**ประกาศกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ**
**เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ**
**ของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ**

---

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ บัญญัติให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐมีหน้าที่ดำเนินมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ ของพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการจึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้ เป็นต้นไป

ข้อ ๒ ในประกาศนี้

“แนวนโยบาย” หมายความว่า หลักการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่กรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ กำหนดขึ้นและประกาศใช้งาน

“แนวปฏิบัติ” หมายความว่า ข้อปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่กรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการกำหนดขึ้นและประกาศใช้งาน เพื่อให้ผู้ใช้งานปฏิบัติตามโดยเคร่งครัด

ข้อ ๓ แนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ ดังนี้

(๑) ให้มีการเข้าถึงหรือควบคุมการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ ได้แก่ ระบบสารสนเทศ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ ระบบงาน อุปกรณ์เครือข่าย และอุปกรณ์อื่น ๆ ที่เกี่ยวข้องให้เป็นไปอย่างมั่นคงปลอดภัย

(๒) ให้มีการเตรียมความพร้อมของการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการอย่างต่อเนื่อง โดยการจัดทำแผนและขั้นตอนการปฏิบัติงานกรณีเกิดเหตุฉุกเฉิน และการจัดให้มีระบบสำรอง ให้สามารถรับมือกรณีเกิดเหตุฉุกเฉินและเพื่อให้สามารถกู้คืนกลับมาได้ภายในระยะเวลาที่เหมาะสม

/ (๓) ให้มีการ...

(๓) ให้มีการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยด้านสารสนเทศและระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการอย่างสม่ำเสมอ

(๔) ให้มีการรักษาไว้ซึ่งความลับ ความถูกต้อง ความสมบูรณ์ และความพร้อมของสารสนเทศและระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ

ข้อ ๔ เพื่อให้การดำเนินงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ เป็นไปอย่างมีประสิทธิภาพ และสามารถปฏิบัติตามได้อย่างเป็นรูปธรรม กรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ จึงกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ ตามแนวปฏิบัติท้ายประกาศนี้

ข้อ ๕ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ เกิดความเสียหาย หรืออันตรายใด ๆ แก่กรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ ให้อธิบดีกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการในฐานะผู้บริหารระดับสูงสุด (Chief Executive Office : CEO) ของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๖ ประกาศนี้ให้กรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ ดำเนินการให้ผู้เกี่ยวข้องและผู้ใช้งานทั้งหมดได้ทราบโดยทั่วกัน พร้อมทั้งสร้างความรู้ ความเข้าใจ และจัดฝึกอบรมแก่ผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยคุกคามไซเบอร์ และผลกระทบที่เกิดจากการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศ โดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์

ข้อ ๗ ให้กองยุทธศาสตร์และแผนงาน โดยศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนแนวนโยบายและแนวปฏิบัตินี้ให้เป็นปัจจุบัน

ประกาศ ณ วันที่ ๒๖ เมษายน พ.ศ. ๒๕๖๖

(นางสาวสราญภัทร อนุมัติราชกิจ)
อธิบดีกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ

**แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ**
**ของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ**

---

เพื่อให้การใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเชื่อถือได้ ตลอดจนดำเนินการให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ จึงกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศไว้ ดังต่อไปนี้

ข้อ ๑ ในแนวปฏิบัตินี้

"ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Department Chief Information Officer : DCIO)" หมายความว่า ผู้บริหารระดับสูงที่อธิบดีกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ แต่งตั้งให้มีหน้าที่รับผิดชอบการบริหารงานด้านสารสนเทศและระบบเทคโนโลยีสารสนเทศ

"ผู้บริหารข้อมูลระดับสูงของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ (Department Chief Data Officer : DCDO)" หมายความว่า ผู้บริหารระดับสูงที่อธิบดีกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ แต่งตั้งให้มีหน้าที่รับผิดชอบการบริหารงานด้านสารสนเทศและระบบเทคโนโลยีสารสนเทศ

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ

"ผู้ใช้งาน" หมายความว่า บุคคลที่เข้าใช้งานระบบสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ แต่ไม่รวมถึงบุคคลภายนอกที่เข้าใช้งานข้อมูลสาธารณะที่เผยแพร่ในเว็บไซต์ของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ

"ผู้ดูแลระบบ" หมายความว่า เจ้าหน้าที่ที่มีหน้าที่ดูแลระบบสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการหรือบุคคลที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลระบบสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ

"ระบบสารสนเทศ" หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูลและสารสนเทศ เป็นต้น

"สินทรัพย์" หมายความว่า ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ เครื่องคอมพิวเตอร์อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ ซอฟต์แวร์โปรแกรมประยุกต์ที่หน่วยงานพัฒนาขึ้น รวมทั้งสิ่งใดก็ตามที่มีคุณค่าสำหรับหน่วยงาน

"โปรแกรมมาตรฐาน" หมายความว่า โปรแกรมที่กรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ กำหนดให้เป็นโปรแกรมมาตรฐานสำหรับใช้งานได้ตามปกติ

/ "หน่วยงาน"...

"หน่วยงาน" หมายความว่า หน่วยงานภายในตามโครงสร้างของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ

"ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์" หมายความว่า พื้นที่ใช้จัดวางเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย และอุปกรณ์ต่าง ๆ ของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการไว้เป็นศูนย์กลางในการประมวลผลข้อมูลสารสนเทศสำหรับใช้ปฏิบัติงานของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ

"เครื่องคอมพิวเตอร์ส่วนตัว" หมายความว่า เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์โน้ตบุ๊ก สมาร์ทโฟน หรืออุปกรณ์คอมพิวเตอร์ ที่สามารถจัดเก็บหรือประมวลผลข้อมูลได้ โดยที่กรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการไม่ได้เป็นผู้จัดหาไว้ใช้งาน

"อุปกรณ์คอมพิวเตอร์" หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อหรือทำงานเป็นส่วนหนึ่งของระบบสารสนเทศ

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ โดยรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง ครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ

"การรักษาความลับ (Confidentiality)" หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

"ข้อมูลสารสนเทศ" หมายความว่า ข้อมูลที่ได้ผ่านกระบวนการประมวลผลแล้ว อาจใช้วิธีง่าย ๆ เช่น หาค่าเฉลี่ย หรือใช้เทคนิคขั้นสูง เช่นการวิจัยดำเนินงาน เพื่อเปลี่ยนแปลงสภาพข้อมูลทั่วไป ให้อยู่ในรูปแบบที่มีความสัมพันธ์ หรือมีความเกี่ยวข้องกัน เพื่อนำไปใช้ประโยชน์ในการตัดสินใจหรือตอบปัญหาต่าง ๆ ได้ ประกอบด้วยข้อมูล เอกสาร เสียง หรือรูปภาพ ไม่ใช่จำกัดเฉพาะตัวเลขเพียงอย่างเดียว ทั้งที่เก็บไว้ในรูปแบบของกระดาษ (Hardcopy) และไฟล์ข้อมูลอิเล็กทรอนิกส์ (Electronic file)

"เจ้าของข้อมูล" หมายความว่า เจ้าหน้าที่ซึ่งได้รับมอบหมายจากกองหรือหน่วยงานภายในที่เรียกชื่ออย่างอื่น ซึ่งเป็นผู้สร้าง เปลี่ยนแปลง หรือแก้ไขข้อมูลที่เกี่ยวกับภารกิจของกองหรือหน่วยงานนั้น รวมทั้งให้สิทธิในการเข้าถึงข้อมูลนั้นแก่ผู้อื่น

"สื่อบันทึกข้อมูล" หมายความว่า สิ่งที่ใช้จัดเก็บข้อมูล ชุดคำสั่ง และสารสนเทศต่าง ๆ เช่น USB drive SD Card CD DVD External HD NAS หรืออื่น ๆ ในลักษณะเดียวกัน

"การเข้ารหัส (Encryption)" หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสได้ จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

/ "อุปกรณ์คอมพิวเตอร์...

"อุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile computing devices)" หมายความว่า อุปกรณ์คอมพิวเตอร์ขนาดเล็กที่สามารถพกพาหรือเคลื่อนย้ายไปกับตัวบุคคลไปยังสถานที่ต่าง ๆ ได้โดยง่าย และมีน้ำหนักเบา เช่น เครื่องคอมพิวเตอร์โน้ตบุ๊ก โทรศัพท์มือถือ สมาร์ทโฟน

"ผู้ให้บริการภายนอก" หมายความว่า หน่วยงานภายนอกที่รับจ้างปฏิบัติงานด้านเทคโนโลยีสารสนเทศตามความต้องการของกรม เช่น ผู้ให้บริการอินเทอร์เน็ต โดยรวมผู้ให้บริการเหล่านี้มีหน้าที่ต้องปฏิบัติตามสัญญา

"บัญชีผู้ใช้งาน (Username)" หมายความว่า บัญชีรายชื่อของผู้ที่ได้รับสิทธิและรหัสผ่านในการใช้งานระบบสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ

"เครือข่าย" หมายความว่า โครงข่ายคอมพิวเตอร์ที่เชื่อมโยงคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่าง ๆ เข้าด้วยกัน ซึ่งทำให้การสื่อสารข้อมูลระหว่างคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทั้งที่อยู่ภายในและภายนอกหน่วยงานสามารถติดต่อสื่อสารและแลกเปลี่ยนข้อมูลกันได้ โครงข่ายนี้โดยพื้นฐานประกอบด้วยโครงข่ายสำหรับการติดต่อสื่อสารภายในหน่วยงาน และโครงข่ายบนอินเทอร์เน็ตซึ่งทำให้คอมพิวเตอร์ภายในหน่วยงานหนึ่งสามารถติดต่อสื่อสารกับคอมพิวเตอร์ของอีกหน่วยงานหนึ่งได้

"เทคโนโลยีเครือข่ายเสมือน (Virtual Private Network : VPN)" หมายความว่า การใช้การเข้ารหัสข้อมูล เช่น โดยผ่านทางซอฟต์แวร์หรือฮาร์ดแวร์หนึ่ง เพื่อให้การเชื่อมต่อโดยผ่านทางเครือข่ายที่ไม่ปลอดภัย เช่น อินเทอร์เน็ต เครือข่ายไร้สาย มีความมั่นคงปลอดภัย ทั้งนี้ เนื่องมาจากข้อมูลจะได้รับการเข้ารหัสก่อนที่จะมีการส่งผ่านไปบนอินเทอร์เน็ตหรือเครือข่ายไร้สายนั้น รวมถึงระบบ อุปกรณ์คอมพิวเตอร์ ซอฟต์แวร์หรือฮาร์ดแวร์ ที่ใช้การเข้ารหัสข้อมูลก่อนส่งข้อมูลออกไป

"ข้อมูลจราจรทางคอมพิวเตอร์ (Log)" หมายความว่า ข้อมูลเหตุการณ์ต่าง ๆ ที่เกิดขึ้นบนระบบใดระบบหนึ่งและได้ถูกบันทึกไว้ในระบบนั้น เช่น ความผิดพลาดในการทำงานของระบบ ทรัพยากรระบบไม่พอ ความพยายามในการบุกรุกระบบ ข้อมูลเหตุการณ์ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ได้กำหนดให้มีการบันทึกและจัดเก็บไว้ ซึ่งข้อมูลเหล่านี้สามารถใช้เพื่อตรวจ ติดตามการทำงาน แจ้งเตือน เป็นดำเนินการเชิงป้องกัน หรือแก้ไขตามความจำเป็น ซึ่งรวมถึงการใช้เป็นหลักฐานในการดำเนินการทางกฎหมาย เช่น กรณีการบุกรุกระบบ หรือการใช้งานที่ทำให้เกิดความเสียหาย

"ความเสี่ยง" หมายความว่า เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อสินทรัพย์สารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาต หน้าเว็บไซต์ถูกเปลี่ยนแปลงแก้ไข ซึ่งอาจทำให้กรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ เสียชื่อเสียง

"ระบบสำรอง" หมายความว่า ระบบสำคัญที่อาจมีการติดตั้งไว้แล้วหรือจะดำเนินการติดตั้งขึ้นมาอย่างรวดเร็ว ณ ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์สำรอง โดยปกติจะมีการใช้ระบบสำรองก็ต่อเมื่อระบบเดียวกันที่ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์หลักไม่สามารถให้บริการได้ จึงเปลี่ยนมาใช้ระบบสำรองแทน

/ "ทรัพย์สินทางปัญญา"...

"ทรัพย์สินทางปัญญา" หมายความว่า ผลงานใด ๆ อันเกิดจากความคิดสร้างสรรค์ของมนุษย์ทรัพย์สินทางปัญญาเป็นทรัพย์สินอีกชนิดหนึ่งที่นอกเหนือจากสังหาริมทรัพย์ และอสังหาริมทรัพย์ ทั้งนี้ ประเภทของทรัพย์สินทางปัญญาประกอบด้วยลิขสิทธิ์ (Copyright) สิทธิบัตร (Patent) เครื่องหมายการค้า (Trademark) แบบผังภูมิของวงจรรวม (Layout - Designs of Integrated Circuit) ความลับทางการค้า (Trade Secrets) และสิ่งบ่งชี้ทางภูมิศาสตร์ (Geographical Indication)

"รหัสผ่าน (Password)" หมายความว่า กลุ่มชุดตัวอักษร ตัวเลข หรืออักขระพิเศษ โดยใช้ร่วมกับบัญชีผู้ใช้งาน (Username) เพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวตนสำหรับเข้าถึงระบบสารสนเทศ

"โปรแกรมไม่พึงประสงค์" หมายความว่า โปรแกรมที่ได้รับการติดตั้งในเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือโดยไม่รู้ตัว อาจก่อให้เกิดความเสียหายต่อข้อมูลในเครื่องคอมพิวเตอร์ ทำงานช้า ทำงานผิดปกติ หรือทำงานในลักษณะที่ไม่เป็นประโยชน์ ไม่สร้างสรรค์ หรือไม่เป็นผลดีต่อเครื่องคอมพิวเตอร์นั้น โปรแกรมที่ทำงานในลักษณะดังกล่าวอย่างน้อยให้หมายความรวมถึง

(๑) โปรแกรมที่สามารถสำเนาตัวเองและแพร่กระจายผ่านทางสื่อบันทึกข้อมูลเพื่อข้ามไปยังเครื่องคอมพิวเตอร์อื่น กล่าวคือ เมื่อมีการใช้สื่อบันทึกข้อมูลดังกล่าวกับเครื่องคอมพิวเตอร์หนึ่ง โปรแกรมดังกล่าวก็จะแพร่กระจายหรือติดไปยังเครื่องคอมพิวเตอร์นั้น

(๒) โปรแกรมที่สามารถสำเนาตัวเองข้ามหรือแพร่กระจายไปยังเครื่องคอมพิวเตอร์ปลายทางหนึ่งเครื่องหรือมากกว่าหนึ่งเครื่องก็ได้ เครื่องคอมพิวเตอร์ปลายทางที่ได้รับการแพร่ระบาดนั้น ก็สามารถสำเนาและแพร่กระจายตัวเองได้ต่อไป โปรแกรมที่แพร่กระจายในลักษณะดังกล่าวมีชื่อเรียกกันว่าหนอนเครือข่าย (Worm)

(๓) โปรแกรมที่เคลื่อนที่จากเครื่องคอมพิวเตอร์อื่นมายังเครื่องคอมพิวเตอร์ของผู้ใช้งานหรือที่เรียกกันว่า Mobile Code เช่น โปรแกรมที่เขียนด้วย Java Script หรือ Active X และถูกสั่งให้ทำงานในเครื่องของผู้ใช้งานนั้น โปรแกรมประเภทนี้อาจฝังตัวอยู่กับโปรแกรมอื่นแต่ถูกเรียกให้ทำงานร่วมกัน เช่น กรณีของการเข้าถึงโปรแกรมบนเว็บไซต์หนึ่งซึ่งมีการเรียกใช้ Java Script ด้วย ก็จะทำให้ Java Script นั้นถูกโอนย้ายเข้ามาและสั่งทำงานบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน

"จดหมายอิเล็กทรอนิกส์หรืออีเมล (E-mail)" หมายความว่า ข้อความอิเล็กทรอนิกส์ที่มีการส่งผ่านระบบเทคโนโลยีสารสนเทศและอินเทอร์เน็ตจากผู้ส่งไปยังผู้รับ ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิกภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ เช่น SMTP POP๓ หรือ IMAP

"ชุดคำสั่ง (Source Code)" หมายความว่า ไฟล์ซึ่งประกอบด้วยชุดคำสั่งที่สามารถสั่งการให้เครื่องคอมพิวเตอร์ทำงานตามที่ต้องการได้ โดยทั่วไปชุดคำสั่งเหล่านี้จะอยู่ในรูปแบบหรือภาษาที่สามารถอ่านและทำความเข้าใจได้โดยมนุษย์ ไฟล์ชุดคำสั่งนี้จะถูกแปลงโดยโปรแกรมแปลภาษา เช่น Compiler Interpreter หรือ Assembler ไปเป็นโค้ดที่เครื่องคอมพิวเตอร์สามารถตีความและสั่งการให้เครื่องทำงาน ตามที่ตีความนั้น โดยปกติมนุษย์จะไม่สามารถอ่านและทำความเข้าใจโค้ดประเภทนี้ได้

/ "ระดับ...

"ระดับความเสี่ยงที่ยอมรับได้" หมายความว่า ค่าความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่งมีค่าน้อยกว่าค่าที่ยอมรับได้นี้จะถือว่าสินทรัพย์สารสนเทศที่เกี่ยวข้องกับเหตุการณ์ มีความมั่นคงปลอดภัยด้านสารสนเทศเพียงพอ

"แผนการลดความเสี่ยง" หมายความว่า แผนการจัดการกับเหตุการณ์ความเสี่ยง สำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการต่อผู้อำนวยการศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศ และ DCIO เพื่อพิจารณาอนุมัติดำเนินการ

"ไซเบอร์" หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

"ภัยคุกคามทางไซเบอร์" หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่มีความเกี่ยวข้องกับข้อมูลสารสนเทศของหน่วยงาน

"การรักษาความมั่นคงปลอดภัยไซเบอร์" หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อรักษาไว้ซึ่งความลับ ความถูกต้อง ความพร้อมใช้ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อหน่วยงาน

## หมวด ๑
## แนวปฏิบัติของผู้ดูแลระบบ

ข้อ ๒ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๒.๑ กำหนดมาตรการควบคุมการเข้า-ออก ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เพื่อดูแลรักษาความปลอดภัย โดยบุคคลที่ต้องการสิทธิในการเข้า-ออก ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศ

๒.๒ พิจารณาอนุมัติและกำหนดสิทธิการเข้า-ออก ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ให้เป็นไปตามภารกิจของแต่ละหน่วยงาน โดยต้องได้รับอนุมัติจากผู้อำนวยการศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศเท่านั้น

/ ๒.๓ ต้องทำการ...

๒.๓ ต้องทำการยืนยันตัวตนก่อนเข้าห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ทุกครั้ง เพื่อป้องกันการเข้า-ออกโดยไม่ได้รับอนุญาต

๒.๔ ควบคุมการลงชื่อ บันทึกวัน เวลา และวัตถุประสงค์การเข้า-ออก ของผู้ใช้งานและบุคคลภายนอก (Visitors) ทุกครั้ง

๒.๕ ควบคุมให้ผู้เข้า-ออก ติดบัตรแสดงตัวตนให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในพื้นที่ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

๒.๖ ดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอก (Visitors) ในขณะที่ปฏิบัติงานในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์จนกระทั่งเสร็จสิ้นภารกิจและออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เพื่อป้องกันการสูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๒.๗ แยกพื้นที่ในการส่งมอบสินทรัพย์ เพื่อตรวจสอบให้เสร็จเรียบร้อยก่อนนำเข้าไปติดตั้งหรือใช้งานภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

๒.๘ ประชาสัมพันธ์มาตรการควบคุมการเข้า-ออก ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์แก่ผู้ใช้งานและบุคคลภายนอก (Visitors)

๒.๙ ห้ามนำอาหารและเครื่องดื่มเข้าไปภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

๒.๑๐ ห้ามสูบบุหรี่ หรือกระทำการใด ๆ อันอาจก่อให้เกิดควันหรือเพลิงในบริเวณภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

๒.๑๑ ต้องทำการยกเลิก หรือเปลี่ยนแปลงการอนุญาตการเข้า-ออกห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ของผู้ใช้งานเมื่อมีการออกจากงาน สิ้นสุดการจ้าง เปลี่ยนตำแหน่ง โอน หรือย้ายหน่วยงาน

๒.๑๒ ทบทวนสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์อย่างสม่ำเสมอ หรืออย่างน้อยปีละหนึ่งครั้ง

ข้อ ๓ การกำหนดการจัดวางและป้องกันระบบสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๓.๑ จัดวางระบบสารสนเทศที่มีความสำคัญในพื้นที่ที่มีความมั่นคงและปลอดภัย เพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต และเพื่อป้องกันการเข้าถึงระบบ

ข้อ ๔ การควบคุมการเดินสายสัญญาณและสายไฟฟ้า ผู้ดูแลระบบต้องปฏิบัติดังต่อไปนี้

๔.๑ ควบคุมการเดินสายสัญญาณและสายไฟฟ้าให้เป็นไปด้วยความเรียบร้อย ปลอดภัย

๔.๒ การเดินสายสัญญาณและสายไฟฟ้า ต้องแยกออกจากกัน เพื่อป้องกันการรบกวน

๔.๓ ทำแผนผังการเดินสายสัญญาณ และสายไฟฟ้าให้ครบถ้วนและถูกต้อง

๔.๔ ปิดประตูตู้ Rack สำหรับติดตั้งอุปกรณ์เครือข่ายและสายสัญญาณให้สนิท รวมถึงการล็อคประตูเพื่อป้องกันการเข้าถึงของบุคคลที่ไม่เกี่ยวข้อง

๔.๕ จัดทำป้ายชื่อสำหรับสายสัญญาณบนอุปกรณ์ เพื่อป้องกันการปฏิบัติงานผิดพลาด

๔.๖ สำรวจระบบสายสัญญาณอย่างสม่ำเสมอ เพื่อความถูกต้องและตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

/ ข้อ ๕ การกำหนด...

ข้อ ๕ การกำหนดการบำรุงรักษาระบบสารสนเทศ ผู้ดูแลระบบต้องปฏิบัติดังต่อไปนี้

๕.๑ จัดทำสัญญาการบำรุงรักษาสำหรับระบบและอุปกรณ์คอมพิวเตอร์ที่มีความสำคัญ

๕.๒ กำหนดเงื่อนไขของสัญญาการบำรุงรักษาให้ชัดเจน เพื่อให้ผู้รับจ้างต้องติดต่อกลับและเข้ามาดำเนินการแก้ไขปัญหาให้แล้วเสร็จภายในระยะเวลาที่เหมาะสม

๕.๓ ตรวจสอบและกำหนดให้มีการรับประกันความเสียหายต่อระบบสารสนเทศ

๕.๔ บำรุงรักษาระบบสารสนเทศตามรอบระยะเวลาที่กำหนดไว้ในสัญญา

๕.๕ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๕.๖ บันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๕.๗ บันทึกปัญหาและข้อบกพร่องที่พบ และรายงานผู้อำนวยการศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศ

๕.๘ ควบคุม และดูแลการปฏิบัติงานของผู้ให้บริการภายนอกให้ปฏิบัติตามสัญญา

๕.๙ กำหนดสิทธิของผู้ให้บริการภายนอกในการเข้าถึงพื้นที่ อุปกรณ์ และข้อมูลที่สำคัญ

ข้อ ๖ การบริหารจัดการสินทรัพย์ ผู้ดูแลระบบต้องปฏิบัติดังต่อไปนี้

๖.๑ บันทึกและตรวจสอบสินทรัพย์ เพื่อเป็นหลักฐานในการตรวจสอบความถูกต้องและป้องกันการสูญหาย

๖.๒ กำหนดมาตรการหรือเทคนิคในการทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะจำหน่ายหรือนำกลับมาใช้งานใหม่ทุกครั้ง เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญ

๖.๓ กรณีสินทรัพย์เกิดความขัดข้อง เสียหาย ต้องทำการส่งซ่อมแซมแก้ไข ให้ควบคุมการส่งออกไปซ่อมแซมนอกสถานที่ เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต กรณีสินทรัพย์มีข้อมูลสำคัญต้องทำการจัดเก็บ/ทำลายข้อมูลก่อน เพื่อไม่ให้ผู้อื่นสามารถเข้าถึงได้

ข้อ ๗ การควบคุมการใช้งานสารสนเทศและบริหารจัดการอุปกรณ์คอมพิวเตอร์แบบพกพา ผู้ดูแลระบบต้องปฏิบัติดังต่อไปนี้

๗.๑ ต้องนำอุปกรณ์คอมพิวเตอร์แบบพกพาส่วนตัว หรืออุปกรณ์คอมพิวเตอร์แบบพกพาของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ ที่ได้รับอนุมัติจากผู้บังคับบัญชาให้เชื่อมต่อระบบเครือข่ายภายในและเข้าถึงระบบสารสนเทศของกรม ต้องปฏิบัติตามขั้นตอนที่ศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศกำหนด เพื่อป้องกันการเข้าถึงระบบสารสนเทศด้วยอุปกรณ์คอมพิวเตอร์แบบพกพาโดยไม่ได้รับอนุญาต

๗.๒ กำหนดมาตรการระบุและพิสูจน์ตัวตนก่อนเข้าถึงอุปกรณ์คอมพิวเตอร์แบบพกพาด้วยบัญชีผู้ใช้งานและรหัสผ่าน หรือเทคโนโลยีไบโอเมตริก (biometric หรือ PIN CODE เพื่อป้องกันการเข้าถึงจากผู้อื่นและระมัดระวังมิให้ผู้อื่นเข้าถึงอุปกรณ์คอมพิวเตอร์แบบพกพาของตน ต้องดูแลรักษาข้อมูลหน่วยงานในอุปกรณ์คอมพิวเตอร์แบบพกพาให้สอดคล้องตามข้อกำหนดการบริหารจัดการข้อมูลหน่วยงาน

/ ๗.๓ ต้องแจ้ง...

๗.๓ ต้องแจ้งผู้อำนวยการศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศทันที ที่พบว่าเครื่องคอมพิวเตอร์ หรืออุปกรณ์ หรือระบบงาน ขัดข้อง หรือเสียหาย หรือเปลี่ยนเครื่องใหม่ เพื่อจัดการเหตุที่เกิดขึ้นได้อย่างมีประสิทธิภาพ

ข้อ ๘ การควบคุมการใช้งานสารสนเทศ ผู้ดูแลระบบต้องปฏิบัติดังต่อไปนี้

๘.๑ การอนุมัติและกำหนดสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งานให้เป็นไปตามภารกิจหรือแนวปฏิบัติของแต่ละหน่วยงานที่ผู้ใช้งานปฏิบัติงาน โดยต้องได้รับอนุมัติจากผู้บังคับบัญชาแล้วเท่านั้น

๘.๒ กำหนดการเข้าถึงด้วยบัญชีผู้ใช้งานแยกเป็นรายบุคคลตามภารกิจหรือแนวปฏิบัติของแต่ละหน่วยงานที่ผู้ใช้งานปฏิบัติงาน

๘.๓ จัดเก็บข้อมูลการลงทะเบียนสำหรับสร้างบัญชีผู้ใช้งานไว้เพื่อการตรวจสอบในภายหลัง

๘.๔ กำหนดให้ยืนยันตัวตน (Authentication) ของผู้ใช้งานก่อนเข้าถึงระบบสารสนเทศ

๘.๕ กำหนดระยะเวลาการออกจากระบบสารสนเทศโดยอัตโนมัติ เมื่อไม่มีการใช้งานเกินสามสิบนาที หรือตามความสำคัญของข้อมูลสารสนเทศ

๘.๖ กำหนดระยะเวลาการเข้าถึงระบบสารสนเทศที่สำคัญของกรม ตามภารกิจและความจำเป็นของผู้ใช้งาน

๘.๗ กำหนดให้เครื่องคอมพิวเตอร์ต้องพักหน้าจอ (Screen saver) โดยอัตโนมัติหากไม่มีการใช้งานเครื่องคอมพิวเตอร์เกินสิบห้านาที

๘.๘ จำกัดระยะเวลาในการเชื่อมต่อ (Limitation of Connection Time) ระบบสารสนเทศเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๘.๙ จำกัดและควบคุมการเข้าถึง Functions ต่าง ๆ ในการใช้งานระบบสารสนเทศของผู้ใช้งานและผู้ดูแลระบบ

๘.๑๐ ระบบซึ่งไวต่อการรบกวน หรือมีผลกระทบ และมีความสำคัญสูง ต้องแยกเครือข่ายออกจากระบบอื่น ๆ ต้องมีการควบคุมสภาพแวดล้อมแยกเป็นสัดส่วน และต้องกำหนดสิทธิการใช้งานเฉพาะผู้ที่มีสิทธิเท่านั้น

๘.๑๑ จัดทำระบบบริหารจัดการรหัสผ่านเชิงโต้ตอบสำหรับการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย โดยผู้ใช้งานกำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยตามการบริหารจัดการบัญชีผู้ใช้งาน (User Account) ด้วยตนเอง

๘.๑๒ การยกเลิกและเพิกถอนสิทธิการอนุญาตให้เข้าถึงระบบสารสนเทศของผู้ใช้งานต้องทำการยกเลิกและเพิกถอนการอนุญาตเมื่อมีการออกจากงาน หรือสิ้นสุดการจ้าง หลังจากได้รับแจ้งจากสำนักงานเลขานุการกรม

๘.๑๓ การเปลี่ยนแปลงสิทธิการอนุญาตให้เข้าถึงระบบสารสนเทศของผู้ใช้งาน กรณีเปลี่ยนตำแหน่ง โอน หรือย้าย ต้องทำการเปลี่ยนแปลงหลังจากได้รับแจ้งจากผู้บังคับบัญชาผู้ใช้งาน

/ ๘.๑๔ ทบทวน...

๘.๑๔ ทบทวนบัญชีผู้ใช้งานและสิทธิการเข้าถึงระบบสารสนเทศ อย่างน้อยปีละหนึ่งครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลง เพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

ข้อ ๙ การบริหารจัดการความปลอดภัยเครือข่าย ผู้ดูแลระบบต้องปฏิบัติดังต่อไปนี้

๙.๑ กำหนดวิธีปฏิบัติเกี่ยวกับการใช้งานเครือข่ายทั้งภายในและภายนอก

๙.๒ กำหนดขั้นตอนการขออนุญาตในการเข้าถึงระบบสารสนเทศและเครือข่ายของกรม

๙.๓ กำหนดขั้นตอนการเชื่อมต่อระบบเครือข่ายจากผู้ใช้งานภายนอกอย่างมั่นคงปลอดภัย เช่น การเชื่อมต่อระบบเครือข่ายด้วยเทคโนโลยีเครือข่ายเสมือน (Virtual Private Network : VPN)

๙.๔ ระบุบริการที่ศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศ อนุญาตให้ใช้งานหรือบริการผ่านระบบเครือข่ายของกรม

๙.๕ กำหนดให้มีการระบุและพิสูจน์ตัวตนในการเข้าถึงระบบสารสนเทศของกรม

๙.๖ จัดทะเบียนอุปกรณ์ที่ใช้งานในระบบเครือข่ายของกรม

๙.๗ ใช้ข้อมูล IP Address เป็นข้อมูลในการระบุอุปกรณ์บนเครือข่าย เพื่อบ่งชี้อุปกรณ์ที่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่ายของกรม และใช้วิธีการทางเทคนิคที่เหมาะสมควบคุมการเข้าถึงอุปกรณ์

๙.๘ กำหนดให้เครื่องคอมพิวเตอร์ของผู้ดูแลระบบเครือข่ายเท่านั้นที่สามารถเชื่อมต่อเครือข่ายเพื่อบริหารจัดการระบบและอุปกรณ์เครือข่าย

๙.๙ ป้องกันและควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการบริหารจัดการอุปกรณ์ในระบบเครือข่ายทั้งจากภายในและภายนอกกรม

๙.๑๐ จัดแบ่งเครือข่ายตามวัตถุประสงค์การใช้งาน บริการ หรือกลุ่มผู้ใช้งาน

๙.๑๑ ใช้วิธีการทางเทคนิคบน Firewall หรืออุปกรณ์เครือข่ายอื่น ๆ โดยจำกัดเส้นทางบนเครือข่าย โดยกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะเส้นทางที่อนุญาตเท่านั้น

๙.๑๒ กำหนดมาตรการป้องกันระบบสารสนเทศที่ต้องเชื่อมโยงกับระบบเครือข่ายสาธารณะอย่างมีประสิทธิภาพ

๙.๑๓ กำหนดมาตรการป้องกันข้อมูลที่ส่งผ่านทางเครือข่ายสาธารณะเพื่อรักษาความลับและความถูกต้องของข้อมูลที่สำคัญ

๙.๑๔ กำหนดเส้นทางบนเครือข่ายที่เหมาะสมเพื่อควบคุมการเชื่อมต่อและการไหลเวียนของสารสนเทศบนเครือข่ายให้มีประสิทธิภาพ

๙.๑๕ ตรวจสอบการใช้งานระบบเครือข่ายด้วยระบบตรวจจับและป้องกันการบุกรุกของบุคคลที่เข้าใช้งานระบบเครือข่ายในลักษณะที่ผิดปกติอย่างสม่ำเสมอ หรืออย่างน้อยเดือนละหนึ่งครั้ง

๙.๑๖ ทดสอบความมั่นคงปลอดภัยของระบบเครือข่ายอย่างน้อยปีละหนึ่งครั้งหรือตามสถานการณ์ของภัยคุกคามทางไซเบอร์ในระบบเครือข่าย และนำผลที่ได้ไปปรับปรุงให้มีความมั่นคงปลอดภัยมากขึ้นและทันต่อภัยคุกคามทางไซเบอร์ในปัจจุบัน

/ ๙.๑๗ ติดตาม...

๙.๑๗ ติดตาม ตรวจสอบ ดูแล และปรับปรุงเครือข่ายของกรม ให้มีความมั่นคงปลอดภัย และทันสมัยอยู่เสมอ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานระบบเครือข่ายให้รีบดำเนินการแก้ไขและแจ้งผู้อำนวยการศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศทันที เพื่อป้องกันหรือบรรเทาความเสียหายที่อาจเกิดขึ้น

๙.๑๘ การยกเลิกและเพิกถอนสิทธิการอนุญาตให้เข้าถึงระบบเครือข่ายของผู้ใช้งาน ต้องทำการยกเลิกและเพิกถอนการอนุญาตเมื่อมีการออกจากงาน หรือสิ้นสุดการจ้าง หลังจากได้รับแจ้งจากสำนักงานเลขานุการกรม

๙.๑๙ การเปลี่ยนแปลงสิทธิการอนุญาตให้เข้าถึงระบบเครือข่ายของผู้ใช้งาน กรณีเปลี่ยนตำแหน่ง โอน หรือย้าย ต้องทำการเปลี่ยนแปลงหลังจากได้รับแจ้งจากผู้บังคับบัญชาผู้ใช้งาน

๙.๒๐ ทบทวนสิทธิการเข้าถึงเครือข่ายของผู้ใช้งานอย่างสม่ำเสมอ หรืออย่างน้อยปีละหนึ่งครั้ง เพื่อป้องกันการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต

ข้อ ๑๐ การบริหารจัดการในการปฏิบัติงาน ผู้ดูแลระบบต้องปฏิบัติดังต่อไปนี้

๑๐.๑ ไม่นำข้อมูลสารสนเทศของกรมเปิดเผยกับบุคคลที่ไม่เกี่ยวข้องกับการปฏิบัติหน้าที่ เว้นแต่ได้รับอนุญาตจากผู้บังคับบัญชา หรือผู้อำนวยการศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศ

๑๐.๒ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้งาน

๑๐.๓ เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) เท่าที่จำเป็นตามที่กำหนดไว้ในกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๑๐.๔ ตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายทั้งหมดของกรม ให้ตรงกับเวลาอ้างอิงสากล (Stratum 0)

๑๐.๕ บันทึกข้อมูลกิจกรรมการใช้งานระบบสารสนเทศและระบบเครือข่าย เพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๑๐.๖ ตรวจสอบและดูแลสภาพแวดล้อมของห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ รวมทั้งระบบสนับสนุนการทำงานต่าง ๆ เพื่อป้องกันความเสียหายต่อระบบสารสนเทศและอุปกรณ์อย่างสม่ำเสมอ

๑๐.๗ จำกัดและควบคุมการใช้งานโปรแกรมสำหรับเครื่องคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมบางชนิดสามารถทำให้ผู้ใช้งานหลีกเลี่ยงมาตรการป้องกันทางความมั่นคงปลอดภัยด้านสารสนเทศของระบบได้ ดังนั้น เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยด้านสารสนเทศที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

(๑) จำกัดสิทธิการเข้าถึงและกำหนดสิทธิอย่างรัดกุม

(๒) กำหนดการอนุญาตใช้งานเป็นรายครั้ง

(๓) จัดเก็บโปรแกรมไว้ในสื่อภายนอกถ้าไม่ต้องใช้งานเป็นประจำ

/ (๔) มีการเก็บ...

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) ถอดถอนโปรแกรมที่ไม่จำเป็นออกจากเครื่องคอมพิวเตอร์

ข้อ ๑๑ การสำรองและกู้คืนข้อมูลสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๑.๑ กำหนดขั้นตอนการสำรองและกู้คืนข้อมูลรวมถึงซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) กำหนดระบบสารสนเทศสำคัญที่จำเป็นต้องสำรองข้อมูลไว้

(๒) ชื่อระบบสารสนเทศ

(๓) ประเภทข้อมูล เช่น ซอฟต์แวร์ ระบบปฏิบัติการ Log File ข้อมูลบัญชีผู้ใช้งาน

(๔) ความถี่ในการสำรองข้อมูล

(๕) วิธีการสำรองข้อมูล

๑๑.๒ สำรองข้อมูลตามขั้นตอนและความถี่ที่กำหนดไว้ในแต่ละระบบ

๑๑.๓ ตรวจสอบผลสำเร็จของการสำรองข้อมูลทุกครั้ง

๑๑.๔ เลือกใช้สื่อที่เหมาะสม โดยมีอายุจัดเก็บตามระยะเวลาที่กำหนด

๑๑.๕ นำข้อมูลสำรองไปเก็บไว้นอกสถานที่อย่างน้อยหนึ่งชุด

๑๑.๖ สุ่มข้อมูลสำรองมาทดสอบกู้คืน เพื่อตรวจสอบความถูกต้องและความพร้อมใช้งานของข้อมูลในกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละหนึ่งครั้ง

๑๑.๗ ทบทวนขั้นตอนสำรองและกู้คืนข้อมูลและประเมินผลการดำเนินการอย่างน้อยปีละหนึ่งครั้ง

ข้อ ๑๒ การบริหารความต่อเนื่องทางธุรกิจ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๒.๑ กำหนดระบบสารสนเทศสำคัญที่จำเป็นต่อการกู้คืนระบบ

๑๒.๒ ประเมินผลกระทบกรณีระบบสารสนเทศหยุดชะงักหรือใช้งานไม่ได้

๑๒.๓ ประเมินความเสี่ยงระบบสารสนเทศสำคัญ โดยพิจารณาจากกระบวนการดำเนินงาน การวิเคราะห์ผลกระทบทางธุรกิจเพื่อระบุเหตุการณ์ที่สามารถทำให้บริการระบบสารสนเทศสำคัญหยุดชะงักหรือไม่สามารถให้บริการได้ กำหนดแผนการลดความเสี่ยง และจัดการกับความเสี่ยงเหล่านั้น ทั้งนี้กำหนดให้มีการทบทวนความเสี่ยงและผลกระทบทางธุรกิจอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงสำคัญ หรืออย่างน้อยปีละหนึ่งครั้ง

๑๒.๔ กำหนดการวางแผนการบริหารความต่อเนื่องทางธุรกิจ ให้มีองค์ประกอบดังนี้

(๑) ขั้นตอนการเตรียมการ : รายละเอียดขั้นตอนก่อนเริ่มดำเนินการตามแผน

(๒) ขั้นตอนกรณีฉุกเฉิน : การปฏิบัติในกรณีฉุกเฉิน เมื่อเกิดเหตุคุกคาม

(๓) ขั้นตอนฟื้นฟู : สิ่งที่ต้องดำเนินการเพื่อฟื้นฟูกระบวนการที่มีความสำคัญ

(๔) ขั้นตอนดำเนินงาน : รายละเอียดขั้นตอนเพื่อกลับคืนสู่การดำเนินงานตามปกติ

/ ๑๒.๕ จัดทำแผน...

๑๒.๕ จัดทำแผนการบริหารความต่อเนื่อง โดยอ้างอิงจากมาตรฐานการบริหารความต่อเนื่องทางธุรกิจ ซึ่งมีรายละเอียดอย่างน้อยดังนี้

(๑) ลำดับของผู้มีอำนาจในการสั่งการใช้แผนกู้คืนระบบ

(๒) โครงสร้างของทีมกู้คืนระบบ

(๓) รายชื่อและข้อมูลติดต่อของทีมกู้คืนระบบ

(๔) การสั่งการใช้แผนกู้คืนระบบ

(๕) การสั่งย้ายสถานที่ไปยังห้องปฏิบัติการเครือข่ายคอมพิวเตอร์สำรอง

(๖) รวบรวมเอกสารและอุปกรณ์จำเป็น สำหรับใช้งานในห้องปฏิบัติการฯ สำรอง

(๗) การเตรียมความพร้อมของห้องปฏิบัติการฯ สำรอง

(๘) การแจ้งข้อมูลเหตุการณ์ฉุกเฉินให้ผู้ให้บริการภายนอกได้รับทราบ

(๙) การเริ่มต้นปฏิบัติงาน ณ ห้องปฏิบัติการฯ สำรอง

(๑๐) การกลับคืนสู่สภาวะการทำงานตามปกติ

(๑๑) ให้ความรู้แก่ผู้ที่เกี่ยวข้องทั้งหมดทั้งทีมกู้คืนระบบและผู้ให้บริการภายนอก เพื่อให้สามารถปฏิบัติได้อย่างถูกต้องเมื่อมีเหตุฉุกเฉินเกิดขึ้น

๑๒.๖ จัดทำแผนการทดสอบการกู้คืนระบบ และทดสอบตาม พร้อมบันทึกผลสรุปการดำเนินงาน และข้อเสนอแนะ พร้อมทั้งติดตามข้อบกพร่องที่พบในระหว่างทดสอบ เพื่อให้มีการปรับปรุงประสิทธิภาพต่อไปอย่างน้อยปีละหนึ่งครั้ง

๑๒.๗ ทบทวนแผนการบริหารความต่อเนื่องทางธุรกิจ โดยคำนึงถึงเหตุการณ์ในปัจจุบันและประสิทธิภาพของการปฏิบัติงานเป็นสำคัญอย่างน้อยปีละหนึ่งครั้ง

ข้อ ๑๓ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๓.๑ ปฏิบัติตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยที่กองงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด

๑๓.๒ จัดให้มีกระบวนการป้องกัน ตรวจสอบ และกู้คืนต่อภัยคุกคามทางไซเบอร์ของกรมอย่างเป็นระบบ รวมทั้งกระบวนการในการแจ้งเหตุและประสานงานกับหน่วยงานต่าง ๆ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ๒๕๖๒

๑๓.๓ ประเมินความเสี่ยงความมั่นคงปลอดภัยทางไซเบอร์ และทำแผนรับมือหรือตอบสนองต่อภัยคุกคามทางไซเบอร์ พร้อมพิจารณาทบทวนอย่างน้อยปีละหนึ่งครั้ง

๑๓.๔ ซักซ้อมแผนรับมือหรือตอบสนองต่อภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่สอดคล้องกับบริบทในปัจจุบันหรือตามสถานการณ์ที่ได้ประเมินความเสี่ยงไว้ และนำผลที่ได้จากการซักซ้อมมาแก้ไขปรับปรุงแผนรับมือหรือตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างน้อยปีละหนึ่งครั้ง

๑๓.๕ อบรม หรือประชาสัมพันธ์ หรือสื่อสาร เพื่อสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์กับผู้ที่เกี่ยวข้องอย่างสม่ำเสมอ

/ ๑๓.๖ ส่งเสริม...

๑๓.๖ ส่งเสริมและสนับสนุนให้ผู้ดูแลระบบได้รับการอบรมเพิ่มพูนความรู้ ทักษะในการจัดการและรักษาความมั่นคงปลอดภัยทางไซเบอร์

ข้อ ๑๔ การคุ้มครองข้อมูลส่วนบุคคล ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๔.๑ ในกรณีที่หน่วยงานจะต้องมีการร้องขอข้อมูลส่วนบุคคลเพื่อประกอบการดำเนินงานหน่วยงานนั้นต้องทำการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการจัดเก็บและดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลนั้น รวมทั้งจัดเก็บข้อมูลการให้ความยินยอมนั้นไว้เป็นหลักฐาน

๑๔.๒ ข้อมูลส่วนบุคคลที่กรมจัดเก็บ ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

๑๔.๓ จัดทำและประกาศใช้นโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลและดำเนินการตามนโยบายและแนวปฏิบัติดังกล่าวอย่างเคร่งครัด รวมทั้งกระบวนการบริหารจัดการเพื่อรองรับสิทธิของผู้เป็นเจ้าของข้อมูลส่วนบุคคลตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนด

๑๔.๔ จัดให้มีกระบวนการในการจัดการและแจ้งเหตุในกรณีที่ข้อมูลส่วนบุคคลถูกละเมิดความมั่นคงปลอดภัย ภายในระยะเวลาเจ็ดสิบสองชั่วโมงนับแต่เกิดเหตุ

ข้อ ๑๕ การปฏิบัติตามกฎหมาย และมาตรฐานสากล ผู้ดูแลระบบต้องปฏิบัติดังต่อไปนี้

๑๕.๑ ปฏิบัติตามกฎหมายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑๕.๒ ตรวจสอบ ควบคุม ไม่ให้มีการละเมิดทรัพย์สินทางปัญญา

๑๕.๓ ตรวจสอบเทคโนโลยีสารสนเทศของกรม ตามระยะเวลาที่เหมาะสม

๑๕.๔ จัดอบรมสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับผู้ใช้งานอย่างน้อยปีละหนึ่งครั้ง

๑๕.๕ ประชาสัมพันธ์ หรือสื่อสารเพื่อสร้างความตระหนักรู้กฎหมาย และมาตรฐานสากลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในลักษณะเกร็ดความรู้หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่ายผ่านทางระบบอินทราเน็ตของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการหรือช่องทางที่เหมาะสม

## หมวด ๒
## แนวปฏิบัติของผู้ใช้งาน

ข้อ ๑๖ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑๖.๑ ปฏิบัติตามมาตรการควบคุมการเข้า-ออก ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์อย่างเคร่งครัด

/ ๑๖.๒ ติดบัตร...

๑๖.๒ ติดบัตรแสดงตัวตนให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในพื้นที่ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์อย่างเคร่งครัด

๑๖.๓ ทำการยืนยันตัวตนก่อนเข้าห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ทุกครั้ง

๑๖.๔ ลงชื่อ บันทึกวัน เวลา และวัตถุประสงค์การเข้า-ออก ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ในสมุดลงชื่อให้ชัดเจนทุกครั้ง

๑๖.๕ ไม่นำอาหารและเครื่องดื่มเข้าไปภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

๑๖.๖ ไม่สูบบุหรี่ หรือกระทำการใด ๆ อันอาจก่อให้เกิดควันหรือเพลิงในบริเวณภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

ข้อ ๑๗ การบริหารจัดการสินทรัพย์ ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑๗.๑ ดูแลรักษาสินทรัพย์ที่กรมมอบไว้ให้ใช้งานเสมือนเป็นทรัพย์สินของตนเอง

๑๗.๒ ห้ามทิ้งสินทรัพย์ของกรมไว้โดยไม่มีผู้ดูแล ซึ่งรวมการทิ้งไว้ในรถยนต์ที่สามารถมองเห็นได้จากภายนอก

๑๗.๓ ห้ามให้ผู้อื่นยืมสินทรัพย์ของกรมไปใช้งาน

๑๗.๔ ใช้งานระบบสารสนเทศด้วยสินทรัพย์ของกรมเท่านั้น

๑๗.๕ แจ้งศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศก่อนดำเนินการเปลี่ยนจุดติดตั้ง หรือตรวจสอบสินทรัพย์ก่อนส่งซ่อม

๑๗.๖ ส่งสินทรัพย์คืนให้เจ้าหน้าที่ผู้รับผิดชอบของกลุ่มงานพัสดุ สำนักงานเลขานุการกรม เมื่อผู้ใช้งานต้องการยกเลิกสิทธิการครอบครองสินทรัพย์นั้น ๆ หรือพ้นสภาพการเป็นผู้ปฏิบัติงาน

๑๗.๗ ต้องดำเนินการป้องกันการเข้าถึงเครื่องคอมพิวเตอร์ส่วนตัวเมื่อนำมาใช้งานภายในเครือข่ายกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ

๑๗.๘ จัดวางสินทรัพย์ต่าง ๆ ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต

๑๗.๙ ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ให้บริการที่ต้องใช้บริการตลอด ๒๔ ชั่วโมง

๑๗.๑๐ ให้ผู้บังคับบัญชาและผู้อำนวยการศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศอนุมัติก่อนทุกครั้งในกรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ

๑๗.๑๑ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกเหนือจากที่กรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการได้ติดตั้งไว้ให้ใช้งาน

๑๗.๑๒ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้งานการตรวจสอบข้อมูลบนระบบเครือข่าย ยกเว้นการติดตั้งเพื่อการปฏิบัติงานของผู้ดูแลระบบที่เกี่ยวข้อง

/ ๑๗.๑๓ ห้ามติดตั้ง...

๑๗.๑๓ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครือข่ายของหน่วยงาน เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์นั้น หรือเครือข่ายของหน่วยงานได้

๑๗.๑๔ ต้องแจ้งผู้บังคับบัญชาและผู้อำนวยการศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศทันทีที่พบว่าสินทรัพย์เสียหาย สูญหาย หรือปรากฏว่ามีผู้อื่นเข้าถึงสินทรัพย์ดังกล่าว โดยที่ผู้ใช้งานมิได้อนุญาตเพื่อจัดการเหตุการณ์ได้อย่างมีประสิทธิภาพ

ข้อ ๑๘ การบริหารจัดการบัญชีผู้ใช้งาน (User Account) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑๘.๑ เปลี่ยนรหัสผ่านทันทีหลังจากได้รับแจ้งจากผู้ดูแลระบบ

๑๘.๒ กำหนดรหัสผ่าน (Password) ตามหลักเกณฑ์ดังนี้

(๑) รหัสผ่านต้องประกอบด้วยตัวอักษรตัวใหญ่ ตัวเล็ก ตัวเลข และตัวอักขระพิเศษ ผสมกันไม่น้อยกว่า ๘ ตัว เช่น YIS๒๐๑๙

(๒) ไม่ตั้งรหัสผ่านด้วยข้อมูลที่เกี่ยวข้องกับตนเอง เช่น ชื่อตนเองหรือครอบครัว ชื่อเล่น วันเดือนปีเกิด หรือทะเบียนรถยนต์

(๓) ไม่ตั้งรหัสผ่านด้วยคำศัพท์ที่มีอยู่ในพจนานุกรม

๑๘.๓ เก็บรักษาชื่อผู้ใช้งาน (Username) และรหัสผ่าน ของตนเองเป็นความลับ ไม่เผยแพร่ ไม่แจกจ่าย ไม่ใช้ร่วมกับผู้อื่น หรือทำให้ผู้อื่นล่วงรู้

๑๘.๔ รับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีผู้ใช้งานไม่ว่าการกระทำนั้น จะเกิดจากผู้ใช้งานหรือไม่ก็ตามสังเกตเห็นของบุคคลอื่นคอมพิวเตอร์

๑๘.๕ ไม่จดหรือบันทึกบัญชีผู้ใช้งานไว้ในสถานที่ที่ง่ายต่อการคาดเดา

๑๘.๖ ปิดเครื่องคอมพิวเตอร์ทุกครั้ง เมื่อผู้ใช้งานไม่อยู่ที่เครื่อง

๑๘.๗ เปลี่ยนรหัสผ่านทันที เมื่อคาดว่ามีบุคคลอื่นรู้รหัสผ่าน

๑๘.๘ ไม่ใช้รหัสผ่านซึ่งเคยใช้มาแล้ว (Password History) อย่างน้อยสามรหัสผ่าน

๑๘.๙ ไม่ควรใช้โปรแกรมคอมพิวเตอร์ช่วยจำรหัสผ่านโดยอัตโนมัติ

๑๘.๑๐ แจ้งผู้ดูแลระบบทันทีหากไม่สามารถใช้งานบัญชีผู้ใช้งานได้

๑๘.๑๑ ตั้งค่าเครื่องคอมพิวเตอร์ให้พักหน้าจอ เมื่อไม่มีการใช้งานเกิน ๑๕ นาที และต้องใส่รหัสผ่านอีกครั้งก่อนใช้งานเสมอ

ข้อ ๑๙ การบริหารจัดการความปลอดภัยเครือข่ายของกรม ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑๙.๑ ต้องใช้บริการสารสนเทศผ่านระบบเครือข่ายที่กำหนดเท่านั้น

๑๙.๒ ยื่นคำร้องขอใช้งาน เพื่อรับอนุญาตจากผู้บังคับบัญชา หรือผู้อำนวยการกองยุทธศาสตร์และแผนงาน และผู้อำนวยการศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศ ก่อนการเข้าถึงเครือข่ายภายในด้วยเครื่องคอมพิวเตอร์ส่วนตัว

/ ๑๙.๓ การใช้งาน...

๑๙.๓ การใช้งานเครือข่ายอินทราเน็ตจากภายนอก ผู้ใช้งานต้องเชื่อมต่อ VPN ตามที่กรมกำหนด

๑๙.๔ ห้ามกระทำการใด ๆ ที่ส่งผลกระทบ หรือรบกวนการส่งผ่านข้อมูลในระบบเครือข่าย ที่อาจทำให้ระบบเครือข่ายไม่สามารถทำงานได้ตามปกติ

ข้อ ๒๐ การใช้งานอุปกรณ์คอมพิวเตอร์ ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๐.๑ อุปกรณ์คอมพิวเตอร์ที่กรมจัดไว้ให้ใช้งาน มีวัตถุประสงค์เพื่อใช้ในการปฏิบัติงานของกรมเท่านั้น

๒๐.๒ ดูแลรักษาอุปกรณ์คอมพิวเตอร์โดยจัดเก็บไว้ในที่ปลอดภัย ไม่วางทิ้งไว้ในสถานที่เสี่ยงต่อการสูญหาย และหลีกเลี่ยงการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพาในสภาพแวดล้อมที่อาจมีผลกระทบต่อความเสียหายของอุปกรณ์

๒๐.๓ รับผิดชอบในการป้องกันการสูญหายของข้อมูล ในกรณีที่คอมพิวเตอร์ หรืออุปกรณ์สูญหาย หรือเสียหาย ผู้ใช้งานต้องแจ้งต่อผู้บังคับบัญชาโดยเร็ว

๒๐.๔ ดูแลรักษาข้อมูลของศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศ ที่จัดเก็บในอุปกรณ์คอมพิวเตอร์ให้สอดคล้องตามการบริหารจัดการข้อมูลหน่วยงาน

๒๐.๕ เมื่อผู้ใช้งานพ้นสภาพการเป็นเจ้าหน้าที่ ต้องส่งอุปกรณ์คอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องทั้งหมดคืนต่อกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ

๒๐.๖ การยืม การคืน หรือส่งซ่อมอุปกรณ์คอมพิวเตอร์แบบพกพาที่จัดไว้ให้ใช้งานให้เป็นไปตามขั้นตอนปฏิบัติที่กลุ่มงานพัสดุ สำนักงานเลขานุการกรมกำหนด

๒๐.๗ ห้ามผู้ใช้งานทำการเปลี่ยนแปลงแก้ไข Configuration หรือส่วนประกอบของอุปกรณ์คอมพิวเตอร์ โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้อำนวยการศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศ

๒๐.๘ การใช้อุปกรณ์คอมพิวเตอร์ที่กรมจัดไว้ให้ในการเข้าถึงระบบสารสนเทศ ผู้ใช้งานต้องยืนยันตัวตน (Authentication) ก่อนเข้าถึงระบบสารสนเทศ

๒๐.๙ เพื่อป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต ผู้ใช้งานจะต้องกำหนดมาตรการป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์ ได้แก่ การใช้บัญชีผู้ใช้งานและรหัสผ่าน หรือเทคโนโลยีไบโอเมตริก (biometric) หรือ PIN CODE

๒๐.๑๐ ก่อนการใช้งานกับสื่อบันทึกข้อมูลต้องตรวจสอบหาไวรัสคอมพิวเตอร์โดยโปรแกรมป้องกันไวรัสคอมพิวเตอร์

๒๐.๑๑ ไม่นำอาหาร เครื่องดื่ม มาวางใกล้บริเวณเครื่องคอมพิวเตอร์

๒๐.๑๒ ไม่วางของทับบนเครื่องคอมพิวเตอร์ หรือแป้นพิมพ์

๒๐.๑๓ กรณีเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าให้เรียบร้อยเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

/ ข้อ ๒๑ การบริหาร...

ข้อ ๒๑ การบริหารจัดการซอฟต์แวร์และทรัพย์สินทางปัญญา ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๑.๑ ไม่คัดลอก แก้ไข ถอดถอนโปรแกรมมาตรฐานต่าง ๆ ที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของกรมที่กำหนด หรือนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือนำไปให้ผู้อื่นใช้งาน

๒๑.๒ ไม่ติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ละเมิดทรัพย์สินทางปัญญา หากตรวจพบความผิดฐานละเมิดทรัพย์สินทางปัญญา จะถือว่าเป็นความผิดส่วนบุคคล

๒๑.๓ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติม

๒๑.๔ ปฏิบัติตามเงื่อนไขการใช้งานหรือที่กำหนดไว้

๒๑.๕ ห้ามเปลี่ยนแปลง แก้ไขซอฟต์แวร์ที่กรมจัดหามาใช้งาน เว้นแต่กรมได้รับอนุญาตให้เปลี่ยนแปลงแก้ไขได้จากเจ้าของลิขสิทธิ์

๒๑.๖ ไม่นำผลงานของผู้อื่นหรือผลงานใด ๆ ที่มีลิขสิทธิ์มาทำการ "คัดลอก" หรือ "ดัดแปลง" ก่อนได้รับอนุญาตจากเจ้าของลิขสิทธิ์

ข้อ ๒๒ การป้องกันโปรแกรมไม่พึงประสงค์ ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๒.๑ ไม่เปิดไฟล์ที่ไม่ทราบแหล่งที่มา หรือมาจากแหล่งที่มาที่ไม่น่าเชื่อถือ

๒๒.๒ การนำอุปกรณ์จัดเก็บข้อมูลต่าง ๆ เช่น Thumb Drive และ External HD มาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องตรวจสอบหาโปรแกรมไม่พึงประสงค์ก่อนทุกครั้ง

ข้อ ๒๓ การใช้งานอินเทอร์เน็ต ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๓.๑ ปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

๒๓.๒ ไม่ใช้งานอินเทอร์เน็ตของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและการเข้าสู่เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเป็นภัยต่อสังคม

๒๓.๓ ไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับของกรม โดยไม่ได้รับอนุญาต

๒๓.๔ ห้ามเปิดเผยข้อมูลสำคัญเกี่ยวกับงานของกรมที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๒๓.๕ ไม่เสนอความคิดเห็นหรือใช้ข้อความยั่วยุ ให้ร้ายบุคคลอื่น หรือข้อมูลที่ผิดกฎหมายในการใช้งานกระดานสนทนา (Web board) สาธารณะ หรือสื่อสังคมออนไลน์

๒๓.๖ ไม่ใช้งานโปรแกรมแบบเพียร์ทูเพียร์ (Peer to Peer : P2P) ผ่านเครือข่ายกรม

๒๓.๗ ไม่เข้าเว็บไซต์เครือข่ายสังคม (Social Network) เช่น Facebook Twitter หรือ Game online เป็นต้น นอกเหนือจากการปฏิบัติงานผ่านเครือข่ายกรม

๒๓.๘ ไม่ใช้งานสตรีมมิ่งมีเดีย (Streaming Media) โดยไม่ได้รับอนุญาต

๒๓.๙ ไม่ใช้โปรแกรมควบคุมระยะไกล (Remote Administrator) ผ่านเครือข่ายกรม

๒๓.๑๐ ปิดเว็บบราวเซอร์เมื่อสิ้นสุดการใช้งานเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

/ ข้อ ๒๔ การใช้งาน...

ข้อ ๒๔ การใช้งานจดหมายอิเล็กทรอนิกส์หรืออีเมล ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๔.๑ การปฏิบัติงานที่เกี่ยวข้องกับกรม ให้ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์หรืออีเมล (E-mail address) ของกรม (ชื่อบัญชีผู้ใช้งาน @dep.go.th) ที่ผู้ดูแลระบบกำหนดให้เท่านั้น

๒๔.๒ ระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์หรืออีเมล เพื่อไม่ให้เกิดความเสียหายต่อกรม เช่น ละเมิดทรัพย์สินทางปัญญา ละเมิดศีลธรรม สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย และต้องไม่แสวงหาผลประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ

๒๔.๓ ห้ามเข้าถึงจดหมายอิเล็กทรอนิกส์ของผู้อื่นโดยไม่ได้รับอนุญาต

๒๔.๔ ห้ามปลอมแปลงจดหมายอิเล็กทรอนิกส์

๒๔.๕ ใช้คำพูดที่สุภาพในการส่งจดหมายอิเล็กทรอนิกส์

๒๔.๖ สำรองข้อมูลจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอ

๒๔.๗ Log out ทุกครั้งเมื่อเลิกใช้งาน เพื่อป้องกันบุคคลอื่นเข้าใช้งาน

๒๔.๘ ตรวจสอบเอกสารที่แนบมาจากจดหมายอิเล็กทรอนิกส์โดยใช้โปรแกรมป้องกันไวรัสก่อนทำเปิดอ่าน

๒๔.๙ ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่ได้รับจากผู้ส่งที่ไม่รู้จัก หรือ Spam Mail เช่น การหลอกลวง การขายสินค้า หรือการสมัครสมาชิก

๒๔.๑๐ ตรวจสอบตู้จดหมายอิเล็กทรอนิกส์ (Inbox) ของตนเองทุกวันและควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้พื้นที่

ข้อ ๒๕ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๕.๑ กรณีใช้การประชาสัมพันธ์ผ่านเครือข่ายสังคมออนไลน์ (Social Network) ในนามของกรม ผู้รับผิดชอบต้องแสดงตำแหน่ง และสังกัดให้ชัดเจน เพื่อความน่าเชื่อถือ โดยอาจใช้รูปสัญลักษณ์หรือเครื่องหมายแสดงสังกัดได้

๒๕.๒ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ควรนำเสนอเกี่ยวกับภารกิจของกรม และข่าวสารที่เป็นประโยชน์ ใช้ภาษาที่สุภาพ มีความถูกต้อง และมีรูปแบบที่น่าสนใจ โดยเนื้อหาต้องผ่านความเห็นชอบจากผู้บังคับบัญชาก่อนทุกครั้ง

๒๕.๓ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของกรมผ่านเครือข่ายสังคมออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๒๕.๔ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่าง ต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนา ปรับปรุง แก้ไขในเรื่องที่เกี่ยวข้องต่อไป

๒๕.๕ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งาน (User) ต้องรับผิดชอบความเสียหายที่เกิดขึ้น และแจ้งต่อผู้อำนวยการกลุ่มสื่อสารองค์กรโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

/ ๒๕.๖ ต้องมีความ...

๒๕.๖ ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบจากการใช้งานเครือข่ายสังคมออนไลน์

๒๕.๗ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่กรมได้กำหนดไว้เท่านั้น

ข้อ ๒๖ การบริหารจัดการข้อมูลหน่วยงาน ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๖.๑ ระมัดระวังในการนำสื่อบันทึกข้อมูลให้ผู้อื่นใช้งาน

๒๖.๒ ดูแลรักษาความลับของข้อมูลลับ โดยหากข้อมูลอยู่ในรูปแบบอิเล็กทรอนิกส์จะต้องมีการป้องกันการเข้าถึงจากผู้ไม่มีสิทธิ หรือพิจารณาใช้มาตรการการเข้ารหัสโดยจะต้องใช้เทคโนโลยีที่ทางกรมกำหนดให้ หรืออย่างน้อยจะต้องเป็นเทคโนโลยีที่ได้รับการยอมรับและเป็นที่รู้จักดี

๒๖.๓ ไม่นำข้อมูลไปเปิดเผยกับบุคคลซึ่งไม่มีความเกี่ยวข้องกับการปฏิบัติหน้าที่ เว้นแต่ได้รับอนุญาตจากผู้บังคับบัญชา

๒๖.๔ กำหนดประเภท ลำดับชั้นความลับ รวมถึงระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึงสำหรับข้อมูลสารสนเทศแต่ละชนิดอย่างเหมาะสม

๒๖.๕ การจัดลำดับชั้นความลับของข้อมูล แบ่งออกเป็น ๕ ระดับ ดังนี้

(๑) ระดับเปิดเผยได้ (Pubic) หมายถึง สารสนเทศที่เปิดเผยสู่สาธารณะชน โดยบุคคลที่มีหน้าที่หรือได้รับมอบอำนาจให้ดำเนินการเผยแพรได้ โดยสารสนเทศที่เปิดเผยดังกล่าวได้ถูกพิจารณาแล้วว่าเมื่อมอบให้บุคคลอื่นแล้วจะไม่ก่อให้เกิดความเสียหายต่อหน่วยงาน

(๒) ระดับส่วนบุคคลของผู้ปฏิบัติงาน (Personal) หมายถึง สารสนเทศที่เป็นข้อมูลของแต่ละบุคคลที่ใช้ในการปฏิบัติงาน

(๓) ระดับส่วนบุคคลของผู้ใช้บริการ (Data Privacy) หมายถึง สารสนเทศที่เป็นข้อมูลของผู้ใช้บริการจัดเก็บไว้ในระบบหรือระบบงานเพื่อดำเนินการต่าง ๆ

(๔) ระดับใช้ภายในเท่านั้น (Internal Use Only หรือ Internal Use) หมายถึง สารสนเทศทั่วไปที่ใช้สื่อสารกันภายในเท่านั้น

(๕) ระดับลับ (Confidential) หมายถึง สารสนเทศที่มีความสำคัญ

๒๖.๖ ระดับการเข้าถึง คือ

(๑) การเข้าถึงเพื่อการอ่าน (Read)

(๒) การเข้าถึงเพื่อการเขียน (Write)

(๓) การเข้าถึงเพื่อการแก้ไข (Edit)

(๔) การเข้าถึงเพื่อการลบ (Delete)

๒๖.๗ เวลาที่ได้เข้าถึง สามารถเข้าถึงข้อมูลได้ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน หรือตามภารกิจและความจำเป็นที่ได้รับมอบหมาย

/ ๒๖.๘ ช่องทางการ...

๒๖.๘ ช่องทางการเข้าถึง ต้องจำกัดช่องทางการใช้งานหรือการเข้าถึงข้อมูลเท่าที่มีความจำเป็นต่อการใช้งานเท่านั้น

ข้อ ๒๗ การบริหารจัดการการเข้ารหัสข้อมูล ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๗.๑ กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูล ครอบคลุม ขอบเขตหน้าที่ ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง วิธีการเข้ารหัสข้อมูล (Cryptographic Algorithm) ที่สอดคล้องตามระดับความสำคัญของข้อมูล และการบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key Management)

๒๗.๒ กำหนดให้มีการเข้ารหัสข้อมูลสำคัญและช่องทางการสื่อสารที่ใช้รับ-ส่งข้อมูลสำคัญกับภายนอก

๒๗.๓ วิธีการเข้ารหัสข้อมูล ควรใช้มาตรฐานการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากล โดยมีการทบทวนประสิทธิภาพของวิธีการเข้ารหัสข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานยังคงมีความแข็งแรงเพียงพอ

๒๗.๔ การบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key Management) ควรกำหนดกระบวนการที่มีความรัดกุม ปลอดภัยครอบคลุมตั้งแต่การสร้าง ติดตั้ง จัดเก็บ และยกเลิก โดยสร้างรหัสที่มีความรัดกุมปลอดภัย มีความยาวเพียงพอ ป้องกันการถูกโจมตี และไม่ใช้กุญแจเข้ารหัสข้อมูลเดียวกันกับหลายระบบสารสนเทศ มีการรักษาความปลอดภัยของกุญแจเข้ารหัสข้อมูลทั้งด้าน Physical และ Logical โดยใช้อุปกรณ์รักษาความปลอดภัย HSM หรืออุปกรณ์ที่ทำหน้าที่ในลักษณะเดียวกัน สำรองข้อมูลกุญแจเข้ารหัสข้อมูล โดยวิธีการเก็บรักษากุญแจต้องมีความปลอดภัยในระดับเดียวกับกุญแจหลัก และต้องเพิกถอนกุญแจเข้ารหัสข้อมูล เช่น กรณีกุญแจหมดอายุ ล้าสมัย หรือไม่ปลอดภัย โดยต้องมั่นใจว่าไม่นำกุญแจนั้นมาใช้งานได้อีก

ข้อ ๒๘ การใช้งานโปรแกรมให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๘.๑ ห้ามติดตั้งซอฟต์แวร์อื่น ๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ไฟล์อื่นที่กรมไม่อนุญาตให้ใช้งาน

๒๘.๒ ซอฟต์แวร์ที่ใช้ต้องมีลิขสิทธิ์การใช้งานที่ถูกต้อง ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบเพียงผู้เดียว

๒๘.๓ หากต้องการใช้งานโปรแกรมที่ไม่อนุญาต เนื่องจากโปรแกรมบางชนิดสามารถทำให้ผู้ใช้ไม่ปลอดภัย ต้องได้รับความเห็นชอบที่เป็นลายลักษณ์อักษรจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้ที่ได้รับมอบหมายให้เป็นผู้พิจารณาอนุญาต

๒๘.๔ กำหนดให้มีการถอดถอนการติดตั้งโปรแกรมอรรถประโยชน์รวมทั้งซอฟต์แวร์ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ไม่จำเป็นออกจากระบบ เมื่อไม่จำเป็นต้องใช้งานรู้รหัสทั้งหมด

/ หมวด ๓...

## หมวด ๓
## การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ

ข้อ ๒๙ การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศของกรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ ให้ปฏิบัติดังต่อไปนี้

๒๙.๑ การจัดหาและพัฒนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ ให้หน่วยงานประสานงานกับศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศ เพื่อพิจารณาให้ความเห็นด้านความมั่นคงปลอดภัย และความสอดคล้องกับโครงสร้างพื้นฐานและเครือข่ายของกรมก่อนนำเสนอพิจารณาอนุมัติจัดหาและพัฒนาทุกครั้ง

๒๙.๒ การจัดหาและพัฒนาที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่มีความสำคัญ และมีลักษณะสุ่มเสี่ยงต่อความล้มเหลวในการให้บริการหากมีเพียงชุดเดียว ให้ผู้รับผิดชอบพิจารณาจัดหาอุปกรณ์สำรองไว้ ทั้งนี้ ต้องได้รับความเห็นชอบจากผู้บริหาร

๒๙.๓ การพิจารณาให้ความเห็นด้านความมั่นคงปลอดภัย ให้คำนึงถึงเรื่องดังต่อไปนี้

(๑) ทรัพย์สินทางปัญญา เช่น ชุดคำสั่ง (Source Code) ในการพัฒนาระบบ

(๒) การตรวจสอบด้านคุณภาพและความถูกต้องของระบบสารสนเทศ

(๓) การตรวจสอบชุดคำสั่งที่ไม่พึงประสงค์

(๔) ข้อจำกัดในการเปิดเผยข้อมูลของกรม

(๕) มาตรฐานและคุณภาพการให้บริการด้านความมั่นคง

(๖) การทดสอบระบบสารสนเทศ

๒๙.๔ ไม่อนุญาตให้นำข้อมูลสำคัญของกรม เช่น ข้อมูลลับ ข้อมูลส่วนบุคคล หรือข้อมูลใช้ภายในเท่านั้น ไปใช้ในการทดสอบกับระบบงาน เพื่อป้องกันการรั่วไหลของข้อมูลเว้นแต่ได้รับการอนุมัติจากผู้บังคับบัญชาก่อน

๒๘.๕ ดูแล ติดตาม และควบคุมการปฏิบัติงานของผู้ให้บริการพัฒนาระบบสารสนเทศจากภายนอก (Outsourced system development) ให้เป็นไปตามนโยบายการพัฒนาระบบสารสนเทศของกรม

๒๔.๖ ต้องทดสอบการทำงานของระบบที่ได้รับการพัฒนาโดยผู้ใช้งานหรือผู้ทดสอบอื่นที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศดังกล่าว เพื่อให้มั่นใจได้ว่าระบบที่ได้รับการพัฒนาดังกล่าวสามารถทำงานได้ถูกต้องตรงความต้องการของผู้ใช้งาน ตามนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งนี้ ควรมีแนวทางควบคุม และป้องกันการรั่วไหลของข้อมูลที่ใช้ในการทดสอบ หากข้อมูลดังกล่าวเป็นความลับหรือมีความสำคัญ

/ ๒๙.๗ ต้องทดสอบ...

๒๙.๗ ต้องทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน พร้อมทั้งปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจ (Business continuity plan) ให้สอดคล้องกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศดังกล่าว

๒๙.๘ ต้องควบคุมสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ (Development Environment) ได้แก่ บุคลากรผู้พัฒนาระบบ ขั้นตอนการพัฒนาระบบ เทคโนโลยีสำหรับการพัฒนาระบบให้มีความมั่นคงปลอดภัย ขั้นตอนการพัฒนาระบบ ดังนี้

(๑) การรักษาความลับของข้อมูลที่นำมาประมวลผล จัดเก็บ ส่งผ่านระบบการควบคุม การนำข้อมูลเข้าและออกจากระบบที่อยู่ระหว่างการพัฒนา

(๒) การควบคุมการเข้าถึงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศอย่างรัดกุมเหมาะสม

(๓) ติดตามการเปลี่ยนแปลงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ

(๔) จัดเก็บข้อมูลสำรองในพื้นที่นอกกรมที่มีความมั่นคงปลอดภัย

๒๙.๙ ควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศตลอดทุกขั้นตอนตามการควบคุมที่ได้กำหนดไว้ โดยอย่างน้อยต้องมีในเรื่องดังต่อไปนี้

(๑) มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง

(๒) กำหนดวิธีปฏิบัติ โดยคำร้องขอให้แก้ไขหรือพัฒนาต้องมาจากผู้ที่มีสิทธิและอนุมัติคำขอโดยผู้มีอำนาจ ต้องควบคุมผลข้างเคียงที่อาจเกิดขึ้นเนื่องจากมีการแก้ไข มีการตรวจรับจากผู้มีอำนาจภายหลังการแก้ไขหรือพัฒนาแล้วเสร็จก่อนโอนย้ายระบบงาน รวมทั้งมีการจัดเก็บรายละเอียดทั้งหมด

(๓) กำหนดวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานในกรณีฉุกเฉิน บันทึกเหตุผลความจำเป็น และขออนุมัติจากผู้มีอำนาจทุกครั้ง

(๔) ปรับปรุงเอกสารประกอบระบบงานทั้งหมด หลังจากที่ได้มีการแก้ไขเปลี่ยนแปลง เพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และต้องจัดเก็บเอกสารดังกล่าว ในที่ปลอดภัยและสะดวกต่อการใช้งาน

(๕) จัดเก็บโปรแกรม version ก่อนการเปลี่ยนแปลงไว้ใช้งาน หรือมีกระบวนการกลับสู่สภาพเดิม (full-back) ของระบบงานในกรณีระบบงานผิดพลาดหรือไม่สามารถใช้งานได้

(๖) สื่อสารให้กับบุคคลที่เกี่ยวข้องได้รับทราบและปฏิบัติงานได้อย่างถูกต้อง

(๗) บันทึกและจัดเก็บหลักฐานทั้งหมดที่เกี่ยวข้องกับการเปลี่ยนแปลงเพื่อใช้ประกอบในกรณีที่มีการตรวจสอบ

/ หมวด ๔...

## หมวด ๔
## การบริหารจัดการความเสี่ยงและการตรวจสอบด้านเทคโนโลยีสารสนเทศ

---

ข้อ ๓๐ การบริหารจัดการความเสี่ยงให้ศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศปฏิบัติดังต่อไปนี้

๓๐.๑ กำหนดปัจจัยต่าง ๆ ที่เกี่ยวข้องกับการประเมินความเสี่ยง ดังนี้

(๑) เป้าหมายการประเมินความเสี่ยง

(๒) กระบวนการ วัตถุประสงค์ และข้อกำหนดทางธุรกิจ

(๓) กฎ ระเบียบ ข้อกำหนดในสัญญา และข้อบังคับที่กรมต้องปฏิบัติ

(๔) ข้อกำหนดด้านความมั่นคงปลอดภัย

(๕) เทคโนโลยีสารสนเทศที่กรมใช้งาน

(๖) ผลกระทบที่เกิดขึ้นหากระบบสารสนเทศไม่สามารถใช้งานได้

(๗) โอกาสการเกิดขึ้นของเหตุการณ์ความเสี่ยง

๓๐.๒ กำหนดเกณฑ์ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงและผลกระทบของเหตุการณ์

๓๐.๓ กำหนดระดับความเสี่ยงที่ยอมรับได้

๓๐.๔ วิเคราะห์และประเมินความเสี่ยงต่อสินทรัพย์สารสนเทศอย่างน้อยปีละหนึ่งครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงสินทรัพย์ของระบบสารสนเทศสำคัญแล้วส่งผลกระทบสูงต่อผลการประเมินความเสี่ยงล่าสุด และบริหารจัดการความเสี่ยงเหล่านั้น ดังนี้

(๑) ทำแผนลดความเสี่ยงโดยพิจารณาถึงลำดับความสำคัญในการดำเนินการ ค่าใช้จ่าย ความคุ้มค่า หรือประโยชน์ที่ได้รับ และผู้รับผิดชอบ

(๒) นำเสนอแผนต่อผู้บังคับบัญชา เพื่อพิจารณาและให้ข้อคิดเห็นตามความจำเป็น

(๓) ผู้บังคับบัญชาสั่งการให้ดำเนินการตามแผนและรายงานผลการดำเนินการให้ได้รับทราบเป็นระยะ ๆ จนกระทั่งเสร็จสิ้น

ข้อ ๓๑ การตรวจสอบด้านเทคโนโลยีสารสนเทศ ให้ศูนย์ข้อมูลคนพิการและเทคโนโลยีสารสนเทศปฏิบัติ ดังต่อไปนี้

๓๑.๑ จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศตามมาตรฐานสากล จากผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระภายนอกอย่างน้อยปีละหนึ่งครั้ง

๓๑.๒ จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศด้วยวิธีทางเทคนิคอย่างน้อยปีละหนึ่งครั้ง