดงชั้นความลับของข้อมูล (ซึ่งประกอบด้วย “ลับ” “ลับมาก” หรือ “ลับที่สุด”) ให้ปรากฏเห็นอย่างเด่นชัดทั้งข้อมูลที่มีสภาพเป็นกระดาษ ไฟล์อิเล็กทรอนิกส์ เทป External Harddisk Flash Drive แผ่น CD/DVD หรือข้อมูลลับที่อยู่ในรูปแบบอื่นๆ

(๒) แสดงชั้นความลับบนเอกสารลับในทุกหน้าของเอกสารให้ปรากฏเห็นอย่างเด่นชัด

ข้อ ๑๐ ในการทำสำเนาหรือแจกจ่ายข้อมูลลับ ให้ปฏิบัติดังนี้

(๑) ทำสำเนาหรือแจกจ่ายข้อมูลลับให้แก่ผู้รับปลายทาง ซึ่งเป็นผู้มีสิทธิในการเข้าถึงข้อมูลตามที่ระบุไว้ในทะเบียนข้อมูลลับ หรือสามารถแจกจ่ายให้ได้ตามความจำเป็นในการเข้าถึงข้อมูลนั้น

(๒) แจ้งให้หน่วยงานภายนอกที่อนุญาตให้เข้าถึงข้อมูลลับนั้นได้ ว่าไม่อนุญาตให้ทำสำเนาเพิ่มเติม เว้นเสียแต่ได้รับอนุญาตจากผู้มีอำนาจลงนามอนุญาตก่อน

ข้อ ๑๑ ในการเก็บรักษาเอกสารลับ ให้ปฏิบัติดังนี้

(๑) จัดเก็บเอกสารลับไว้ในแฟ้มข้อมูลลับ และนำไปเก็บไว้ในตู้เอกสารลับโดยแยกเก็บเป็นแต่ละเรื่องหรือแต่ละหัวข้อ

(๒) ไม่จัดเก็บเอกสารลับร่วมกับเอกสารที่อยู่ในชั้นความลับอื่นๆ เช่น ข้อมูลใช้ภายในเท่านั้น ข้อมูลส่วนบุคคลหรือข้อมูลที่เปิดเผยได้

(๓) จัดเก็บแฟ้มข้อมูลลับไว้ในตู้และปิดล็อคด้วยกุญแจที่มั่นคง

ข้อ ๑๒ ในกรณียืมหรือขอเข้าถึงข้อมูลลับ ให้ปฏิบัติดังนี้

(๑) เมื่อมีการขอยืมหรือขอเข้าถึงข้อมูลลับโดยผู้อื่นที่ไม่ได้เป็นผู้มีสิทธิในการเข้าถึงข้อมูลตามทะเบียนข้อมูลลับ ให้หัวหน้าหน่วยงานภายใน เป็นผู้พิจารณาตรวจสอบคุณสมบัติของผู้ยืม หรือขอเข้าถึงก่อนว่าเป็นผู้มีหลักฐานการยืมหรือการขอเข้าถึงข้อมูลนั้นด้วย แจ้งให้ผู้ยืมหรือขอเข้าถึงทราบว่าห้ามทำการสำเนาเพิ่มเติม

(๒) เมื่อหมดความจำเป็นในการใช้งานแล้ว หัวหน้าหน่วยงานภายในกำหนดให้ผู้ขอยืมจัดส่งข้อมูลนั้นกลับคืนมาโดยทันที สำหรับกรณีการเข้าถึงระบบเทคโนโลยีสารสนเทศให้ทำการยกเลิกบัญชีผู้ใช้งานที่ขอเข้าถึงข้อมูลลับโดยทันที

ข้อ ๑๓ ในการส่งเอกสารลับ ให้ปฏิบัติตามระเบียบการส่งเอกสารลับของกรมฯ ตรวจสอบการแสดงที่อยู่อีเมล์ของผู้รับปลายทางให้ถูกต้องก่อนจัดส่งไฟล์นั้นไปยังผู้รับเพื่อป้องกันการส่งผิดตัวบุคคล

ข้อ ๑๔ ในการทำลายข้อมูลลับ ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ

ประเภท สื่อบันทึกข้อมูล	**วิธีการทำลาย แบบไม่นำกลับมาใช้อีก**	**วิธีการทำลาย แบบนำกลับมาใช้ได้อีก**
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย	ใช้วิธีการทำลายข้อมูลตามมาตรฐานกระทรวงกลาโหมสหรัฐอเมริกา DOD ๕๒๐๐-๓๓-M
กระดาษ	ใช้วิธีการหั่นด้วยเครื่องหั่นทำลายเอกสาร	-
แผ่น CD/DVD	ใช้วิธีการหั่นด้วยเครื่องหั่นทำลาย CD/DVD	-
เทป	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย	-
ฮาร์ดดิสก์	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย	ใช้วิธีการทำลายข้อมูลตามมาตรฐานกระทรวงกลาโหมสหรัฐอเมริกา DOD ๕๒๐๐-๓๓-M

ข้อ ๑๕ ในการจัดการกับไฟล์ข้อมูลลับ ให้ปฏิบัติดังนี้

(๑) จัดหมวดหมู่ข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือที่มีระดับความสำคัญสูงไว้ต่างหาก และป้องกันให้มีความปลอดภัยอย่างพอเพียงต่อการเข้าถึง และควรแสดงชั้นความลับบนไฟล์ข้อมูลลับ

(๒) การสำเนาข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับหรือเอกสารที่มีระดับความสำคัญสูงต้องได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูล

(๓) ระมัดระวังการกระจายหรือแจกจ่ายข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับของกรมตรวจบัญชีสหกรณ์ ไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

(๔) ผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ต้องตรวจสอบความถูกต้องของข้อมูลอิเล็กทรอนิกส์ก่อนนำไปใช้งาน

(๕) ห้ามผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับหรือที่มีระดับความสำคัญสูง ส่งข้อมูลดังกล่าวไปทางไปรษณีย์ เว้นแต่จะได้ใช้วิธีเข้ารหัสที่กรมตรวจบัญชีสหกรณ์กำหนดไว้

(๖) ให้ผู้ใช้งานนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ

(๗) ห้าม share ไฟล์ข้อมูลลับบนเครือข่ายของกรมฯ เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ (ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการ share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)

(๘) ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลลับว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

(๙) ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่เพื่อแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่

(๑๐) ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

(๑๑) ต้องทำลายข้อมูลอิเล็กทรอนิกส์บนฮาร์ดแวร์ของเครื่องคอมพิวเตอร์ที่ถูกยกเลิกการใช้งาน

หมวด ๓
แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

ข้อ ๑ ผู้ใช้งาน ต้องยืนยันตัวตนด้วยชื่อผู้ใช้และรหัสผ่าน (User account) ของตนเองก่อนเข้าใช้งานระบบปฏิบัติการเครื่องคอมพิวเตอร์ทุกครั้ง

ข้อ ๒ ผู้ใช้งาน ต้องไม่อนุญาตให้บุคคลอื่นใช้ชื่อผู้ใช้และรหัสผ่าน (User account) ของตนเองในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

ข้อ ๓ ผู้ดูแลระบบ ต้องตั้งค่าระบบให้มีการแจ้งเตือนแก่ผู้ใช้งาน เมื่อผู้ใช้งานใส่รหัสผ่านผิดเกิน ๓ ครั้ง โดยระบบจะล็อคสิทธิการเข้าถึงของผู้ใช้งาน ทำให้ผู้ใช้งานรายนั้นไม่สามารถเข้าถึงระบบปฏิบัติการได้อีกจนกว่าผู้ดูแลระบบจะดำเนินการปลดล็อคให้

ข้อ ๔ ติดตั้งโปรแกรมแก้ไขช่องโหว่ต่างๆ (patch) ที่เกี่ยวข้องกับระบบงานตามความจำเป็น เช่น โปรแกรมแก้ไขช่องโหว่สำหรับระบบปฏิบัติการ เป็นต้น

ข้อ ๕ การจำกัดการใช้งานโปรแกรมประเภทอรรถประโยชน์

(๑) ให้ผู้ดูแลระบบทำบัญชีรายชื่อโปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้งานได้เท่านั้น

(๒) ห้ามผู้ใช้งานติดตั้งหรือใช้งานโปรแกรมที่ละเมิดลิขสิทธิ์

หมวด ๔
แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย

ข้อ ๑ การควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่าย ผู้รับผิดชอบด้านเครือข่ายของหน่วยงานภายในกรมฯ ต้องปฏิบัติตามข้อกำหนดดังนี้

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

(๒) การเข้าถึงห้องควบคุมระบบเครือข่าย ต้องทำการสแกนลายนิ้วมือรวมทั้งมีการเก็บบันทึกการเข้า-ออกห้องระบบเครือข่ายจากเครื่องสแกนลายนิ้วมือ และจัดเก็บรายละเอียดลงในฐานข้อมูล

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

(๔) เมื่อมีบุคคลภายนอกต้องการเข้ามายังห้องควบคุมระบบเครือข่าย ต้องมีการขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

(๕) เจ้าหน้าที่ที่รับผิดชอบด้านเครือข่ายของศูนย์เทคโนโลยีสารสนเทศ อยู่ภายในห้องควบคุมระบบเครือข่าย เมื่อมีบุคคลภายนอกเข้ามายังห้องควบคุมระบบเครือข่าย

(๖) ต้องทำการทบทวนสิทธิการเข้า-ออกห้องควบคุมระบบเครือข่าย อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ การควบคุมการเข้าถึงระบบเครือข่าย ต้องปฏิบัติตามข้อกำหนดดังนี้

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

(๒) ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๓) ผู้ใช้งาน ต้องรับผิดชอบระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งผู้ใช้งานต้องไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่ายจากบัญชีผู้ใช้ของตนเอง

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

(๕) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน ผ่านทางระบบอินเตอร์เน็ต ต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

(๖) ทบทวนบัญชีและสิทธิผู้ใช้งานทั้งหมด พร้อมทั้งปรับปรุงอย่างสม่ำเสมอทุก ๖ เดือน เพื่อป้องกันการเข้าถึงระบบโดยมิได้รับอนุญาต

(๗) ข้อมูลหมายเลขชุดอินเตอร์เน็ตของคอมพิวเตอร์ (IP Address) ของระบบงานเครือข่ายภายในของกรมฯ จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของกรมฯ ได้โดยง่าย

(๘) ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์เครือข่ายส่วนกลาง ได้แก่ อุปกรณ์จัดหาเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) หรืออุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

(๙) บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายของหน่วยงาน ต้องทำหนังสือขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย เพื่อขอรับชื่อผู้ใช้ และรหัสผ่านในการเข้าใช้งานระบบ

(๑๐)ผู้ใช้งาน ต้องใช้เครือข่ายสารสนเทศอย่างมีประสิทธิภาพ เช่น ห้ามดาวน์โหลดไฟล์ หรืออัพโหลดไฟล์ที่มีขนาดใหญ่เกินไปหรือดูหนังฟังเพลงออนไลน์ในระหว่างเวลาปฏิบัติงาน ซึ่งมีผลกระทบต่อการใช้งานเครือข่ายของกรมฯ

(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 เช่น 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 ต้องทำการเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปในการให้บริการอินเตอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากศูนย์เทคโนโลยีสารสนเทศก่อน

(๑๙) ผู้ดูแลระบบ ต้องกำหนดการเปิด-ปิดพอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่าย โดยปิดพอร์ตที่มีความเสี่ยงอันจะก่อให้เกิดความเสียหายต่อระบบเครือข่าย

(๒๐) ผู้ดูแลระบบ ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๒๑) ผู้ดูแลระบบ ต้องแบ่งแยกเครือข่ายเป็นเครือข่ายย่อยๆ ตามอาคารต่างๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

(๒๒) ผู้ดูแลระบบ ต้องจัดแบ่งเครือข่ายภายในหน่วยงานออกเป็นเครือข่ายภายในและเครือข่ายภายนอก

(๒๓) ผู้ดูแลระบบ ต้องใช้ไฟร์วอลล์กั้น หรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อยๆ

(๒๔) ผู้ดูแลระบบ ต้องใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่ายทั้งจากภายในและภายนอกหน่วยงาน ซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของหน่วยงาน

(๒๕) ผู้ดูแลระบบ ต้องทำการตรวจสอบเกตเวย์หรืออุปกรณ์เครือข่าย IP Address ของทั้งต้นทางและปลายทางและควบคุมการไหลของข้อมูลผ่านเครือข่ายต่างๆ จากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง โดยให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

(๒๖) ผู้ดูแลระบบ จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องแม่ข่าย เพื่อไม่อนุญาตให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้ นอกจากเส้นทางที่ได้กำหนดไว้ให้เท่านั้น

(๒๗) ผู้ดูแลระบบ ตรวจสอบและกำหนดเส้นทางบนเครือข่ายให้เหมาะสม โดยผ่านทางอุปกรณ์เครือข่าย เพื่อควบคุมการเชื่อมต่อทางเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึงของหน่วยงาน

ข้อ ๓ การควบคุมการเข้าใช้งานระบบจากภายนอก ต้องปฏิบัติตามข้อกำหนดดังนี้

(๑) การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายของกรมฯ ซึ่งก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของกรมฯ การควบคุมบุคคลที่เข้าสู่ระบบของกรมฯ จากระยะไกลจึงต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๒) ผู้ใช้งาน ต้องทำหนังสือระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอในการขอสิทธิการเข้าสู่ระบบจากระยะไกล และต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

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

ข้อ ๔ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ผู้รับผิดชอบต้องปฏิบัติตามข้อกำหนดดังนี้

(๑) ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของกรมฯ จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการพิจารณาจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร

(๒) ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(๓) ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

(๔) ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ (Access Point) ให้เหมาะสม เพื่อควบคุมไม่ให้สัญญาณรั่วไหลออกนอกบริเวณพื้นที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับ-ส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๕) ผู้ดูแลระบบ ต้องควบคุมไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

(๖) ผู้ดูแลระบบ ควรเลือกใช้วิธีการควบคุม MAC address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address และชื่อผู้ใช้รหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

(๗) ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

(๘) ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

หมวด ๕
แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

ข้อ ๑ การใช้คอมพิวเตอร์ของกรมฯ ให้ปฏิบัติดังนี้

(๑) ต้องตรวจสอบว่าโปรแกรมป้องกันไวรัส มีการทำงานตามปกติและมีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ หากพบว่าโปรแกรมดังกล่าวทำงานผิดปกติให้รีบแจ้งศูนย์เทคโนโลยีสารสนเทศเพื่อดำเนินการแก้ไขโดยเร็ว

(๒) คอมพิวเตอร์ที่ใช้ในกรมฯ ให้ติดตั้งเฉพาะโปรแกรมพื้นฐาน หากมีการติดตั้งโปรแกรมเพิ่มเติม ต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานภายใน หรือผู้ที่ได้รับมอบหมาย

(๓) ต้องลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่อคอมพิวเตอร์เพื่อประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

(๔) ต้องออกจากระบบ (Log off) ทุกครั้งที่มิได้ปฏิบัติงานอยู่หน้าคอมพิวเตอร์ หรือปิดคอมพิวเตอร์เมื่อใช้งานประจำวันเสร็จสิ้น

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

(๖) ให้ผู้ใช้งานล็อคอุปกรณ์คอมพิวเตอร์สำคัญเมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว เพื่อป้องกันการสูญหายหรือถูกขโมย

(๗) การยืมคอมพิวเตอร์ต้องได้รับอนุญาตจากหน่วยงานผู้รับผิดชอบ โดยจัดทำเป็นลายลักษณ์อักษร

(๘) การนำคอมพิวเตอร์ส่วนตัวมาใช้กับระบบเครือข่ายของกรมฯ ต้องได้รับการตรวจสอบและอนุญาตจากศูนย์เทคโนโลยีสารสนเทศโดยผ่านการลงทะเบียน และต้องสแกนไวรัสก่อนการใช้งานทุกครั้ง

ข้อ ๒ การใช้คอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพา ให้ปฏิบัติดังนี้

(๑) กำหนดให้ใช้งานเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของหน่วยงานอย่างมีประสิทธิภาพและโปรแกรมที่ติดตั้งต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย

(๒) ไม่ทำการปิดหรือยกเลิก หรือเปลี่ยนระบบโปรแกรมป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

(๓) หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมไวรัส ห้ามเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของไวรัสไปยังเครื่องคอมพิวเตอร์อื่นๆ และแจ้งผู้ดูแลระบบทราบ

(๔) ผู้ใช้งาน ต้องรับผิดชอบในการตรวจหาไวรัสจากสื่อต่างๆ เช่น Flash Drive และ External Hard disk อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ ตรวจสอบหาไวรัสจากเครื่องคอมพิวเตอร์ที่ใช้งาน รวมทั้งตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ต

ข้อ ๓ ในกรณีที่เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนคอมพิวเตอร์แบบพกพา ตรวจพบความเสียหาย และหากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทเลินเล่ออย่างร้ายแรงของผู้นำไปใช้ ต้องให้ผู้นำไปใช้รับผิดชอบต่อความเสียหายที่เกิดขึ้นดังกล่าว

ข้อ ๔ การใช้งานอินเตอร์เน็ต ผู้ใช้งานต้องปฏิบัติดังนี้

(๑) ต้องไม่ใช้ระบบอินเตอร์เน็ตของกรมฯ เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน เป็นต้น

(๒) ต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมฯ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเตอร์เน็ต

(๓) การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Webboard) ของหน่วยงาน ต้องไม่เสนอความคิดเห็นหรือใช้ข้อความยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน

(๔) หลังจากการใช้งานเสร็จแล้ว ให้ปิดเว็บเบราเซอร์ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ข้อ ๕ การใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ผู้ใช้งานต้องปฏิบัติดังนี้

(๑) ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) เพื่อใช้ในราชการ ตามที่กรมฯ กำหนดเท่านั้น

(๒) เมื่อได้รับรหัสผ่าน (Password) ต้องทำการเปลี่ยนรหัสผ่านโดยทันทีเมื่อมีการเข้าสู่ระบบในครั้งแรก

(๓) ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (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 (Logout) จากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)

(๘) การให้บริการ E-mail Address จะสิ้นสุดลงเมื่อผู้ใช้งานไม่มีการใช้งานในช่วงระยะเวลา ๓ เดือน ศูนย์เทคโนโลยีสารสนเทศขอสงวนสิทธิ์ในการลบ Account ทันทีโดยไม่แจ้งให้ทราบล่วงหน้า

ข้อ ๖ การใช้งานรหัสผ่าน (password use) ผู้ใช้งานต้องใช้งานรหัสผ่าน และเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

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

(๒) กำหนดรหัสผ่านที่มีความยาวไม่น้อยกว่า ๘ ตัวอักษร มีการผสมกันระหว่างตัวเลขตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ต่างๆ

(๓) เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับครั้งแรกทันทีที่ทำการ login เข้าสู่ระบบงาน

(๔) หลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น ๑๒๓๔, abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน เช่น ๙๙๙, aaa เป็นต้น

(๕) ไม่กำหนดรหัสผ่านจากชื่อ หรือชื่อสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว หรือจากหมายเลขโทรศัพท์

(๖) ตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำตนเอง แต่ควรเป็นรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

(๗) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันกับระบบงานต่างๆ ที่มีสิทธิใช้งาน

(๘) ไม่กำหนดให้ระบบงานทำการบันทึกหรือบันทึกไว้ในหน้าจอ Login

(๙) เก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย และต้องไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่น

(๑๐) เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

ข้อ ๗ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ ผู้ใช้งานต้องปฏิบัติดังนี้

(๑) ต้องเก็บเอกสาร ข้อมูลในการทำงาน หรือสื่อบันทึกข้อมูลไว้ในที่ปลอดภัย เช่น ใส่ตู้หรือโต๊ะที่สามารถล็อคกุญแจได้ เป็นต้น

(๒) ต้องระมัดระวังและดูแลทรัพย์สินของหน่วยงานที่ตนเองใช้งาน หรือถือครองเสมือนเป็นทรัพยสินของตนเอง หากเกิดความสูญหาย หรือเสียหายโดยประมาทเลินเล่อ ต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

(๓) ต้องไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล ให้อยู่ในสถานที่ที่ไม่ปลอดภัย

(๔) ต้องรับผิดชอบในการสำรองข้อมูลของตนเอง และต้องเก็บรักษาไว้ในที่ปลอดภัย

(๕) การป้องกันทรัพย์สินสารสนเทศที่สำคัญและการเข้าถึงระบบสารสนเทศ ต้องมีความสอดคล้องกับวัฒนธรรมของหน่วยงานในการป้องกันทรัพย์สิน เช่น วัฒนธรรมการปฏิบัติตามนโยบาย ๕ ส. ซึ่งจะกำหนดให้มีการจัดการกับเอกสารสำคัญอย่างเหมาะสม เช่น การจัดใส่ไว้ในตู้และมีกุญแจล็อค การแยกเอกสารสำคัญไว้สำหรับทำลายต่างหาก เป็นต้น

(๖) ต้องมีกลไกการพิสูจน์ตัวตนที่เหมาะสม เพื่อป้องกันเครื่องคอมพิวเตอร์หรือระบบงานของหน่วยงานก่อนเข้าใช้งาน เช่น การ Login ด้วยรหัสผ่าน หรือการใช้อุปกรณ์ token เพื่อสร้างรหัสผ่าน ซึ่งสามารถสร้างรหัสผ่านที่แตกต่างกันในแต่ละครั้งที่ใช้งานอุปกรณ์นี้ เป็นต้น

(๗) จัดเก็บข้อมูลสำคัญหรือลับไว้ในสถานที่ที่มีความปลอดภัย ภายหลังจากใช้งานเสร็จ เช่น ใส่ตู้ที่ล็อคกุญแจได้ เป็นต้น

(๘) ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์สารสนเทศต่างๆ โดยไม่ได้รับอนุญาต

หมวด ๖
แนวปฏิบัติในการสำรองข้อมูล

ข้อ ๑ ด้านการสำรองข้อมูล

(๑) ผู้ดูแลระบบ ต้องคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม ดังนี้

(๑.๑) ระบบงานหลักที่มีความสำคัญระดับเคร่งครัดให้สำรองข้อมูลแบบ Full System Backup และ Full Data Backup (เดือนละ ๑ ครั้ง)

(๑.๒) ระบบงานหลักที่มีความสำคัญระดับกลางให้สำรองข้อมูลแบบ Full Data Backup (สัปดาห์ละ ๑ ครั้ง)

(๑.๓) ระบบงานหลักที่มีความสำคัญระดับพื้นฐานให้สำรองข้อมูลแบบ Incremental Backup (เฉพาะส่วนที่มีการเปลี่ยนแปลงแต่ละวัน)

(๒) จัดเก็บข้อมูลที่สำรอง ต้องกำหนดวันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

(๓) ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องสมบูรณ์ในการ Backup

(๔) การจัดทำบันทึกการสำรองข้อมูล (Operator Logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น และรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

(๕) การรายงานข้อผิดพลาด (Fault Logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

(๖) ในกรณีพบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการสำรองข้อมูลอย่างสมบูรณ์ได้ ให้ผู้ดูแลระบบดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหา และรายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๗) การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted Backup) ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลที่สำรองเหล่านั้นถูกเปิดเผย

(๘) ต้องจัดเก็บข้อมูลที่สำรองไว้ในสถานที่เก็บข้อมูลสำรอง ซึ่งติดตั้งแยกสถานที่กับห้องควบคุมระบบเครือข่าย เพื่อให้เป็นไปตามนโยบายของกรมฯ ในการป้องกันไม่ให้ข้อมูลสูญหายเมื่อเกิดภัยพิบัติ และสามารถใช้งานได้อย่างต่อเนื่อง

(๙) ผู้ดูแลระบบ ดำเนินการตามกระบวนการสำรองข้อมูลสำหรับแต่ละระบบสารสนเทศโดยเคร่งครัด

(๑๐)ผู้ดูแลระบบ ทำการทบทวนข้อมูลที่มีการสำรองอย่างน้อยทุก ๖ เดือน

(๑๑)ผู้ดูแลระบบ ทำการทดสอบข้อมูลระบบสารสนเทศที่สำรองไว้อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ ด้านการกู้คืนระบบ

(๑) ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่าย จนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไข และรายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

(๒) ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Lastest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

(๓) หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งให้ผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

หมวด ๗
แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยง

ข้อ ๑ กระบวนการในการบริหารจัดการกับความเสี่ยงของระบบฐานข้อมูลสารสนเทศให้ปฏิบัติตามวงจรบริหารงานคุณภาพ PDCA (plan-do-check-act) ดังต่อไปนี้

(๑) การกำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan)

(๑.๑) กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย โดยพิจารณาจากลักษณะการดำเนินงานของกรมฯ สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยีที่กรมฯ ใช้งาน

(๑.๒) กำหนดนโยบายความมั่นคงปลอดภัยเพื่อให้ครอบคลุมตามขอบเขตที่กำหนดไว้

(๑.๓) กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศของกรมฯ

(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 ภายในขอบเขตเพื่อให้เป็นไปตามนโยบายความมั่นคงปลอดภัยของกรมฯ

(๒.๖) จัดทำขั้นตอนปฏิบัติ และ/หรือกำหนดมาตรการที่จำเป็นสำหรับการติดตามและบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Security incident management procedures and controls) รวมทั้งกำหนดให้ผู้ที่เกี่ยวข้องให้ปฏิบัติตามโดยเคร่งครัด

(๓) การเฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย (Check)

(๓.๑) ดำเนินการตามขั้นตอนปฏิบัติและมาตรการในการเฝ้าระวังและติดตาม (ที่กำหนดไว้ในนโยบายความมั่นคงปลอดภัย) เพื่อตรวจหาข้อผิดพลาดจากการประมวลผล ตรวจหาการละเมิดหรือความพยายามในการละเมิดความมั่นคงปลอดภัย ตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น ตรวจสอบว่าการดำเนินการจัดการกับเหตุการณ์การละเมิดความมั่นคงปลอดภัยที่ได้ดำเนินการไปแล้วได้ผลหรือไม่ เป็นต้น

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

(๓.๓) ดำเนินการทบทวนความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ โดยดูว่าแผนการวัดความสัมฤทธิ์ผลฯ เป็นไปตามเป้าหมายหรือตัวชี้วัดที่กำหนดไว้ในแผนหรือไม่

(๓.๔) ทบทวนผลการประเมินความเสี่ยงอย่างเป็นระยะๆ (เช่น ทุกๆ ๓-๖ เดือน เป็นต้น) ทบทวนระดับความเสี่ยงที่ยังเหลืออยู่ และระดับความเสี่ยงที่ยอมรับได้ ตามการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นกับกรมฯ เทคโนโลยีที่กรมฯ ใช้งาน วัตถุประสงค์และกระบวนการทางธุรกิจของกรมฯ ภัยคุกคามที่มีการระบุเพิ่มเติมหรือเปลี่ยนแปลง ความสัมฤทธิ์ผลของมาตรการต่างๆ ที่กรมฯ ใช้งาน เหตุการณ์ภายนอกต่างๆ เช่น การเปลี่ยนแปลงด้านกฎหมาย ระเบียบ ข้อบังคับหรือสิ่งที่อยู่ในสัญญาจ้าง และการเปลี่ยนแปลงด้านสังคม เป็นต้น

(๓.๕) ดำเนินการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบระยะเวลาที่ได้กำหนดไว้

(๓.๖) บันทึกข้อมูลการดำเนินการและเหตุการณ์ต่างๆ ซึ่งอาจมีผลกระทบต่อความสัมฤทธิ์ผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย ซึ่งประกอบด้วย การประชุมทบทวนด้านความมั่นคงปลอดภัยโดยผู้บริหาร ให้จัดทำรายงานการประชุมและแจ้งเวียนมติให้ผู้ที่เกี่ยวข้องได้รับทราบและปฏิบัติตาม การปฏิบัติตามนโยบายและขั้นตอนปฏิบัติต่างๆ ในในโยบายความมั่นคงปลอดภัยของกรมฯ ให้ผู้รับผิดชอบบันทึกหลักฐานการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเหล่านั้นไว้เพื่อให้สามารถตรวจสอบได้ในภายหลัง

(๔) การทบทวนและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย (Act)

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

(๔.๒) แจ้งการปรับปรุงและการดำเนินการให้แก่ทุกหน่วยที่เกี่ยวข้องทราบ โดยให้รายละเอียดที่เพียงพอและเหมาะสมตรวจสอบว่าการปรับปรุงที่ได้ดำเนินการไปแล้วนั้นบรรลุผลตามที่ต้องการหรือไม่

ข้อ ๒ การวางแผนระบบบริหารความเสี่ยงของระบบฐานข้อมูลสารสนเทศ ต้องดำเนินการดังต่อไปนี้

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

(๒) มีการจัดทำแผนแก้ไขปัญหาจากความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan)

(๓) มีระบบการรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล เช่น ระบบ Anti Virus ระบบไฟฟ้าสำรอง เป็นต้น

(๔) มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access Rights)

ข้อ ๓ ต้องมีการทบทวนระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศเป็นประจำทุกปี อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๔ ต้องมีการตรวจประเมินเชิงประจักษ์ด้านประสิทธิภาพของระบบสารสนเทศ โดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) ดังนี้

(๑) แสดงรายชื่อฐานข้อมูลที่ครอบคลุมที่ใช้สนับสนุนการปฏิบัติงาน

(๒) แสดงผลการกำหนดผู้รับผิดชอบในการตรวจสอบข้อมูลและการจัดเก็บข้อมูล รวมถึงการดำเนินการตามแผนการจัดเก็บและตรวจสอบข้อมูลแต่ละประเภทในระบบฐานข้อมูล ในระยะเวลาที่เหมาะสม

(๓) แสดงระบบการตรวจสอบสิทธิการเข้าถึง (Login) ที่สามารถ Verify User name และ Password

(๔) แสดงวิธีการ/ข้อกำหนดเกี่ยวกับรอบของการจัดเก็บข้อมูล

(๕) แสดงการอัพเดทข้อมูลที่จำเป็นอย่างสม่ำเสมอและทันท่วงที

(๖) แสดงระบบการสืบค้นข้อมูล (Search Engine) บนเว็บไซต์ของส่วนราชการ ที่สามารถค้นหาได้ถูกต้องสอดคล้องกับความต้องการและในระยะเวลาที่เหมาะสม

(๗) แสดงผลของการพัฒนาปรับปรุงเทคโนโลยีสารสนเทศจากข้อคิดเห็น/เสนอแนะ/ข้อร้องเรียนของผู้ใช้งาน

(๘) แสดงเอกสารแนวทาง/มาตรการป้องกันความเสียหาย และมีการสำรองข้อมูลสารสนเทศ (Backup)

(๙) แสดงระบบรักษาความมั่นคงและปลอดภัยของระบบฐานข้อมูลและสารสนเทศ เช่น ระบบการตรวจสอบการบุกรุก การติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของส่วนราชการ และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล ที่เป็นไปตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๑๐) แสดงการจัดทำแผนบริหารความเสี่ยงด้านคอมพิวเตอร์และสารสนเทศ

(๑๑) แสดงระบบ Access Right ที่ถูกต้องและทันสมัย เช่น มีการกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมถึงการเปลี่ยนแปลงหรือยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก พ้นจากตำแหน่งหรือยกเลิกการใช้งาน และมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ
