นโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมส่งเสริมคุณภาพสิ่งแวดล้อม
พ.ศ. ๒๕๕๙

สารบัญ

คำนิยาม

“กรมฯ” หมายถึง กรมส่งเสริมคุณภาพสิ่งแวดล้อม

“หน่วยงาน หรือ หน่วยงานภายใน” หมายถึง สำนัก ศูนย์ กอง หรือที่เรียกชื่อเป็นอย่างอื่นในสังกัดของกรมส่งเสริมคุณภาพสิ่งแวดล้อม

“ผู้บริหารสูงสุด (Chief Executive Office: CEO)” หมายถึง อธิบดีของกรมฯ เป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหาย และภารกิจด้านการบริหาร

“ผู้บังคับบัญชา” หรือ “ผู้มีอำนาจ” หรือ “ผู้บริหารระดับสูงของหน่วยงาน” หมายถึง ผู้บริหารระดับสูงในตำแหน่งอื่น ๆ ตามที่หน่วยงานเห็นว่าเหมาะสม และมีหน้าที่ต้องปฏิบัติตามนโยบาย และแนวปฏิบัติ

“ผู้ใช้งาน หรือ พนักงาน” หมายถึง ข้าราชการ เจ้าหน้าที่ ลูกจ้าง ผู้บริหารองค์กร หรือผู้ใช้บริการระบบเทคโนโลยีสารสนเทศของกรมฯ ซึ่งปฏิบัติงานให้กรมฯ หรือมีกิจที่ต้องปฏิบัติกับกรมฯ ในลักษณะใดลักษณะหนึ่ง

“ผู้ดูแลระบบ” หมายถึง พนักงานของกรมฯ หรือผู้ที่ได้รับมอบหมายให้ให้ทำหน้าที่ดูแลและบริหารจัดการระบบเทคโนโลยีสารสนเทศของกรมฯ

“ผู้ดูแลเครือข่าย” หมายถึง พนักงานของกรมฯ หรือผู้ที่ได้รับมอบหมายให้ทำหน้าที่ดูแลและบริหารจัดการเครือข่ายของกรมฯ

“ผู้พัฒนาระบบ” หมายถึง พนักงานของกรมฯ หรือผู้ที่ได้รับมอบหมายให้ทำหน้าที่เกี่ยวข้องกับการพัฒนาระบบงานของกรมฯ

“ผู้รับผิดชอบระบบสารสนเทศ” หมายถึง ผู้อำนวยการกลุ่มงานต่างๆ ของศูนย์สารสนเทศสิ่งแวดล้อม ผู้มีอำนาจที่รับผิดชอบการเข้าถึงข้อมูลในระบบงานของกรมฯ ผู้ดูแลระบบ ผู้ดูแลเครือข่าย หรือผู้พัฒนาระบบ

“ผู้ให้บริการภายนอก (External Service Provider)” หมายถึง หน่วยงานภายนอกที่รับจ้างปฏิบัติงานด้านเทคโนโลยีสารสนเทศตามความต้องการของกรมฯ เช่น ผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการด้านฮาร์ดแวร์ ผู้ให้บริการด้านซอฟต์แวร์ ผู้ให้บริการด้านระบบงาน โดยรวมผู้ให้บริการเหล่านี้มีหน้าที่ ที่จะต้องปฏิบัติตามสัญญาการให้บริการที่มีการจัดทำร่วมกันกับกรมฯ รวมทั้งปฏิบัติตามแนวนโยบายและแนวปฏิบัติต่างๆ ที่เกี่ยวข้องกับตนเอง

หน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรในข้างต้น ได้แก่ ผู้บริหารสูงสุด ผู้บังคับบัญชา ผู้ใช้งาน ผู้ดูแลระบบ ผู้ดูแลเครือข่าย ผู้พัฒนาระบบ ผู้รับผิดชอบระบบสารสนเทศ และ ผู้ให้บริการภายนอก คือการปฏิบัติตามแนวนโยบายและแนวปฏิบัติต่างๆ ที่เกี่ยวข้องกับตนเองอย่างเคร่งครัด

“ความมั่นคงปลอดภัยด้านสารสนเทศ หรือ ความมั่นคงปลอดภัยสารสนเทศ” หมายถึง การสร้างหรือการรักษาความมั่นคงปลอดภัยให้กับสินทรัพย์สารสนเทศของกรมฯ ทั้งนี้เพื่อป้องกันการสูญเสีย การสูญหาย การถูกขโมย การเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยโดยไม่ได้รับอนุญาต การ

ปลอมแปลง การปฏิเสธความรับผิดชอบ หรือ การกระทำใดๆ ก็ตามที่ก่อให้เกิดการความเสียหายต่อองค์ประกอบ ๓ ส่วน ดังนี้ การรักษาความลับ การรักษาความครบถ้วน การรักษาความพร้อมใช้

“การรักษาความลับ (Confidentiality)” หมายถึง การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

“การรักษาความครบถ้วน (Integrity)” หมายถึง การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งาน ประมวลผล โอน หรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

“การรักษาความพร้อมใช้ (Availability)” หมายถึง การจัดทำให้ทรัพย์สินสารสนเทศสามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

“ความมั่นคงปลอดภัย” หมายถึง ความมั่นคงปลอดภัยด้านสารสนเทศ

“สารสนเทศ” หมายถึง ข้อมูลในรูปแบบต่างๆ ที่สามารถนำมาใช้ประกอบการตัดสินใจ หรือใช้ประโยชน์เพื่อการดำเนินงานต่างๆ ตามภารกิจของกรมฯ

“คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ” (คณะกรรมการบริหารฯ) หมายถึง กลุ่มบุคลากรซึ่งเป็นผู้บริหารระดับกองหรือฝ่ายที่ได้รับมอบหมายจากกรมฯ ให้มีอำนาจในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของกรมฯ ซึ่งโดยรวมมีหน้าที่ดังนี้

- กำหนดให้มีการทบทวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ ๑ ครั้ง
- กำหนดให้มีการจัดทำ ทบทวน และปรับปรุงแนวนโยบายและแนวปฏิบัติต่างๆ ในเอกสารฉบับนี้อย่างน้อยปีละ ๑ ครั้ง
- กำกับดูแลให้ผู้ที่อยู่ในขอบเขตของเอกสารฉบับนี้ปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้กำหนดไว้อย่างเคร่งครัด
- กำหนดให้มีการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ ๑ ครั้ง
- กำหนดให้มีการประเมินและบริหารจัดการความเสี่ยงที่มีต่อสินทรัพย์สารสนเทศของกรมฯ
- ทบทวนรายงานสรุปเหตุการณ์ด้านความมั่นคงปลอดภัย และกำหนดให้มีการจัดการที่เหมาะสมตามสมควร
- กำหนดโครงสร้างและหน้าที่ความรับผิดชอบของคณะทำงานกู้คืนระบบ

- กำหนดให้มีการจัดทำและปรับปรุงแผนกู้คืนระบบ (แผนเตรียมความพร้อมกรณีฉุกเฉิน)
- ศึกษา และติดตาม ภัยคุกคามใหม่ๆ ที่อาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกรมฯ รวมทั้งกำหนดมาตรการรองรับที่จำเป็น

“ระบบงาน (Application systems)” หมายถึง ระบบสารสนเทศที่ทำงานอยู่บนเครื่องคอมพิวเตอร์เพื่อให้บริการต่างๆ ซึ่งรวมถึงให้บริการงานตามภารกิจของกรมฯ ด้วย เช่น ระบบงานบุคคลากร ระบบงานบัญชี เป็นต้น

“สินทรัพย์ (Information assets)” หมายถึง ทรัพย์สิน ๕ หมวด ซึ่งประกอบด้วย บุคลากร ฮาร์ดแวร์ (เช่น เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์ต่อพ่วง) ซอฟต์แวร์ (เช่น โปรแกรมคอมพิวเตอร์ โปรแกรมระบบงาน) ข้อมูล และระบบงาน

“เครือข่าย หรือ ระบบเครือข่าย (Computer networks or network systems)” หมายถึง โครงข่ายคอมพิวเตอร์ที่เชื่อมโยงคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่างๆ เข้าด้วยกัน ซึ่งทำให้การสื่อสารข้อมูลระหว่างคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทั้งที่อยู่ภายในและภายนอกองค์กรสามารถติดต่อสื่อสารและแลกเปลี่ยนข้อมูลกันได้ โครงข่ายนี้โดยพื้นฐานประกอบด้วยโครงข่ายสำหรับการติดต่อสื่อสารภายในองค์กร และโครงข่ายบนอินเทอร์เน็ตซึ่งทำให้คอมพิวเตอร์ภายในองค์กรหนึ่งสามารถติดต่อสื่อสารกับคอมพิวเตอร์ขององค์กรหนึ่งได้

“อุปกรณ์คอมพิวเตอร์” หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อกับหรือทำงานเป็นส่วนหนึ่งของคอมพิวเตอร์ ทำงานบนระบบเครือข่าย หรือทำงานเป็นคอมพิวเตอร์อย่างหนึ่ง ซึ่งอาจทำหน้าที่ในการสื่อสารข้อมูล ประมวลผลข้อมูล บันทึกข้อมูล หรือสนับสนุนการทำงานของคอมพิวเตอร์ในลักษณะต่างๆ เช่น อุปกรณ์เครือข่าย (เช่น สวิทซ์ เร้าเตอร์) เครื่องพิมพ์ เครื่องสแกนภาพ เครื่องสำรองไฟฟ้า (UPS)

“ระบบเทคโนโลยีสารสนเทศ (Information technology systems)” หมายถึง ระบบงาน โปรแกรมประยุกต์ ระบบปฏิบัติการ เครื่องคอมพิวเตอร์ เซิร์ฟเวอร์ให้บริการระบบงาน เครือข่าย อุปกรณ์เครือข่าย (เช่น สวิทซ์ เร้าเตอร์ ไฟร์วอลล์) และอุปกรณ์คอมพิวเตอร์อื่นๆ

เมื่อกล่าวถึงคำว่า “ระบบเทคโนโลยีสารสนเทศ” มีความมุ่งหมายให้เป็นคำเรียกโดยรวมของอุปกรณ์ทุกชนิดทุกประเภทที่สามารถประมวลผลหรือสนับสนุนการประมวลผลคอมพิวเตอร์

“ระบบ (Systems)” หมายถึง ระบบเทคโนโลยีสารสนเทศ

“อุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile computing devices)” หมายถึง อุปกรณ์คอมพิวเตอร์ขนาดเล็กที่สามารถพกพาหรือเคลื่อนย้ายไปกับตัวบุคคลไปยังสถานที่ต่างๆ ได้โดยง่าย และมีน้ำหนักเบา เช่น เครื่องคอมพิวเตอร์โน้ตบุ๊ก โทรศัพท์มือถือ Smart phone Tablet พีดีเอ เป็นต้น

“รหัสผ่าน” หมายถึง กลุ่มชุดตัวอักษร ตัวเลข หรือเครื่องหมายต่างๆ ที่กำหนดขึ้นมาโดยผู้ใช้งานสำหรับใช้ในการพิสูจน์ตัวตนในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งมีความหมายตรงกับคำในภาษาอังกฤษว่า Password

“บัญชีผู้ใช้งาน” หมายถึง บัญชีรายชื่อของผู้ที่ได้รับสิทธิและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมฯ

“สิทธิการเข้าถึง หรือ สิทธิของผู้ใช้งาน” หมายถึง การอนุญาตให้ผู้ใช้งานสามารถเข้าถึงข้อมูลในระบบเทคโนโลยีสารสนเทศของกรมฯ โดยผู้มีอำนาจ การอนุญาตให้เข้าถึงข้อมูลนี้โดยทั่วไปจะกำหนดจากบทบาทหรือหน้าที่ความรับผิดชอบของผู้ใช้งานหรือตามความจำเป็นในการเข้าถึงข้อมูลนั้น กล่าวคือหากมีบทบาทหรือหน้าที่ความรับผิดชอบ หรือความจำเป็นในการเข้าถึงข้อมูลนั้นก็จะอนุญาตให้เข้าถึงได้ หรือที่เรียกว่าได้รับ “สิทธิ” ในการเข้าถึงข้อมูลนั่นเอง การได้รับสิทธิของผู้ใช้งานยังหมายรวมถึงความสามารถของผู้ใช้งานในการที่จะเปลี่ยนแปลง แก้ไข เพิ่มเติม หรือลบข้อมูลตามที่ตนเองได้รับสิทธินั้น

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาตให้ผู้ใช้งานเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศของกรมฯ โดยได้รับสิทธิการเข้าถึงตามบทบาทหรือหน้าที่ความรับผิดชอบของผู้ใช้งาน หรือตามความจำเป็นในการเข้าถึง

“ตารางควบคุมการเข้าถึงระบบ” หมายถึง ตารางแสดงการเข้าถึงระบบงานต่างๆ ของกรมฯ ซึ่งประกอบด้วยชื่อระบบงาน ประเภทของข้อมูลในระบบงานนั้น และหน่วยงานภายในที่มีสิทธิการเข้าถึงระบบงานและข้อมูลเหล่านั้นได้

“ศูนย์ปฏิบัติการคอมพิวเตอร์” หมายถึง ห้องที่ประกอบไปด้วยระบบเทคโนโลยีสารสนเทศต่างๆ ของกรมฯ มีระบบงานสำคัญต่างๆ ตั้งอยู่ที่นี่ และมีระบบควบคุมด้านสภาพแวดล้อมเพื่อหล่อเลี้ยงการทำงานของระบบดังกล่าวของกรมฯ ด้วย เช่น ระบบไฟฟ้า ระบบดับเพลิง เครื่องปรับอากาศ เครื่องสำรองไฟฟ้า ระบบระบายอากาศ ระบบการรักษาความปลอดภัยทางกายภาพ เป็นต้น

“ไวรัสคอมพิวเตอร์ (ไวรัส) หรือ โปรแกรมไม่ประสงค์ดี” หมายถึง โปรแกรมที่ได้รับการติดตั้งในเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือโดยไม่รู้ตัว อาจก่อให้เกิดความเสียหายต่อข้อมูลต่างๆ ในเครื่องนั้น อาจทำให้เครื่องคอมพิวเตอร์เสียหาย อาจสร้างความรำคาญ อาจทำให้เครื่องคอมพิวเตอร์ทำงานช้าหรือทำงานผิดปกติ หรือทำงานในลักษณะที่ไม่เป็นประโยชน์ ไม่สร้างสรรค์หรือไม่เป็นผลดีต่อเครื่องคอมพิวเตอร์นั้น โปรแกรมที่ทำงานในลักษณะดังกล่าวอย่างน้อยหมายรวมถึง

- โปรแกรมที่สามารถสำเนาตัวเองและแพร่กระจายผ่านทางสื่อบันทึกข้อมูลเพื่อข้ามไปยังเครื่องคอมพิวเตอร์อื่น กล่าวคือ เมื่อมีการใช้สื่อบันทึกข้อมูลดังกล่าวกับเครื่องคอมพิวเตอร์หนึ่ง โปรแกรมดังกล่าวก็จะแพร่กระจายหรือติดไปยังเครื่องคอมพิวเตอร์นั้น
- โปรแกรมที่สามารถสำเนาตัวเองข้ามหรือแพร่กระจายไปยังเครื่องคอมพิวเตอร์ปลายทางหนึ่งเครื่องหรือมากกว่าหนึ่งเครื่องก็ได้ เครื่องปลายทางที่ได้รับการแพร่ระบาดนั้นก็สามารถสำเนาและแพร่กระจายตัวเองได้ต่อไป โปรแกรมที่แพร่กระจายในลักษณะดังกล่าวมีชื่อเรียกกันว่าหนอนเครือข่าย (Worm)
- โปรแกรมที่เคลื่อนที่จากเครื่องคอมพิวเตอร์อื่นมายังเครื่องคอมพิวเตอร์ของผู้ใช้งานหรือที่เรียกกันว่า Mobile Code เช่น โปรแกรมที่เขียนด้วย Java Script, Active X

เป็นต้น และถูกสั่งให้ทำงานในเครื่องของผู้ใช้งานนั้น โปรแกรมประเภทนี้อาจฝังตัวอยู่กับโปรแกรมอื่นแต่ถูกเรียกทำงานร่วมกัน เช่น กรณีของการเข้าถึงโปรแกรมบนเว็บไซต์หนึ่งซึ่งมีการเรียกใช้ Java Script ด้วย ก็จะทำให้ Java Script นั้นถูกโอนย้ายเข้ามาและสั่งทำงานบนเครื่องของผู้ใช้งาน

“ข้อมูลล็อก (Log)” หมายถึง ข้อมูลเหตุการณ์ต่างๆ ที่เกิดขึ้นบนระบบๆ หนึ่งและได้ถูกบันทึกไว้ในระบบนั้น เช่น ความผิดพลาดในการทำงานของระบบ ทรัพยากรระบบไม่พอ ความพยายามในการบุกรุกระบบ ข้อมูลเหตุการณ์ซึ่ง พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ได้กำหนดให้มีการบันทึกและจัดเก็บไว้ เป็นต้น ข้อมูลเหล่านี้สามารถใช้เพื่อตรวจ ติดตามการทำงานของระบบ เตือนว่ามีเหตุการณ์หนึ่งเกิดขึ้นแล้วในระบบ ดำเนินการเชิงป้องกันหรือแก้ไขตามความจำเป็น ซึ่งรวมถึงการใช้เป็นหลักฐานในการดำเนินการทางกฎหมาย เช่น กรณีการบุกรุกระบบ กรณีการส่งอีเมล์ซึ่งพาดพิงถึงผู้อื่นและทำให้ผู้นั้นเกิดความเสียหาย เป็นต้น

“ช่องโหว่ (Software/hardware vulnerabilities)” หมายถึง จุดอ่อนที่พบในซอฟต์แวร์หรือฮาร์ดแวร์ที่กรมฯ ใช้งาน โดยที่ซอฟต์แวร์หรือฮาร์ดแวร์นั้นอาจถูกพัฒนาหรือจัดทำขึ้นมาโดยผู้ผลิตซอฟต์แวร์หรือฮาร์ดแวร์หนึ่ง โดยทั่วไปผู้ใช้งานซอฟต์แวร์หรือฮาร์ดแวร์นั้นจะเป็นผู้ค้นพบจุดอ่อน เช่น ในระหว่างที่ใช้งานซอฟต์แวร์หรือฮาร์ดแวร์ และรายงานให้ผู้ผลิตได้รับทราบเพื่อขอให้ช่วยดำเนินการแก้ไข จุดอ่อนดังกล่าวในหลายๆ กรณีทำให้ซอฟต์แวร์หรือฮาร์ดแวร์นั้นทำงานผิดพลาดในลักษณะต่างๆ ซึ่งรวมถึงความผิดพลาดในด้านข้อมูลด้วย ในบางกรณีที่ร้ายแรง ผู้ไม่ประสงค์ดีสามารถใช้ประโยชน์จากจุดอ่อนดังกล่าวเพื่อทำการบุกรุกระบบได้ด้วย ซึ่งหมายถึงสามารถเข้าสู่ระบบได้โดยไม่ได้รับอนุญาต

“โปรแกรมแก้ไขช่องโหว่ (Patch for software/hardware vulnerabilities)” หมายถึง โปรแกรมสำหรับแก้ไขที่ผู้ผลิตซอฟต์แวร์หรือฮาร์ดแวร์จัดทำขึ้นมาเพื่อแก้ไขปัญหาช่องโหว่ที่ผู้ใช้งานซอฟต์แวร์หรือฮาร์ดแวร์ค้นพบและรายงานเข้ามาให้ผู้ผลิตได้รับทราบ

“พอร์ต (Ports)” หมายถึง ช่องสัญญาณบนอุปกรณ์เครือข่าย เช่น บนสวิทช์ เร้าเตอร์ โดยทั่วไปช่องสัญญาณนี้สามารถใช้ในการติดต่อสื่อสารข้อมูลกับเครือข่าย คอมพิวเตอร์ และอุปกรณ์เครือข่ายต่างๆ โดยทั่วไปอุปกรณ์เครือข่ายจะมีช่องสัญญาณดังกล่าวจำนวนหนึ่ง

นอกจากนั้นพอร์ตยังหมายถึงบริการต่างๆ บนเครื่องเซิร์ฟเวอร์ให้บริการ โดยทั่วไปบริการเหล่านี้จะได้รับการกำหนดหมายเลขเป็นหมายเลขมาตรฐาน เช่น พอร์ต ๘๐ หมายถึงบริการเว็บซึ่งบริการข้อมูลต่างๆ บนเว็บหนึ่ง พอร์ต ๒๕ หมายถึงบริการรับส่งอีเมล์บนอินเทอร์เน็ต พอร์ต ๕๓ หมายถึงบริการค้นหาไอพีแอดเดรสของเครื่องหรืออุปกรณ์คอมพิวเตอร์ต่างๆ

ในลักษณะของพอร์ตที่เป็นช่องสัญญาณหรือให้บริการต่างๆ ก็ตาม เมื่อไม่มีความจำเป็นต้องใช้ช่องสัญญาณหรือบริการนั้นโดยผ่านทางพอร์ตดังกล่าว และโดยหลักการด้านความมั่นคงปลอดภัยผู้รับผิดชอบควรจะปิดช่องสัญญาณหรือบริการนั้นทิ้งไป ซึ่งเรียกโดยรวมว่าเป็นการปิดพอร์ตที่ไม่ได้ใช้งาน

“ทรัพย์สินทางปัญญา (Intellectual Properties)” หมายถึง ผลงานใดๆ อันเกิดจากความคิดสร้างสรรค์ของมนุษย์ ทรัพย์สินทางปัญญาเป็นทรัพย์สินอีกชนิดหนึ่งที่นอกเหนือจากสังหาริมทรัพย์ (คือทรัพย์สินที่สามารถเคลื่อนย้ายได้ เช่น นาฬิกา รถยนต์ โต๊ะ เป็นต้น) และ

อสังหาริมทรัพย์ (คือทรัพย์สินที่ไม่สามารถเคลื่อนย้ายได้ เช่น บ้าน ที่ดิน เป็นต้น) ประเภทของทรัพย์สินทางปัญญาประกอบด้วย

- ลิขสิทธิ์ (Copyright)
- สิทธิบัตร (Patent)
- เครื่องหมายการค้า (Trademark)
- แบบผังภูมิของวงจรรวม (Layout - Designs of Integrated Circuit)
- ความลับทางการค้า (Trade Secrets)
- สิ่งบ่งชี้ทางภูมิศาสตร์ (Geographical Indication)

“ซอร์สโค้ด (Source code)” หมายถึง ไฟล์ซึ่งประกอบด้วยชุดคำสั่งที่สามารถสั่งการให้เครื่องคอมพิวเตอร์ทำงานตามที่ต้องการได้ โดยทั่วไปชุดคำสั่งเหล่านี้จะอยู่ในรูปแบบหรือภาษาที่สามารถอ่านและทำความเข้าใจได้โดยมนุษย์ ไฟล์ชุดคำสั่งนี้จะถูกแปลงโดยโปรแกรมแปรภาษา เช่น Compiler, Interpreter หรือ Assembler ไปเป็นโค้ดที่เครื่องคอมพิวเตอร์สามารถตีความและสั่งการให้เครื่องทำงานตามที่ตีความนั้น โดยปกติมนุษย์จะไม่สามารถอ่านและทำความเข้าใจโค้ดประเภทนี้ได้

“VPN (Virtual Private Network)” หมายถึง การเข้ารหัสข้อมูล เช่น โดยผ่านทางซอฟต์แวร์หรือฮาร์ดแวร์หนึ่ง เพื่อให้การเชื่อมต่อโดยผ่านทางเครือข่ายที่ไม่ปลอดภัย เช่น อินเทอร์เน็ต เครือข่ายไร้สาย มีความมั่นคงปลอดภัย เนื่องจากข้อมูลจะได้รับการเข้ารหัสก่อนที่จะมีการส่งผ่านไปบนอินเทอร์เน็ตหรือเครือข่ายไร้สายนั้น เมื่อกล่าวถึง VPN จะหมายรวมถึงระบบอุปกรณ์คอมพิวเตอร์ ซอฟต์แวร์ หรือฮาร์ดแวร์ ที่ใช้การเข้ารหัสข้อมูลก่อนส่งข้อมูลออกไป

“ลายมือชื่อดิจิทัล (Digital signature)” หมายถึง รูปแบบหรือสิ่งซึ่งเป็นเครื่องหมายสัญลักษณ์เฉพาะซึ่งเป็นผลจากการใช้วิธีการทางคณิตศาสตร์เพื่อให้สามารถพิสูจน์หรือแสดงได้ว่าใครเป็นเจ้าของข้อความหรือเอกสารหนึ่งที่ได้รับมา เช่น ที่ได้รับมาทางอีเมล์ ทางอินเทอร์เน็ต เป็นต้น รูปแบบหรือสิ่งซึ่งเป็นเครื่องหมายสัญลักษณ์ที่ปรากฏจะทำให้ผู้รับข้อความหรือเอกสารเชื่อถือได้ว่าผู้ส่งคือใครและข้อความหรือเอกสารนั้นไม่ถูกเปลี่ยนแปลงแก้ไขในระหว่างทางที่ส่งมา

ลายมือชื่อดิจิทัลมักจะมีการใช้งานกับการส่งมอบซอฟต์แวร์ การทำธุรกรรมอิเล็กทรอนิกส์ หรือกรณีที่จำเป็นต้องป้องกันการปลอมแปลงหรือการเปลี่ยนแปลงแก้ไขข้อความหรือเอกสารที่ส่งมาโดยไม่ได้รับอนุญาต

“กุญแจ (Public/Private key)” หมายถึง กุญแจส่วนตัวและกุญแจสาธารณะ กุญแจส่วนตัวใช้ในการลงลายมือชื่อดิจิทัล ในขณะที่กุญแจสาธารณะจะใช้ในการเข้ารหัสข้อมูลเพื่อซ่อนไม่ให้ผู้อื่นสามารถอ่านข้อความหรือข้อมูลเหล่านั้นได้

กุญแจส่วนตัวและกุญแจสาธารณะจะถูกสร้างขึ้นมาคู่กันและมอบให้กับผู้ใช้งานหนึ่ง โดยรวมคู่กุญแจดังกล่าวของผู้ใช้งานแต่ละคนที่ถูกสร้างขึ้นมาจะแตกต่างกัน (ไม่เหมือนกัน)

กุญแจส่วนตัวของผู้ใช้งานหนึ่ง เมื่อนำไปใช้ในการลงลายมือชื่อดิจิทัลกับข้อความหนึ่ง เมื่อผู้รับได้รับข้อความนั้น จะทราบได้โดยทันทีว่าผู้ที่ส่งมาหรือผู้ที่เป็นเจ้าของข้อความก็คือผู้ที่ลงลายมือชื่อดิจิทัลนั้นเท่านั้น จะไม่มีทางเป็นผู้อื่นได้ ซึ่งเปรียบเสมือนเป็นลายเซ็นของผู้ที่ส่งข้อความมาให้

สำหรับกุญแจสาธารณะซึ่งใช้ในการเข้ารหัสเมื่อได้มีการเข้ารหัสข้อความหนึ่งแล้วและส่งข้อมูลมาให้ เฉพาะผู้ที่ถือกุญแจส่วนตัวที่เป็นคู่ของกุญแจสาธารณะนั้นเท่านั้นจึงจะสามารถถอดรหัสข้อความที่ส่งมานั้นได้

“เหตุการณ์ความเสี่ยง หรือ ความเสี่ยง” หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อสินทรัพย์สารสนเทศของกรมฯ เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาต หน้าเว็บไซต์ถูกเปลี่ยนแปลงแก้ไขซึ่งอาจทำให้กรมฯ เสียชื่อเสียง

“ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite หรือ Acceptable level of risk)” หมายถึง ค่าความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่ง มีค่าน้อยกว่าหรือเท่ากับค่าที่ยอมรับได้นี้ จะถือว่าสินทรัพย์สารสนเทศที่เกี่ยวข้องกับเหตุการณ์ฯ มีความมั่นคงปลอดภัยเพียงพอ (และผู้ประเมินความเสี่ยงไม่จำเป็นต้องนำเสนอแผนการลดความเสี่ยงใดๆ เพิ่มเติม)

“แผนการลดความเสี่ยง (Treatment plan)” หมายถึง แผนการจัดการกับเหตุการณ์ความเสี่ยงสำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานหรือผู้บังคับบัญชาเพื่อพิจารณาอนุมัติการดำเนินการ

“เหตุการณ์ด้านความมั่นคงปลอดภัย (information security events)” หมายถึง เหตุการณ์สองกรณีดังนี้

กรณีที่ ๑ คือ เหตุการณ์ที่เกิดขึ้นแล้วกับระบบคอมพิวเตอร์และเครือข่ายของกรมฯ

กรณีที่ ๒ คือ เหตุการณ์ที่เป็นจุดอ่อนหรือสงสัยว่าจะเป็นจุดอ่อนกับระบบคอมพิวเตอร์และเครือข่ายของกรมฯ

โดยเหตุการ์ด้านความมั่นคงปลอดภัยทั้งสองกรณีสามารถสร้างความเสียหายให้กับกรมฯ ได้ในลักษณะใดลักษณะหนึ่ง หรือหลายๆ ลักษณะ ซึ่งเหตุการณ์ที่เกิดขึ้นในทั้งสองกรณี เป็นเหตุการณ์ที่ไม่พึงประสงค์หรือไม่คาดคิดมาก่อน และอาจส่งผลให้

- เกิดการหยุดชะงักต่อกระบวนการทางธุรกิจสำคัญ (เช่น บริการสำคัญเกิดการหยุดชะงัก เป็นต้น)
- เกิดความเสียหายหรือส่งผลกระทบต่อทรัพย์สินขององค์กร เช่น บุคลากร ระบบเทคโนโลยีสารสนเทศ อาคาร สถานที่ ระบบไฟฟ้า ระบบสาธารณูปโภค หรือทรัพย์สินอื่นๆ
- เป็นการละเมิดแนวนโยบายความมั่นคงปลอดภัยของกรมฯ
- เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่างๆ ที่กรมฯ ต้องปฏิบัติตาม

- เกิดภาพลักษณ์ที่ไม่ดีต่อกรมฯ หรือทำให้สูญเสียชื่อเสียง (เช่น การไปโพสต์ข้อความพาดพิงถึงกรมฯ ในเว็บไซต์ภายนอกซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงของกรมฯ)

ตัวอย่างของเหตุการณ์ที่เกิดขึ้นแล้ว ได้แก่

- การพบการแพร่ระบาดของโปรแกรมไม่ประสงค์ดีในเครือข่ายของกรมฯ
- การพบจุดอ่อนในซอฟต์แวร์ ระบบงาน หรือฮาร์ดแวร์ที่ใช้งาน
- การแจ้งเตือนของระบบป้องกันการบุกรุก
- ระบบถูกบุกรุก
- ระบบถูกโจมตีจนไม่สามารถให้บริการได้
- ข้อมูลสำคัญในระบบงานถูกเปลี่ยนแปลงหรือแก้ไข
- หน้าเว็บไซต์ของกรมฯ ถูกเปลี่ยนแปลง
- การเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต
- การใช้ทรัพยากรขององค์กรผิดวัตถุประสงค์ (เช่น การใช้เครือข่ายขององค์กรเพื่อกระทำการที่ขัดต่อ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐)
- ระบบ อุปกรณ์ ฮาร์ดแวร์ หรือสินทรัพย์สารสนเทศอื่นๆ ถูกขโมย
- การแอบติดตั้งซอฟต์แวร์เพื่อดักขโมยข้อมูลหรือดักดูข้อมูลในเครือข่ายของกรมฯ
- การหยุดชะงักของระบบ หรือเหตุการณ์อื่นๆ ที่เป็นการละเมิดนโยบายความมั่นคงปลอดภัยของกรมฯ

ตัวอย่างของเหตุการณ์ที่เป็นจุดอ่อน ได้แก่

- ผู้ใช้งานมีการตั้งรหัสผ่านที่น้อยกว่า ๘ ตัวอักษร
- ประตูของศูนย์ปฏิบัติการคอมพิวเตอร์ไม่สามารถล็อกได้
- ระบบงานมีช่องทางอื่นในการเข้าสู่ระบบได้โดยไม่ผ่านการพิสูจน์ตัวตนตามปกติ
- เครื่องคอมพิวเตอร์ถูกวางไว้ในสถานที่ที่อาจถูกขโมยได้
- เครื่องคอมพิวเตอร์ไม่ได้ติดตั้งโปรแกรมป้องกันไวรัส
- ผู้ใช้งานยังมีการใช้โปรแกรมที่ไม่มีลิขสิทธิ์การใช้งานถูกต้อง
- บุคคลภายนอกที่ไม่ได้มีการแลกบัตร
- บุคคลภายนอกไม่ได้ลงชื่อก่อนเข้าศูนย์คอมพิวเตอร์
- ระบบงานไม่ได้มีการลบทิ้งบัญชีของผู้ให้บริการภายนอกที่เป็นผู้พัฒนาระบบงานนั้น

ทั้งเหตุการณ์ที่เกิดขึ้นแล้วหรือเหตุการณ์ที่เป็นจุดอ่อน จำเป็นต้องได้รับรายงานจากผู้ใช้งานที่พบเหตุ เพื่อให้มีการจัดการกับเหตุการณ์เหล่านั้นอย่างเหมาะสม ได้ผล และทันกาล

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง เหตุการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด อันเนื่องมาจากการถูกบุกรุกหรือโจมตีจากภัยคุกคามประเภทต่างๆ ซึ่งอาจส่งผลให้กระบวนการทางธุรกิจสำคัญเกิดการหยุดชะงัก เกิดความเสียหายหรือส่งผลกระทบต่อทรัพย์สินขององค์กร

“สื่อลามกอนาจาร” หมายถึง สื่อประเภทอันเป็นที่น่ารังเกียจ น่าอับอาย นอกรีต นอกแบบ ผิดปกติไปจากศีลธรรมอันดีของประชาชน

“ลิขสิทธิ์” หมายถึง สิทธิที่ได้รับแต่เพียงผู้เดียวตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๗ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น

“อินเทอร์เน็ต” หมายถึง เครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายคอมพิวเตอร์ทั่วโลกเข้าด้วยกัน โดยอาศัยเครือข่ายโทรคมนาคมเป็นตัวเชื่อมโยง

“อีเมล์” หมายถึง ข้อความอิเล็กทรอนิกส์ที่มีการส่งผ่านระบบเทคโนโลยีสารสนเทศและอินเทอร์เน็ตจากผู้ส่งไปยังผู้รับ ซึ่งมีความหมายตรงกับคำในภาษาอังกฤษว่า Electronic Mail หรือ E-mail (คล้ายกับการส่งจดหมายทางไปรษณีย์) โดยทั่วไปผู้ส่งสามารถส่งจดหมายดังกล่าวผ่านอินเทอร์เน็ตไปยังผู้รับได้โดยที่ผู้รับอาจจะอยู่ห่างไกลออกไปจากผู้ส่งทางกายภาพมากน้อยเพียงใดก็ตาม

“อีเมล์ขยะ (Spam E-mail)” หมายถึง อีเมล์ที่ไม่เป็นประโยชน์หรือไม่เป็นที่ต้องการของผู้รับ

“อีเมล์ลูกโซ่ (Chain E-mail/Letter)” หมายถึง อีเมล์ที่มีข้อความในลักษณะที่ต้องการให้ผู้รับส่งต่อข้อความนั้นไปเรื่อยๆ แบบไม่รู้จบเพื่อให้ข้อความดังกล่าวแพร่กระจายออกไปในวงกว้างโดยที่ข้อความอาจจะเป็นจริงหรือไม่ก็ตาม

“โปรแกรมมาตรฐาน” หมายถึง โปรแกรมที่กรมส่งเสริมคุณภาพสิ่งแวดล้อมกำหนดให้ติดตั้งและใช้งานภายในเครื่องคอมพิวเตอร์ทั้งหมดของกรมฯ เช่น Microsoft Office Microsoft Windows เป็นต้น

“ข้อมูลลับ” หมายถึง ข้อมูลที่กำหนดให้เปิดเผยได้เฉพาะกับผู้ที่ได้รับสิทธิการเข้าถึงเท่านั้น

“เอกสารลับ” หมายถึง ข้อมูลลับที่อยู่ในรูปของเอกสาร

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

“ทะเบียนข้อมูลลับ” หมายถึง เอกสารแสดงรายการของข้อมูลลับของหน่วยงานภายในว่าประกอบไปด้วยข้อมูลลับอะไรบ้าง ใครเป็นเจ้าของข้อมูล หน่วยงานใดบ้างที่อนุญาตให้เข้าถึง สถานที่ใดที่ใช้ในการจัดเก็บข้อมูล เป็นต้น โดยทั่วไปทะเบียนนี้ถูกใช้เพื่อควบคุมการเข้าถึงและการนำข้อมูลลับไปใช้งาน

“เจ้าของข้อมูล” หมายถึง พนักงานในหน่วยงานภายในของกรมฯ ซึ่งเป็นผู้สร้าง เปลี่ยนแปลง หรือแก้ไขข้อมูล ที่เกี่ยวกับภารกิจของหน่วยงานนั้น รวมทั้งให้สิทธิในการเข้าถึงข้อมูลนั้นแก่ผู้อื่น

“สื่อบันทึกข้อมูล” หมายถึง กระดาษ เทป Hard disk Flash Drive และแผ่น CD/DVD หรือสื่อชนิดอื่นๆ ที่ใช้ในการบันทึกข้อมูล

“ผู้ใช้งานข้อมูล” หมายถึง

- พนักงานของกรมฯ ซึ่งเป็นผู้ใช้ข้อมูลเพื่อปฏิบัติงานตามภารกิจหรือหน้าที่ความรับผิดชอบของตนเองหรือของกรมฯ เจ้าของข้อมูลถือเป็นผู้ใช้งานข้อมูลด้วย ผู้ที่ได้รับสำเนาข้อมูลทั้งที่เป็นกระดาษและอิเล็กทรอนิกส์ก็ถือว่าเป็นผู้ใช้งานข้อมูลด้วย ผู้ที่เกี่ยวข้องกับการจัดทำข้อมูล เปลี่ยนแปลงแก้ไขข้อมูล หรือดำเนินการอื่นๆ กับข้อมูล (เช่น ลบ ทำลาย หรือแจกจ่ายข้อมูล) ก็ถือว่าเป็นผู้ใช้งานข้อมูลด้วยเช่นกัน
- หน่วยงานภายนอกอื่นๆ ซึ่งกรมฯ อนุญาตให้เข้าถึงข้อมูลนั้นได้ หรือกรมฯ จำเป็นต้องส่งข้อมูลนั้นให้กับหน่วยงานภายนอกนั้น
- ลูกค้า ประชาชน ผู้ใช้บริการ หรือผู้ให้บริการภายนอก ซึ่งกรมฯ อนุญาตให้เข้าถึงข้อมูลนั้นได้

หมวด ๑
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางกายภาพ

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศ จัดการและควบคุมการเข้า-ออกพื้นที่ควบคุม เช่น ศูนย์ปฏิบัติการคอมพิวเตอร์ของกรมฯ ดังนี้

(๑) กำหนดระดับความสำคัญของพื้นที่ควบคุม สำหรับระบบเทคโนโลยีสารสนเทศของกรมฯ และแยกพื้นที่ควบคุมออกจากพื้นที่สำหรับการใช้งานทั่วไป

(๒) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่ควบคุม เว้นแต่จะได้รับการอนุญาตก่อน

(๓) ทดสอบระบบ ประตู หรือสิ่งปิดกั้น เพื่อดูว่ายังสามารถใช้งานได้ตามปกติหรือไม่

(๔) กำหนดให้มีกลไกการอนุญาตการเข้าถึงพื้นที่ควบคุมของบุคคลภายนอก และต้องมีการชี้แจงเหตุผลความจำเป็นในการเข้าถึงพื้นที่ดังกล่าว

(๕) กำหนดให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่ควบคุม ของบุคคลภายในและภายนอก

(๖) จัดเก็บบันทึกแสดงวันและเวลาการเข้า-ออกพื้นที่สำคัญ เพื่อใช้ในการตรวจสอบในภายหลัง

(๗) จัดทำระบบสำหรับการพิสูจน์ตัวตนในการเข้าถึงพื้นที่ควบคุม เช่น ใช้บัตรแถบแม่เหล็ก ใช้รหัสผ่าน ใช้ fingerprint เป็นต้น

(๘) ดูแลและเฝ้าระวังบุคคลภายนอก ซึ่งอยู่ในพื้นที่ควบคุมจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของสินทรัพย์หรือป้องกันการเข้าถึงระบบหรืออุปกรณ์ทางกายภาพโดยไม่ได้รับอนุญาต

(๙) อธิบายหรือสร้างความตระหนักให้บุคคลภายนอกเข้าใจกฎเกณฑ์ หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติตามในระหว่างที่อยู่ในพื้นที่ควบคุม

(๑๐) กำหนดให้บุคคลภายนอกต้องติดบัตรให้เห็นอย่างเด่นชัดตลอดระยะเวลาที่อยู่ในพื้นที่ควบคุม

(๑๑) กำหนดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่ควบคุมอย่างสม่ำเสมอ

ข้อ ๒ ผู้รับผิดชอบระบบสารสนเทศ จัดวางและป้องกันระบบเทคโนโลยีสารสนเทศฮาร์ดแวร์ และอุปกรณ์คอมพิวเตอร์ ดังนี้

(๑) จัดวางหรือจัดเก็บระบบเทคโนโลยีสารสนเทศ ฮาร์ดแวร์ และอุปกรณ์คอมพิวเตอร์ในบริเวณที่มีความปลอดภัย เพื่อป้องกันการขโมย การเข้าถึงทางกายภาพ หรือการสูญหาย

(๒) แยกการจัดเก็บระบบเทคโนโลยีสารสนเทศ ฮาร์ดแวร์ และอุปกรณ์คอมพิวเตอร์สำคัญไว้ในพื้นที่แยกต่างหากที่มีความปลอดภัยสูง

ข้อ ๓ ผู้รับผิดชอบระบบสารสนเทศ จัดทำและดูแลระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศ ดังนี้

(๑) จัดทำระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศอย่างน้อยดังต่อไปนี้

(ก) เครื่องสำรองไฟฟ้า

(ข) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

(ค) ระบบระบายอากาศ

(ง) ระบบปรับอากาศ และควบคุมความชื้น

(๒) กำหนดให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนสำหรับกรณีที่ระบบสนับสนุนการทำงานภายในศูนย์ปฏิบัติการคอมพิวเตอร์ทำงานผิดปกติ หรือหยุดการทำงาน

ข้อ ๔ ผู้รับผิดชอบระบบสารสนเทศ จัดการและควบคุมการเดินสายสัญญาณต่างๆ ดังนี้

(๑) เดินสายสัญญาณ (เช่น สายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ) ผ่านหรือเข้าไปในบริเวณที่ปลอดภัยจากการถูกเข้าถึงทางกายภาพโดยบุคคลภายนอก

(๒) เดินสายสัญญาณให้เป็นระเบียบเรียบร้อย ไม่เกะกะขวางทางเดิน หรืออาจทำให้สะดุดล้มได้โดยง่าย

(๓) ร้อยสายสัญญาณเข้าไปในท่อเพื่อป้องกันการดักจับสัญญาณในสาย การตัดสาย การทำให้เกิดความเสียหายต่างๆ ซึ่งรวมถึงการกัดแทะโดยหนู

(๔) เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงหรือรบกวนของสัญญาณซึ่งกันและกัน

(๕) ทำป้ายชื่อสำหรับสายสัญญาณต่างๆ ให้ชัดเจนเพื่อป้องกันการตัดต่อสายสัญญาณผิดเส้น และปรับปรุงป้ายชื่อให้ทันสมัยอยู่เสมอ

(๖) จัดทำแผนผังการเดินสายสัญญาณต่างๆ ให้ครบถ้วนและถูกต้อง

(๗) ปิดล็อกตู้ Rack ที่มีสายสัญญาณต่างๆ ให้สนิทเพื่อป้องกันการเข้าถึงโดยผู้อื่น

ข้อ ๕ ผู้รับผิดชอบระบบสารสนเทศ ดำเนินการบำรุงรักษาระบบและอุปกรณ์คอมพิวเตอร์ ดังนี้

(๑) จัดทำสัญญาการบำรุงรักษาสำหรับระบบและอุปกรณ์คอมพิวเตอร์ที่มีความสำคัญ

(๒) กำหนดเงื่อนไขของการให้บริการในสัญญาบำรุงรักษาให้ชัดเจนเพื่อให้ผู้รับจ้างต้องติดต่อกลับและเข้ามาดำเนินการแก้ไขปัญหาให้แล้วเสร็จภายในระยะเวลาที่เหมาะสม

(๓) ตรวจสอบและกำหนดให้มีการรับประกันความเสียหายของระบบและอุปกรณ์คอมพิวเตอร์ใหม่

(๔) บำรุงรักษาระบบและอุปกรณ์คอมพิวเตอร์ตามรอบระยะเวลาที่กำหนดไว้ในสัญญาการบำรุงรักษา

(๕) จัดให้มีการติดต่อเพื่อแจ้งปัญหาให้ผู้ให้บริการภายนอกได้รับทราบและเข้ามาดำเนินการแก้ไขภายในระยะเวลาตามที่ระบุไว้ในสัญญาการบำรุงรักษาหรือการรับประกัน ในกรณีระบบและอุปกรณ์ตามสัญญาการบำรุงรักษาเกิดความเสียหาย

(๖) บันทึกปัญหาที่พบของระบบและอุปกรณ์คอมพิวเตอร์ เพื่อใช้ในการประเมินและเสนอปรับปรุงระบบและอุปกรณ์ดังกล่าว

(๗) บันทึกกิจกรรมการบำรุงรักษาระบบและอุปกรณ์คอมพิวเตอร์ทุกครั้งตามที่กำหนดไว้ในสัญญาการบำรุงรักษาหรือการรับประกัน

(๘) ระมัดระวังการใช้ระบบและอุปกรณ์คอมพิวเตอร์เพื่อไม่ให้เกิดความเสียหายโดยง่าย

(๙) ปฏิบัติตามคำแนะนำในการบำรุงรักษาระบบและอุปกรณ์คอมพิวเตอร์ตามที่ผู้ผลิตกำหนด

(๑๐) ควบคุมและสอดส่องดูแลผู้ให้บริการภายนอกเพื่อให้มีการปฏิบัติงานบำรุงรักษาหรือแก้ไขปัญหาตามที่แจ้ง

ข้อ ๖ ผู้รับผิดชอบระบบสารสนเทศ ควบคุมและป้องกันการนำระบบหรืออุปกรณ์คอมพิวเตอร์ต่างๆ ออกนอกสำนักงาน ดังนี้

(๑) กำหนดให้มีการขออนุญาตก่อนนำระบบ หรืออุปกรณ์คอมพิวเตอร์ต่างๆ ออกไปใช้งานนอกสำนักงานของกรมฯ

(๒) บันทึกข้อมูลการนำระบบหรืออุปกรณ์คอมพิวเตอร์ออกไปใช้งานนอกสำนักงาน ไว้เป็นหลักฐานเพื่อป้องกันการสูญหาย

(๓) กรณีที่ระบบหรืออุปกรณ์คอมพิวเตอร์เกิดความเสียหายและต้องส่งซ่อม ต้องมีการควบคุมการส่งระบบหรืออุปกรณ์ออกไปซ่อมแซมนอกสถานที่ เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต กรณีที่ระบบหรืออุปกรณ์มีข้อมูลสำคัญต้องกำหนดให้มีการล้างข้อมูลทิ้ง เพื่อไม่ให้ผู้อื่นสามารถเข้าถึงข้อมูลได้ หรือนำส่วนของระบบหรืออุปกรณ์ที่มีข้อมูลสำคัญ เช่น ฮาร์ดดิสก์ ถอดแยกไว้ต่างหากก่อนส่งซ่อม

(๔) เมื่อนำระบบหรืออุปกรณ์คอมพิวเตอร์ของกรมฯ ไปใช้งานในที่สาธารณะหรือนอกสถานที่ ต้องไม่ทิ้งระบบหรืออุปกรณ์ไว้โดยลำพัง ระมัดระวังการสูญหาย การเสียหาย หรือการถูกขโมยเพราะผู้ที่นำออกไปใช้งานจะไม่ใช่ผู้รับผิดชอบระบบสารสนเทศ

ข้อ ๗ ผู้รับผิดชอบระบบสารสนเทศ กำหนดให้มีการทำลายข้อมูลบนสื่อบันทึกข้อมูลของระบบและอุปกรณ์คอมพิวเตอร์ต่างๆ ดังนี้

(๑) จัดให้มีการทำลายข้อมูลบนสื่อบันทึกข้อมูลของระบบหรืออุปกรณ์คอมพิวเตอร์ที่จะมีการแทงจำหน่ายเพื่อป้องกันการเข้าถึงข้อมูลสำคัญบนสื่อฯ (ดูแนวปฏิบัติสำหรับการทำลายข้อมูลบนสื่อบันทึกข้อมูล)

(๒) จัดให้มีการทำลายข้อมูลบนสื่อบันทึกข้อมูลของระบบหรืออุปกรณ์คอมพิวเตอร์ก่อนที่จะอนุญาตให้ผู้อื่นนำระบบหรืออุปกรณ์นั้นไปใช้งานต่อ

หมวด ๒
แนวปฏิบัติในการควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ

ข้อ ๘ ผู้รับผิดชอบระบบสารสนเทศ กำหนดให้มีการควบคุมการเข้าถึงระบบต่างๆ ของกรมฯ ดังนี้

(๑) กำหนดให้เฉพาะพนักงานหรือผู้ที่เกี่ยวข้องกับงานตามภารกิจของกรมฯ เท่านั้นที่จะอนุญาตให้สามารถเข้าถึงระบบงานและข้อมูลของกรมฯ ได้

(๒) จัดทำตารางแสดงการเข้าถึงระบบงานต่างๆ ของกรมฯ โดยอย่างน้อยให้ระบุ

- ชื่อระบบงาน
- ประเภทของข้อมูลในระบบงานนั้น และ
- หน่วยงานภายในที่มีสิทธิเข้าถึงระบบงานและข้อมูลเหล่านั้นได้

ข้อ ๙ กลุ่มบริหารทรัพยากรบุคคล ทำการแจ้งเกี่ยวกับการเปลี่ยนแปลง การโยกย้าย การลาออก หรือการเกษียณอายุของพนักงานของกรมฯ ให้ผู้รับผิดชอบระบบสารสนเทศและหน่วยงานภายในของกรมฯ อื่นๆ ได้รับทราบเพื่อดำเนินการเปลี่ยนแปลงสิทธิการเข้าถึงให้ถูกต้องและเหมาะสมต่อไป

ข้อ ๑๐ ผู้รับผิดชอบระบบสารสนเทศ บริหารจัดการสิทธิการเข้าถึงระบบของผู้ใช้งาน ดังนี้ (แนวปฏิบัติในการบริหารจัดการสิทธิการเข้าถึงระบบ)

(๑) กำหนดให้พนักงานใหม่ต้องขออนุมัติการใช้งานระบบของกรมฯ โดย

- จัดทำบันทึกร้องขอใช้งานผ่านทางหัวหน้างาน หรือจากผู้บังคับบัญชาระดับหัวหน้างานขึ้นไป
- พิจารณาว่าผู้ร้องขอมีสิทธิในการใช้งานหรือสมควรได้รับอนุญาตหรือไม่ และคำร้องขอมีความครบถ้วนและถูกต้องหรือไม่ กรณีที่ผู้ร้องขอไม่ได้เป็นพนักงานของกรมฯ ผู้ร้องขอใช้งานจะต้องผ่านการรับรองหรือเห็นชอบจากผู้บังคับบัญชาในระดับกองหรือฝ่ายของกรมฯ ก่อน รวมทั้งต้องใช้หลักฐานแสดงตัวตน เช่น บัตรประชาชน หรือเอกสารอื่นที่มีความน่าเชื่อถือ เพื่อประกอบเป็นหลักฐานการอนุมัติ
- ดำเนินการสร้างบัญชีผู้ใช้งานและรหัสผ่าน (โดยปฏิบัติตามแนวปฏิบัติสำหรับการตั้งและใช้งานรหัสผ่าน) เพื่อใช้เป็นข้อมูลที่ใช้ยืนยันตัวตนของผู้ใช้งาน ให้ตามที่ร้องขอ

(๒) กำหนดสิทธิการใช้ระบบของผู้ร้องขอโดยให้สิทธิให้สอดคล้องกับตารางควบคุมการเข้าถึงระบบ ตามความจำเป็นในการใช้งาน หรือตามหน้าที่ความรับผิดชอบของผู้ร้องขอ

(๓) กำหนดให้มีการถอดถอนหรือเปลี่ยนแปลงสิทธิการเข้าถึงระบบให้ถูกต้องและเหมาะสม เมื่อมีการลาออก การเปลี่ยนแปลง การโยกย้าย หรือการเกษียณอายุของพนักงาน

(๔) จัดเก็บข้อมูลหรือเอกสารการลงทะเบียนของผู้ที่ร้องขอใช้ระบบไว้ เพื่อเอาไว้ใช้ในการอ้างอิงหรือตรวจสอบในภายหลัง

(๕) กรณีมีความจำเป็นต้องให้สิทธิในระดับสูงกับผู้ใช้งาน ต้องให้สิทธินั้นเท่าที่จำเป็นและควบคุมให้จำนวนผู้ได้รับสิทธิในระดับสูงนี้มีจำนวนไม่มากนัก และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของผู้ใช้งานนั้นก่อน รวมทั้งให้ปฏิบัติตามแนวทาง ดังนี้

- ให้ความรู้หรือสร้างความตระหนักโดยสังเขปเกี่ยวกับการระมัดระวังการใช้สิทธิในระดับสูง เช่น การกำหนดรหัสผ่านที่มีความปลอดภัย
- จำกัดระยะเวลาการให้สิทธิในระยะอันสั้น และระงับสิทธิโดยทันทีเมื่อพ้นระยะเวลาดังกล่าว
- กำหนดให้มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ใช้รหัสผ่านที่มีความยาวตั้งแต่ ๑๐ ตัวอักษร เปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

(๖) กำหนดให้มีการทบทวนบัญชีผู้ใช้งานของระบบต่างๆ อย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทางการทบทวนดังนี้ (แนวปฏิบัติในการทบทวนสิทธิการเข้าถึงระบบ)

- พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงานภายในของกรมฯ
- จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานภายในเพื่อดำเนินการตรวจสอบว่ามีรายชื่อที่ออกไปแล้ว หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้รับการแก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่
- ผู้บังคับบัญชาของหน่วยงานภายในแจ้งกลับว่ามีรายชื่อใดที่ต้องดำเนินการแก้ไขให้ถูกต้อง
- ดำเนินการแก้ไขข้อมูลสิทธิให้ถูกต้องตามที่ได้รับแจ้ง

ข้อ ๑๑ ผู้รับผิดชอบระบบสารสนเทศ ต้องจัดทำและส่งมอบบัญชีผู้ใช้งานและรหัสผ่าน ดังนี้ (แนวปฏิบัติในการจัดทำและส่งมอบบัญชีผู้ใช้งานและรหัสผ่าน)

(๑) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา (โดยปฏิบัติตามแนวปฏิบัติสำหรับการตั้งและใช้งานรหัสผ่าน หรือตั้งรหัสผ่านแบบสุ่มแต่ต้องมีความยาวอย่างน้อย ๘ ตัวอักษร)

(๒) กำหนดบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือ ข้อมูลที่ใช้ในการยืนยันตัวตนของผู้ใช้งานต้องไม่ซ้ำซ้อนกัน

(๓) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มซึ่งมีการใช้งานร่วมกัน กล่าวคือ อนุญาตให้ใช้งานได้ก็ต่อเมื่อมีเหตุผลความจำเป็นในการใช้งานเท่านั้นและต้องแจ้งให้ผู้ใช้งานบัญชีแบบกลุ่มต้องรับทราบว่าต้องรับผิดชอบการใช้งานร่วมกัน

(๔) กำหนดให้มีการส่งมอบรหัสผ่านให้กับผู้ใช้งานโดยใช้วิธีการที่มีความปลอดภัย ดังนี้

- ใส่ซองปิดผนึกและประทับตรา “ลับ”
- โทรศัพท์แจ้งผู้ใช้งานนั้นโดยตรง

หมวด ๓
แนวปฏิบัติในการบริหารจัดการข้อมูลตามระดับชั้นความลับ

กรมฯ ได้ยึดการปฏิบัติตาม พ.ร.บ.ข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๐ ในการบริหารจัดการข้อมูลของกรมฯ จึงได้ออกแนวปฏิบัติที่เกี่ยวข้องดังนี้

ข้อ ๑๒ กรมฯ กำหนดแนวทางปฏิบัติสำหรับการกำหนดชั้นความลับของข้อมูลของกรมฯไว้ดังนี้ (แนวปฏิบัติสำหรับการกำหนดชั้นความลับของข้อมูล)

(๑) เจ้าของข้อมูล ต้องกำหนดชั้นความลับของข้อมูลของกรมฯ โดยแบ่งเป็น ๖ ระดับ ดังนี้

- ลับ ซึ่งประกอบด้วยชั้นความลับย่อย ดังนี้
    - ลับที่สุด (Top secret)
    - ลับมาก (Secret)
    - ลับ (Confidential)
- ส่วนบุคคล (Personal)
- ใช้ภายในเท่านั้น (Internal use)
- สาธารณะ (Public)

(๒) เจ้าของข้อมูล พิจารณาจากองค์ประกอบต่อไปนี้เพื่อกำหนดชั้นความลับของข้อมูลของตนเอง

(ก) ความสำคัญของเนื้อหา เช่น เนื้อหาของข้อมูลนั้นมีความสำคัญต่อความสำเร็จของงานตามภารกิจของกรมฯ มากน้อยเพียงใด หากมีความสำคัญสูง ข้อมูลนั้นอาจจัดอยู่ในชั้นความลับประเภทใช้ภายในเท่านั้น หรือ ลับ

(ข) แหล่งที่มาของข้อมูล เช่น หากข้อมูลนั้นมาจากภายนอกและเป็นข้อมูลลับ ชั้นความลับก็จะต้องคงไว้เช่นเดิม หรือหากข้อมูลนั้นมาจากอินเทอร์เน็ต ชั้นความลับก็อาจเป็นประเภทสาธารณะ

(ค) วิธีการนำไปใช้ประโยชน์ เช่น หากข้อมูลนั้นสามารถนำไปใช้ประโยชน์ในเชิงพาณิชย์ได้ ข้อมูลนั้นอาจจัดอยู่ในประเภทลับ เช่น ความลับทางการค้า เป็นต้น

(ง) จำนวนบุคคลที่ควรรับทราบ เช่น หากข้อมูลนั้นสามารถเปิดเผยต่อผู้ใช้งานข้อมูลเป็นจำนวนมาก ชั้นความลับอาจจัดอยู่ในประเภทข้อมูลสาธารณะ

(จ) ผลกระทบหากมีการเปิดเผย เช่น หากข้อมูลนั้นถูกเปิดเผย จะมีผลกระทบด้านชื่อเสียงและภาพลักษณ์ ด้านการดำเนินงานภายในหรือด้านการปฏิบัติตามกฎระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม ชั้นความลับอาจจัดอยู่ในประเภทใช้ภายในเท่านั้น หรือเป็นข้อมูลลับ

(ฉ) หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่อง เช่น ข้อมูลสำคัญหรือข้อมูลลับที่มาจากเจ้าของเรื่องใดจะต้องคงชั้นความลับไว้เช่นเดิม การนำไปใช้งานควรขออนุญาตจากผู้ที่เป็นเจ้าของเรื่องก่อน

(๓) เจ้าของข้อมูล ใช้แนวทางต่อไปนี้ในการเรียงลำดับการจัดชั้นความลับของข้อมูล

(ก) พิจารณาว่าเป็นข้อมูลลับหรือไม่ ซึ่งกรณีนี้อาจเป็นข้อมูล “ลับที่สุด” “ลับมาก” หรือ “ลับ”

(ข) หากไม่เป็นข้อมูลลับ ให้พิจารณาต่อว่าเป็นข้อมูลที่สามารถบ่งชี้ตัวบุคคลหรือไม่ ซึ่งกรณีนี้อาจเป็น “ข้อมูลส่วนบุคคล”

(ค) หากไม่เป็นข้อมูลส่วนบุคคล ให้พิจารณาต่อว่าเป็นข้อมูลสำหรับการดำเนินงานภายในของบริษัทฯ หรือไม่ ซึ่งกรณีนี้อาจเป็น “ข้อมูลใช้ภายในเท่านั้น”

(ง) หากไม่เข้าเกณฑ์ใดเกณฑ์หนึ่ง ข้อมูลใหม่ดังกล่าวจะถือว่าเป็นข้อมูลทั่วไปที่การดำเนินการต่างๆ ให้อยู่ในดุลยพินิจของผู้เป็นเจ้าของข้อมูล ซึ่งกรณีนี้อาจเป็น “ข้อมูลสาธารณะ”

ข้อ ๑๓ กรมฯ กำหนดแนวทางปฏิบัติสำหรับการจัดการโดยทั่วไปของข้อมูลในทุกชั้นความลับไว้ ดังนี้ (แนวทางปฏิบัติสำหรับการจัดการโดยทั่วไปของข้อมูลในทุกชั้นความลับ)

(๑) ในการสร้างและแสดงชั้นความลับบนข้อมูล เจ้าของข้อมูล ปฏิบัติดังนี้

- สร้างและแสดงชั้นความลับบนข้อมูล กล่าวคือ
    - กรณีเป็นข้อมูลใช้ภายใน แสดงด้วยคำว่า “ข้อมูลใช้ภายในเท่านั้น”
    - กรณีเป็นข้อมูลลับ ลับมาก ลับที่สุด แสดงด้วยคำว่า “ลับ” “ลับมาก” “ลับที่สุด” ตามลำดับ

ให้ปรากฏเห็นอย่างเด่นชัดทั้งข้อมูลที่มีสภาพเป็นกระดาษ ไฟล์อิเล็กทรอนิกส์ เทป External Hard Disk Flash Drive แผ่น CD/DVD หรือข้อมูลที่อยู่ในรูปแบบอื่นๆ

(๒) ในการเก็บรักษาเอกสาร เจ้าของข้อมูล ปฏิบัติดังนี้

- จัดเก็บเอกสารไว้ในแฟ้มข้อมูลและนำไปเก็บไว้ในตู้เก็บเอกสารโดยแยกเก็บเป็นแต่ละเรื่องหรือแต่ละหัวข้อ
- แยกจัดเก็บเอกสารในแต่ละชั้นความลับ ไม่เก็บร่วมกับชั้นความลับอื่นๆ เช่น ข้อมูลลับ ข้อมูลส่วนบุคคล หรือข้อมูลสาธารณะ ต้องไม่จัดเก็บร่วมกัน
- จัดเก็บแฟ้มข้อมูลไว้ในตู้ที่สามารถล็อกได้เพื่อป้องกันการสูญหาย

(๓) ในการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ เจ้าของข้อมูล ปฏิบัติตามแนวทางการทำลาย ดังนี้ (แนวปฏิบัติสำหรับการทำลายข้อมูลบนสื่อบันทึกข้อมูล)

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือ เผาทำลาย
ฮาร์ดดิสก์/Flash Drive	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหม สหรัฐอเมริกา DOD ๕๒๒๐.๓๓-M (คือการ Format ฮาร์ดดิสก์อย่างน้อย ๓ รอบ)

(๔) ในการจัดการกับไฟล์ข้อมูลอิเล็กทรอนิกส์ เจ้าของข้อมูล ปฏิบัติดังนี้

- ป้องกันไฟล์ข้อมูลอิเล็กทรอนิกส์ ซึ่งจัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยการใช้รหัสผ่านที่มีความมั่นคงปลอดภัย
- ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลอิเล็กทรอนิกส์ ว่ามีการทำงานป้องกันไวรัสได้ตามปกติหรือไม่
- ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่

- ดำเนินการสำรองไฟล์ข้อมูลอิเล็กทรอนิกส์ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอ

(๕) ในการส่งไฟล์ข้อมูลอิเล็กทรอนิกส์ทางอีเมล์ เจ้าของข้อมูล ปฏิบัติดังนี้

- ตรวจสอบที่อยู่อีเมล์ของผู้รับปลายทางให้ถูกต้อง ก่อนจัดส่งไฟล์นั้นไปยังผู้รับเพื่อป้องกันการส่งผิดตัวบุคคลและทำให้ข้อมูลเกิดการรั่วไหล

(๖) ในการอนุญาตให้ผู้ให้บริการภายนอกเข้าถึงข้อมูลของกรมฯ ไม่ว่าจะอยู่ในรูปแบบใดก็ตาม โดยที่กรมฯ ไม่ประสงค์ให้ผู้ให้บริการนั้นนำไปเผยแพร่ต่อหรือให้ข้อมูลของกรมฯ แก่ผู้อื่น เจ้าของข้อมูลต้องกำหนดให้มีการทำสัญญาการไม่เปิดเผยความลับกับผู้ให้บริการนั้น รวมทั้งแจ้งให้ทราบทางวาจาด้วย

(๗) จำกัดช่องทางการใช้งานหรือการเข้าถึงข้อมูลเท่าที่มีความจำเป็นต่อการใช้งาน โดยสามารถเข้าถึงได้ไม่จำกัดเวลา

ข้อ ๑๔ กรมฯ กำหนดแนวทางปฏิบัติสำหรับการจัดการกับข้อมูลลับของกรมฯ ไว้ ดังนี้ (แนวปฏิบัติสำหรับการจัดการกับข้อมูลลับ)

(๑) สำหรับข้อมูลในชั้นความลับ “ลับ” ได้แก่ ลับ ลับมาก หรือลับที่สุด เจ้าของข้อมูลลับฯ พิจารณาเกณฑ์ต่อไปนี้เพิ่มเติมเพื่อกำหนดชั้นความลับที่ถูกต้อง

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

(๒) เจ้าของข้อมูลลับฯ ดำเนินการจัดทำทะเบียนข้อมูลลับที่ตนเองดูแลหรือรับผิดชอบ ซึ่งมีรายละเอียดประกอบด้วย

- ชื่อของข้อมูล
- ชั้นความลับ
- เจ้าของข้อมูลลับฯ
- เหตุผลประกอบการกำหนดชั้นความลับ
- หน่วยงานภายในที่สามารถเข้าถึงได้
- หน่วยงานภายนอกที่อนุญาตให้เข้าถึงได้
- สถานที่ที่จัดเก็บข้อมูล

- ระบบงานที่ใช้จัดเก็บข้อมูล
- ระยะเวลาการเก็บรักษาข้อมูล

(๓) เจ้าของข้อมูลลับฯ พิจารณาปรับชั้นความลับ (ปรับลด เพิ่ม หรือยกเลิกชั้นความลับ) ให้ถูกต้องตามความจำเป็น ปรับปรุงทะเบียนข้อมูลลับให้ถูกต้องและทันสมัย และต้องแจ้งให้หน่วยงานที่สามารถเข้าถึงข้อมูลลับหรือที่ได้รับการแจกจ่ายทราบด้วยทุกครั้งเพื่อแก้ไขชั้นความลับให้ถูกต้อง

(๔) ในการจัดทำหรือจัดเตรียมข้อมูลลับ เจ้าของข้อมูลลับฯ ปฏิบัติดังนี้

- จัดทำหรือจัดเตรียมข้อมูลในสถานที่ที่ปลอดภัย เช่น จัดทำในสำนักงาน ไม่ทำในสถานที่ที่เป็นสาธารณะซึ่งบุคคลภายนอกสามารถเห็นข้อมูลที่จัดทำได้ และจำกัดผู้ที่เป็นผู้ดำเนินการจัดทำ
- ในการจัดทำข้อมูลลับซึ่งใช้กระดาษหรือวัสดุชั่วคราว เช่น กระดาษร่าง กระดาษคาร์บอน ต้องทำลายกระดาษหรือวัสดุนั้นทันทีที่จัดทำเสร็จเรียบร้อย (ดูวิธีการทำลายในแนวปฏิบัติสำหรับการทำลายข้อมูลบนสื่อบันทึกข้อมูล) หากไม่ทำลาย ต้องเก็บรักษาไว้ในสถานที่ที่ปลอดภัย ถ้าเป็นการจัดทำโดยใช้เครื่องคอมพิวเตอร์ อย่างน้อยต้องป้องกันเครื่องคอมพิวเตอร์ด้วยการใช้รหัสผ่านที่มีความปลอดภัย
- จัดทำข้อมูลโดยแสดงเลขที่หน้าของจำนวนหน้าทั้งหมดไว้ในทุกหน้าของข้อมูลลับ และแสดงไว้ในส่วนที่สามารถเห็นได้อย่างชัดเจน เช่น มุมขวาด้านบนของเอกสาร (การบันทึกเลขหน้ามีจุดประสงค์เพื่อให้ทราบว่าข้อมูลลับนั้นเป็นหน้าใดของจำนวนทั้งหมดกี่หน้า หากมีการสูญหายไปหน้าใดหน้าหนึ่ง จะได้สังเกตพบ อาจสามารถติดตามหาผู้ละเมิดได้ และ/หรือ หาทางลดความเสียหายหรือผลกระทบที่อาจเกิดขึ้นได้)

(๕) เจ้าของข้อมูลลับฯ แสดงชั้นความลับบนเอกสารลับในทุกหน้าของเอกสารให้ปรากฏเห็นอย่างเด่นชัด

(๖) ในการทำสำเนาหรือแจกจ่ายข้อมูลลับ เจ้าของข้อมูลลับฯ ปฏิบัติดังนี้

- ทำสำเนาหรือแจกจ่ายข้อมูลลับให้แก่ผู้รับปลายทาง ซึ่งเป็นผู้ที่มีสิทธิในการเข้าถึงข้อมูลตามที่ระบุไว้ในทะเบียนข้อมูลลับ หรือสามารถแจกจ่ายให้ได้ตามความจำเป็นในการเข้าถึงข้อมูลนั้น
- แจ้งให้หน่วยงานภายนอกที่อนุญาตให้เข้าถึงข้อมูลลับนั้น ว่าไม่อนุญาตให้ทำสำเนาเพิ่มเติม เว้นเสียแต่จะได้รับอนุญาตจากผู้มีอำนาจของกรมฯ ก่อน
- เข้ารหัสไฟล์ข้อมูลลับอิเล็กทรอนิกส์ก่อนที่จะมีการจัดส่งไปทางเครือข่ายไปยังผู้รับปลายทาง

(๗) ในการยืมหรือขอเข้าถึงข้อมูลลับ เจ้าของข้อมูลลับฯ ปฏิบัติดังนี้

- เมื่อมีการขอยืม หรือขอเข้าถึงข้อมูลลับโดยผู้อื่นที่ไม่ได้เป็นผู้มีสิทธิในการเข้าถึงข้อมูลตามทะเบียนข้อมูลลับ ให้พิจารณาตรวจสอบคุณสมบัติของผู้ยืมหรือขอเข้าถึงก่อนว่าเป็นผู้มีอำนาจหน้าที่ที่เกี่ยวข้องหรือไม่ หรือมีความจำเป็นในการเข้าถึงข้อมูลนั้นหรือไม่ พร้อมทั้งต้องทำบันทึกหลักฐานการยืมหรือการขอเข้าถึงข้อมูลนั้นด้วย และแจ้งให้ผู้ยืมหรือขอเข้าถึงทราบว่าห้ามทำการสำเนาเพิ่มเติมโดยไม่ได้รับอนุญาต
- เมื่อหมดความจำเป็นในการใช้งานแล้ว กำหนดให้ผู้ขอยืมจัดส่งข้อมูลนั้นกลับคืนมาโดยทันที สำหรับกรณีการเข้าถึงระบบเทคโนโลยีสารสนเทศให้ทำการยกเลิกบัญชีผู้ใช้งานที่ขอเข้าถึงข้อมูลลับโดยทันที

(๘) ในการส่งเอกสารลับทางไปรษณีย์ เจ้าของข้อมูลลับฯ ปฏิบัติตามระเบียบการส่งเอกสารลับของราชการ และให้ระมัดระวังตรวจสอบที่อยู่ของผู้รับปลายทางให้ถูกต้องก่อนจัดส่งเอกสารนั้นไปยังผู้รับเพื่อป้องกันการส่งผิดตัวบุคคล

(๙) ในการจัดการกับไฟล์ข้อมูลลับอิเล็กทรอนิกส์ เจ้าของข้อมูลลับฯ ปฏิบัติดังนี้

- จัดหมวดหมู่ไฟล์ข้อมูลลับอิเล็กทรอนิกส์ในเครื่องคอมพิวเตอร์ที่ใช้งานไว้ต่างหาก ไม่ปะปนกับไฟล์ข้อมูลประเภทอื่นๆ
- แสดงชั้นความลับบนทุกหน้าของไฟล์ข้อมูลลับอิเล็กทรอนิกส์ เช่น โดยการทำลายน้ำ
- ห้าม Share ไฟล์ข้อมูลลับอิเล็กทรอนิกส์บนเครือข่ายของกรมฯ เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ (ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการ Share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)

ข้อ ๑๕ กรมฯ กำหนดแนวทางปฏิบัติสำหรับการจัดการกับข้อมูลใช้ภายในเท่านั้นของกรมฯ ไว้ ดังนี้

(๑) ในการส่ง การสำเนา หรือการให้ยืมเอกสารที่เป็นข้อมูลใช้ภายในเท่านั้น เจ้าของข้อมูลใช้ภายในฯ จำกัดการส่ง การสำเนา หรือการให้ยืมเอกสารดังกล่าวแก่หน่วยงานหรือผู้ใช้งานทั้งภายในและภายนอกกรมฯ ที่มีความจำเป็นต้องใช้งานหรือเข้าถึงข้อมูลนั้นเท่านั้น หากไม่ต้องการให้ผู้รับเอกสารเปิดเผยข้อมูลนั้นต่อผู้อื่น ให้แจ้งให้ผู้รับเอกสารได้รับทราบด้วย

(๒) ในการ Share ไฟล์ข้อมูลอิเล็กทรอนิกส์บนเครือข่ายของกรมฯ ที่เป็นข้อมูลใช้ภายในเท่านั้น เจ้าของข้อมูลใช้ภายในฯ สามารถ Share ไฟล์ข้อมูลดังกล่าวแก่หน่วยงานหรือผู้ใช้งานภายในกรมฯ ได้โดยพิจารณาจากหน้าที่หรือความจำเป็น

ในการเข้าถึงข้อมูลนั้น แต่ต้องใช้รหัสผ่านที่มีความมั่นคงปลอดภัยเพื่อป้องกันข้อมูลที่ Share นั้น

หมวด ๔
แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

ข้อ ๑๖ ผู้ใช้งาน ปฏิบัติตามแนวทางการใช้งานหรือห้ามใช้งานโปรแกรมคอมพิวเตอร์ ดังนี้

(๑) ใช้งานโปรแกรมมาตรฐานตามที่กรมฯ ได้ติดตั้งไว้ให้ ห้ามเปลี่ยนแปลงโปรแกรมเหล่านั้นหรือติดตั้งโปรแกรมอื่นๆ เพิ่มเติม

(๒) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์เพิ่มเติมในเครื่องคอมพิวเตอร์หรือระบบเครือข่ายของกรมฯ

(๓) หากมีความจำเป็นต้องใช้โปรแกรมอื่นๆ เพิ่มเติม เช่น โปรแกรมอรรถประโยชน์ ต้องขออนุมัติและได้รับความเห็นชอบจากกลุ่มระบบคอมพิวเตอร์ก่อน

(๔) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพื่อใช้ในการตรวจสอบข้อมูลบนระบบเครือข่ายของกรมฯ

ข้อ ๑๗ ผู้ใช้งาน ปฏิบัติตามเงื่อนไขการใช้งานและไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น ดังนี้

(๑) ห้ามทำซ้ำ สำเนา เปลี่ยนแปลง หรือแก้ไขทั้งหมดหรือบางส่วนของซอฟต์แวร์ หนังสือ บทความ รายงาน เอกสาร หรือทรัพย์สินทางปัญญาอื่นๆ ที่เป็นการละเมิดเงื่อนไขหรือข้อตกลงการใช้งานของเจ้าของทรัพย์สินทางปัญญา

(๒) ปฏิบัติตามเงื่อนไขการใช้งานหรือที่กำหนดไว้ของทรัพย์สินทางปัญญาต่างๆ ที่กรมฯ หรือผู้ใช้งานมีใช้งานหรือครอบครอง

(๓) ปฏิบัติตามเงื่อนไขการใช้งานเอกสารหรือข้อมูลต่างๆ ที่ได้รับทางอินเทอร์เน็ตอย่างเคร่งครัด

(๔) ปฏิบัติตามเงื่อนไขการใช้งานโปรแกรมอรรถประโยชน์อย่างเคร่งครัด โดยผู้บังคับบัญชาของผู้ใช้งานต้องหมั่นตรวจสอบการใช้งานให้เป็นไปตามเงื่อนไขที่ระบุไว้เพื่อมิให้เป็นการละเมิดลิขสิทธิ์การใช้งาน

(๕) ห้ามติดตั้งซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องหรือมีลักษณะเป็นการละเมิดลิขสิทธิ์

(๖) ห้ามเปลี่ยนแปลงหรือแก้ไขซอฟต์แวร์สำเร็จรูปที่กรมฯ จัดหามาใช้งาน เว้นเสียแต่กรมฯ ได้รับอนุญาตให้เปลี่ยนแปลงแก้ไขได้จากเจ้าของลิขสิทธิ์

ข้อ ๑๘ ผู้ใช้งาน กำหนดหรือใช้งานรหัสผ่านโดยปฏิบัติ ดังนี้ (แนวปฏิบัติสำหรับการตั้งและใช้งานรหัสผ่าน)

(๑) เก็บรักษารหัสผ่านที่ได้รับไว้เป็นความลับ

(๒) กำหนดรหัสผ่านที่มีความยาวมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษร ตัวเลข และสัญลักษณ์ต่างๆ เข้าด้วยกัน

(๓) ไม่กำหนดรหัสผ่านจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๔) ใช้รหัสผ่านเพื่อป้องกันไฟล์ที่มีการใช้งานร่วมกับผู้อื่นทางเครือข่ายคอมพิวเตอร์

(๕) ไม่บันทึกรหัสผ่านไว้ในระบบเพื่อเป็นการช่วยจำและเพื่อให้สามารถย้อนกลับมาใช้ระบบโดยไม่ต้องใส่รหัสผ่านอีกครั้งหนึ่ง

(๖) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยผู้อื่น

(๗) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านของตนเองแก่ผู้อื่นเนื่องจากไม่สามารถมาปฏิบัติงานได้หรือความจำเป็นอื่นใดก็ตาม เมื่อกลับมาปฏิบัติงานได้ตามปกติ ให้ทำการเปลี่ยนรหัสผ่านใหม่โดยทันที

ข้อ ๑๙ ผู้ใช้งาน ตรวจสอบและป้องกันไวรัสโดยปฏิบัติ ดังนี้ (แนวปฏิบัติสำหรับการป้องกันไวรัส)

(๑) ตรวจสอบให้แน่ใจว่าโปรแกรมป้องกันไวรัสในเครื่องที่ใช้งานยังมีการทำงานตามปกติ

(๒) ตรวจสอบและสแกนไวรัสในเครื่องคอมพิวเตอร์ที่ใช้งานอย่างน้อยสัปดาห์ละครั้ง

(๓) ตรวจสอบว่าโปรแกรมป้องกันไวรัสยังทำงานตามปกติและมีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ หากพบว่าโปรแกรมฯ ทำงานผิดปกติ ให้รีบแจ้งส่วนคอมพิวเตอร์เพื่อดำเนินการแก้ไขโดยเร็ว

(๔) ห้ามถอดถอนโปรแกรมป้องกันไวรัสที่กรมฯ ได้ติดตั้งไว้ให้

(๕) ระมัดระวังการเปิดไฟล์แนบที่ได้รับทางอีเมล์ หรือทางโปรแกรมประเภท Instant Messaging ที่อาจมีการติดไวรัสมาด้วย

(๖) ระมัดระวังการเข้าเว็บไซต์ที่ไม่ได้มีการใช้งานเป็นประจำ การเปิดไฟล์หรือเข้าไปตามหน้าต่างๆ ของเว็บไซต์อาจได้รับไวรัสจากไฟล์หรือหน้าต่างๆ เหล่านั้น

(๗) ระมัดระวังไวรัสที่เกิดจากการใช้ไฟล์ข้อมูลร่วมกันบนเครือข่าย ซึ่งบางไฟล์อาจมีการติดไวรัสและแพร่กระจายได้

ข้อ ๒๐ ผู้ใช้งาน ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การขโมย การสูญหาย หรือการเสียหายของข้อมูล เอกสาร คอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์ของกรมฯ โดยปฏิบัติ ดังนี้

(๑) จัดเก็บข้อมูลหรือเอกสารสำคัญไว้ในตู้ที่มีกุญแจล็อก

(๒) ไม่วางข้อมูลหรือเอกสารสำคัญทิ้งไว้ในที่ที่เปิดเผย หรือที่สาธารณะ

(๓) ระมัดระวังและสอดส่องบุคคลภายนอกที่เข้ามาในสำนักงานเพื่อป้องกันการสูญหาย การเสียหาย หรือการถูกขโมยทรัพย์สินโดยบุคคลภายนอก

(๔) ออกจากระบบงานหรือเครื่องคอมพิวเตอร์โดยทันทีที่ใช้งานเสร็จ (เช่น ด้วยการ Log-off)

(๕) ปิดเครื่องคอมพิวเตอร์พีซีที่ใช้งานอยู่เมื่อปฏิบัติงานประจำวันเสร็จสิ้น หรือเมื่อจะไม่มีการใช้งานเกินกว่า ๔ ชั่วโมง

(๖) ตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ใช้งานให้มีการล็อกหน้าจอโดยอัตโนมัติหลังจากที่ไม่มีการใช้งานเกินกว่า ๑๕ นาที พร้อมทั้งต้องใส่รหัสผ่านให้ถูกต้อง จึงจะสามารถกลับเข้าใช้งานได้ตามปกติ

(๗) ระมัดระวังการใช้งานและดูแลคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของกรมฯ เพื่อป้องกันไม่ให้เกิดความเสียหายก่อนเวลาอันควร

(๘) เมื่อออกนอกสำนักงานเป็นคนสุดท้ายหรือระหว่างพักเที่ยง ให้ปิดและล็อกประตูทุกครั้ง เพื่อป้องกันการสูญหายของข้อมูล เอกสาร คอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์

ข้อ ๒๑ ผู้ใช้งาน ป้องกันอุปกรณ์หรือเครื่องคอมพิวเตอร์แบบพกพาซึ่งสินทรัพย์เป็นของกรมฯ โดยปฏิบัติ ดังนี้ (แนวปฏิบัติสำหรับการใช้อุปกรณ์หรือเครื่องคอมพิวเตอร์แบบพกพา)

(๑) จัดเก็บอุปกรณ์ฯ ไว้ในสถานที่ที่ปลอดภัยและสามารถล็อกได้

(๒) กำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยเพื่อป้องกันผู้อื่นเข้าถึงข้อมูลภายในอุปกรณ์

(๓) ระมัดระวังเมื่อมีการนำอุปกรณ์ฯ ไปใช้งานในที่สาธารณะเพื่อป้องกันการสูญหาย การถูกขโมย หรือการเข้าถึงข้อมูลในอุปกรณ์ฯ โดยไม่ได้รับอนุญาต

(๔) ห้ามทิ้งอุปกรณ์ฯ ไว้โดยไม่มีผู้ดูแล ซึ่งรวมถึงการทิ้งไว้ในรถยนต์ที่สามารถมองเห็นได้จากภายนอก

(๕) ห้ามให้ผู้อื่นยืมอุปกรณ์ฯ ไปใช้งาน เช่น เพื่อน พี่น้อง หรือญาติ

(๖) ห้ามให้ผู้อื่น เช่น บุคคลภายนอก ทำการซ่อมหรือแก้ไขอุปกรณ์ฯ หากอุปกรณ์หรือเครื่องคอมพิวเตอร์นั้นมีปัญหาหรือไม่สามารถใช้งานได้ ให้นำมาให้ส่วนคอมพิวเตอร์เป็นผู้ดำเนินการซ่อมแซมหรือแก้ไขให้ (ปกติใช้วิธีส่งให้ผู้ให้บริการภายนอกซ่อม โดยเจ้าของอุปกรณ์เป็นผู้ดำเนินการเอง)

(๗) สำหรับอุปกรณ์ฯ ที่มีการยืม เมื่อเสร็จสิ้นการใช้งานแล้ว ให้รีบนำส่งคืนพนักงานผู้รับผิดชอบในการยืม-คืนโดยทันที ทั้งนี้ในการรับคืน ให้พนักงาน

ผู้รับผิดชอบตรวจสอบสภาพของอุปกรณ์ฯ ที่รับคืนด้วยว่ามีการชำรุดหรือเสียหายหรือไม่

ในกรณีที่พนักงานผู้รับผิดชอบในการรับคืนอุปกรณ์ฯ ตรวจพบความเสียหาย ให้แจ้งผู้ยืม ผู้บังคับบัญชาของผู้ยืม และส่วนคอมพิวเตอร์ ได้รับทราบโดยเร็ว หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทเลินเล่อของผู้ยืมหรือผู้ที่นำไปใช้งาน ผู้ยืมต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ข้อ ๒๒ ผู้ใช้งาน ใช้ระบบงานของกรมฯ โดยปฏิบัติ ดังนี้

(๑) ทำบันทึกข้อความเพื่อขออนุมัติเข้าใช้ระบบงาน และนำเสนอต่อผู้บังคับบัญชาตามสายงานเพื่อพิจารณาอนุมัติ

(๒) ให้ใช้งานตามภารกิจของหน่วยงานหรือหน้าที่ความรับผิดชอบของตนเองเท่านั้น ห้ามใช้งานนอกเหนือจากความรับผิดชอบของตนเอง

ข้อ ๒๓ ผู้ใช้งาน ทำบันทึกข้อความขอใช้งาน VPN เพื่อขออนุมัติจาก ผู้อำนวยการศูนย์สารสนเทศสิ่งแวดล้อมสำหรับการเข้าถึงระบบงานของกรมฯ จากระยะไกล โดยต้องแสดงเหตุผลหรือความจำเป็นในการใช้งาน พร้อมระบุระยะเวลาการใช้งานตามที่ต้องการ (แนวปฏิบัติในการเข้าถึงระบบงานจากระยะไกล)

ข้อ ๒๔ ผู้ใช้งาน ห้ามใช้งานระบบเทคโนโลยีสารสนเทศ อินเทอร์เน็ต และเครือข่ายของกรมฯ ในลักษณะที่ผิดวัตถุประสงค์ ดังนี้ (แนวปฏิบัติสำหรับการป้องกันการใช้งานระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์)

(๑) ห้ามเข้าเว็บไซต์ที่มีเนื้อหาที่ไม่เหมาะสมในประเภทดังต่อไปนี้

(ก) การพนัน

(ข) การประมูล

(ค) การวิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และ พระมหากษัตริย์

(ง) ลามกอนาจาร

(๒) ห้ามใช้โปรแกรมประเภท Peer to Peer ที่สามารถรับส่งไฟล์ข้อมูลโดยตรงระหว่างผู้ส่งและผู้รับ เช่น Bittorrent

(๓) ห้ามเล่นเกมส์ หรือดูภาพยนตร์ทางอินเทอร์เน็ตในระหว่างเวลาทำงาน

(๔) ห้ามใช้อินเทอร์เน็ตเพื่อ

(ก) เข้าร่วมกิจกรรมที่อาจก่อให้เกิดความเสียหายต่อภาพลักษณ์หรือชื่อเสียงของกรมฯ

(ข) แสดงความคิดเห็นบนเว็บไซต์ในเรื่องที่เกี่ยวข้องกับการดำเนินงานของกรมฯ ในลักษณะที่อาจก่อให้เกิดความเข้าใจที่ไม่ตรงกับความเป็นจริง หรือก่อให้เกิดความเสียหายต่อกรมฯ

(๕) ทำการอันผิดหรือขัดต่อกฎหมาย พระราชบัญญัติ หรือระเบียบข้อบังคับอื่นๆ ที่องค์กรต้องปฏิบัติตาม หรือก่อให้เกิดความเสียหายแก่ผู้อื่น หรือขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

(๖) ละเมิดทรัพย์สินทางปัญญาของกรมฯ หรือของผู้อื่น

(๗) บุกรุกระบบหรือเข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาต

(๘) ขัดขวางการใช้งานเครือข่ายของกรมฯ และของผู้อื่น

(๙) กระทำการอื่นใดที่ขัดต่อการดำเนินงานตามอำนาจหน้าที่ของกรมฯ หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายต่อกรมฯ

ข้อ ๒๕ ผู้ใช้งาน ใช้ระบบงานอีเมล์โดยปฏิบัติ ดังนี้

(๑) ใช้ระบบงานอีเมล์ที่กรมฯ กำหนดให้ใช้งานสำหรับการรับส่งข้อมูลที่เป็นงานหรือภารกิจของกรมฯ

(๒) ห้ามใช้ที่อยู่อีเมล์ที่กรมฯ กำหนดให้เพื่อลงทะเบียนตามเว็บไซต์ต่างๆ ที่ไม่เกี่ยวข้องกับงานหรือภารกิจของกรมฯ

(๓) ห้ามเข้าถึงข้อมูลอีเมล์ของผู้อื่นโดยไม่ได้รับอนุญาต

(๔) ห้ามปลอมแปลงอีเมล์

(๕) ห้ามส่งอีเมล์ที่มีลักษณะดังต่อไปนี้

(ก) อีเมล์ขยะ (Spam Mail)

(ข) อีเมล์ลูกโซ่ (Chain Letter)

(ค) อีเมล์มีไวรัสไปให้กับผู้อื่น

(๖) จำกัดการส่งอีเมล์ที่มีขนาดใหญ่เท่าที่จำเป็นเพื่อลดปริมาณข้อมูลในเครือข่ายของกรมฯ

(๗) ระบุชื่อเรื่อง (Subject) ในอีเมล์ทุกฉบับที่ส่งไป

(๘) ไม่ส่งกระจายอีเมล์ออกไปยังผู้รับเป็นจำนวนมากที่เกินความจำเป็น กล่าวคือจำกัดกลุ่มผู้รับเท่าที่มีความจำเป็นต้องรับรู้เท่านั้น

(๙) ใช้คำพูดที่สุภาพในการส่งอีเมล์

(๑๐) สำรองข้อมูลอีเมล์อย่างสม่ำเสมอ

ข้อ ๒๖ ในการจัดการกับข้อมูลของกรมฯ ตามชั้นความลับ ผู้ใช้งานข้อมูล ปฏิบัติตามแนวปฏิบัติในการบริหารจัดการข้อมูลตามระดับชั้นความลับ ที่กรมฯ ได้กำหนดไว้

ข้อ ๒๗ เมื่อผู้ใช้งานพบเหตุการณ์หรือจุดอ่อนด้านความมั่นคงปลอดภัย ให้รีบแจ้งไปยังกลุ่มระบบคอมพิวเตอร์ หรือศูนย์สารสนเทศสิ่งแวดล้อมโดยทันทีที่พบเห็น

ข้อ ๒๘ ผู้บังคับบัญชา ต้องดำเนินการตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้งานที่ลาออกก่อนวันที่มาปฏิบัติงานวันสุดท้ายเพื่อดูว่ายังอยู่ในสภาพที่ใช้งานได้ตามปกติหรือไม่ หากเกิดการชำรุดหรือเสียหาย ให้ตรวจสอบว่าเป็นการเสียหายตามสภาพการใช้งานหรือไม่ หากเป็นการชำรุดหรือเสียหายโดยประมาทหรือเลินเล่อ ให้แจ้งหน่วยงานพัสดุเพื่อดำเนินการสอบสวนต่อไป

หมวด ๕
แนวปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยของระบบ

ข้อ ๒๙ ผู้รับผิดชอบระบบสารสนเทศ บริหารจัดการความมั่นคงปลอดภัยของระบบต่างๆ ของกรมฯ ดังนี้ (แนวปฏิบัติสำหรับการบริหารจัดการความมั่นคงปลอดภัยของระบบ)

(๑) กำหนดให้มีการบันทึกและจัดเก็บข้อมูลล็อกของระบบต่างๆ พร้อมทั้งกำหนดระยะเวลาการจัดเก็บข้อมูลล็อกย้อนหลังจากปัจจุบัน เพื่อเอาไว้ใช้ในกรณีที่มีความจำเป็นต้องตรวจสอบข้อมูลล็อกเหล่านั้นเพื่อค้นหาปัญหาหรือความผิดปกติของระบบที่เกิดขึ้น (ซึ่งเริ่มเกิดขึ้น ณ จุดเวลาหนึ่งในอดีต) กรณีการจัดเก็บข้อมูลล็อกตาม พ.ร.บ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ต้องกำหนดระยะเวลาการจัดเก็บข้อมูลล็อกย้อนหลังอย่างน้อย ๙๐ วัน

(๒) กำหนดให้มีการตั้งสัญญาณนาฬิกาของระบบต่างๆ ของกรมฯ ให้ถูกต้องและตรงตามเวลามาตรฐานสากลอยู่เสมอ

(๓) กำหนดรายชื่อโปรแกรมที่มีความมั่นคงปลอดภัยสำหรับใช้ในการล็อกอินเข้าสู่ระบบจากระยะไกลโดยผู้ดูแลระบบ ผู้ดูแลเครือข่าย และผู้พัฒนาระบบ เพื่อเข้าไปบริหารจัดการ ดูแล หรือบำรุงรักษาระบบต่างๆ ของกรมฯ และกำหนดให้ผู้ที่เกี่ยวข้องต้องใช้โปรแกรมดังกล่าวในการดูแลและบริหารจัดการระบบเหล่านั้นของกรมฯ

(๔) ตรวจสอบและปิดพอร์ตของระบบต่างๆ ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ

(๕) จัดทำระบบบริหารจัดการรหัสผ่านเชิงโต้ตอบสำหรับการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย โดยที่ระบบควรสามารถกำหนดให้ผู้ใช้งานตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยตามแนวปฏิบัติสำหรับการตั้งและใช้งานรหัสผ่าน

(๖) พิจารณาตั้งค่าบนระบบให้ตัดและหมดเวลาการใช้งาน (Session time-out) กล่าวคือ หลังจากที่เข้าระบบและไม่ได้ใช้งานเกินกว่าระยะเวลาหนึ่งที่กำหนดไว้ เช่น ๑๕-๓๐ นาที

(๗) พิจารณาตั้งค่าบนระบบให้จำกัดระยะเวลาการใช้งานระบบต่อหนึ่งครั้ง (Limitation of connection time) เช่น ใช้งานได้ครั้งละ ๓ ชั่วโมง

ข้อ ๓๐ ผู้รับผิดชอบระบบสารสนเทศ ต้องดำเนินการติดตั้งระบบต่างๆ ของกรมฯ โดยปฏิบัติตามขั้นตอน ดังนี้ (แนวปฏิบัติสำหรับการติดตั้งระบบ)

(๑) กำหนดพื้นที่หรือบริเวณที่จะทำการติดตั้งให้อยู่ในบริเวณที่มีความมั่นคงปลอดภัยเพียงพอ

(๒) ตรวจสอบปริมาณกระแสไฟฟ้าที่ระบบต้องการ และสำรองไฟฟ้าให้เพียงพอต่อความต้องการ

(๓) ติดตั้งเครื่องสำรองไฟฟ้าที่สามารถรองรับการทำงานของระบบได้อย่างเพียงพอ หรือตรวจสอบว่าเครื่องสำรองไฟฟ้าปัจจุบันยังสามารถรองรับระบบใหม่ที่จะทำการติดตั้งหรือไม่

(๔) กำหนดแผนการติดตั้งสำหรับระบบ รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้าในระยะเวลาที่นานเพียงพอ เช่น แผนการติดตั้งฮาร์ดแวร์ ซอฟต์แวร์ และอื่นๆ

(๕) ปฏิบัติตามคู่มือหรือเอกสารที่เกี่ยวข้องกับการติดตั้งซอฟต์แวร์บนระบบ เช่น คู่มือการติดตั้งเว็บเซิร์ฟเวอร์ คู่มือการติดตั้งระบบบริหารจัดการฐานข้อมูล เป็นต้น

(๖) ดำเนินการติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ต่างๆ ในระบบที่ขออนุมัติการติดตั้งเพื่อปรับปรุงหรือแก้ไขให้ระบบมีความสมบูรณ์และมั่นคงปลอดภัย

(๗) ตรวจสอบและปิดพอร์ตต่างๆ ที่ไม่มีความจำเป็นในการใช้งาน

(๘) กรณีการติดตั้งระบบงาน

(ก) ห้ามติดตั้งซอฟต์แวร์คอมไพเลอร์บนระบบ ยกเว้นในกรณีที่ระบบงานต้องเรียกใช้ซอฟต์แวร์คอมไพเลอร์ในขณะที่ทำงาน

(ข) ห้ามติดตั้งซอร์สโค้ดของระบบงานลงไปในระบบ ยกเว้นในกรณีที่ระบบงานต้องเรียกใช้ซอร์สโค้ดในขณะที่ทำงาน

(๙) อ่านและปฏิบัติตามเงื่อนไขหรือข้อตกลงการใช้งานซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งอย่างเคร่งครัด ซึ่งรวมถึงซอฟต์แวร์ประเภทฟรีแวร์และแชร์แวร์ด้วย

(๑๐) ก่อนการติดตั้งโปรแกรมอรรถประโยชน์บนระบบให้ปฏิบัติตามแนวทางดังนี้ก่อนการติดตั้ง

(ก) ศึกษาหรือทดสอบก่อนว่าเป็นซอฟต์แวร์ที่น่าเชื่อถือหรือไม่

(ข) มีการประมวลผลที่ถูกต้องหรือไม่

(ค) มีผู้ใช้งานอยู่ในจำนวนที่มากพอหรือไม่

(ง) มีผู้ผลิตซอฟต์แวร์อย่างชัดเจนหรือไม่

(จ) มีผู้ร่วมอาชีพหรือสายงานเดียวกันด้านสารสนเทศให้การรับรองหรือไม่

(ฉ) สามารถรายงานผลกลับไปยังผู้ผลิตซอฟต์แวร์หากพบข้อผิดพลาดจากการใช้งานได้หรือไม่

(ช) มีการใช้งานกันมาเป็นระยะเวลานานพอแล้วหรือไม่

หากพบว่าคำตอบโดยรวมอยู่ในทางบวก จึงจะดำเนินการติดตั้ง

(๑๑) ตรวจสอบและลบบัญชีผู้ใช้งานในระบบที่ไม่ได้มีการใช้งาน ซึ่งรวมถึงบัญชีต่างๆ ที่กำหนดหรือติดมากับซอฟต์แวร์ที่ได้รับเหล่านั้น

(๑๒) ตรวจสอบและติดตั้งระบบป้องกันไวรัสสำหรับระบบที่ทำการติดตั้ง

(๑๓) จำกัดการเชื่อมต่อทางเครือข่ายเพื่ออนุญาตให้เฉพาะกลุ่มผู้ใช้งานที่เกี่ยวข้องเท่านั้น จึงจะสามารถเชื่อมต่อและล็อกอินเข้าสู่ระบบที่ทำการติดตั้งนั้นได้

ข้อ ๓๑ เมื่อมีความจำเป็นต้องติดตั้ง เปลี่ยนแปลง แก้ไข หรือปรับปรุงระบบต่างๆ ของกรมฯ ให้ผู้รับผิดชอบระบบสารสนเทศ ปฏิบัติ ดังนี้ (แนวปฏิบัติสำหรับการเปลี่ยนแปลงระบบ)

(๑) บันทึกคำขออนุมัติและรายละเอียดที่เกี่ยวข้องของการเปลี่ยนแปลงระบบ

(๒) หารือการเปลี่ยนแปลงนั้นกับผู้บังคับบัญชาและผู้ที่เกี่ยวข้อง

(๓) พิจารณาระดับผลกระทบและความเร่งด่วนของการเปลี่ยนแปลงนั้น

(๔) จัดทำแผนดำเนินการเปลี่ยนแปลง (แผนดำเนินการเปลี่ยนแปลง (Rollout Plan) หมายถึง แผนการติดตั้ง แผนการทดสอบ และ/หรือ แผนการแจ้งกำหนดการต่างๆ ให้ผู้ที่เกี่ยวข้องได้รับทราบ)

(๕) จัดทำแผนถอยหลังกลับพร้อมทั้งสำรองข้อมูลต่างๆ ที่เกี่ยวข้องของระบบนั้นตามความจำเป็น (แผนการถอยหลังกลับ (Fallback Plan) หมายถึง แผนการย้อนกลับไปสู่สถานะก่อนดำเนินการเปลี่ยนแปลง ส่วนใหญ่แผนนี้จะหมายถึงการสำรองข้อมูลต่างๆ ที่จำเป็นก่อนดำเนินการเปลี่ยนแปลง ทั้งข้อมูลในฐานข้อมูล ข้อมูล Configuration ของระบบ ตัวซอฟต์แวร์ของระบบ และข้อมูลอื่นๆ ที่เกี่ยวข้อง หากติดตั้งไม่สำเร็จ จะได้กลับไปใช้สถานะของระบบเดิมก่อนการเปลี่ยนแปลงได้)

(๖) ประกาศช่วงระยะเวลาการติดตั้งระบบให้ผู้ใช้งานได้รับทราบก่อนล่วงหน้า

(๗) ทดสอบการเปลี่ยนแปลงนั้นกับระบบทดสอบ (สำหรับกรณีที่สามารถทำได้) รวมทั้งร่วมกับผู้ใช้งานและผู้ที่เกี่ยวข้องในการทดสอบจนกระทั่งมั่นใจว่าไม่มีปัญหาใดๆ

(๘) ติดตั้งบนระบบจริง

(๙) เปิดระบบใช้งาน

(๑๐) ประกาศแจ้งให้ผู้ใช้งานและผู้ที่เกี่ยวข้องได้รับทราบตามความจำเป็น

(๑๑) เฝ้าระวังว่าระบบมีปัญหาข้างเคียงใดๆ เกิดขึ้นหรือไม่

ข้อ ๓๒ ผู้รับผิดชอบระบบสารสนเทศ พิจารณาบรรจุคุณสมบัติด้านความมั่นคงปลอดภัยสำหรับการล็อกอินเข้าใช้ระบบต่างๆ ของกรมฯ ให้มากที่สุดเท่าที่จะทำได้ดังนี้ (แนวปฏิบัติสำหรับคุณสมบัติด้านความมั่นคงปลอดภัยสำหรับการล็อกอินเข้าใช้ระบบ)

(๑) การไม่แสดงชื่อหรือรายละเอียดของระบบจนกว่าจะล็อกอินสำเร็จ

(๒) การไม่มีหรือไม่แสดงฟังก์ชั่นให้การช่วยเหลือในระหว่างที่ทำการ ล็อกอิน

(๓) การตัดการเชื่อมต่อหลังจากที่ทำการล็อกอินไม่สำเร็จเกินกว่า ๓ ครั้ง

(๔) การบันทึกข้อมูลความสำเร็จหรือการล้มเหลวในการล็อกอินแต่ละครั้งของผู้ใช้งาน (เพื่อใช้ในการตรวจสอบในภายหลัง)

(๕) การไม่แสดงข้อมูลรหัสผ่านให้เห็นบนจอในขณะที่ผู้ใช้งานใส่ข้อมูลรหัสผ่านของตน

(๖) การแสดงข้อความเตือนที่หน้าจอภายหลังจากการล็อกอินเสร็จสิ้น ข้อความเตือนดังกล่าว ได้แก่ “ระบบงานนี้เป็นระบบที่เป็นสินทรัพย์ของกรมส่งเสริมคุณภาพสิ่งแวดล้อม การใช้งานจะต้องได้รับการอนุมัติก่อนเท่านั้นจึงจะสามารถใช้งานได้ ผู้ที่ไม่ได้รับสิทธิและเข้ามาใช้ระบบงาน หากมีการตรวจพบและเป็นความผิดจะดำเนินการลงโทษทางวินัย หรือดำเนินการทางกฎหมายตามความเหมาะสม กรมส่งเสริมคุณภาพสิ่งแวดล้อมมีสิทธิในการตรวจสอบพฤติกรรมการใช้งานในระหว่างที่ผู้ใช้งานใช้ระบบงานนี้โดยไม่ถือว่าเป็นการละเมิดความเป็นส่วนตัว”

ข้อ ๓๓ ผู้รับผิดชอบระบบสารสนเทศ เฝ้าระวังและติดตามการทำงานของระบบต่างๆ ของกรมฯ ดังนี้

(๑) จัดทำแผนการเฝ้าระวังและติดตามการทำงานของระบบโดย

(ก) กำหนดชื่อของระบบที่มีจำเป็นต้องเฝ้าระวังและติดตามอย่างสม่ำเสมอ

(ข) กำหนดประเภทของข้อมูลปริมาณการใช้ทรัพยากรบนระบบที่จำเป็นต้องเฝ้าระวังและติดตาม เช่น

- ร้อยละของการใช้ CPU
- ร้อยละของการใช้หน่วยความจำ

- ร้อยละของการใช้ Hard Disk
- ร้อยละของปริมาณการใช้เครือข่าย

เป็นต้น และกำหนดค่าปริมาณการใช้ทรัพยากรสูงสุดบนระบบที่ยอมรับได้ (หากมีการใช้ทรัพยากรใกล้เคียงหรือสูงกว่าปริมาณสูงสุดที่กำหนดไว้ ต้องดำเนินการแจ้งให้ผู้บังคับบัญชาได้รับทราบเพื่อวางแผนปรับปรุงทรัพยากรของระบบเพิ่มเติมต่อไป)

(ค) กำหนดความถี่ในการเข้าตรวจสอบ ว่าระบบยังทำงานตามปกติหรือไม่ (ระบบมีปัญหาหรือหยุดให้บริการหรือไม่)

(ง) กำหนดความถี่ในการเข้าตรวจสอบปริมาณการใช้ทรัพยากรบนระบบ ว่ายังมีเพียงพอต่อการใช้งานหรือไม่ (โดยดูเปรียบเทียบกับค่าปริมาณสูงสุดที่กำหนดไว้)

(จ) กำหนดผู้รับผิดชอบในการตรวจสอบ

(๒) ปฏิบัติตามแผนการเฝ้าระวังฯ ติดตามและตรวจสอบว่าระบบทำงานตามปกติหรือไม่

(๓) ตามแผนการเฝ้าระวังฯ ติดตามและตรวจสอบระดับการใช้ทรัพยากรว่ามีการใช้ทรัพยากรตามปกติหรือไม่ (ไม่ควรเกินค่าปริมาณการใช้ทรัพยากรสูงสุดที่กำหนดไว้)

(๔) ภายหลังการติดตามและตรวจสอบ กรณีที่พบปัญหาที่ต้องแก้ไข ดำเนินการแก้ไขปัญหาที่พบตามความเหมาะสม

(๕) รายงานให้ผู้บังคับบัญชาได้รับทราบสำหรับกรณีที่ปัญหาที่เกิดขึ้นมีความสำคัญหรือมีผลกระทบสูง

หมวด ๖
แนวปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย

ข้อ ๓๔ ผู้รับผิดชอบระบบสารสนเทศ ต้องบริหารจัดการความมั่นคงปลอดภัยบนเครือข่ายของกรมฯ ดังนี้

(๑) จัดแบ่งเครือข่ายของกรมฯ ออกเป็นแต่ละวงเครือข่ายโดยใช้แนวทางปฏิบัติดังนี้

(ก) แยกตามหน่วยงานภายในของกรมฯ

(ข) แยกตามชั้นความลับของข้อมูล (กล่าวคือ จัดให้เครื่องลูกข่ายที่มีความจำเป็นต้องเข้าถึงข้อมูลลับเดียวกันอยู่ในวงเครือข่ายเดียวกัน)

(ค) แยกตามลักษณะงานของกรมฯ (กล่าวคือ จัดให้เครื่องลูกข่ายที่มีลักษณะงานเดียวกันอยู่ในวงเครือข่ายเดียวกัน)

(ง) แยกวงเครือข่ายต่างหากสำหรับเครื่องเซิร์ฟเวอร์ให้บริการระบบงานต่างๆ ของกรมฯ

(จ) แยกวงเครือข่ายของเครื่องเซิร์ฟเวอร์ให้บริการระบบงานภายในและภายนอกออกจากกัน

(๒) จัดทำระบบสำหรับการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย โดยที่ระบบควรสามารถกำหนดให้ผู้ใช้งานตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยตามแนวปฏิบัติสำหรับการตั้งและใช้งานรหัสผ่านของกรมฯ

(๓) ใช้วิธีการทางเทคนิคบนไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่นๆ เพื่อจำกัดการเข้าถึงหรือจำกัดการเชื่อมต่อทางเครือข่ายของหน่วยงานภายในและผู้ใช้งานให้เป็นไปตามความจำเป็นในการเข้าถึงระบบงานต่างๆ ของกรมฯ หรือให้สอดคล้องกับตารางควบคุมการเข้าถึงระบบ

(๔) ใช้วิธีการทางเทคนิคบนไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่นๆ จำกัดเส้นทางบนเครือข่ายที่กรมฯ ไม่อนุญาตให้ใช้งาน เพื่อกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๕) ตรวจสอบและปิดพอร์ตของระบบและอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๖) ตรวจสอบ ติดตาม และเฝ้าระวังการทำงานของเครือข่ายอย่างสม่ำเสมอเพื่อดูว่าทำงานตามปกติหรือไม่

(๗) กำหนดให้เฉพาะเครื่องคอมพิวเตอร์ของผู้ดูแลเครือข่ายที่สามารถเชื่อมต่อเข้าไปบริหารจัดการระบบและอุปกรณ์เครือข่ายของกรมฯ ได้

(๘) กำหนดให้ใช้ MAC Address และ/หรือ IP Address เป็นข้อมูลในการระบุอุปกรณ์บนเครือข่าย เพื่อบ่งชี้อุปกรณ์ที่ได้รับอนุญาตให้เชื่อมต่อเข้าไปยังเครือข่ายของกรมฯ และใช้วิธีการทางเทคนิคที่เหมาะสมเพื่อควบคุมการเข้าถึงอุปกรณ์เครือข่ายเหล่านั้น

(๙) สำหรับเครือข่ายของกรมฯ ที่มีการเชื่อมโยงโดยตรงไปยังเครือข่ายของหน่วยงานภายนอกอื่นๆ ให้ติดตั้งไฟร์วอลล์กั้นไว้ เพื่อป้องกันเครือข่ายของกรมฯ จากการถูกบุกรุก

(๑๐) ติดตั้งระบบป้องกันการบุกรุกในส่วนของเครือข่ายที่สำคัญของกรมฯ เพื่อตรวจสอบ หรือตรวจจับความพยายามในการบุกรุกระบบ หรือความผิดปกติทางเครือข่ายอื่นๆ

(๑๑) ป้องกันไม่ให้เครือข่ายในส่วนของอินเทอร์เน็ตสามารถมองเห็นหมายเลขไอพีแอดเดรสของเครือข่ายภายในหรือของระบบงานภายในของกรมฯ เพื่อป้องกันไม่ให้บุคคลภายนอกสามารถล่วงรู้ข้อมูลเกี่ยวกับโครงสร้างของเครือข่ายและระบบงานภายในของกรมฯ

(๑๒) จัดทำแผนผังเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดของเครือข่ายตามสำนักงานและอาคารทั้งหมดของกรมฯ ที่ผู้ดูแลเครือข่ายรับผิดชอบ และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

ข้อ ๓๕ ผู้รับผิดชอบระบบสารสนเทศ กำหนดมาตรการความมั่นคงปลอดภัยสำหรับการใช้งาน VPN เพื่อเข้าถึงระบบงานของกรมฯ จากระยะไกล ดังนี้ (แนวปฏิบัติสำหรับการบริหารจัดการการเข้าถึงเครือข่ายจากระยะไกล)

(๑) จัดทำระบบสำหรับการพิสูจน์ตัวตนบนหรือผ่าน VPN ที่มีความมั่นคงปลอดภัยสูง ซึ่งต้องใช้การเข้ารหัสข้อมูลในช่วงที่ทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน และ/หรือ บังคับการตั้งรหัสผ่านที่มีความยาวอย่างน้อย ๘ ตัวอักษร

(๒) จัดทำระบบรับ-ส่งข้อมูลจากต้นทางมายังปลายทางที่ต้องใช้การเข้ารหัสข้อมูล

(๓) ตรวจสอบและปิดพอร์ตบนระบบและอุปกรณ์เครือข่ายต่างๆ ที่เกี่ยวข้องเพื่อให้เหลือเฉพาะพอร์ตที่จำเป็นต่อการใช้งาน VPN

(๔) จัดให้มีการขออนุมัติการใช้งานจากผู้มีอำนาจก่อน กำหนดให้ผู้ใช้งานต้องแสดงเหตุผลหรือความจำเป็นในการใช้งานและระยะเวลาการใช้งาน ลงทะเบียนผู้ใช้งานนั้น กำหนดบัญชีผู้ใช้งานและรหัสผ่านที่มีความมั่นคงปลอดภัยเพื่อใช้เป็นข้อมูลในการยืนยันตัวตนของผู้ใช้งาน และควบคุมการใช้งานหรือเข้าถึงให้เป็นไปอย่างเข้มงวด กรณีผู้ร้องขอใช้งานคือผู้ให้บริการภายนอก การอนุมัติให้ใช้งานต้องจำกัดระยะเวลาที่ยังคงสามารถใช้งานได้ไม่เกินระยะเวลาของสัญญาจ้าง

(๕) กำหนดให้ผู้ใช้งานต้องใช้ VPN ที่กรมฯ จัดเตรียมไว้ให้ ก่อนเข้าใช้ระบบงานภายในของกรมฯ

(๖) กำหนดให้ผู้ใช้งานต้องใช้รหัสผ่านที่มีความยาวอย่างน้อย ๘ ตัวอักษร

(๗) กำหนดให้มีการทบทวนสิทธิการเข้าถึงระบบสำหรับการพิสูจน์ตัวตนดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๓๖ ผู้รับผิดชอบระบบสารสนเทศ ควบคุมการเข้าถึงและใช้งานระบบเครือข่ายไร้สายภายในกรมฯ ดังนี้

(๑) แยกวงเครือข่ายของระบบเครือข่ายไร้สายไว้เป็นอีกวงหนึ่งต่างหาก

(๒) จัดให้มีการขออนุมัติการใช้งานจากผู้มีอำนาจก่อน

(๓) กรณีบุคคลภายนอก ผู้รับจ้าง ที่ปรึกษา หรือบุคคลภายนอกอื่นๆ ขออนุญาตใช้งานเครือข่ายซึ่งรวมถึงระบบเครือข่ายไร้สายของกรมฯ ให้จำกัดระยะเวลาการใช้งานเท่าที่จำเป็น

หมวด ๗
แนวปฏิบัติในการพัฒนาระบบให้มีความมั่นคงปลอดภัย

ข้อ ๓๗ ผู้รับผิดชอบระบบสารสนเทศ ควบคุมการดำเนินโครงการพัฒนาหรือปรับปรุงระบบเทคโนโลยีสารสนเทศ ดังนี้

(๑) ให้ระบุวัตถุประสงค์ด้านความมั่นคงปลอดภัยไว้ในแต่ละโครงการ

(๒) ประเมินความเสี่ยงที่จะทำให้เกิดความไม่สอดคล้องกับวัตถุประสงค์ที่กำหนดไว้

(๓) กำหนดความต้องการด้านความมั่นคงปลอดภัยเพื่อลดความเสี่ยงที่ประเมิน

(๔) กำหนดแผนดำเนินการโครงการโดยพิจารณาความต้องการด้านความมั่นคงปลอดภัยเข้าไว้เป็นส่วนหนึ่งของแผนด้วย

(๕) ติดตาม กำกับ ดูแลกิจกรรมการดำเนินการของโครงการให้เป็นไปตามแผนที่กำหนดไว้

ข้อ ๓๘ ผู้รับผิดชอบระบบสารสนเทศ ควบคุมการพัฒนาหรือจัดหาระบบงานตามหลักการวิศวกรรมด้านความมั่นคงปลอดภัยสำหรับระบบ ดังนี้

(๑) ออกแบบระบบให้มีระดับการป้องกันมากกว่าหนึ่งระดับ

(๒) ออกแบบระบบให้มีความเรียบง่ายและสามารถเข้าใจได้โดยผู้อื่น

(๓) ปิดช่องโหว่ต่างๆ ของระบบที่ผู้บุกรุกสามารถตรวจสอบพบจากภายนอก

(๔) ตั้งค่าระบบเริ่มต้นให้มีความมั่นคงปลอดภัย

(๕) กรณีระบบเกิดการล้มเหลว ระบบต้องมีกลไลการป้องกันไม่ให้ผู้ไม่ประสงค์ดีสามารถเข้าระบบได้

(๖) เริ่มต้นการทำงานของระบบโดยไม่ใช้ระดับสิทธิ์ของผู้ดูแลระบบ

(๗) จัดให้มีระบบป้องกันการบุกรุกระบบงานที่จะพัฒนาหรือจัดหา

(๘) เมื่อมีการเชื่อมต่อกับระบบหรือบริการอื่น ต้องตรวจสอบความมั่นคงปลอดภัยของระบบหรือบริการนั้นก่อนดำเนินการเชื่อมต่อ

(๙) กรณีระบบมีช่องโหว่หรือปัญหาด้านความมั่นคงปลอดภัย พิจารณาหาสาเหตุและดำเนินการแก้ไขกับช่องโหว่นั้นอย่างเหมาะสม เพื่อไม่ก่อให้เกิดปัญหาสืบเนื่องในภายหลัง

ข้อ ๓๙ ผู้รับผิดชอบระบบสารสนเทศ ควบคุมการพัฒนาหรือจัดหาระบบงานเพื่อให้ระบบที่ได้มีความมั่นคงปลอดภัยเพียงพอ ดังนี้

(๑) จัดให้มีการประเมินความเสี่ยงและระบุข้อกำหนดด้านความมั่นคงปลอดภัย (Security Requirements) ของระบบงานที่จะจัดหาหรือพัฒนาอย่างเป็นลายลักษณ์อักษร ข้อกำหนดดังกล่าวอย่างน้อยควรครอบคลุมประเด็นสำคัญต่างๆ ดังนี้

(ก) คุณสมบัติของการล็อกอินเข้าสู่ระบบงานที่มีความมั่นคงปลอดภัย (ดูในแนวปฏิบัติสำหรับคุณสมบัติด้านความมั่นคงปลอดภัยสำหรับการล็อกอินเข้าใช้ระบบ)

(ข) การกำหนดหรือตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงระบบงานโดยให้สอดคล้องกับแนวปฏิบัติสำหรับการตั้งและใช้งานรหัสผ่านของกรมฯ

(ค) กรณีระบบงานมีข้อมูลที่มีความสำคัญ เช่น ข้อมูลลับ ข้อมูลส่วนบุคคล และข้อมูลนั้นจะมีการส่งผ่านไปมาบนเครือข่ายระหว่างเครื่องลูกข่ายกับเครื่องเซิร์ฟเวอร์สำหรับให้บริการระบบงาน พิจารณากำหนดให้มีการเข้ารหัสข้อมูลที่มีการรับส่งนั้น

(ง) กรณีระบบงานมีความจำเป็นต้องตรวจสอบความถูกต้องของข้อมูลที่ได้รับว่าถูกเปลี่ยนแปลงหรือแก้ไขในระหว่างทางที่ส่งมาหรือไม่ หรือมีความจำเป็นต้องตรวจสอบตัวตนของผู้ส่งข้อมูล พิจารณากำหนดให้มีการใช้การลงลายมือชื่อดิจิทัล

(จ) กรณีระบบงานมีความเสี่ยงเรื่องการถูกสวมรอยเข้าใช้ระบบโดยผู้อื่น เช่น ในขณะที่ผู้ใช้งานไม่อยู่ที่เครื่องช่วงระยะเวลาหนึ่ง พิจารณากำหนดให้มีการตัดและหมดเวลาการใช้งานหลังจากที่ไม่ได้ใช้ระบบเกินกว่าระยะเวลาตามที่กำหนดไว้ เช่น ๑๕-๓๐ นาที

(ฉ) การบันทึกข้อมูลล็อกเพื่อแสดงการเข้าถึงหรือใช้ระบบงาน อย่างน้อยข้อมูลล็อกควรมีชื่อบัญชีผู้ใช้งานที่ล็อกอินเข้าใช้ระบบ หมายเลขไอพีแอดเดรสของเครื่องของผู้ใช้งานนั้น วันเวลาที่เข้าใช้ระบบ และความสำเร็จหรือไม่สำเร็จในการล็อกอินของผู้ใช้งาน

(๒) พัฒนาหรือจัดหาระบบงานให้สอดคล้องตามข้อกำหนดด้านความมั่นคงปลอดภัยในข้อที่แล้ว

(๓) พัฒนาหรือจัดหาระบบงานเพื่อให้มีหน้าจอสำหรับผู้ดูแลหรือผู้พัฒนาระบบเพื่อทำการบันทึก เปลี่ยนแปลง แก้ไข หรือถอดถอนสิทธิของผู้ใช้งานได้

(๔) กำหนดให้มีการจัดทำแผนการทดสอบระบบ นำเสนอแผนดังกล่าวเพื่อพิจารณาอนุมัติโดยผู้มีอำนาจ ดำเนินการทดสอบตามแผนฯ บันทึกผลการทดสอบ และรายงานผลการทดสอบให้ผู้มีอำนาจได้รับทราบ เพื่อให้คำแนะนำในการ

ปรับปรุงหรือแก้ไขต่างๆ ตามความจำเป็น แผนการทดสอบที่จัดทำอย่างน้อยประกอบด้วย

(ก) แผนการทดสอบ UAT (User Acceptance Test)

(ข) แผนการทดสอบ System Integration Test

(ค) แผนการทดสอบข้อกำหนดด้านความมั่นคงปลอดภัย (Security Test)

ผู้พัฒนาระบบต้องนำเสนอแผนการทดสอบ UAT โดยอย่างน้อยให้แสดงเป็นหน้าจอต่างๆ ที่จะทำการทดสอบและข้อมูลตัวอย่างที่จะใช้ในการทดสอบกับหน้าจอเหล่านั้น ทั้งข้อมูลที่คาดว่าระบบจะทำงานอย่างถูกต้องและที่คาดว่าระบบจะแสดงข้อผิดพลาดในการทำงาน

(๕) ไม่อนุญาตการนำข้อมูลสำคัญของกรมฯ เช่น ข้อมูลลับ ข้อมูลส่วนบุคคล ข้อมูลใช้ภายในเท่านั้น ไปใช้ในการทดสอบกับระบบงานเพื่อป้องกันการรั่วไหลของข้อมูล เว้นเสียแต่ได้รับการอนุมัติจากผู้บังคับบัญชาระดับสูงก่อน และหากเป็นไปได้ ให้ตัดข้อมูลส่วนที่เป็นความลับ หรือข้อมูลส่วนบุคคลทิ้งไป ให้เหลือเฉพาะส่วนที่เพียงพอต่อการนำไปใช้ในการทดสอบ

ข้อ ๔๐ ภายหลังจากที่ระบบงานพัฒนาเสร็จแล้วและพร้อมติดตั้ง ผู้รับผิดชอบระบบสารสนเทศ ควบคุมการติดตั้งระบบลงไปยังเครื่องเซิร์ฟเวอร์ให้บริการระบบงาน ดังนี้ (แนวปฏิบัติสำหรับการติดตั้งระบบ)

(๑) กำหนดให้เฉพาะผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายที่มีความชำนาญเท่านั้น ที่จะเป็นผู้ดำเนินการติดตั้ง

(๒) ในกรณีที่เป็นการติดตั้งระบบเพื่อทดแทนระบบงานเดิม ให้ทำการสำรองข้อมูลที่จำเป็น เช่น ฐานข้อมูล ซอฟต์แวร์ ค่าคอนฟิกกูเรชัน หรืออื่นๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งทำไม่สำเร็จ จะได้สามารถถอยหลังกลับไปใช้ระบบงานเดิมได้

(๓) ในกรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบงานเดิมไปสู่ข้อมูลบนระบบงานที่จะทำการติดตั้ง ให้กำหนดแผนการถ่ายโอนหรือแปลงข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ ถ่ายโอนข้อมูลตามแผนฯ และร่วมกับผู้ใช้งานเพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้องและครบถ้วนหรือไม่

(๔) กำหนดพื้นที่หรือบริเวณที่จะทำการติดตั้งระบบที่มีความมั่นคงปลอดภัยทางกายภาพเพียงพอ

(๕) คำนวณและตรวจสอบปริมาณความต้องการใช้กระแสไฟฟ้า และเครื่องสำรองไฟฟ้าให้เพียงพอกับความต้องการของระบบ

(๖) ปฏิบัติตามคู่มือหรือเอกสารที่เกี่ยวข้องกับการติดตั้งซอฟต์แวร์บนระบบ เช่น คู่มือการติดตั้งเว็บเซิร์ฟเวอร์ คู่มือการติดตั้งระบบบริหารจัดการฐานข้อมูล เป็นต้น

(๗) ดำเนินการติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ต่างๆ ในระบบ (เช่น ซอฟต์แวร์ระบบปฏิบัติการ ระบบบริหารจัดการฐานข้อมูล) ที่ขออนุมัติการติดตั้งเพื่อปรับปรุงหรือแก้ไขให้ระบบมีความสมบูรณ์และมั่นคงปลอดภัย

(๘) ตรวจสอบและปิดพอร์ตต่างๆ บนระบบที่ไม่มีความจำเป็นในการใช้งาน

(๙) สำหรับซอฟต์แวร์ในระบบที่จะทำการติดตั้งประเภทฟรีแวร์หรือแชร์แวร์ ตรวจสอบก่อนที่จะทำการติดตั้งว่าสามารถใช้งานได้ด้วยเงื่อนไขอะไรบ้าง และจะต้องไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตซอฟต์แวร์นั้น

(๑๐) ตรวจสอบและลบบัญชีผู้ใช้งานในระบบที่ไม่ได้มีการใช้งาน ซึ่งรวมถึงบัญชีผู้ใช้งานต่างๆ ที่มีมากับซอฟต์แวร์ที่ได้รับเหล่านั้น

(๑๑) กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารี่สำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความปลอดภัย และจำกัดการเข้าถึงโดยผู้ที่เกี่ยวข้องเท่านั้น

(๑๒) กำหนดวิธีเรียกเวอร์ชั่นของซอร์สโค้ดและไลบรารี่สำหรับซอฟต์แวร์ของระบบงาน เมื่อมีการเปลี่ยนแปลงซอร์สโค้ดหรือไลบรารี่ จะต้องเปลี่ยนแปลงเวอร์ชั่นให้ถูกต้องตามวิธีการที่กำหนดไว้

ข้อ ๔๑ ในการขอเปลี่ยนแปลงระบบงานภายหลังจากที่ได้มีการติดตั้งและใช้ระบบงานไปแล้ว ผู้รับผิดชอบระบบสารสนเทศ กำหนดให้มีการขออนุมัติการเปลี่ยนแปลงระบบงาน ดังนี้ (แนวปฏิบัติสำหรับการเปลี่ยนแปลงระบบงานตามความต้องการของผู้ใช้งาน)

(๑) กำหนดให้มีการทำบันทึกข้อความเพื่อขออนุมัติเปลี่ยนแปลงระบบงาน เช่น ขอเพิ่มรายงานในระบบ เพิ่มฟังก์ชั่นการทำงาน เป็นต้น โดยผ่านผู้บังคับบัญชาในสายงานเพื่อพิจารณาอนุมัติ

(๒) พิจารณาปริมาณการเปลี่ยนแปลง ผลกระทบของการเปลี่ยนแปลง ความเร่งด่วน ความเหมาะสม และค่าใช้จ่ายในการดำเนินการ

(๓) อนุมัติตามที่ร้องขอ หากเห็นสมควร

(๔) จัดประชุมกับผู้ร้องขอเพื่อรวบรวมความต้องการด้านระบบงานโดยละเอียดและสรุปความต้องการทั้งหมด

(๕) เริ่มต้นพัฒนาระบบงานตามความต้องการที่ได้รับ

ข้อ ๔๒ ผู้รับผิดชอบระบบสารสนเทศ กำหนดให้มีการทบทวนการทำงานของระบบงานในระหว่างหรือภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน ดังนี้ (แนวปฏิบัติสำหรับ

การทบทวนการทำงานของระบบงานภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน)

(๑) ปฏิบัติตามแนวปฏิบัติสำหรับการเปลี่ยนแปลงระบบ เพื่อขออนุมัติการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน

(๒) ในระหว่างที่มีการทดสอบระบบโดยผู้ใช้งาน ให้ตรวจสอบว่าฟังก์ชั่นการทำงานของระบบสามารถใช้งานได้ตามปกติและครบถ้วน

ข้อ ๔๓ ผู้รับผิดชอบระบบสารสนเทศ กำหนดให้มีการบริหารจัดการกุญแจที่ใช้สำหรับการเข้ารหัสข้อมูล และ/หรือ การลงลายมือชื่อดิจิทัล ดังนี้

(๑) กำหนดให้มีการขออนุมัติใช้งานกุญแจสำหรับการเข้ารหัสจากผู้มีอำนาจ โดยต้องผ่านการรับรองของผู้บังคับบัญชาของผู้ที่ต้องการใช้งานกุญแจ

(๒) กำหนดให้มีการระมัดระวังการส่งมอบกุญแจให้ถึงมือผู้ร้องขอโดยตรง ห้ามส่งมอบกุญแจโดยผ่านทางผู้อื่น

(๓) กำหนดให้ผู้ร้องขอพิจารณาปฏิบัติตามแนวปฏิบัติสำหรับการจัดการกับข้อมูลลับ (เนื่องจากกุญแจถือเป็นข้อมูลลับประเภทหนึ่ง)

(๔) กำหนดให้ผู้ร้องขอจัดเก็บกุญแจและสำเนาของกุญแจของตนเองไว้ในสถานที่ที่มีความปลอดภัย

(๕) กำหนดให้ผู้ร้องขอจำกัดการสำเนากุญแจที่ได้รับให้น้อยที่สุดเท่าที่จะทำได้

(๖) เมื่อได้รับแจ้งจากผู้เป็นเจ้าของกุญแจ เกี่ยวกับกุญแจถูกเปิดเผยโดยไม่ได้รับอนุญาต หรือกุญแจสูญหาย ให้ยกเลิกกุญแจนั้นโดยทันทีเพื่อไม่ให้ผู้อื่นสามารถนำกุญแจไปใช้งานได้

(๗) เมื่อมีความจำเป็นต้องทำลายกุญแจ ให้ปฏิบัติตามแนวปฏิบัติสำหรับการทำลายข้อมูลบนสื่อบันทึกข้อมูล

หมวด ๘
แนวปฏิบัติในการจัดการการสำรองข้อมูลของระบบและการบริหารจัดการการกู้คืนระบบ

ข้อ ๔๔ ผู้รับผิดชอบระบบสารสนเทศ ดำเนินการจัดการเกี่ยวกับการสำรองและกู้คืนข้อมูล ดังนี้ (แนวปฏิบัติสำหรับการสำรองข้อมูลและทดสอบกู้คืนข้อมูล)

(๑) กำหนดแผนการสำรองข้อมูลของระบบสำคัญ ดังนี้

(ก) กำหนดระบบสำคัญ (เช่น ระบบงานและอุปกรณ์เครือข่าย) ที่จำเป็นต้องสำรองข้อมูลไว้

(ข) กำหนดผู้รับผิดชอบในการสำรองข้อมูล

(ค) กำหนดประเภทของข้อมูลที่จำเป็นต้องสำรองข้อมูลเก็บไว้ (อย่างน้อยต้องประกอบด้วย ข้อมูลในฐานข้อมูลของระบบ ข้อมูลสำหรับตัวระบบ เช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง ข้อมูลล็อก ข้อมูลบัญชีผู้ใช้งานในระบบ เป็นต้น)

(ง) กำหนดความถี่ในการสำรองข้อมูลของระบบ

(๒) ปฏิบัติตามแผนการสำรองข้อมูลที่กำหนดไว้

(๓) ตรวจสอบว่าการสำรองที่เกิดขึ้นนั้นสำเร็จและครบถ้วนหรือไม่ หากไม่สำเร็จ ให้หาสาเหตุ ดำเนินการแก้ไข และดำเนินการใหม่อีกครั้งหนึ่ง

(๔) นำข้อมูลที่สำรองไว้นั้นไปเก็บไว้นอกสถานที่อย่างน้อยอย่างละ ๑ ชุด

(๕) ทดสอบกู้คืนข้อมูลที่สำรองเก็บไว้บนสื่อบันทึกข้อมูลอย่างน้อยปีละ ๑ ครั้ง เพื่อดูว่าข้อมูลยังคงสามารถใช้งานได้ตามปกติหรือไม่ เช่น โดยการเปิดดูข้อมูลบนสื่อบันทึกข้อมูลว่าสามารถเรียกดูหรือใช้งานได้หรือไม่

ข้อ ๔๕ ผู้รับผิดชอบระบบสารสนเทศ ดำเนินการทดสอบการกู้คืนระบบ หรือดำเนินการกู้คืนระบบ ดังนี้ (แนวปฏิบัติสำหรับการกู้คืนระบบจากข้อมูลหรือซอฟต์แวร์ที่มีการสำรองเก็บไว้)

(๑) จัดหาเครื่องหรืออุปกรณ์คอมพิวเตอร์ที่จำเป็นต้องใช้ในการติดตั้งระบบ

(๒) นำข้อมูลหรือซอฟต์แวร์ที่มีการสำรองเก็บไว้มาดำเนินการติดตั้งเรียงตามลำดับที่เหมาะสมนับตั้งแต่ระบบปฏิบัติการและอื่นๆ ตามลำดับ (โดยปฏิบัติตามคู่มือการติดตั้งระบบที่ได้จัดทำไว้ก่อน)

(๓) ทดสอบการใช้งานระบบภายหลังการติดตั้ง

(๔) ประสานงานขอให้ผู้ใช้งานร่วมทำการทดสอบระบบด้วย

(๕) เปิดใช้ระบบ

ข้อ ๔๖ ผู้รับผิดชอบระบบสารสนเทศ บริหารจัดการการกู้คืนระบบสำคัญโดยภาพรวม ดังนี้ (แนวปฏิบัติสำหรับการบริหารจัดการการกู้คืนระบบ)

(๑) กำหนดระบบสำคัญที่จำเป็นต้องเตรียมการกู้คืนระบบ

(๒) ประเมินผลกระทบกรณีระบบสำคัญเกิดการหยุดชะงักหรือไม่สามารถให้บริการได้ เช่น ผลกระทบต่อการดำเนินงาน ต่อลูกค้า ผู้ใช้บริการ หรือประชาชน ผลกระทบด้านกฎหมายหรือระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม ด้านชื่อเสียงภาพลักษณ์ขององค์กร เป็นต้น

(๓) ประเมินความเสี่ยงกับระบบสำคัญ กำหนดแผนการลดความเสี่ยง และจัดการกับความเสี่ยงเหล่านั้น (โดยปฏิบัติตามแนวปฏิบัติสำหรับการวิเคราะห์ ประเมินและจัดการกับความเสี่ยงของกรมฯ ที่ได้กำหนดไว้)

(๔) ดำเนินการเตรียมการล่วงหน้าหรือเตรียมความพร้อมที่จำเป็นสำหรับการกู้คืนระบบสำคัญ โดยปฏิบัติตามแนวทางดังนี้

(ก) กำหนดชื่อของระบบที่จำเป็นต้องเตรียมการกู้คืนและระยะเวลาเป้าหมายในการกู้คืนระบบ

(ข) กำหนดสถานที่ตั้งและความต้องการพื้นฐานของศูนย์ปฏิบัติการคอมพิวเตอร์สำรองเพื่อรองรับการติดตั้งระบบสำรอง (ระบบสำรอง หมายถึง ระบบสำคัญที่อาจมีการติดตั้งไว้แล้วหรือจะดำเนินการติดตั้งขึ้นมาอย่างรวดเร็ว ณ ศูนย์ปฏิบัติการคอมพิวเตอร์สำรอง โดยปกติจะมีการใช้ระบบสำรองก็ต่อเมื่อระบบเดียวกันที่ศูนย์ปฏิบัติการคอมพิวเตอร์หลักไม่สามารถให้บริการได้ จึงเปลี่ยนมาใช้ระบบสำรองแทน) รวมทั้งจัดเตรียมศูนย์ปฏิบัติการคอมพิวเตอร์สำรองตามความต้องการที่กำหนดไว้

(ค) จัดหาและติดตั้งระบบสำรองตามความจำเป็น

(ง) กำหนดบุคลากรผู้รับผิดชอบการกู้คืนระบบและผู้ให้บริการภายนอกที่เกี่ยวข้อง

(จ) กำหนดรายละเอียดด้านฮาร์ดแวร์และซอฟต์แวร์ของระบบสำรองที่ต้องการ พร้อมทั้งจัดหาและติดตั้งตามความจำเป็น

(ฉ) กำหนดข้อมูลสำคัญที่จำเป็นสำหรับการกู้คืนระบบ จัดทำแผนการสำรองข้อมูล และดำเนินการสำรองข้อมูลตามแผนที่ได้กำหนดไว้

(ช) กำหนดสถานที่สำหรับจัดเก็บซอฟต์แวร์/เฟิร์มแวร์นอกสถานที่ และนำซอฟต์แวร์/เฟิร์มแวร์ไปเก็บไว้ยังสถานที่นั้น

(ซ) จัดทำสัญญาการให้บริการกับผู้ให้บริการภายนอกเพื่อให้สามารถให้บริการระบบได้อย่างต่อเนื่องมากที่สุดทั้งที่ศูนย์ปฏิบัติการคอมพิวเตอร์หลักและศูนย์ปฏิบัติการคอมพิวเตอร์สำรอง

(ฌ) บันทึกข้อมูลของแต่ละประเด็นในข้างต้นให้ครบถ้วนสมบูรณ์มากที่สุด

(๕) จัดทำแผนกู้คืนระบบสำคัญ (แผนเตรียมความพร้อมกรณีฉุกเฉิน) โดยอย่างน้อยให้กำหนดรายละเอียดลงในแต่ละหัวข้อดังนี้

(ก) ลำดับของผู้มีอำนาจในการสั่งการใช้แผนกู้คืนระบบ

(ข) โครงสร้างของทีมกู้คืนระบบ

(ค) รายชื่อและข้อมูลติดต่อของทีมกู้คืนระบบ

(ง) การสั่งการใช้แผนกู้คืนระบบ

(จ) การสั่งย้ายสถานที่ปฏิบัติงานไปยังศูนย์ปฏิบัติการคอมพิวเตอร์สำรอง

(ฉ) การเก็บรวบรวมเอกสารและอุปกรณ์ที่จำเป็นเพื่อนำไปใช้งานยังศูนย์ปฏิบัติการคอมพิวเตอร์สำรอง

(ช) การเตรียมความพร้อมของศูนย์ปฏิบัติการคอมพิวเตอร์สำรอง (ก่อนเปิดใช้งานกรณีที่ศูนย์ปฏิบัติการคอมพิวเตอร์หลักไม่สามารถใช้งานได้)

(ซ) การแจ้งข้อมูลเกี่ยวกับเหตุการณ์ฉุกเฉินให้ผู้ให้บริการภายนอกได้รับทราบ

(ฌ) การเริ่มต้นปฏิบัติงาน ณ ศูนย์ปฏิบัติการคอมพิวเตอร์สำรอง

(ญ) การกลับคืนสู่สภาวะการทำงานตามปกติ (ภายหลังจากที่ได้แก้ไขสถานการณ์ของศูนย์ปฏิบัติการคอมพิวเตอร์หลักแล้ว)

(๖) ให้ความรู้แก่ผู้ที่เกี่ยวข้องทั้งหมดทั้งทีมกู้คืนระบบและผู้ให้บริการภายนอกเพื่อให้สามารถปฏิบัติได้อย่างถูกต้องเมื่อมีเหตุฉุกเฉินเกิดขึ้น

(๗) ทบทวนและปรับปรุงแผนกู้คืนระบบอย่างน้อยปีละ ๑ ครั้ง

(๘) จัดให้มีการทำแผนการทดสอบการกู้คืนระบบ กำหนดสถานการณ์การทดสอบ ดำเนินการทดสอบตามแผนการทดสอบ บันทึกผลการทดสอบ สรุปผลและข้อเสนอแนะ และนำเสนอต่อผู้บริหารระดับสูงของกรมฯ เพื่อพิจารณาและให้ข้อคิดเห็นในการปรับปรุงตามความจำเป็น การดำเนินการทดสอบระบบดังกล่าวควรดำเนินการอย่างสม่ำเสมอปีละ ๑ ครั้ง

(๙) ทบทวนการดำเนินการในทุกหัวข้อข้างต้นอย่างน้อยปีละ ๑ ครั้ง

หมวด ๙
แนวปฏิบัติในการควบคุมการปฏิบัติงานของผู้ให้บริการภายนอก

ข้อ ๔๗ ผู้รับผิดชอบสารสนเทศ ศึกษาลักษณะงานจ้างผู้ให้บริการภายนอก กำหนดและตกลงความต้องการด้านความมั่นคงปลอดภัยสารสนเทศกับผู้ให้บริการภายนอกในเรื่องที่เกี่ยวข้องกับการเข้าถึง การประมวลผล การจัดเก็บ การสื่อสาร และการให้บริการโครงสร้างพื้นฐานของระบบของกรมฯ

ข้อ ๔๘ ผู้รับผิดชอบสารสนเทศ นำแนวปฏิบัติที่เกี่ยวข้องในเอกสารฉบับนี้กำหนดไว้ในสัญญาจ้างและให้ผู้ให้บริการภายนอกต้องปฏิบัติตามอย่างเคร่งครัด (ดูจากตารางด้านล่าง)

ลักษณะงานจ้าง	แนวปฏิบัติที่ควรนำไปกำหนดไว้ในสัญญาจ้าง
พัฒนาระบบให้มีความมั่นคงปลอดภัย	● แนวปฏิบัติในการพัฒนาระบบให้มีความมั่นคงปลอดภัย (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง) ● แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง)
บริหารจัดการระบบ	● แนวปฏิบัติสำหรับการบริหารจัดการความมั่นคงปลอดภัยของระบบ (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง) ● แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง)
บริหารจัดการเครือข่าย	● แนวปฏิบัติสำหรับการบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง) ● แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง)

ข้อ ๔๙ ผู้รับผิดชอบสารสนเทศ แจ้งให้ผู้ให้บริการภายนอกได้รับทราบถึงในการจ้างช่วงไปยังผู้รับจ้างอื่นๆ ต้องมีการแจ้งให้กรมฯ ได้รับทราบ อย่างเป็นลายลักษณ์อักษรและระบุในสัญญาเกี่ยวกับความรับผิดชอบต่อความเสี่ยงที่เกิดขึ้นจากการจ้างช่วงนั้น ทั้งนี้เพื่อป้องกันความเสี่ยงต่างๆ อันจะส่งผลกระทบต่อลักษณะงานจ้างที่กรมฯ กำหนด

ข้อ ๕๐ ผู้รับผิดชอบสารสนเทศ ติดตาม ทบทวน และประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอให้สอดคล้องกับข้อกำหนดที่ระบุไว้ในสัญญาจ้าง

ข้อ ๕๑ กรณีมีการเปลี่ยนแปลงขอบเขตงานของผู้ให้บริการภายนอก ผู้รับผิดชอบสารสนเทศบริหารจัดการการเปลี่ยนแปลงนั้นโดยดำเนินการตามข้อ ๔๗ - ๔๙ ใหม่อีกครั้งและกำหนดไว้ในสัญญาจ้าง

หมวด ๑๐
แนวปฏิบัติในการบริหารจัดการความเสี่ยงและการตรวจสอบด้านความมั่นคงปลอดภัย

ข้อ ๕๒ คณะกรรมการบริหารฯ กำหนดปัจจัยและเกณฑ์การประเมินความเสี่ยงดังนี้

(๑) กำหนดปัจจัยต่างๆ ที่เกี่ยวข้องกับการประเมินความเสี่ยง เช่น

- เป้าหมายของการประเมินความเสี่ยง
- กระบวนการ วัตถุประสงค์ และข้อกำหนดทางธุรกิจ
- กฎ ระเบียบ ข้อกำหนดในสัญญา และข้อบังคับอื่นๆ ที่ กรมฯ ต้องปฏิบัติตาม
- วัตถุประสงค์ตามมาตรฐานความมั่นคงปลอดภัย ISO/IEC ๒๗๐๐๑ Information Security Management Systems
- ข้อกำหนดด้านความมั่นคงปลอดภัยอื่นๆ เช่น ข้อกำหนดด้านความปลอดภัยในการปฏิบัติงานในสำนักงาน เป็นต้น
- ผลการสแกนตรวจสอบช่องโหว่ในระบบต่างๆ
- เทคโนโลยีสารสนเทศที่กรมฯ ใช้งาน

(๒) กำหนดเกณฑ์การประเมินความเสี่ยง ได้แก่ วิธีการคิดโอกาสการเกิดขึ้นของเหตุการณ์ความเสี่ยง และวิธีการคิดผลกระทบของเหตุการณ์ความเสี่ยง

(๓) กำหนดระดับความเสี่ยงที่กรมฯ ยอมรับได้

ข้อ ๕๓ ผู้รับผิดชอบระบบสารสนเทศ กำหนดให้มีการวิเคราะห์และประเมินความเสี่ยงต่อสินทรัพย์สารสนเทศที่ตนเองรับผิดชอบอย่างน้อยปีละ ๑ ครั้ง และบริหารจัดการความเสี่ยงเหล่านั้นตามขั้นตอนดังนี้ (แนวปฏิบัติสำหรับการวิเคราะห์ ประเมิน และจัดการกับความเสี่ยง)

(๑) วิเคราะห์และระบุเหตุการณ์ความเสี่ยงซึ่งอาจทำให้ปัจจัยต่างๆ ตามที่คณะกรรมการบริหารฯ ได้กำหนดไว้เกิดความเสียหายหรือไม่สอดคล้องได้

(๒) ประเมินค่าความเสี่ยงของเหตุการณ์ความเสี่ยงที่ได้ระบุไว้ (โดยใช้เกณฑ์การประเมินความเสี่ยงของกรมฯ ที่กำหนดไว้)

(๓) จัดลำดับค่าความเสี่ยงของเหตุการณ์ความเสี่ยงต่างๆ เรียงตามลำดับจากมากไปน้อย

(๔) บันทึกผลการประเมินความเสี่ยงในข้างต้น

(๕) จัดทำแผนการลดความเสี่ยง โดยพิจารณาถึงลำดับการดำเนินการ ค่าใช้จ่าย ความคุ้มค่าหรือประโยชน์ที่ได้รับ และผู้รับผิดชอบในการดำเนินการ

(๖) นำเสนอแผนฯ ต่อผู้บังคับบัญชาเพื่อพิจารณาและให้ข้อคิดเห็นตามความจำเป็น

(๗) ผู้บังคับบัญชาสั่งการให้ดำเนินการตามแผนฯ และรายงานให้ได้รับทราบเป็นระยะๆ จนกระทั่งเสร็จสิ้น

ข้อ ๕๔ กรมฯ จัดให้มีการตรวจสอบและประเมินด้านความมั่นคงปลอดภัยอย่างน้อยปีละ ๑ ครั้ง โดยผู้ตรวจสอบภายใน และ/หรือ ผู้ตรวจสอบอิสระภายนอก การตรวจสอบควรพิจารณาความสอดคล้องในการปฏิบัติตามแนวนโยบายและแนวปฏิบัติต่างๆ ที่กรมฯ ได้กำหนดไว้ด้วย

ผลการตรวจสอบและประเมินจะนำไปสู่การจัดทำแผนการดำเนินการแก้ไขหรือป้องกันเพื่อปฏิบัติโดยผู้รับผิดชอบต่อไป

หมวด ๑๑
แนวปฏิบัติในการเชื่อมโยงระบบงานของกรมฯ กับระบบงานของหน่วยงานภายนอก

ข้อ ๕๕ ในการเชื่อมโยงระบบงานและข้อมูลของกรมฯ กับระบบงานและข้อมูลของหน่วยงานภายนอก ผู้รับผิดชอบระบบสารสนเทศ ร่วมกับผู้แทนหรือตัวแทนของหน่วยงานภายนอก เพื่อดำเนินการ ดังนี้

(๑) ประเมินความเสี่ยงของระบบงานและข้อมูลที่จะมีการแลกเปลี่ยนกันระหว่างกรมฯ กับหน่วยงานภายนอก (ดูแนวปฏิบัติสำหรับการวิเคราะห์ ประเมิน และจัดการกับความเสี่ยง ที่กรมฯ กำหนดไว้)

(๒) จัดทำแผนการลดความเสี่ยง ซึ่งรวมถึงมาตรการป้องกันต่างๆ เพื่อป้องกันระบบงานและข้อมูลที่จะมีการแลกเปลี่ยนกันนั้น

(๓) กรณีพบว่ามีความเสี่ยงสำคัญ ให้จัดทำข้อตกลงสำหรับการเชื่อมโยงระบบงานทั้งสอง ข้อตกลงที่จะมีการจัดทำควรมีมาตรการป้องกันตามข้อ (๒) (ข้อตกลงควรครอบคลุมประเด็นดังต่อไปนี้

- รายชื่อผู้รับผิดชอบระบบงานทั้งสองฝั่ง
- สิทธิการเข้าถึงระบบงานทั้งสอง
- วิธีการทางเทคนิคเพื่อป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลที่มีการส่งจากระบบงานหนึ่งไปยังอีกระบบงานหนึ่ง
- วิธีการทางเทคนิคเพื่อรับรองว่าใครเป็นผู้ที่ส่งข้อมูลจากระบบงานหนึ่งไปยังอีกระบบงานหนึ่ง
- วิธีการทางเทคนิคเพื่อเข้ารหัสข้อมูลเพื่อป้องกันไม่ให้เห็นข้อมูลที่มีการแลกเปลี่ยนกันทางเครือข่าย
- การกำหนดหรือการใช้รหัสผ่านที่มีความมั่นคงปลอดภัย
- การเฝ้าระวังและติดตามสภาพความพร้อมใช้ของเครือข่ายที่มีการเชื่อมโยงระบบงานทั้งสองเข้าด้วยกัน (เพื่อให้เครือข่ายมีสภาพความพร้อมใช้มากที่สุด)
- การเฝ้าระวังและติดตามการทำงานของระบบงานทั้งสอง
- การสำรองข้อมูลในระบบงานทั้งสอง
- การป้องกันไวรัสของระบบงานทั้งสอง

(๔) กำหนดให้มีการติดตามการปฏิบัติตามข้อตกลงที่ได้กำหนดไว้นั้นอย่างเข้มงวด

(๕) ติดตามการปฏิบัติเพื่อดูว่ามีความเสี่ยงที่จำเป็นต้องจัดทำแผนการลดความเสี่ยงเพิ่มเติมหรือไม่ หากมี ให้จัดทำและปฏิบัติตามแผนฯ พร้อมทั้งติดตามจนกระทั่งแล้วเสร็จ

หมวด ๑๒
แนวปฏิบัติในการบริหารจัดการเหตุการณ์หรือจุดอ่อนด้านความมั่นคงปลอดภัยและการจัดการกับการละเมิดความมั่นคงปลอดภัย

ข้อ ๕๖ ผู้รับผิดชอบระบบสารสนเทศ เมื่อได้รับแจ้งจากผู้ใช้งานเกี่ยวกับเหตุการณ์หรือจุดอ่อนด้านความมั่นคงปลอดภัยที่เกิดขึ้นหรือที่พบ ให้ปฏิบัติตามขั้นตอนดังนี้

(๑) ประเมินผลกระทบของเหตุการณ์หรือจุดอ่อนที่พบว่ามีผลกระทบในระดับใด (สูง กลาง หรือ ต่ำ)

(๒) วิเคราะห์หาสาเหตุและแก้ไขสถานการณ์ตามความจำเป็น เช่น กรณีการบุกรุกระบบ การโจมตีระบบ หรือระบบได้รับความเสียหาย ประสานงานขอความช่วยเหลือจากผู้รู้ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT)

(๓) กรณีมีความจำเป็นต้องเก็บหลักฐานทางคอมพิวเตอร์ ให้ผู้รู้หรือผู้ที่ผ่านการอบรมหรือฝึกฝนการเก็บหลักฐานฯ เท่านั้นเป็นผู้ดำเนินการเพื่อป้องกันไม่ให้หลักฐานเกิดความเสียหาย จัดเก็บหลักฐานไว้ในสถานที่ที่ปลอดภัย และจำกัดการเข้าถึงหลักฐานนั้น

(๔) กรณีเหตุการณ์มีผลกระทบสูง ให้จัดทำรายงานสรุปเหตุการณ์และแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ ข้อมูลในรายงานสรุปอย่างน้อยต้องมีข้อมูลที่เกี่ยวข้องดังนี้

- รายละเอียดเหตุการณ์
- วันเวลาที่เกิดขึ้น
- ชื่อผู้แจ้ง/หน่วยงานผู้แจ้ง
- สถานะของเหตุการณ์ในแต่ละช่วงเวลา
- ความคืบหน้าในการดำเนินการในแต่ละช่วงเวลา
- สาเหตุและวิธีการแก้ไข
- ข้อเสนอแนะเพื่อป้องกันการเกิดขึ้นอีกในอนาคต

ข้อ ๕๗ กรณีพบว่ามีการละเมิดแนวนโยบายและแนวปฏิบัติต่างๆ ของกรมฯ ที่กำหนดไว้ ผู้บริหารสูงสุด จะต้องเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นจากการละเมิดนั้นและต้องสั่งการให้ ส่วนบริหารทรัพยากรบุคคล และผู้บังคับบัญชา พิจารณาดำเนินการดังนี้ (แนวปฏิบัติสำหรับกระบวนการลงโทษ)

(๑) แจ้งตามสายการบังคับบัญชาให้ผู้บริหารตามลำดับชั้นได้รับทราบ

(๒) กำหนดให้มีการสอบสวนโดยเร็ว

(๓) พิจารณาว่าสินทรัพย์สารสนเทศใดบ้างของกรมฯ ที่ได้รับผลกระทบหรือความเสียหาย และมีความเสียหายในระดับใด

(๔) พิจารณาหาสาเหตุของการละเมิดที่เกิดขึ้น

(๕) พิจารณาดำเนินการลงโทษทางวินัยโดยเริ่มต้นจากการเรียกตักเตือน ทำทัณฑ์บน กรณีรุนแรง ให้ดำเนินคดีตามกฎหมายต่อผู้ละเมิดและผู้ที่เกี่ยวข้องกับการละเมิด

(๖) กำหนดแผนงาน แนวทาง หรือวิธีปฏิบัติที่เหมาะสมเพื่อแก้ไขจากสาเหตุของการเกิดขึ้น และลงมือปฏิบัติตามแผนงานหรือวิธีปฏิบัตินั้น

หมวด ๑๓
แนวปฏิบัติในการเผยแพร่ข้อมูลของกรมฯ สู่สาธารณะ

ข้อ ๕๘ ในการเผยแพร่ข้อมูลทั้งในนามของกรมฯ หรือเป็นความรับผิดชอบของหน่วยงานภายใน สู่สาธารณะโดยผ่านระบบหรือเว็บไซต์ของกรมฯ พนักงานผู้รับผิดชอบของหน่วยงานภายในต้องตรวจสอบความถูกต้องและสมบูรณ์ของข้อมูลก่อนนำออกเผยแพร่

หากข้อมูลที่นำออกเผยแพร่เป็นเรื่องที่เกี่ยวกับนโยบายหรือภาพรวมของกรมฯ จะต้องได้รับความเห็นชอบจากอธิบดีกรมส่งเสริมคุณภาพสิ่งแวดล้อม หรือผู้ที่ได้รับมอบหมายก่อนนำออกเผยแพร่

ในกรณีที่ข้อมูลที่นำออกเผยแพร่มีความผิดพลาดและก่อให้เกิดความเสียหายขึ้นไม่ว่าจะโดยความจงใจหรือประมาทเลินเล่อก็ตาม ให้เป็นความรับผิดของพนักงานที่นำข้อมูลดังกล่าวออกเผยแพร่