บันทึกข้อความ

ส่วนราชการ กรมพินิจและคุ้มครองเด็กและเยาวชน ศูนย์เทคโนโลยีสารสนเทศ โทร ๐ ๒๑๔๑ ๓๕๘๖

ที่ ยธ ๐๖๑๐๕/ว ๒๐๓ **วันที่** ๒๕ พฤษภาคม ๒๕๖๖

เรื่อง ประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ. ๒๕๖๖

เรียน หัวหน้าหน่วยงานในสังกัดกรมพินิจและคุ้มครองเด็กและเยาวชน

ด้วยกรมพินิจและคุ้มครองเด็กและเยาวชน ได้ดำเนินการจัดทำประกาศกรมพินิจและคุ้มครองเด็กและเยาวชน เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ. ๒๕๖๖ เพื่อให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย สอดคล้องกับการพัฒนาของเทคโนโลยีสารสนเทศในปัจจุบัน และใช้เป็นกรอบและทิศทางในการปฏิบัติหน้าที่ของบุคลากรของกรมพินิจและคุ้มครองเด็กและเยาวชน

ในการนี้ กรมพินิจและคุ้มครองเด็กและเยาวชน จึงขอประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ. ๒๕๖๖ รายละเอียดปรากฏตามเอกสารแนบ ทั้งนี้ กรมพินิจและคุ้มครองเด็กและเยาวชน ได้ดำเนินการประชาสัมพันธ์ผ่านเว็บไซต์ของกรมพินิจและคุ้มครองเด็กและเยาวชน (https://www.djop.go.th) เมนูเอกสารเผยแพร่ อีกช่องทางหนึ่งด้วย

จึงเรียนมาเพื่อทราบ และถือปฏิบัติต่อไป

พันตำรวจโท
(วรรณพงษ์ คชรักษ์)
อธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชน

ประกาศกรมพินิจและคุ้มครองเด็กและเยาวชน
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมพินิจ
และคุ้มครองเด็กและเยาวชน พ.ศ. ๒๕๖๖

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กรมพินิจและคุ้มครองเด็กและเยาวชน จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมพินิจและคุ้มครองเด็กและเยาวชน เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ. ๒๕๖๖”

ข้อ ๒ ประกาศนี้ให้มีผลบังคับใช้นับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ บรรดาประกาศ หลักเกณฑ์ คำสั่ง หรือแนวปฏิบัติอื่นใดในส่วนที่ได้กำหนดไว้แล้วในประกาศนี้ หรือซึ่งขัดแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

ข้อ ๔ แนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ. ๒๕๖๖ มีดังนี้

(๑) ให้มีการเข้าถึงหรือควบคุมการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน ได้แก่ ระบบสารสนเทศ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่ายให้บริการระบบงานอุปกรณ์เครือข่าย และอุปกรณ์คอมพิวเตอร์อื่น ๆ ให้เป็นไปอย่างมั่นคงปลอดภัย

(๒) ให้มีการเตรียมความพร้อมของการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนอย่างต่อเนื่อง โดยการจัดทำแผนและขั้นตอนการปฏิบัติงานกรณีเกิดเหตุฉุกเฉิน และการจัดให้มีระบบสำรอง ให้สามารถรับมือกับกรณีเกิดเหตุฉุกเฉินและเพื่อให้สามารถกู้คืนระบบกลับมาได้ภายในระยะเวลาที่เหมาะสม

(๓) ให้มีการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศและระบบเทคโนโลยีสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนอย่างสม่ำเสมอ

(๔) ให้มีการรักษาไว้ซึ่งความลับ ความถูกต้อง ความสมบูรณ์ และความพร้อมใช้ของสารสนเทศและระบบเทคโนโลยีสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน

ข้อ ๕ กำหนด...

ข้อ ๕ กำหนดบทบาทหน้าที่รับผิดชอบตามแนบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน ดังนี้

(๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) เป็นผู้มีหน้าที่กำกับดูแล การดำเนินงานให้เป็นไปตามแนวนโนบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน

(๒) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่กำกับดูแลการใช้งานระบบสารสนเทศ การจัดทำและทบทวนปรับปรุงแนวนโนบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนให้เป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง

(๓) ผู้ดูแลระบบ มีหน้าที่ควบคุม ติดตาม และตรวจสอบ การใช้งานระบบสารสนเทศให้เป็นไปตามแนวนโนบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน

(๔) ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนตามสิทธิ์ที่ได้รับและอนุญาต และปฏิบัติตามแนวนโนบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน

ข้อ ๖ เพื่อให้การดำเนินการสอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนและสามารถปฏิบัติตามได้อย่างเป็นรูปธรรม กรมพินิจและคุ้มครองเด็กและเยาวชนจึงกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนตามแนวปฏิบัติท้ายประกาศนี้

ข้อ ๗ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่กรมพินิจและคุ้มครองเด็กและเยาวชน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) ของกรมพินิจและคุ้มครองเด็กและเยาวชน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๘ ประกาศนี้ให้กรมพินิจและคุ้มครองเด็กและเยาวชน ดำเนินการให้ผู้ที่เกี่ยวข้องและผู้ใช้งานทั้งหมดได้รับทราบโดยทั่วกันผ่านทางเว็บไซต์ http://www.djop.go.th ของกรมพินิจและคุ้มครองเด็กและเยาวชน พร้อมทั้งสร้างความรู้ ความเข้าใจ และจัดฝึกอบรมแก่ผู้ใช้งานเพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยคุกคามต่าง ๆ และผลกระทบที่เกิดจากการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

ข้อ ๙ ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้และให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง

ประกาศ ณ วันที่ ๒๙ พฤษภาคม พ.ศ. ๒๕๖๖

พันตำรวจโท

(วรรณพงษ์ คชรักษ์)

อธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชน

เอกสารแนบท้ายประกาศ
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ. ๒๕๖๖

สารบัญ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ. ๒๕๖๖

เพื่อให้การใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชน มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเชื่อถือได้ ตลอดจนดำเนินการให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กรมพินิจและคุ้มครองเด็กและเยาวชน จึงกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ พนักงานราชการ ลูกจ้างประจำ และลูกจ้างชั่วคราว ที่มีการปฏิบัติเกี่ยวกับระบบคอมพิวเตอร์ และบุคคลภายนอกที่ได้รับการแต่งตั้งจากอธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชนหรือผู้ซึ่งอธิบดีมอบหมายให้ใช้ระบบคอมพิวเตอร์ของกรมพินิจและคุ้มครองเด็กและเยาวชน

ข้อ ๒ คำนิยามในระเบียบนี้

"หน่วยงาน" หมายถึง หน่วยงานภายในของกรมพินิจและคุ้มครองเด็กและเยาวชน ในระดับต่าง ๆ เช่น กอง (ทุกกอง) งานตรวจราชการ (ทุกงาน) กลุ่ม (ทุกกลุ่ม) ศูนย์ (ทุกศูนย์) สำนักงานเลขานุการกรม ศูนย์ฝึกและอบรมเด็กและเยาวชน (ทุกศูนย์ฝึกฯ) สถานพินิจและคุ้มครองเด็กและเยาวชน (ทุกสถานพินิจฯ) รวมถึงหน่วยงานเฉพาะกิจที่กรมพินิจและคุ้มครองเด็กและเยาวชนจัดตั้ง

"ห้องเครื่องคอมพิวเตอร์แม่ข่าย" หมายถึง ห้องสำหรับเก็บเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายและอุปกรณ์ต่อพ่วง ของกรมพินิจและคุ้มครองเด็กและเยาวชน

"พื้นที่ปลอดภัย" หมายถึง ห้องเครื่องคอมพิวเตอร์แม่ข่าย ต้องมีมาตรฐานความมั่นคงปลอดภัยที่ดีพอกับระบบข้อมูลและเอกสารต่าง ๆ มาตรฐานด้านความมั่นคงปลอดภัย ได้แก่ การป้องกันการบุกรุกทางกายภาพ การลักขโมย เหตุการณ์ไฟไหม้ น้ำท่วม เหตุวินาศภัย รวมทั้งต้องมีมาตรฐานในด้านอุณหภูมิ ความชื้น และการควบคุมการเข้าออกในบริเวณพื้นที่อนุญาตให้ผ่านเข้าออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น

"ผู้บริหารระดับสูง" หมายถึง อธิบดีของกรมพินิจและคุ้มครองเด็กและเยาวชน และรองอธิบดีหรือผู้ที่ได้รับมอบอำนาจให้ดำเนินการแทน

"หัวหน้าหน่วยงาน" หมายถึง ผู้อำนวยการกอง ผู้ตรวจราชการกรม หัวหน้ากลุ่ม ผู้อำนวยการศูนย์ เลขานุการกรม ผู้อำนวยศูนย์ฝึกและอบรมเด็กและเยาวชน ผู้อำนวยการสถานพินิจและคุ้มครองเด็กและเยาวชน และให้หมายความรวมถึงหัวหน้าหน่วยงานเฉพาะกิจที่กรมพินิจและคุ้มครองเด็กและเยาวชนแต่งตั้ง

"ผู้มีอำนาจ" หมายถึง หัวหน้าหน่วยงาน หรือผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน ให้มีอำนาจตัดสินใจดำเนินการในเรื่องที่ได้รับมอบอำนาจ

"เลขานุการ" หมายถึง ผู้ทำหน้าที่จัดการดูแลและปฏิบัติงานในระบบรับ-ส่งหนังสือ และข่าวสารทางอิเล็กทรอนิกส์ให้กับหัวหน้าหน่วยงาน และให้กับเจ้าหน้าที่อื่น ๆ ของหน่วยงานนั้น

"เจ้าหน้าที่...

"เจ้าหน้าที่ดูแลเครื่องคอมพิวเตอร์และเครือข่ายสื่อสาร (Computer Operation Officer : COO)" หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลรับผิดชอบและประสานงานด้านเทคนิคเกี่ยวกับระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารภายในหน่วยงานทุกหน่วยงาน

"เจ้าหน้าที่ดูแลระบบความปลอดภัยสารสนเทศ" หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านระบบความปลอดภัยสารสนเทศ ภายในหน่วยงานทุกหน่วยงาน

"เจ้าหน้าที่บริหารระบบความปลอดภัยสารสนเทศ" หมายถึง หัวหน้าหน่วยงาน หรือเจ้าหน้าที่ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน

"ผู้ดูแลระบบ" หมายถึง ข้าราชการ พนักงานราชการ ผู้ที่ได้รับการแต่งตั้งให้ดูแลระบบคอมพิวเตอร์หรือบุคคลที่กรมพินิจและคุ้มครองเด็กและเยาวชน กำหนดให้ดูแลระบบคอมพิวเตอร์ และบริหารจัดการระบบคอมพิวเตอร์ของกรมพินิจและคุ้มครองเด็กและเยาวชน

"ผู้ดูแลระบบเครือข่ายสื่อสาร" หมายถึง ข้าราชการ พนักงานราชการ ผู้ที่ได้รับการแต่งตั้งให้ดูแลระบบเครือข่ายสื่อสาร หรือบุคคลที่กรมพินิจและคุ้มครองเด็กและเยาวชนกำหนดให้ดูแลและบริหารจัดการระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชน

"ผู้ตรวจระบบ" หมายถึง การตรวจระบบคอมพิวเตอร์ตามที่ได้รับแต่งตั้งและมอบหมาย

"ผู้ใช้งาน" หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว และบุคคลภายนอกที่ได้รับการแต่งตั้งจากอธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชนหรือผู้ซึ่งอธิบดีมอบหมายที่ต้องใช้ระบบงานและระบบคอมพิวเตอร์ตามความรับผิดชอบ

"ทรัพย์สิน (Asset)" หมายถึง เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายสื่อสารและความปลอดภัย อุปกรณ์คอมพิวเตอร์ อุปกรณ์ที่เกี่ยวข้อง ข้อมูลและสารสนเทศหรือทรัพย์สินอื่นใดที่เกี่ยวข้องกับระบบงานและระบบคอมพิวเตอร์

"สิทธิผู้ใช้งาน" หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบคอมพิวเตอร์ของกรมพินิจและคุ้มครองเด็กและเยาวชน

"บุคคลภายนอก" หมายถึง ผู้รับจ้าง เจ้าหน้าที่ของหน่วยงานภายนอกอื่น ๆ ทั้งที่เป็นหน่วยงานราชการหรือเอกชน

"ผู้รับบริการ" หมายถึง ประชาชน หรือผู้มีส่วนได้ส่วนเสีย หรือผู้รับบริการจากระบบสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงสารสนเทศ การประมวลผลข้อมูล หรือระบบเครือข่าย หรือใช้งานระบบคอมพิวเตอร์ทางอิเล็กทรอนิกส์ของกรมพินิจและคุ้มครองเด็กและเยาวชน

"ความมั่นคงปลอดภัยด้านสารสนเทศ (Information security)" หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ การพิสูจน์ตัวตน (Authentication) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

"การรักษา...

"การรักษาความมั่นคงปลอดภัยไซเบอร์" หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

"ภัยคุกคามทางไซเบอร์" หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

"ไซเบอร์" หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

"เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์" หมายถึง เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security incident)" หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"หนังสือ" หมายถึง หนังสือราชการ ตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๔๘ หรือข้อความที่ได้สร้าง ส่ง รับ จัดเก็บ โดยผ่านการประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์

"สารสนเทศ" หมายถึง ข้อมูลที่ผ่านการประมวลผล วิเคราะห์ ให้อยู่ในรูปแบบที่มีความหมายเพื่อนำไปใช้ประโยชน์ในงานของกรมพินิจและคุ้มครองเด็กและเยาวชน

"ข่าวสารอิเล็กทรอนิกส์" หมายถึง เรื่องราว หรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของข้อความ เสียงและภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้ โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ

"รหัสผู้ใช้ (Username)" หมายถึง รหัสประจำตัวผู้ใช้งานที่ถูกกำหนดขึ้น เพื่อการเข้าใช้ระบบคอมพิวเตอร์

"รหัสผ่าน (Password)" หมายถึง รหัสลับที่ผู้ใช้งานในระบบแต่ละราย ต้องใช้ควบคู่กับรหัสผู้ใช้ในการเข้าใช้ระบบคอมพิวเตอร์

"ที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (E-Mail Address)" หมายถึง หมายเลขประจำตัว หรือรหัสประจำตัวที่กำหนดให้แก่ผู้ใช้งาน หมายเลขนี้จะใช้สำหรับส่งจดหมาย หรือเรียกดูข้อความที่ส่งมาทางไปรษณีย์อิเล็กทรอนิกส์ ตัวโปรแกรมที่ใช้จะต้องทำหน้าที่เหมือนที่ทำการไปรษณีย์ โดยจะรับข่าวสารที่มีผู้ส่งมาแล้วเก็บรอไว้จนกว่าผู้รับจะเรียกออกมาดู

"การประมวลผล" หมายถึง การใช้คำสั่ง ชุดคำสั่ง หรือโปรแกรมจัดการกับข้อมูลเพื่อให้ได้สารสนเทศที่ต้องการ

"ระบบคอม...

"ระบบคอมพิวเตอร์" หมายถึง เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ (Hardware) โปรแกรมชุดคำสั่ง (Software) ระบบเครือข่ายสื่อสาร (Communication Network System) ระบบเครือข่ายคอมพิวเตอร์ (Computer Network) ระบบงาน (Application) ระบบสารสนเทศ (Information System) บุคลากร (People) และสภาพแวดล้อมทางกายภาพ (Physical Environment)

"โปรแกรมประยุกต์เฉพาะงาน" หมายถึง โปรแกรมหรือชุดคำสั่งที่เขียนขึ้น เพื่อให้ระบบคอมพิวเตอร์ทำงานเฉพาะอย่างหรือเฉพาะด้าน

"ข้อมูล (Data)" หมายถึง

(๑) "ข้อมูลนำเข้า" หมายถึง ข้อมูลที่ได้จากแบบรายงานข้อเท็จจริงหรือเอกสารอื่น ข้อมูลที่ได้มาจากสื่อบันทึกต่าง ๆ เช่น สื่อบันทึกข้อมูลต่าง ๆ ข้อมูลที่ได้รับมาจากระบบอิเล็กทรอนิกส์และข้อมูลที่ได้รับจากระบบอื่น ๆ

(๒) "ข้อมูลผลลัพธ์" หมายถึง ข้อมูลหรือข้อมูลสารสนเทศที่ได้จากการประมวลผลข้อมูลนำเข้า

(๓) "ข้อมูลคอมพิวเตอร์" หมายถึง ข้อมูลนำเข้า และข้อมูลผลลัพธ์ ซึ่งเป็นข้อมูลชนิดข้อความ รูปภาพ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจทำการประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์และกฎหมายที่เกี่ยวข้อง

(๔) "ข้อมูลจราจรทางคอมพิวเตอร์" หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของการบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"ระบบงานคอมพิวเตอร์" หมายถึง ระบบงานที่กรมพินิจและคุ้มครองเด็กและเยาวชนใช้ในการพัฒนาขึ้นแล้ว หรือจัดให้มีเพื่อใช้ในการปฏิบัติงานของกรมพินิจและคุ้มครองเด็กและเยาวชน

"ระบบรับ-ส่งหนังสือ และข่าวสารทางอิเล็กทรอนิกส์" หมายถึง

(๑) ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ ใช้สำหรับ สร้าง ส่ง และรับหนังสือหรือข่าวสารอิเล็กทรอนิกส์

(๒) ระบบจัดเก็บเอกสารอิเล็กทรอนิกส์ ใช้สำหรับ สร้าง ส่ง รับ และจัดเก็บ หนังสือ หรือข่าวสารอิเล็กทรอนิกส์

"ระบบลงลายมือชื่ออิเล็กทรอนิกส์" หมายถึง ระบบสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนที่สามารถลงลายมือชื่ออิเล็กทรอนิกส์ได้ และเป็นไปตามมาตรฐานที่สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์กำหนด

"ระบบเครือข่ายสื่อสาร" หมายถึง การติดต่อระหว่างคอมพิวเตอร์ระบบหนึ่งไปยังคอมพิวเตอร์อีกระบบหนึ่ง โดยผ่านสื่อที่เป็นสายเคเบิลหรือสื่อไร้สายและอุปกรณ์เครือข่ายสื่อสาร เป็นตัวเชื่อมโยงระหว่างกันเพื่อให้ผู้ใช้สามารถที่จะใช้งานข้ามระบบคอมพิวเตอร์ระหว่างกันได้ และติดต่อระหว่างผู้ใช้ได้อย่างกว้างขวางมากขึ้น

"ระบบเครือข่ายภายในกรม (Intranet)" หมายถึง ระบบเครือข่ายที่กำหนดให้มีการติดต่อสื่อสารระหว่างผู้ใช้เฉพาะภายในหน่วยงานของกรมพินิจและคุ้มครองเด็กและเยาวชนเท่านั้น

"ระบบเครือข่ายอินเทอร์เน็ต (Internet)" หมายถึง ระบบเครือข่ายที่ให้บริการข้อมูลข่าวสารและสารสนเทศ รวมถึงการติดต่อสื่อสารระหว่างผู้ใช้ภายในกรมพินิจและคุ้มครองเด็กและเยาวชนกับผู้ใช้ภายนอกกรมพินิจและคุ้มครองเด็กและเยาวชน

"ระบบเครือข่าย...

“ระบบเครือข่ายเอกซ์ทราเน็ต (Extranet)” หมายถึง ระบบเครือข่ายที่กำหนดเฉพาะให้มีการติดต่อสื่อสารระหว่างกรมพินิจและคุ้มครองเด็กและเยาวชนกับหน่วยงานภายนอกทั้งภาคราชการหรือเอกชน เช่นระบบ DXC เป็นต้น

“เลขที่อยู่ไอพี (IP Address)” หมายถึง เลขที่อยู่ประจำอุปกรณ์ หรือเครื่องคอมพิวเตอร์ชนิดต่าง ๆ โทรศัพท์สมาร์ทโฟน (Smart Phone) หรืออุปกรณ์พกพาอื่น (Mobile Devices) ที่ใช้บอกสถานที่ตั้ง ทิศทางและที่หมายที่ข้อมูลจะถูกส่งและรับเข้ามาว่ามาจากที่ใดและกลุ่มใดบนระบบเครือข่ายสื่อสารที่ได้มีการเชื่อมโยงกันไว้

“MAC Address” หมายถึง หมายเลขเฉพาะของการ์ดแลน (Lan Card) และการ์ดไวไฟ (Wifi Card) ที่ใช้กับเครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง ระบบเครือข่ายสื่อสาร และโทรศัพท์มือถือ โทรศัพท์สมาร์ทโฟน (Smart Phone) อุปกรณ์พกพาอื่น ๆ หมายเลขแมคเป็นเลขฐาน ๑๖ จำนวน ๖ ชุด คั่นด้วยเครื่องหมาย ":" เช่น ๐๐:๐๐:E๒:๙E:F๓:๖๓

“Web browser” หมายถึง เป็นโปรแกรมที่ทำให้เราสามารถอ่านไฮเปอร์เทกซ์ (hypertext) บนเวิลด์ไวด์เว็บได้ โปรแกรมที่มีชื่อที่เป็นที่นิยมในขณะนี้คือ Nestcape และ Microsoft Internet Explorer ดู world wide web ได้

“Cookies” หมายถึง ข้อมูลขนาดเล็กซึ่งถูกเก็บไว้ที่ web browser เช่น ข้อมูลการเข้าถึงเว็บไซต์หรือข้อมูลส่วนตัวของเราที่ได้มีการลงทะเบียนกับเว็บไซต์นั้นๆ

“Tunnel” หมายถึง การรับ-ส่งข้อมูล โดยพยายามหลีกเลี่ยงหรือหลบหลีกมาตรการป้องกัน (Firewall) ซึ่งอาศัยการเปลี่ยนแปลงข้อมูลต่าง ๆ ก่อนส่งออกจากเครื่องคอมพิวเตอร์ หนึ่ง ๆ เช่น การเปลี่ยนแปลงหมายเลข Port ให้บริการ

“Port” หมายถึง เลขฐาน ๑๖ บิต ตั้งแต่ ๐ ถึง ๖๕๕๓๕ หมายเลขพอร์ต แต่ละหมายเลขจะถูกกำหนดโดยเฉพาะจากระบบปฏิบัติการ หน่วยงาน Internet Assigned Numbers Authority (IANA) เป็นหน่วยงานกลางในการประสานการเลือกใช้พอร์ตว่าหมายเลขใดเหมาะสำหรับบริการใด

หมวด ๑...

หมวด ๑
บททั่วไป

ข้อ ๓ ความมุ่งหมายของระเบียบนี้

(๑) เพื่อเป็นมาตรฐานแนวทางปฏิบัติและความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง ได้แก่ ข้าราชการ พนักงานราชการ ลูกจ้างและบุคคลภายนอกที่ต้องใช้ระบบคอมพิวเตอร์ตามหน้าที่ความรับผิดชอบ

(๒) เพื่อเป็นกรอบและแนวทางการปรับปรุงและพัฒนาระบบสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน และยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยไปสู่ระดับสากล

(๓) เพื่อให้เกิดความเชื่อมั่นในระบบการรักษาความมั่นคงปลอดภัยการในการใช้ระบบสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนที่มีประสิทธิภาพ และประสิทธิผล

ข้อ ๔ ระบบคอมพิวเตอร์ของกรมพินิจและคุ้มครองเด็กและเยาวชน ถือเป็นทรัพย์สินของกรมพินิจและคุ้มครองเด็กและเยาวชนจึงให้ใช้ระบบคอมพิวเตอร์ เพื่อการปฏิบัติงานในราชการของกรมพินิจและคุ้มครองเด็กและเยาวชนเท่านั้น

หมวด ๒
การบริหารจัดการเครื่องคอมพิวเตอร์อุปกรณ์คอมพิวเตอร์ อุปกรณ์ด้านระบบรักษาความปลอดภัย และอุปกรณ์ด้านระบบเครือข่ายสื่อสาร

ข้อ ๕ การลงทะเบียนควบคุมดูแลเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์

(๑) ให้ฝ่ายบริหารงานทั่วไป/งานธุรการ ของแต่ละหน่วยงาน ดำเนินการ ดังนี้

(๑.๑) ให้ตรวจสอบหมายเลขเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์กับเอกสารใบส่งของให้ถูกต้อง ไม่ว่าจะได้รับการจัดสรร จัดซื้อจัดหาเอง หรือได้รับบริจาค

(๑.๒) ให้บันทึก/ปรับปรุงข้อมูลเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ลงในระบบจัดเก็บข้อมูลที่กรมพินิจและคุ้มครองเด็กและเยาวชนกำหนด ได้แก่ ระบบรายงานครุภัณฑ์คอมพิวเตอร์ ในแต่ละกรณี ดังนี้

(๑.๒.๑) ได้รับเครื่องคอมพิวเตอร์ และ/หรือ อุปกรณ์คอมพิวเตอร์ จากการจัดสรรใหม่ จากการบริจาค หรือการจัดซื้อจัดหาเอง

(๑.๒.๒) การปรับปรุง หรือการเพิ่มประสิทธิภาพเครื่องคอมพิวเตอร์ และ/หรือ อุปกรณ์คอมพิวเตอร์ เช่น เพิ่มขนาดหน่วยความจำ (Ram) เปลี่ยนขนาดฮาร์ดดิสก์ เป็นต้น

(๑.๒.๓) การโยกย้าย สับเปลี่ยน หรือการจำหน่ายเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์

(๒) ให้หัวหน้าหน่วยงานแต่งตั้งเจ้าหน้าที่ดูแลเครื่องคอมพิวเตอร์และเครือข่ายสื่อสาร (Computer Operation Officer : COO) เจ้าหน้าที่ดูแลระบบความปลอดภัยสารสนเทศ และเจ้าหน้าที่บริหารระบบความปลอดภัยสารสนเทศ พร้อมทั้งบันทึกรายชื่อเจ้าหน้าที่ดังกล่าวเข้าในระบบจัดการบัญชีผู้ใช้และสิทธิ์ในระบบรักษาความปลอดภัยกลาง (Single Sign On : SSO)

(๓) การนำ...

(๓) การนำอุปกรณ์คอมพิวเตอร์เข้าหรือออกนอกหน่วยงานของกรมพินิจและคุ้มครองเด็กและเยาวชน จะต้องได้รับอนุมัติจากหัวหน้าหน่วยงานหรือผู้ได้รับมอบหมาย และผู้ใช้งานต้องรับผิดชอบต่อความปลอดภัยของอุปกรณ์คอมพิวเตอร์ และความปลอดภัยของข้อมูลที่อยู่ภายในเครื่องคอมพิวเตอร์นั้น

(๔) ห้ามถอดและ/หรือประกอบชิ้นส่วนใด ๆ ของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ เว้นแต่จะได้รับอนุมัติจากหัวหน้าหน่วยงานหรือผู้ได้รับมอบหมาย และให้ดำเนินการตามข้อ (๑.๒)

(๕) ให้กำหนดชื่อเครื่องคอมพิวเตอร์ (Computer Name) โดยให้ใช้หมายเลขเครื่อง (Serial Number) เป็นชื่อเครื่องคอมพิวเตอร์ ซึ่งต้องปฏิบัติตามขั้นตอนในการกำหนดชื่อเครื่องคอมพิวเตอร์ ตามที่ศูนย์เทคโนโลยีสารสนเทศกำหนดไว้บนระบบเครือข่ายภายในกรม (Intranet)

(๖) ในกรณีที่เครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์สูญหาย ให้ผู้ใช้งานปฏิบัติตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการพัสดุ พ.ศ. ๒๕๓๕ และที่แก้ไขเพิ่มเติม

ข้อ ๖ การบำรุงดูแลรักษาเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์

(๑) ให้ศูนย์เทคโนโลยีสารสนเทศ ตรวจสอบดูแลและควบคุมสัญญาการบำรุงรักษาระบบคอมพิวเตอร์ ตลอดทั้งอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องกับระบบคอมพิวเตอร์ทุกชนิดให้เป็นไปตามสัญญา เช่น การจัดทำโครงการจัดจ้างบำรุงรักษาซ่อมแซมแก้ไข และแจ้งให้หน่วยงานที่เกี่ยวข้องทุกแห่งทราบกำหนดเวลาการบำรุงรักษาซ่อมแซมแก้ไขตามสัญญาที่กรมพินิจและคุ้มครองเด็กและเยาวชนทำไว้กับผู้รับจ้าง

(๒) ในกรณีที่เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ อุปกรณ์ด้านระบบรักษาความปลอดภัย และอุปกรณ์ด้านระบบเครือข่ายสื่อสารเกิดขัดข้อง ให้ผู้ใช้งานแจ้งไปยังผู้รับจ้างบำรุงรักษาซ่อมแซมแก้ไข เพื่อดำเนินการซ่อมแซมแก้ไขในทันที พร้อมทั้งบันทึกการแจ้งซ่อมในระบบแจ้งซ่อมคอมพิวเตอร์บนระบบเครือข่ายภายในกรม (Intranet) โดยผู้ใช้งานต้องแจ้งข้อมูลรายละเอียด วัน เวลาที่ผู้รับจ้าง ได้ดำเนินการตรวจซ่อมตามข้อเท็จจริง หากอุปกรณ์ดังกล่าวเกิดขัดข้องและหมดอายุการรับประกัน หรือหมดสัญญาบำรุงรักษา ให้ผู้ใช้งานปฏิบัติตามคำสั่งกรมพินิจและคุ้มครองเด็กและเยาวชนที่เกี่ยวข้อง

(๓) ผู้ใช้งานควรดูแลจัดการเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ให้สามารถทำงานได้อย่างมีประสิทธิภาพ เช่น การลบข้อมูลที่ไม่จำเป็นออกจากฮาร์ดดิสก์ (Cleanup Disk) การจัดเรียงข้อมูลฮาร์ดดิสก์ (Defragment Disk) ตามแนวทางที่ศูนย์เทคโนโลยีสารสนเทศ กรมพินิจและคุ้มครองเด็กและเยาวชนกำหนด

หมวด ๓...

หมวด ๓
การบริหารจัดการด้านโปรแกรมชุดคำสั่ง และโปรแกรมประยุกต์เฉพาะงาน

ข้อ ๗ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operation System Access Control)

แบ่งออกเป็นระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์ลูกข่ายประเภทที่ใช้ช่องสัญญาณมีสาย (Wired LAN) ระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์ลูกข่ายประเภทที่ใช้ช่องสัญญาณไร้สาย (Wireless LAN) และระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่าย โดยมีรายละเอียด ดังนี้

๗.๑ สำหรับผู้ดูแลระบบ

(๑) ระบุและยืนยันตัวตนของผู้ดูแลระบบ โดยชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ซึ่งได้รับมอบหมายอย่างเป็นทางการ

(๒) ผู้ดูแลระบบประจำกรมพินิจและคุ้มครองเด็กและเยาวชน (Super Administrator) ต้องติดตั้งและบริหารจัดการโปรแกรมช่วยบริหารจัดการ (Domain Controller) บนเครื่องคอมพิวเตอร์แม่ข่ายที่กำหนดขึ้น เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงานที่ใช้ช่องสัญญาณประเภทมีสายและไร้สาย โดยกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงานตามสิทธิการเข้าใช้งานระบบปฏิบัติการในระดับต่าง ๆ

(๓) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธียืนยันตัวตนที่มั่นคงปลอดภัย โดยมีข้อกำหนด ดังนี้

(๓.๑) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการคาดเดารหัสผ่าน จากเครื่องปลายทาง

(๓.๒) ดำเนินการปิดการเชื่อมต่อโดยตรงผ่านทาง Command Line เพื่อป้องกันการสูญเสียที่อาจจะเกิดขึ้นได้

(๓.๓) ดำเนินการปิดการเข้าสู่การตั้งค่าต่าง ๆ ในระบบปฏิบัติการของระบบคอมพิวเตอร์ลูกข่ายที่ได้เชื่อมต่อเข้าสู่ระบบเครือข่ายแบบมีสาย

(๔) การเข้าถึงระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย โดยใช้สิทธิในการติดตั้งโปรแกรมต่าง ๆ จะต้องเข้าถึงและดำเนินการโดยผู้ดูแลระบบในระดับของกรมเท่านั้น

(๕) การใช้งานโปรแกรมอรรถประโยชน์ (user of system utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมดังกล่าวในเครื่องคอมพิวเตอร์ที่มีข้อมูล หรือใช้ในงานสำคัญ เนื่องจากโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้งานหลีกเลี่ยงจากการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ ดังนั้น เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงจากการตรวจสอบ ให้เจ้าหน้าที่ที่ได้รับมอบหมายดำเนินการ ดังนี้

(๕.๑) กำหนด...

(๕.๑) กำหนดระดับสิทธิการติดตั้งโปรแกรมอรรถประโยชน์

(๕.๒) ผู้ดูแลระบบประจำกรมพินิจและคุ้มครองเด็กและเยาวชน (Super Administrator) จะมีสิทธิในการติดตั้งโปรแกรมอรรถประโยชน์เพิ่มเติมบนระบบปฏิบัติการของเครื่องคอมพิวเตอร์ส่วนบุคคลที่เชื่อมต่อผ่านระบบเครือข่ายของกรมพินิจและคุ้มครองเด็กและเยาวชน

(๕.๓) อนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์ในรายบุคคล จะต้องได้รับอนุญาตการขอติดตั้งโปรแกรมดังกล่าวโดยหัวหน้าหน่วยงาน/ส่วนราชการ เพื่อขอสิทธิการใช้งานดังกล่าว

(๕.๔) จัดเก็บข้อมูลการเรียกใช้งานโปรแกรมอรรถประโยชน์

(๕.๕) มีการถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๖) เครื่องคอมพิวเตอร์แม่ข่ายที่ได้ดำเนินการติดตั้งใหม่ ให้ดำเนินการปรับตั้งค่าคอนฟิกสำหรับอ้างอิงเวลาตามมาตรฐานเวลาของประเทศไทยตามอุปกรณ์อ้างอิงเวลาสากลในทันทีที่มีการติดตั้ง ณ พื้นที่กรมพินิจและคุ้มครองเด็กและเยาวชน ทั้งนี้ หากพบว่ามีเครื่องคอมพิวเตอร์แม่ข่ายเครื่องใดยังไม่ได้ดำเนินการปรับตั้งค่าอ้างอิงเวลาดังกล่าว ขอให้ผู้มีส่วนเกี่ยวข้องดำเนินการโดยทันที เพื่อประโยชน์ในการจัดเก็บ log ที่ถูกต้อง

๗.๒ สำหรับผู้ใช้งานทั่วไป

(๑) ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ซึ่งสามารถระบุตัวตนของผู้ใช้งาน โดยเลือกใช้เทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้

(๑.๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

(๑.๒) การอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกันได้นั้น พิจารณาตามความจำเป็นทางด้านธุรกรรมหรือด้านเทคนิค

(๑.๓) กำหนดอุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Smart Card หรือ Token เมื่อมีความจำเป็นเพิ่มเติม

(๒) กำหนดการบริหารจัดการรหัสผ่าน (password management system) โดยใช้ระบบบริหารจัดการรหัสผ่านที่สามารถสอบทานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ โดยกำหนดให้มาตรฐานการกำหนดรหัสผ่านของระบบ Active Directory เป็นพื้นฐานข้อกำหนด ทั้งนี้ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้กำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

(๓) ในการติดตั้งระบบปฏิบัติการตั้งต้น เมื่อได้ดำเนินการติดตั้งระบบเสร็จสิ้นแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้กำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันทีเพื่อป้องกันการเข้าติดตั้งโปรแกรมในระบบปฏิบัติการโดยผู้ใช้งานทั่วไป ทั้งนี้เพื่อป้องกันการติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์

(๔) ผู้ใช้งาน...

(๔) ผู้ใช้งานทั่วไปไม่สามารถติดตั้งโปรแกรมต่าง ๆ บนระบบปฏิบัติการของเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่ายประเภทมีสายด้วยตัวเองได้ ทั้งนี้เพื่อป้องกันการติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์

(๕) เมื่อมีการเว้นจากการใช้งานระยะหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(๕.๑) หลักเกณฑ์การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๑๕ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๐ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๕.๒) เมื่อไม่มีการใช้งานระบบต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๖) การเข้าถึงระบบปฏิบัติการของเครื่องคอมพิวเตอร์ลูกข่ายประเภทไร้สาย สามารถเข้าถึงได้โดยผู้ใช้งานทั่วไป แต่จะถูกจำกัดสิทธิการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด ซึ่งหมายถึงมีระดับสิทธิเสมือนเป็นผู้ใช้งานที่เป็นบุคคลภายนอกเท่านั้น

(๗) ผู้ใช้งานทั่วไปไม่สามารถเข้าใช้งานระบบปฏิบัติการที่ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายของกรมพินิจและคุ้มครองเด็กและเยาวชน

(๘) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ในการเชื่อมต่อระบบสารสนเทศ โปรแกรมที่มีความเสี่ยง หรือมีความสำคัญสูง ควรจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น และมีการยกเลิกการเชื่อมต่อระบบเครือข่ายไร้สายในเวลา ๓๐ นาที หรือตามความเหมาะสม หากไม่มีการใช้งานข้อมูลผ่านระบบเครือข่ายไร้สาย

ข้อ ๘ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ (Application and information access control)

๘.๑ สำหรับผู้ดูแลระบบ

(๑) ดำเนินการจำกัดการเข้าถึงสารสนเทศ (information access restriction) โดยการควบคุมผู้ใช้งาน และบุคลากรฝ่ายสนับสนุน ที่มีการเข้าใช้งานระบบสารสนเทศ โปรแกรมประยุกต์หรือแอพพลิเคชัน ดังนี้

(๑.๑) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของหน่วยงานตามข้อกำหนดการลงทะเบียนผู้ใช้งานหรือการบริหารจัดการสิทธิ์ของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิ์การเข้าถึงระบบสารสนเทศและข้อมูลต่าง ๆ

(๑.๒) ต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่าง ๆ และหากไม่มีการใช้งานเกินระยะเวลาที่กำหนด หรือยกเลิกการเชื่อมต่อระบบ

(๑.๓) ผู้ให้บริการภายนอก (Outsource) ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลหน่วยงาน

(๑.๔) ผู้ดูแล...

(๑.๔) ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิ์การเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

(๑.๕) ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource) ให้มีสิทธิ์การเข้าถึงข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ทุกครั้ง

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อกรมพินิจและคุ้มครองเด็กและเยาวชน จะต้องดำเนินการ ดังนี้

(๒.๑) ต้องมีการระบุความสำคัญของระบบงานซึ่งไวต่อการรบกวน หรือมีผลกระทบสูงต่อหน่วยงาน

(๒.๒) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ

(๒.๓) มีการประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกัน ระหว่างระบบงานที่มีความสำคัญสูงกับระบบงานอื่น ๆ ที่มีความสำคัญน้อยกว่า

(๒.๔) ต้องควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ ได้แก่การตรวจสอบและดูแลสภาพแวดล้อมภายในบริเวณพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในพื้นที่รับผิดชอบของกรมพินิจและคุ้มครองเด็กและเยาวชน

(๒.๕) มีการสำรองและทดสอบการกู้คืนระบบ ตามนโยบายระบบสารสนเทศและระบบสำรองสารสนเทศ

(๒.๖) ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

(๒.๗) ทำการควบคุมเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกตามข้อกำหนดที่ตั้งค่าไว้ใน Firewall หรืออุปกรณ์ระบุเส้นทางบนเครือข่าย (Routing)

๘.๒ สำหรับผู้ใช้งานทั่วไป

การเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศด้วยอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ (Mobile Computing) จะต้องมีการควบคุมการใช้งาน โดยมีขั้นตอนการควบคุม ดังนี้

(๑) ผู้ที่จะใช้งานผ่านอุปกรณ์เคลื่อนที่ดังกล่าว จะต้องกรอกแบบฟอร์มตามรูปแบบที่เจ้าหน้าที่ผู้รับชอบดูแลระบบกำหนดไว้

(๒) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ พิจารณาอนุญาตเป็นรายกรณีเมื่อผ่านการพิจารณาและจะส่งต่อให้ผู้ดูแลระบบประจำกรมพินิจและคุ้มครองเด็กและเยาวชนตรวจสอบและดำเนินการกำหนดสิทธิ์การใช้งาน และแจ้งกลับบุคคลดังกล่าวทราบ เป็นลายลักษณ์อักษรหรือผ่านช่องทางจดหมายอิเล็กทรอนิกส์

(๓) ผู้ใช้งาน...

(๓) ผู้ใช้งานทั่วไปที่ใช้อุปกรณ์สื่อสารเคลื่อนที่ในการเข้าถึงระบบเครือข่ายของหน่วยงานจะไม่สามารถเข้าถึงระบบเครือข่ายที่จัดทำขึ้นเพื่อใช้สำหรับเป็นช่องทางเฉพาะ เว้นแต่ได้รับสิทธิ์พร้อมทั้งมีการยืนยันตัวบุคคลจากรหัสผู้ใช้งานและรหัสผ่าน ก่อนการเข้าใช้งานระบบแล้วเท่านั้น

(๔) การเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงานต้องใช้งานตามสิทธิ์ที่ตนเองได้รับ หากมีการส่งมอบรหัสผู้ใช้งานและรหัสผ่านของตนเองให้บุคคลอื่นดำเนินการต่าง ๆ ในระบบสารสนเทศแทนตนเองแล้ว และหากเกิดความเสียหายขึ้น ผู้ส่งมอบรหัสผ่านจะต้องรับผิดชอบต่อความเสียหายนั้นในทุกกรณี

๘.๓ สำหรับผู้ดำเนินการจากภายนอก (Out Source) ตามโครงการที่มีการจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์แม่ข่ายและระบบงานสารสนเทศ หรือโครงการในลักษณะที่มีการจัดจ้างดำเนินการอื่นๆ ที่มีความเกี่ยวข้องกับข้อมูลสารสนเทศหรือระบบเครือข่ายของหน่วยงาน มีข้อปฏิบัติที่ต้องดำเนินการ ดังนี้

(๑) พิสูจน์ตัวตนก่อนเข้าดำเนินการบำรุงรักษาระบบสารสนเทศ

(๒) ดำเนินการทดสอบการใช้งานของระบบสารสนเทศตามรอบระยะเวลาที่เหมาะสม

(๓) หากพบปัญหาในระหว่างดำเนินการบำรุงรักษาระบบงาน จะต้องแจ้งต่อผู้ดูแลระบบทราบในทันทีพร้อมดำเนินการแก้ไขให้แล้วเสร็จตามข้อกำหนดในสัญญาว่าจ้าง หรือระยะเวลาที่เหมาะสม และจัดทำรายงานสรุปผล และข้อเสนอข้อแก้ไขดังกล่าว

(๔) การดำเนินการใด ๆ ของผู้ดำเนินการจากหน่วยงานภายนอก จนทำให้เกิดความเสียหายต่อโปรแกรมประยุกต์ แอพพลิเคชัน หรือสารสนเทศของหน่วยงาน รวมถึงข้อมูลบนระบบฐานข้อมูลที่ติดตั้งบนระบบคอมพิวเตอร์แม่ข่าย และส่งผลกระทบต่อการทำงานของหน่วยงานจนทำให้เกิดความเสียหายต่อหน่วยงาน ผู้ดำเนินการดังกล่าวจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นในทุกกรณี ทั้งนี้ จะต้องกำหนดไว้ในสัญญาจัดจ้างทุกครั้ง

(๕) การเข้าถึงและใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงาน จะต้องใช้งานตามสิทธิ์ที่ตนเองได้รับ ซึ่งหากมีการส่งมอบรหัสผู้ใช้งานและรหัสผ่านของตนเองให้บุคคลอื่น ๆ ดำเนินการต่างๆ ในระบบสารสนเทศแทนตนเอง และเกิดความเสียหายขึ้น ผู้ส่งมอบรหัสผ่านจะต้องรับผิดชอบต่อความเสียหายนั้นในทุกกรณี

(๖) ผู้ดำเนินการจากหน่วยงานภายนอก ต้องยอมรับในข้อกำหนดการรักษาความลับของข้อมูลสารสนเทศ ข้อมูลระบบเครือข่าย และข้อมูลระบบรักษาความปลอดภัยต่าง ๆ ที่เกี่ยวข้องต่อความมั่นคงปลอดภัยด้านข้อมูลและสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน

ข้อ ๙ ต้องจัดให้มีระบบสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและต้องจัดทำแผนรองรับ ความเสี่ยง (Risk Plan) หรือแผนถอยกลับไปที่ระบบงานก่อนการเปลี่ยนแปลง (Fall Back Procedure) และทดสอบแผนงานดังกล่าวให้สามารถปฏิบัติได้จริง

ข้อ ๑๐ การพัฒนาโปรแกรมที่มีการติดต่อสื่อสารระหว่างหน่วยงาน ให้แจ้งหมายเลข Port ที่ให้บริการในโปรแกรมนั้นๆต่อผู้ดูแลระบบเครือข่ายสื่อสารเพื่อพิจารณาความเหมาะสมในการเปิด Port ให้บริการก่อนนำโปรแกรมขึ้นใช้งาน

หมวด ๔...

หมวด ๔
การบริหารจัดการระบบเครือข่ายสื่อสาร

ข้อ ๑๑ การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

๑๑.๑ ผู้ดูแลระบบประจำกรมพินิจและคุ้มครองเด็กและเยาวชน ต้องมีการออกแบบระบบเครือข่ายให้ชัดเจนและรัดกุม เพื่อทำให้การควบคุมและป้องกันการบุกรุกเป็นไปอย่างมีประสิทธิภาพ

๑๑.๒ ผู้ดูแลระบบประจำกรมพินิจและคุ้มครองเด็กและเยาวชน ต้องกำหนดวิธีในการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถ ใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น ดังนี้

(๑) มีการกำหนดการเข้าถึงระบบสารสนเทศ โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้ โดยการใช้รหัสผู้ใช้งาน และรหัสผ่านในการยืนยันตัวบุคคล โดยภายหลังระบุตัวตนแล้วจะสามารถเข้าถึงระบบเครือข่ายตามระดับการควบคุม ดังนี้

- ระดับการควบคุมการเข้าถึงระบบเครือข่าย แบ่งเป็นระบบเครือข่ายสำหรับผู้แลระบบระดับกรม ผู้ดูแลระบบระดับหน่วยงาน และสำหรับผู้ใช้งานทั่วไป
- ระดับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงาน โดยแบ่งเป็นผู้ดูแลระบบสารสนเทศระดับกรม ผู้ดูแลระบบสารสนเทศ และผู้ใช้งานทั่วไปที่มีสิทธิ์เข้าถึงระบบ
- ควบคุมการเข้าถึงระบบปฏิบัติการ โปรแกรมประยุกต์หรือแอพพลิเคชันต่าง ๆ แบ่งเป็นผู้ดูแลระบบระดับหน่วยงาน และผู้ใช้งานทั่วไป

(๒) ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น ได้แก่ ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นจากผู้บังคับบัญชาระดับหัวหน้างานขึ้นไปเป็นลายลักษณ์อักษรและต้องทบทวนสิทธิดังกล่าว อย่างน้อยทุก ๓ เดือน

(๓) กรณีที่มีการเปลี่ยนแปลงผู้ใช้งาน หรือพ้นสภาพจากการปฏิบัติงานของกรมพินิจและคุ้มครองเด็กและเยาวชน หน่วยงานต้นสังกัดของผู้ใช้งานดังกล่าว จะต้องแจ้งศูนย์เทคโนโลยีสารสนเทศทราบเป็นลายลักษณ์อักษร ภายใน ๗ วันทำการ หรือในกรณีที่เป็นผู้ใช้งานจากหน่วยงานภายนอกให้เป็นไปตามที่ผู้ดูแลระบบกำหนด

๑๑.๓ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องดำเนินการตามข้อปฏิบัติหรือกระบวนการเพื่อยืนยันบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

(๑) กำหนดผู้ใช้งานที่จะเข้าใช้งานระบบเครือข่าย แสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อยืนยันตัวบุคคล (Authentication) ตามกระบวนการขอเข้าใช้งานระบบงาน

(๒) การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต จะต้องกำหนดให้มีการตรวจสอบสิทธิผู้ใช้งานด้วยทุกครั้ง โดยตรวจสอบสิทธิเพื่อพิสูจน์ตัวตน

(๓) เข้าใช้งาน...

(๓) เข้าใช้งานโปรแกรมควบคุมเครื่องจากระยะไกล (VPN) เพื่อใช้งานระบบภายในกรมพินิจและคุ้มครองเด็กและเยาวชน จะต้องประสานผู้รับผิดชอบดูเครือข่ายของกรมพินิจและคุ้มครองเด็กและเยาวชน ซึ่งผู้ใช้งานจำเป็นต้องปฏิบัติงานทุกครั้ง

๑๑.๔ ผู้ดูแลประจำกรมพินิจและคุ้มครองเด็กและเยาวชน เป็นผู้พิจารณาและกำหนดช่องทาง/เส้นทางการเข้าถึงเครือข่าย โดยควบคุมการเข้าถึงการใช้งาน ให้สอดคล้องกับแนวปฏิบัติ ดังนี้

(๑) มีการตรวจสอบการเชื่อมต่อเครือข่าย และกำหนดสิทธิตามสิทธิผู้ใช้งาน

(๒) มีระบบป้องกันการบุกรุกระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๓) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

๑๑.๕ ผู้ดูแลระบบประจำกรมพินิจและคุ้มครองเด็กและเยาวชน จะต้องกำหนดการใช้เส้นทางบนเครือข่ายจากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้

๑๑.๖ ต้องมีการมอบหมายบุคคลที่รับผิดชอบในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน

๑๑.๗ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ให้เชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก เช่น ผ่านอุปกรณ์ Firewall

ข้อ ๑๒ การขอเลขที่อยู่ไอพี (IP Address)

(๑) ศูนย์เทคโนโลยีสารสนเทศมีหน้าที่กำหนดเลขที่อยู่ไอพี (IP Address) และกำหนดช่วงเลขที่อยู่ไอพี (IP Address) สำหรับอุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์อื่น ๆ

(๒) เลขที่อยู่ไอพี (IP Address) เป็นทรัพยากรที่อยู่ภายใต้การดูแลของศูนย์เทคโนโลยีสารสนเทศ เมื่อมีความต้องการขอเลขที่อยู่ไอพี (IP Address) เพิ่มหรือแก้ไขเปลี่ยนแปลงเลขที่อยู่ไอพี (IP Address) เพื่อเชื่อมต่อระบบเครือข่ายสื่อสารกับอุปกรณ์ (Device) หรือเครื่องคอมพิวเตอร์ให้ดำเนินการแจ้งขอหรือแก้ไขเลขที่อยู่ไอพี (IP Address) มายังศูนย์เทคโนโลยีสารสนเทศ

(๓) ข้อมูลที่ใช้ประกอบการขอเลขที่อยู่ไอพี (IP Address) ได้แก่

- ชื่อ นามสกุล
- ตำแหน่ง
- เลขตำแหน่ง(ถ้ามี)
- ประเภทอุปกรณ์ที่ใช้ เช่น เครื่องคอมพิวเตอร์ เครื่องพิมพ์ เป็นต้น
- MAC Address ของอุปกรณ์ และหมายเลขเครื่อง (Serial Number)
- สถานที่ติดตั้งอุปกรณ์

(๔) เจ้าหน้าที่ดูแลเครื่องคอมพิวเตอร์และเครือข่ายสื่อสารประจำหน่วยงานมีหน้าที่ตรวจสอบและบันทึกปรับปรุงข้อมูลรายชื่อผู้ใช้งานผ่านระบบเครือข่ายภายในกรม เมื่อมีการเปลี่ยนแปลงโยกย้ายเจ้าหน้าที่ดูแลเครื่องคอมพิวเตอร์และเครือข่ายสื่อสารประจำหน่วยงานมีหน้าที่ดำเนินการลงทะเบียนเลขที่อยู่ไอพีเข้าระบบแจกจ่ายเลขที่อยู่ไอพีอัตโนมัติ บันทึกข้อมูลประกอบการขอเลขที่อยู่ไอพีลงฐานข้อมูล รวมถึงกรณีที่มีการเปลี่ยนแปลงหรือยกเลิกเลขที่อยู่ไอพี

(๕) ให้ผู้ดูแล...

(๕) ให้ผู้ดูแลระบบเครือข่ายสื่อสารดำเนินการกำหนดเลขที่อยู่ไอพี (IP Address) และให้ดำเนินการลงทะเบียนเลขที่อยู่ไอพีเข้าระบบแจกจ่ายเลขที่อยู่ไอพีอัตโนมัติ

(๖) กรณีต้องการยกเลิกใช้งานเลขที่อยู่ไอพี (IP Address) ที่ได้รับจากศูนย์เทคโนโลยีสารสนเทศ ให้ดำเนินการแจ้งยกเลิกการใช้งานกับศูนย์เทคโนโลยีสารสนเทศ เพื่อให้ผู้ดูแลระบบเครือข่ายสื่อสารดำเนินการยกเลิกการใช้งานเลขที่อยู่ไอพี

(๗) ห้ามผู้ใช้งานแก้ไขหรือเปลี่ยนแปลงค่าเลขที่อยู่ไอพี (IP Address) หรือ MAC Address ในกรณีที่มีความจำเป็นต้องมีการเปลี่ยนแปลงค่าเลขที่อยู่ไอพี หรือ Mac Address เช่นมีความจำเป็นต้องเปลี่ยนเลขที่อยู่ไอพี หรือมีการเปลี่ยนแปลงอุปกรณ์คอมพิวเตอร์ ให้แจ้งกับศูนย์เทคโนโลยีสารสนเทศ

การเชื่อมต่อระบบเครือข่ายสื่อสารกับเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่เกี่ยวข้องให้ใช้เฉพาะเลขที่อยู่ไอพี(IP Address) ที่ได้ลงทะเบียนไว้แล้วเท่านั้น

ข้อ ๑๓ ให้ทุกหน่วยงานมีหน้าที่จัดเตรียมสถานที่ติดตั้งอุปกรณ์คอมพิวเตอร์และระบบเครือข่ายสื่อสารให้เป็นไปตามแนวทางในคู่มือการจัดทำ Site Preparation ตามที่ศูนย์เทคโนโลยีสารสนเทศได้กำหนดไว้บนระบบเครือข่ายภายในกรม (Intranet) โดยสถานที่ดังกล่าวต้องมีความยืดหยุ่นในการรองรับการขยายระบบงานเพื่อใช้ปฏิบัติงานของเจ้าหน้าที่ ทั้งในปัจจุบันและอนาคตได้อย่างรวดเร็ว และจัดทำแผนภาพ (Diagram) แสดงจุดติดตั้งระบบเครือข่ายสื่อสารจุดติดตั้งอุปกรณ์คอมพิวเตอร์ภายในหน่วยงาน เพื่อขออนุมัติต่อศูนย์เทคโนโลยีสารสนเทศก่อนดำเนินการ โดยจัดทำแผนภาพ (Diagram) จำนวน ๒ ชุด เก็บไว้ที่หน่วยงาน ๑ ชุด และส่งศูนย์เทคโนโลยีสารสนเทศ ๑ ชุด เพื่อใช้ในการบริหารจัดการระบบเครือข่ายสื่อสารต่อไป

ข้อ ๑๔ ในกรณีที่หน่วยงานต้องการจัดทำวง LAN หรือปรับปรุงจุดติดตั้งภายในหน่วยงานให้ขออนุมัติต่อศูนย์เทคโนโลยีสารสนเทศก่อนดำเนินการ โดยข้อมูลที่ใช้ประกอบการจัดทำวง LAN ได้แก่

- วัตถุประสงค์ของการจัดทำวง LAN
- ผังการเชื่อมต่ออุปกรณ์เครือข่ายสื่อสาร
- จำนวนจุดติดตั้ง

ข้อ ๑๕ ให้เจ้าหน้าที่ดูแลเครื่องคอมพิวเตอร์และเครือข่ายสื่อสาร ตรวจสอบความถูกต้องของการใช้เลขที่อยู่ไอพี (IP Address) ของผู้ใช้งาน และตรวจสอบแผนภาพ (Diagram) แสดงจุดติดตั้งระบบเครือข่ายสื่อสาร จุดติดตั้งอุปกรณ์คอมพิวเตอร์ภายในหน่วยงาน ให้มีความถูกต้องและเป็นปัจจุบัน

ข้อ ๑๖ การเผยแพร่ข้อมูลโครงสร้างหรือแผนภาพ (Diagram) ของระบบเครือข่ายสื่อสารให้เผยแพร่ได้เฉพาะที่ผู้ดูแลระบบเครือข่ายสื่อสารได้จัดเตรียมไว้สำหรับเผยแพร่เท่านั้น

ข้อ ๑๗ ห้ามทุกหน่วยงานทำการเชื่อมต่อระบบเครือข่ายสื่อสารโดยตรงออกไปยังหน่วยงานภายนอกโดยเด็ดขาด รวมถึงการวางสายเครือข่ายหลักเองโดยไม่ได้รับอนุญาต กรณีต้องการเชื่อมต่อจะต้องได้รับการอนุมัติจากผู้บริหารระดับสูงก่อน โดยให้ยื่นคำขออนุมัติผ่านผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และห้ามนำอุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายสื่อสารต่าง ๆ เช่น อุปกรณ์สวิตช์ (Switch) อุปกรณ์เราเตอร์ (Router) อุปกรณ์เชื่อมต่อไร้สาย อุปกรณ์สื่อสารเคลื่อนที่ เครื่องคอมพิวเตอร์พกพา หรืออุปกรณ์อื่น ๆ ที่ไม่เกี่ยวข้องกับกรมพินิจและคุ้มครองเด็กและเยาวชนมาเชื่อมต่อกับระบบเครือข่ายสื่อสารก่อนได้รับการอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

ข้อ ๑๘ ในกรณี...

ข้อ ๑๘ ในกรณีที่จำเป็นต้องนำเครื่องคอมพิวเตอร์ที่มีการใช้ Air Card หรือการเชื่อมต่อ Internet ไร้สายด้วยวิธีการอื่นใดก็ตามมาใช้ภายในหน่วยงานของกรมพินิจและคุ้มครองเด็กและเยาวชน ไม่อนุญาตให้นำเครื่องคอมพิวเตอร์เชื่อมต่อเข้ากับระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชนโดยเด็ดขาด

ข้อ ๑๙ ห้ามผู้ใช้งานกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ หรือกระทำด้วยประการใดเพื่อให้การทำงานของคอมพิวเตอร์ของผู้อื่นถูกระงับ เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานได้ตามปกติ

ข้อ ๒๐ ผู้ใช้งานต้องรายงานการล่วงละเมิดการใช้งานระบบเครือข่ายสื่อสารหรือการใช้งานที่ผิดปกติให้แก่ผู้ดูแลระบบเครือข่ายสื่อสารทราบโดยทันที

ข้อ ๒๑ ห้ามจัดตั้งหรือใช้งานอุปกรณ์หรือโปรแกรมใด ๆ เพื่อทำการเปลี่ยนกลุ่มเลขที่อยู่ไอพี Proxy หรือเปลี่ยน Port ที่ให้บริการ Tunnel เพื่อเชื่อมต่อกับระบบเครือข่ายสื่อสาร ทั้งระบบเครือข่ายภายในกรม และระบบเครือข่ายอินเทอร์เน็ต

ข้อ ๒๒ ห้ามผู้ใช้งานจัดตั้งระบบที่ใช้สำหรับการกำหนดเลขที่อยู่ไอพี (IP Address) อัตโนมัติแก่เครื่องคอมพิวเตอร์ที่ติดตั้งอยู่บนระบบเครือข่ายสื่อสาร

ข้อ ๒๓ ห้ามผู้ใช้งานเข้าถึงอุปกรณ์เครือข่ายเพื่อทำการแก้ไขหรือตรวจสอบค่า Configuration ของอุปกรณ์เครือข่ายสื่อสาร

ข้อ ๒๔ ผู้ดูแลระบบเครือข่ายสื่อสารมีหน้าที่กำหนดการแบ่งแยกระบบเครือข่ายสื่อสาร (Segregation In Networks) ต้องทำการแบ่งแยกเครือข่ายสื่อสารตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบงาน และดำเนินการแบ่งแยกระบบเครือข่ายสื่อสารเฉพาะที่ไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงของกรมพินิจและคุ้มครองเด็กและเยาวชน

ข้อ ๒๕ ผู้ดูแลระบบเครือข่ายสื่อสาร หรือผู้ที่ได้รับมอบหมายให้ดูแลระบบเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้เก็บรักษา ข้อมูลจราจรคอมพิวเตอร์ไว้เกินเก้าสิบวัน แต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ เพื่อให้สามารถระบุตัวผู้ใช้บริการได้

ข้อ ๒๖ ผู้ดูแลระบบเครือข่ายสื่อสารมีหน้าที่ควบคุมการจัดเส้นทางบนระบบเครือข่ายสื่อสาร (Network Routing Control) เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่าน หรือการไหลของข้อมูลหรือสารสนเทศ (Flows) ให้สามารถใช้งานเป็นไปอย่างเรียบร้อยและปกติ ทั้งนี้ ผู้ดูแลระบบเครือข่ายสื่อสารมีสิทธิดำเนินมาตรการตามสมควรเพื่อรักษาประสิทธิภาพ และความมั่นคงของระบบเครือข่ายสื่อสาร เพื่อให้การใช้งานเป็นไปอย่างเรียบร้อยและปกติ

ข้อ ๒๗ ผู้ดูแล...

ข้อ ๒๗ ผู้ดูแลระบบเครือข่ายสื่อสารมีสิทธิตรวจสอบข้อมูลที่อยู่ระหว่างการรับ-ส่งข้อมูลในระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชน เพื่อการวิเคราะห์และแก้ไขปัญหาต่าง ๆ

ข้อ ๒๘ ผู้ดูแลระบบเครือข่ายสื่อสารต้องเฝ้าดูแล (Monitor) ระบบเฝ้าระวังเครือข่ายสื่อสาร (Network Monitoring Tools) ตลอดเวลาเพื่อการแจ้งปัญหาอุปสรรค ความผิดปกติของระบบเครือข่ายสื่อสารที่เกิดขึ้นให้หัวหน้าหน่วยงาน หรือผู้มีอำนาจทราบโดยเร็ว

ข้อ ๒๙ ในกรณีฉุกเฉินและมีความจำเป็นเร่งด่วนหากล่าช้าอาจเกิดผลเสียต่อราชการได้ ผู้มีอำนาจสามารถอนุญาตผู้ดูแลระบบเครือข่ายสื่อสาร ดำเนินการแก้ปัญหาก่อนได้ และผู้ดูแลระบบเครือข่ายสื่อสารจะต้องจัดทำเอกสารการขออนุญาตดำเนินการเป็นลายลักษณ์อักษรในภายหลังโดยเร็ว ทั้งนี้ ต้องไม่เกินวันทำการถัดไป

ข้อ ๓๐ ผู้ดูแลระบบเครือข่ายสื่อสารต้องจัดให้มีการป้องกันและควบคุม Port ที่ใช้สำหรับตรวจสอบและปรับการตั้งค่าของระบบ (Remote Diagnostic and Configuration Port Protection) ทั้งการเข้าถึงทางกายภาพและทางระบบเครือข่ายสื่อสาร ทั้งนี้ ผู้ดูแลระบบสามารถเข้าถึงอุปกรณ์เครือข่ายสื่อสารเพื่อปรับปรุงหรือแก้ไขระบบเครือข่ายสื่อสาร ให้สามารถใช้งานได้อย่างถูกต้องและมีประสิทธิภาพ โดยจะต้องดำเนินการผ่านระบบการพิสูจน์ตัวตน (Authentication) จากส่วนกลาง และหากมีความจำเป็นต้องทำการปิดระบบเพื่อปรับปรุงหรือเปลี่ยนแปลงต้องแจ้งต่อหน่วยงานที่ส่งผลกระทบทราบก่อนดำเนินการ

ข้อ ๓๑ ห้ามเปิดเผยหรือส่งมอบข้อมูลโครงสร้างระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชนให้แก่บุคคลใดที่ไม่เกี่ยวข้องก่อนได้รับการอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

ข้อ ๓๒ ห้ามเปิดเผยข้อมูลที่ได้จากการตรวจสอบข้อมูลที่อยู่ระหว่างการรับส่งในระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชน ให้แก่บุคคลใดที่ไม่เกี่ยวข้องก่อนได้รับการอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

หมวด ๕
การปฏิบัติงานบนเครือข่ายอินเทอร์เน็ต และเครือข่ายภายในกรม

ข้อ ๓๓ การปฏิบัติงานบนเครือข่ายอินเทอร์เน็ต (Internet) และเครือข่ายภายในกรม (Intranet)

(๑) ห้ามเผยแพร่หรือใช้เครือข่ายอินเทอร์เน็ต (Internet) และเครือข่ายภายในกรม (Intranet) โดยใช้เนื้อที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) ของกรมพินิจและคุ้มครองเด็กและเยาวชนในการละเมิดลิขสิทธิ์ การหาประโยชน์ในเชิงธุรกิจ เพื่อประโยชน์ส่วนตัว การติดต่องานที่ไม่ใช่ในหน้าที่ราชการ การเผยแพร่หรือใช้งานชุดคำสั่งเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด การใช้งานเว็บไซต์ที่มีเนื้อหาที่เป็นภัยต่อความมั่นคงของประเทศชาติ ศาสนา พระมหากษัตริย์ เป็นต้น

(๒) การเผยแพร่ข้อมูลข่าวสารบนเครือข่ายอินเทอร์เน็ต (Internet) และเครือข่ายภายในกรม (Intranet) ให้ปฏิบัติตามแนวปฏิบัติในการนำข้อมูลขึ้นระบบเครือข่ายอินเทอร์เน็ต (Internet) และเครือข่ายภายในกรม (Intranet)

(๓) ในกรณี...

(๓) ในกรณีมีการนำโปรแกรมประยุกต์เฉพาะงาน ขึ้นใช้งานบนระบบเครือข่ายอินเทอร์เน็ต (Internet) และเครือข่ายภายในกรม (Intranet) ให้ศูนย์เทคโนโลยีสารสนเทศพิจารณา คำขออนุมัติใช้งานโปรแกรมฯ ประกอบการนำขึ้นใช้งานบนระบบเครือข่ายอินเทอร์เน็ต (Internet) และเครือข่ายภายในกรม (Intranet) หากไม่ได้มีการขออนุมัติการใช้งานโปรแกรมฯ ดังกล่าว ศูนย์เทคโนโลยีสารสนเทศ สามารถยกเลิกการใช้งานและนำ URL ออกจากระบบเครือข่ายภายในกรม (Intranet) และระบบเครือข่ายอินเทอร์เน็ต (Internet) ได้

(๔) ห้ามนำเสนอข้อมูลที่ไม่เหมาะสมทางศีลธรรม ข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับกรมพินิจและคุ้มครองเด็กและเยาวชนและผู้ใช้งานต้องรับผิดชอบกับผลเสียหายที่เกิดขึ้นจากการใช้งานดังกล่าว

(๕) ห้ามใช้ระบบเครือข่ายอินเทอร์เน็ต (Internet) และเครือข่ายภายในกรม (Intranet) ของกรมพินิจและคุ้มครองเด็กและเยาวชนในทางที่ไม่เหมาะสม หากพบเห็นการใช้อินเทอร์เน็ตและอินทราเน็ตของกรมพินิจและคุ้มครองเด็กและเยาวชนในทางที่ไม่เหมาะสม หรือพบเห็นการบุกรุกหรือการละเมิดสิทธิของกรมพินิจและคุ้มครองเด็กและเยาวชน ต้องรายงานต่อศูนย์เทคโนโลยีสารสนเทศทันที

(๖) ห้ามสร้างภาระงานให้กับระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสาร เช่น การรับ-ส่งจดหมายอิเล็กทรอนิกส์ (e-Mail) การดาวน์โหลด (Download) การอัพโหลด (Upload) หรือการแชร์ (Share) ข้อมูลที่ไม่เกี่ยวข้องกับการปฏิบัติงาน ในกรณีข้อมูลที่ใช้ในการปฏิบัติงานมีขนาดใหญ่ หรือมีจำนวนมาก ให้บีบอัดหรือแบ่งแฟ้มข้อมูลให้มีขนาดเล็กลง

(๗) ให้หน่วยงานที่มีการพัฒนาเว็บเพจ (Web Page) เพื่อเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต (Internet) และเครือข่ายภายในกรม (Intranet) หรือระบบเครือข่ายเอกซ์ทราเน็ต (Extranet) พิจารณาแต่งตั้งเจ้าหน้าที่ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่าย (ถ้ามี) และผู้จัดทำเว็บเพจ (Web Page) และแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบ เพื่อให้เป็นผู้ประสานงาน ทั้งนี้ให้หัวหน้าหน่วยงานเป็นผู้รับผิดชอบข้อมูลในเว็บเพจ (Web Page) ที่ได้จัดทำขึ้น

(๘) การสร้างหรือพัฒนาเว็บเพจ (Web Page) ต้องดำเนินการให้เป็นไปตามมาตรฐานเว็บเพจที่กรมพินิจและคุ้มครองเด็กและเยาวชนกำหนด

(๙) การใช้งานสังคมออนไลน์ (Social Network) ผ่านระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชนให้ปฏิบัติตามแนวปฏิบัติในการใช้สังคมออนไลน์ (Social Network) ของกรมพินิจและคุ้มครองเด็กและเยาวชนที่ได้ประกาศไว้บนระบบเครือข่ายภายในกรม (Intranet) และห้ามใช้จดหมายอิเล็กทรอนิกส์ (e-Mail) ของกรมพินิจและคุ้มครองเด็กและเยาวชนในการสมัครใช้งานสังคมออนไลน์ (Social Network)

หมวด ๖...

หมวด ๖
การใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์

ข้อ ๓๔ การใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์

(๑) ให้ปฏิบัติตามคู่มือการใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์

(๒) การแต่งตั้งเจ้าหน้าที่ให้ปฏิบัติงาน

(๒.๑) ให้หัวหน้าหน่วยงานเป็นผู้กำหนดบุคคลที่ทำหน้าที่เป็นเลขานุการและเจ้าหน้าที่รับ-ส่งข่าวสารอิเล็กทรอนิกส์ประจำหน่วยงาน

(๒.๒) ให้หน่วยงานที่มีห้องประชุมอยู่ในระบบการจองห้องประชุม แต่งตั้งผู้รับผิดชอบการจองห้องประชุม เพื่อจองห้องประชุมที่อยู่ในอาคารกรมพินิจและคุ้มครองเด็กและเยาวชน

(๓) การขอใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ ผู้ใช้ที่ต้องการใช้งานระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ ให้ร้องขอต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และจะใช้งานระบบรับ-ส่งหนังสือ และข่าวสารทางอิเล็กทรอนิกส์ได้ต่อเมื่อศูนย์เทคโนโลยีสารสนเทศได้อนุมัติให้ใช้งาน และได้กำหนดชื่อผู้ใช้และรหัสผ่านแจ้งให้ทราบ

(๔) การเปลี่ยนแปลงผู้ใช้ตามตำแหน่ง กรณีมีการเปลี่ยนแปลงผู้ดำรงตำแหน่งใหม่ให้ผู้ดำรงตำแหน่งเดิมมอบชื่อผู้ใช้ตามตำแหน่งพร้อมรหัสผ่านให้ผู้ดำรงตำแหน่งใหม่ หรือหัวหน้าส่วนราชการ หรือผู้รักษาราชการแทน เว้นแต่ผู้ดำรงตำแหน่งเดิมมิได้แจ้งไว้ ให้ผู้ดำรงตำแหน่งใหม่ร้องขอต่อศูนย์เทคโนโลยีสารสนเทศในการขอชื่อผู้ใช้ตามตำแหน่งและรหัสผ่านใหม่ และเมื่อผู้ใช้ตามตำแหน่งได้รับชื่อผู้ใช้และรหัสผ่านแล้วให้เปลี่ยนรหัสผ่านใหม่ทันที

(๕) การยกเลิกบัญชีผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์

(๕.๑) ผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ส่วนบุคคลที่ไม่เปิดใช้งานเป็นระยะเวลาติดต่อกันตั้งแต่ ๑๘๐ วันขึ้นไปจะถูกระงับการใช้งาน หากต้องการใช้งานอีก ต้องยื่นคำร้องต่อศูนย์เทคโนโลยีสารสนเทศ

(๕.๒) ผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ตามตำแหน่งให้หัวหน้าหน่วยงานยื่นคำร้องขอยกเลิกบัญชีผู้ใช้ต่อศูนย์เทคโนโลยีสารสนเทศ

(๖) ระบบรับ-ส่งหนังสือและข่าวสารอิเล็กทรอนิกส์ ประกอบด้วยระบบงาน ๔ ระบบโดยแต่ละระบบงานมีการกำหนดสิทธิการใช้งานดังนี้

(๖.๑) ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ ผู้ที่มีสิทธิใช้งาน ได้แก่ ผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ตามตำแหน่งที่เป็นหัวหน้าหน่วยงาน เลขานุการ เจ้าหน้าที่รับ-ส่งข่าวสารอิเล็กทรอนิกส์ ผู้ได้รับมอบหมาย หรือผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ส่วนบุคคล หรือผู้ใช้ที่เป็นบุคคลภายนอกที่ได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๖.๒) ระบบจัดเก็บเอกสารอิเล็กทรอนิกส์ ผู้ที่มีสิทธิใช้งานได้แก่ ผู้ใช้ตามตำแหน่งที่เป็นหัวหน้าหน่วยงาน เลขานุการ เจ้าหน้าที่รับ-ส่งข่าวสารอิเล็กทรอนิกส์ หรือผู้ได้รับมอบหมาย

(๖.๓) ระบบ...

(๖.๓) ระบบการจองห้องประชุม การจองห้องประชุมอาคารกรมพินิจและคุ้มครองเด็กและเยาวชน เพื่อการประชุมปกติ ผู้ที่มีสิทธิใช้งาน ได้แก่ ผู้ที่มีบัญชีผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์

(๗) ให้ผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์เปลี่ยนรหัสผ่านของตนเป็นประจำครั้งละไม่เกิน ๖๐ วัน หรือให้ทำการเปลี่ยนรหัสผ่านของตนทันทีหากพบว่ามีผู้ทราบรหัสผ่านดังกล่าว

(๘) ห้ามผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ เปิดเผยรหัสผ่านของตนเองให้ผู้อื่นทราบ

(๙) การเปลี่ยนบัญชีผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ส่วนบุคคล ให้ผู้ใช้ส่วนบุคคลยื่นคำร้องขอเปลี่ยนที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (e-Mail Address) ต่อศูนย์เทคโนโลยีสารสนเทศ

(๑๐) ให้เปิดตู้จดหมายของตนเป็นประจำ และลบหนังสือที่พิจารณาเห็นว่าไม่ใช้งานแล้ว

(๑๑) ห้ามเปิดจดหมายอิเล็กทรอนิกส์ (e-Mail) ของผู้ส่งที่ไม่รู้จัก ให้ลบทิ้งออกจากเครื่องคอมพิวเตอร์ทันที รวมทั้งต้องใช้ความระมัดระวังในการเปิด หรือสั่งการทำงานกับไฟล์ที่แนบในจดหมายอิเล็กทรอนิกส์ (e-Mail)

(๑๒) ให้ผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ รับ-ส่งหนังสือหรือข่าวสารอิเล็กทรอนิกส์ ที่เกี่ยวข้องกับการปฏิบัติราชการเท่านั้น

(๑๓) ผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ จากบุคคลภายนอกที่ได้รับอนุมัติต้องปฏิบัติตามระเบียบฯ นี้ โดยเคร่งครัด

ข้อ ๓๕ ผู้ดูแลระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ต้องจัดให้มีการตรวจสอบการใช้งานของผู้ใช้ระบบงานและการทำงานของระบบงานให้มีความพร้อมในการใช้งานอยู่เสมอ รวมทั้งต้องดำเนินการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างน้อยปีละ ๑ ครั้ง หากผู้ใช้ตามตำแหน่ง หรือผู้ได้รับมอบหมาย ไม่มีการใช้งานเป็นระยะเวลาติดต่อกัน ๑ ปีขึ้นไป ผู้ดูแลระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ ขอสงวนสิทธิระงับการใช้งานของผู้ใช้ระบบ

ข้อ ๓๖ ผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ต้องรับผิดชอบต่อข่าวสารอิเล็กทรอนิกส์ที่มีอยู่ในความรับผิดชอบของตนเองในทุกกรณี

ข้อ ๓๗ ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์เป็นทรัพย์สินของกรมพินิจและคุ้มครองเด็กและเยาวชนมีไว้เพื่อใช้ในการปฏิบัติราชการเท่านั้น ผู้ใช้ระบบงานจะต้องไม่กระทำการอย่างหนึ่งอย่างใด ต่อไปนี้

(๑) กระทำการก่อให้เกิดความเสียหายต่อกรมพินิจและคุ้มครองเด็กและเยาวชน หรือละเมิดสิทธิหรือก่อให้เกิดความเดือดร้อนรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และแสวงหาผลประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาประโยชน์ในเชิงธุรกิจจากการใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์

(๒) ส่งจดหมายลูกโซ่

(๓) ภาพลามกอนาจาร

(๔) ส่งข้อความหยาบคาย ดูหมิ่นผ่านระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์

(๕) ปลอมแปลงบัญชีผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์

(๖) ตัดต่อ...

(๖) ตัดต่อ เติม หรือดัดแปลงภาพของผู้อื่น ด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ที่จะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย หากตรวจพบจะดำเนินการยกเลิกการใช้งานของผู้นั้นทันที และดำเนินการตามกฎหมายที่เกี่ยวข้อง ทั้งนี้ผู้ดูแลระบบข่าวสารทางอิเล็กทรอนิกส์ขอสงวนสิทธิในการตรวจสอบ แก้ไขเปลี่ยนแปลงยกเลิกการใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์โดยไม่ต้องแจ้งให้ผู้ใช้ระบบงานทราบล่วงหน้า

หมวด ๗
การปฏิบัติงานภายในห้องเครื่องคอมพิวเตอร์แม่ข่าย

ข้อ ๓๘ พื้นที่ปลอดภัย เป็นสถานที่สำหรับใช้ทำห้อง สถานที่ตั้งห้องเครื่องคอมพิวเตอร์แม่ข่าย (Data Center) ซึ่งมีการเก็บข้อมูลสารสนเทศที่สำคัญต้องมีการควบคุมการเข้า-ออก ที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น และระบบควบคุมประตูปิดเปิดอัตโนมัติต้องเป็นระบบที่ได้มาตรฐาน

ข้อ ๓๙ ผู้ดูแลระบบ ต้องกำหนดสิทธิในการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานและสอดคล้องกับหน้าที่ความรับผิดชอบ รวมทั้งให้มีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ข้อ ๔๐ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น (Administrator) ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลสารสนเทศได้

ข้อ ๔๑ ผู้ดูแลระบบจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเครือข่ายกรมพินิจและคุ้มครองเด็กและเยาวชน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญอย่างสม่ำเสมอและต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบต่าง ๆ และการผ่านเข้าออก สถานที่ตั้งระบบเครือข่ายทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

หมวด ๘
การรักษาความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๔๒ การใช้ระบบคอมพิวเตอร์อย่างปลอดภัย

(๑) ต้องดูแลเครื่องคอมพิวเตอร์และโปรแกรมชุดคำสั่งที่อยู่ในความรับผิดชอบให้มีความปลอดภัยจากการติดไวรัสคอมพิวเตอร์และภัยคุกคามในรูปแบบต่าง ๆ ตรวจสอบการป้องกันช่องโหว่ของโปรแกรมระบบปฏิบัติการและโปรแกรมอื่น ๆ ที่ติดตั้งในเครื่องคอมพิวเตอร์ให้เป็นปัจจุบันอยู่เสมอ และเมื่อพบความผิดปกติของอุปกรณ์คอมพิวเตอร์ให้รีบดำเนินการแก้ไขหรือแจ้งเจ้าหน้าที่ดูแลระบบความมั่นคงปลอดภัยสารสนเทศ หรือเจ้าหน้าที่บริหารระบบความมั่นคงปลอดภัยสารสนเทศทราบโดยเร็ว

(๒) ห้ามนำเครื่องคอมพิวเตอร์ที่ยังไม่ได้รับการติดตั้งโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ที่เป็นปัจจุบันเชื่อมต่อกับระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชน

(๓) ห้ามใช้บริการที่ส่งผลกระทบต่อการใช้งานเครือข่ายสื่อสารและความปลอดภัย เช่น การดูภาพยนตร์ ฟังเพลง เล่นเกมส์ และบริการที่ให้ความบันเทิงต่าง ๆ

(๕) ห้ามติดตั้ง...

(๕) ห้ามติดตั้งโปรแกรมชุดคำสั่งที่มีผลกระทบต่อระบบความปลอดภัยของกรมพินิจและคุ้มครองเด็กและเยาวชน

(๖) ห้ามดาวน์โหลดโปรแกรมแจกฟรีในลักษณะ Freeware หรือ Shareware ที่ไม่มีให้บริการสำหรับดาวน์โหลดภายในเครือข่ายภายในกรม (Intranet)

(๗) ห้ามพัฒนาโปรแกรมไวรัสคอมพิวเตอร์ขึ้นเอง ห้ามทดสอบโปรแกรมไวรัสคอมพิวเตอร์และโปรแกรมในลักษณะที่ไม่ประสงค์ดีอื่น ๆ ที่อาจก่อให้เกิดความเสี่ยงและเป็นอันตรายต่อระบบคอมพิวเตอร์

(๘) ผู้ใช้งานที่ได้รับการจัดสรรเครื่องคอมพิวเตอร์ หรือผู้ดูแลการใช้เครื่องคอมพิวเตอร์จะต้องดูแลเครื่องคอมพิวเตอร์ให้อยู่ในสภาพดี ติดตั้งใช้งานอยู่ในสถานที่ที่ปลอดภัย มีการควบคุมผู้มีสิทธิในการเข้าใช้เครื่องคอมพิวเตอร์ มีการเก็บรักษาข้อมูลให้เป็นความลับ ใช้ความระมัดระวังในการเปิดเผยข้อมูลและเครื่องคอมพิวเตอร์ต้องมีความพร้อมในการใช้งานอยู่เสมอ

๙) ป้องกันไม่ให้นำอุปกรณ์คอมพิวเตอร์ที่มิใช่ของกรมพินิจและคุ้มครองเด็กและเยาวชนหรือบุคคลที่ไม่ได้รับอนุญาต ในการใช้ระบบคอมพิวเตอร์ของกรมพินิจและคุ้มครองเด็กและเยาวชน สามารถเข้าใช้อุปกรณ์คอมพิวเตอร์ โปรแกรมชุดคำสั่ง ระบบสารสนเทศ ระบบเครือข่ายสื่อสาร ของกรมพินิจและคุ้มครองเด็กและเยาวชน และส่วนที่เกี่ยวข้องอื่น ๆ จนกว่า จะได้รับอนุญาตจากหัวหน้าหน่วยงาน พร้อมทั้งตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์นั้นแล้ว

ข้อ ๔๓ การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์

(๑) กรณีที่มีการนำอุปกรณ์คอมพิวเตอร์และระบบสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนไปปฏิบัติงานภายนอกสำนักงาน เช่น ที่บ้าน เป็นต้น ผู้ใช้งานจะต้องปกปิดระบบสารสนเทศให้เป็นความลับและไม่เปิดเผยแก่บุคคลภายนอก พร้อมทั้งต้องดูแลรักษาอุปกรณ์คอมพิวเตอร์และระบบสารสนเทศให้มีความปลอดภัยตลอดเวลา

(๒) กรณีที่มีการนำอุปกรณ์คอมพิวเตอร์และระบบสารสนเทศเข้ามาใช้ภายในสำนักงาน จะต้องมีการตรวจสอบโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ให้เป็นปัจจุบัน รวมทั้งสื่อต่าง ๆ ที่จะนำกลับเข้ามาใช้งานให้ปลอดภัยก่อนการเชื่อมต่อกับระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชน

ข้อ ๔๔ การป้องกันไวรัสคอมพิวเตอร์และปิดช่องโหว่ของซอฟต์แวร์

(๑) เครื่องคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่อกับเครือข่ายสื่อสาร ของกรมพินิจและคุ้มครองเด็กและเยาวชนจะต้องติดตั้งโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ (Antivirus) ที่เป็นลิขสิทธิ์ของกรมพินิจและคุ้มครองเด็กและเยาวชนรวมทั้งโปรแกรมการปิดช่องโหว่ (Patch) หรือเครื่องมือด้านความปลอดภัยอื่นๆ เพื่อความปลอดภัยในการใช้งาน

(๒) ตรวจสอบการปรับปรุงฐานข้อมูลไวรัสคอมพิวเตอร์ (Virus Pattern File Number และ Virus Pattern Release Date) และตรวจสอบการป้องกันช่องโหว่ของโปรแกรมระบบปฏิบัติการ และโปรแกรมอื่น ๆ ที่ติดตั้งในเครื่องคอมพิวเตอร์ให้เป็นปัจจุบัน (Patch Update) โดยตรวจสอบได้จาก Web Site ระบบความปลอดภัยคอมพิวเตอร์

(๓) ผู้ดูแล...

(๓) ผู้ดูแลระบบต้องตรวจสอบช่องโหว่ของระบบงาน และต้องปรับปรุงแก้ไขช่องโหว่เป็นประจำ เพื่อป้องกัน การถูกบุกรุกหรือโจมตีระบบงาน

(๔) เมื่อพบว่าเครื่องคอมพิวเตอร์ติดไวรัสคอมพิวเตอร์ ให้หยุดการใช้งานโปรแกรมทั้งหมดและให้กำจัดไวรัสฯ รวมทั้งปรับปรุงโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Virus Definition File) และโปรแกรมการปิดช่องโหว่ให้เป็นปัจจุบันอยู่เสมอ หากไม่สามารถกำจัดไวรัสคอมพิวเตอร์ได้ ให้ตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ออกจากระบบเครือข่ายสื่อสาร (ดึงสาย UTP ออกจาก Port) และแจ้งเจ้าหน้าที่ดูแลระบบความปลอดภัยสารสนเทศ ให้ดำเนินการกำจัดไวรัสคอมพิวเตอร์โดยเร็ว พร้อมทั้งควรตรวจสอบ การใช้สื่อบันทึกข้อมูลอื่น ๆ ให้ปลอดภัยจากไวรัสคอมพิวเตอร์ก่อนการใช้งานเสมอ

(๕) ผู้ดูแลระบบและผู้ใช้งานระบบคอมพิวเตอร์จะต้องทำการสำรองข้อมูลให้เป็นปัจจุบันอยู่เสมอ และจัดเก็บไว้ในที่ปลอดภัย เพื่อสามารถนำกลับคืนมาใช้งานในกรณีที่มีการสูญเสียข้อมูลจากการติดไวรัสคอมพิวเตอร์

(๖) ติดตามข่าวสารด้านความปลอดภัยสารสนเทศ ตลอดจนปฏิบัติตามคำแนะนำเกี่ยวกับการป้องกันและกำจัดไวรัสคอมพิวเตอร์ รวมทั้งทำความเข้าใจกับภัยคุกคามและโทษของภัยคุกคามในรูปแบบต่างๆ ให้เป็นปัจจุบันอยู่เสมอ

(๗) ผู้ใช้ต้องมีความตระหนักและความระมัดระวัง (Awareness) ในการใช้ระบบสารสนเทศอย่างปลอดภัย

ข้อ ๔๕ การใช้งานรหัสผ่าน (Password)

(๑) การตั้งรหัสผ่าน (Password) ควรใช้รหัสผ่านที่คาดเดาได้ยาก รหัสผ่านควรมีความยาวไม่น้อยกว่า ๘ หลัก ประกอบด้วยตัวอักษรพิมพ์เล็ก ตัวอักษรพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์พิเศษ มีการแปลงคำที่ใช้ด้วยวิธีเฉพาะ เช่น การใช้ตัวเลขกับตำแหน่งต่าง ๆ ของคำ นำสัญลักษณ์พิเศษเข้ามาใช้ร่วมกับตัวเลขในคำที่กำหนด สร้างคำจากชื่อย่อของเพลง คำกลอนหรือลำดับในคำ กำหนดคำที่เจตนาพิมพ์ผิด ไม่ควรกำหนดค่าใด ๆ ที่เกี่ยวข้องกับข้อมูลส่วนตัว เช่น หมายเลขบัตรต่าง ๆ ชื่อคู่สมรส หรือที่อยู่ รหัสผ่านที่กำหนดต้องไม่เป็นชื่อเดียวกันกับรหัสผู้ใช้งาน (User ID) ไม่ใช้รหัสผ่านที่ซ้ำกับรหัสผ่านเดิมก่อนหน้านี้ และรหัสผ่านที่กำหนดต้องไม่มีคำในพจนานุกรม หรือเป็นส่วนของคำพูด เช่น ชื่อเฉพาะ ชื่อสถานที่ คำศัพท์ด้านเทคนิค และคำหยาบ ไม่สร้างรหัสผ่านที่มีการพิมพ์เรียงตามลำดับตัวอักษร เช่น ๑๒๓๔๕ หรือ abcdef เป็นต้น ถ้าต้องการกำหนดรหัสผ่านเป็นวันเดือนปีจะต้องมีส่วนประกอบอื่น ๆ เพิ่มเติม เช่น ๑๑๑๐๒๐๑๕@Mypass

(๒) ต้องเปลี่ยนรหัสผ่าน (Password) ในกรณีที่ได้รับสิทธิการเข้าใช้ระบบงานในครั้งแรก

(๓) ต้องเก็บรักษารหัสผ่าน (Password) ให้เป็นความลับโดยไม่เปิดเผยรหัสผ่านให้กับบุคคลอื่นๆ ทราบการกระทำใด ๆ ภายใต้รหัสผู้ใช้ ถือเป็นความรับผิดชอบของเจ้าของรหัสผู้ใช้นั้น

(๔) ให้เปลี่ยนรหัสผ่านทันทีที่สงสัยว่ารหัสผ่านถูกใช้จากบุคคลที่ไม่ได้รับอนุญาต หรือถูกขโมย และให้เปลี่ยนรหัสผ่าน (Password) เป็นประจำทุก ๆ ๖๐ วัน

(๕) ไม่เขียนรหัสผ่าน (Password) ในที่ใดที่หนึ่งที่บุคคลอื่นเข้าถึงได้ ไม่จัดเก็บรหัสผ่านในไฟล์ Batch file หรือ Script ที่ทำงานอัตโนมัติได้ และเมื่อไม่มีกิจกรรมใด ๆ บนเครื่องคอมพิวเตอร์ ต้องกำหนดให้ล็อคหน้าจอ เมื่อกลับมาใช้งานใหม่ต้องระบุรหัสผ่านที่ถูกต้องก่อน โดยกำหนดค่าเวลาในการล็อคหน้าจอให้มีความปลอดภัยตามความเหมาะสม

(๖) ไม่ใช้รหัส...

(๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่าย

(๗) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

(๘) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ระบบคอมพิวเตอร์ ของกรมพินิจและคุ้มครองเด็กและเยาวชน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล็อค หรือเกิดจากความผิดพลาดใด ๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

(๘.๑) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าใช้งานระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๘.๒) การใช้งานระบบคอมพิวเตอร์ในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๘.๓) การใช้งานระบบเครือข่ายอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

(๘.๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(๘.๕) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที และมีการใช้รหัสผ่านในการเข้าถึงใหม่อีกครั้ง

(๙) ผู้ดูแลระบบต้องทำการกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ โดยใช้รหัสผ่านสำหรับผู้มีสิทธิเข้าไปใช้ระบบงานข้อมูลสารสนเทศ และประมวลผลข้อมูล

หมวด ๙
แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติต่าง ๆ

ข้อ ๔๖ การบริหารจัดการควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control) เพื่อควบคุมการเข้าถึงสารสนเทศตามภารกิจให้ปฏิบัติดังนี้

(๑) มีการควบคุมการเข้าถึงสารสนเทศโดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวกับระบบสารสนเทศ

(๒) การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย

(๓) ผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและสารสนเทศได้ ต้องมีการบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และเฝ้าระวัง ประเมินความปลอดภัยที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

ข้อ ๔๗ การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต โดยมีการกำหนดขั้นตอนปฏิบัติ ต่อไปนี้

(๑) มีแบบฟอร์มขอใช้ระบบสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๒) ระบุชื่อบัญชีผู้ใช้งานแยกเป็นรายบุคคล และไม่ซ้ำกัน

(๓) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

(๔) มีการ...

(๔) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(๕) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

(๖) มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(๗) มีการตรวจสอบข้อมูลสิทธิและหน้าที่ที่เกี่ยวข้องของผู้ขอใช้งานระบบสารสนเทศโดยผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เป็นผู้พิจารณา

(๘) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยมุก ๓ เดือน หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ มีการลาออก เปลี่ยนตำแหน่ง โยกย้าย หรือสิ้นสุดการจ้าง เป็นต้น

ข้อ ๔๘ ข้อปฏิบัติในการเข้าถึงระบบสารสนเทศ (Access Control)

(๑) ต้องมีการยืนยันตัวตนผู้ใช้งานโดยต้องบันทึกรหัสผู้ใช้ (User ID) ตามที่กรมพินิจและคุ้มครองเด็กและเยาวชนกำหนดและรหัสผ่าน (Password) ทุกครั้งที่มีการเปิดใช้เครื่องคอมพิวเตอร์หรือเมื่อมีการเริ่มใช้ระบบงาน หรืออาจมีระบบความปลอดภัยอื่น ๆ เช่น Token, Smart Card, Finger Print ที่นำมาใช้ร่วมกันเพื่อพิสูจน์ตัวตนของผู้ใช้งาน (Multi Factors Authentication)

(๒) ระบบงานต้องกำหนดสิทธิ ของผู้ใช้งานตามลักษณะงานและหน้าที่ ความรับผิดชอบ

(๓) กรณีจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ผู้ดูแลระบบต้องเป็นผู้รับผิดชอบและต้องจัดเจ้าหน้าที่อยู่เฝ้าระวังความปลอดภัยอย่างใกล้ชิดตลอดเวลาจนแล้วเสร็จ หากมีปัญหาหรือข้อสงสัยด้านความปลอดภัยให้ปรึกษาหรือสอบถามจากเจ้าหน้าที่บริหารระบบความปลอดภัยสารสนเทศ

(๔) ให้ใช้ข้อมูลสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนทั้งที่มีอยู่ภายในหน่วยงานและได้รับจากภายนอกหน่วยงาน ซึ่งอยู่ในระบบเครือข่ายภายในกรม ระบบอินเทอร์เน็ต และระบบงานต่างๆ เพื่องานในราชการเท่านั้น กรณีข้อมูลที่มีความสำคัญหรือชั้นความลับ ต้องมีการกำหนดสิทธิผู้ใช้งานและสิทธิในการเข้าถึง โดยกำหนดระยะเวลา หรือให้ใช้งานได้เฉพาะเวลาราชการเท่านั้น

(๕) ผู้ใช้งานจะเข้าถึงระบบสารสนเทศเพื่อการปฏิบัติงานได้เฉพาะในส่วนที่ได้รับอนุญาตตามการกำหนดสิทธิจากผู้ดูแลระบบคอมพิวเตอร์เท่านั้น

(๖) การเข้าถึงระบบสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนจากภายนอกหน่วยงานจะต้องใช้งานผ่านระบบ ตามที่กรมพินิจและคุ้มครองเด็กและเยาวชนอนุญาตเท่านั้น

(๗) การทิ้งทำลายสื่อบันทึกข้อมูลที่อาจมีข้อมูลสำคัญหรือชั้นความลับ เช่น กระดาษจดรหัสผ่าน รายงานสารสนเทศที่เป็นความลับจะต้องผ่านกระบวนการทำลาย เช่น การตัดย่อยกระดาษ การเผาทำลาย

(๘) ผู้ใช้งานที่ต้องการได้รับสิทธิในการเข้าใช้ระบบงาน ต้องขออนุญาตผู้มีอำนาจของหน่วยงานและส่งให้ผู้ดูแลระบบเพื่อดำเนินการกำหนดสิทธิในการเข้าใช้งานต่อไป

(๙) การเปลี่ยนแปลงสิทธิการเข้าใช้งานระบบงาน ผู้มีอำนาจจะต้องดำเนินการตรวจสอบเจ้าหน้าที่ว่ามีสิทธิการใช้ระบบงานในระบบนั้น ๆ และแจ้งต่อผู้ดูแลระบบงานเพื่อเปลี่ยนแปลงสิทธิการเข้าใช้งานระบบงาน

(๑๐) ห้ามผู้ใช้งานเข้าใช้งาน พิมพ์ หรือสำรองข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล

ข้อ ๔๙ การรักษา...

ข้อ ๔๙ การรักษาความปลอดภัยข้อมูลสารสนเทศ

(๑) ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

(๒) ผู้ดูแลระบบ จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๓) การรับ-ส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะผู้ใช้งานควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN เป็นต้น

(๔) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่กรมพินิจและคุ้มครองเด็กและเยาวชน

ข้อ ๕๐ หน้าที่ความรับผิดชอบของเจ้าหน้าที่ดูแลระบบความปลอดภัยสารสนเทศ

(๑) ติดตามให้มีการปฏิบัติตามนโยบาย (Policy) ระเบียบและแนวปฏิบัติ (Procedure) มาตรฐาน (Standard) และคำแนะนำ (Guideline)

(๒) ดูแลการรับแจ้งและแก้ไขปัญหาจากผู้ใช้งาน (Incident Response) รวมทั้ง เฝ้าระวังความปลอดภัยระบบคอมพิวเตอร์

(๓) ให้ความรู้ (Education) สร้างความตระหนักและความระมัดระวัง (Awareness) ในการใช้บริการระบบสารสนเทศอย่างปลอดภัย

(๔) ตรวจสอบการใช้อุปกรณ์คอมพิวเตอร์ให้มีความปลอดภัยและสามารถใช้งานได้อย่างต่อเนื่องตลอดเวลา

(๕) รายงานผู้ใช้งานที่ฝ่าฝืน ละเลย ไม่ปฏิบัติ ตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ. ๒๕๖๖ ต่อเจ้าหน้าที่บริหารระบบความปลอดภัยสารสนเทศ

(๖) ประสานงานกับเจ้าหน้าที่บริหารระบบความปลอดภัยสารสนเทศของหน่วยงานสำหรับให้เจ้าหน้าที่ดูแลระบบความปลอดภัยสารสนเทศประสานงานกับเจ้าหน้าที่ดูแลระบบความปลอดภัยสารสนเทศของหน่วยงานที่อยู่ในความรับผิดชอบ

ข้อ ๕๑ หน้าที่ความรับผิดชอบของเจ้าหน้าที่บริหารระบบความปลอดภัยสารสนเทศ

(๑) บริหาร จัดการ ควบคุม และดูแลผู้ใช้งานให้มีการใช้ระบบคอมพิวเตอร์ อย่างปลอดภัย

(๒) ให้ความรู้ (Education) อบรม (Training) สร้างความตระหนักและความระมัดระวัง (Awareness) ในการใช้บริการระบบสารสนเทศ และควบคุมให้มีการปฏิบัติตามนโยบาย (Policy) ระเบียบและแนวปฏิบัติ (Procedure) มาตรฐาน (Standard) และคำแนะนำ (Guideline)

(๓) รายงานผู้ใช้งานที่ฝ่าฝืน ละเลย ไม่ปฏิบัติตามระเบียบกรมพินิจและคุ้มครองเด็กและเยาวชนว่าด้วยการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชนอย่างปลอดภัย พ.ศ. ๒๕๖๖ ต่อหัวหน้าหน่วยงาน

(๔) ให้ความ...

(๔) ให้ความร่วมมือในการดำเนินการตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit) ของกรมพินิจและคุ้มครองเด็กและเยาวชน เพื่อการปรับปรุงประสิทธิภาพการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนอย่างต่อเนื่อง

ข้อ ๕๒ ให้ทำการเก็บรักษา Log File ของการประมวลผล โดยมีระยะเวลาในการเก็บรักษาข้อมูลไว้ไม่น้อยกว่า ๙๐ วันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ข้อ ๕๓ การปฏิบัติงานจากภายนอกสำนักงาน

(๑) ผู้ใช้งานต้องขออนุญาตจากผู้มีอำนาจหรือผู้ที่ได้รับมอบหมายเพื่อขอสิทธิการใช้งานสำหรับการปฏิบัติงานจากภายนอกสำนักงาน

(๒) ผู้ใช้งานต้องไม่นำสิทธิที่ได้ไปให้บุคคลอื่นใช้งาน

(๓) ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์จากการปฏิบัติงานจากภายนอกสำนักงาน

(๔) การปฏิบัติงานจากภายนอกสำนักงาน ให้คำนึงถึงความมั่นคงปลอดภัยด้านสารสนเทศ

(๕) ศูนย์เทคโนโลยีสารสนเทศไม่อนุญาตให้คอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ที่กำลังปฏิบัติงานจากภายนอกสำนักงานเข้าเชื่อมต่อระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชน หากมีเหตุอันน่าสงสัยว่าคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์นั้นไม่ปลอดภัยต่อระบบคอมพิวเตอร์กรมพินิจและคุ้มครองเด็กและเยาวชน

(๖) ผู้ใช้งานต้องใช้ระบบเครือข่ายภายในกรม (Intranet) และระบบงานเพื่อการปฏิบัติงานของราชการเท่านั้น

ข้อ ๕๔ ข้อปฏิบัติการบริหารจัดการข้อมูลและการทำลายข้อมูล

(๑) การจัดการข้อมูลประเภทสำเนาถาวร (Hard Copy) ให้มีการกำหนดป้ายชั้นความลับบนเอกสาร ดังนี้

(๑.๑) ลับที่สุด ระบุคำว่า “ลับที่สุด” ในหน้าแรกและทุกหน้าบริเวณส่วนหัวของเอกสาร

(๑.๒) ลับมาก ระบุคำว่า “ลับมาก” ในหน้าแรกและทุกหน้าบริเวณส่วนหัวของเอกสาร

(๑.๓) ลับ ระบุคำว่า “ลับ” ในหน้าแรกและทุกหน้าบริเวณส่วนหัวของเอกสาร

(๒) การทำลายเอกสาร (Destruction) แบ่งตามชั้นความลับของเอกสาร ดังนี้

(๒.๑) ลับที่สุด ให้ทำลายเอกสารโดยใช้เครื่องย่อยเอกสาร และเผาทำลายเศษเอกสารที่ได้จากการย่อย

(๒.๒) ลับมาก ให้ทำลายเอกสารโดยใช้เครื่องย่อยเอกสาร และเผาทำลายเศษเอกสารที่ได้จากการย่อย

(๒.๓) ลับ ให้ทำลายเอกสารโดยใช้เครื่องย่อยเอกสาร

(๓) การทำลาย...

(๓) การทำลายข้อมูลในสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ (Information Destruction in Electronic Media) ให้ทำลายข้อมูลโดยแบ่งตามชั้นความลับของสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ ดังนี้

(๓.๑) ลับที่สุด ให้ลบข้อมูลโดยใช้โปรแกรมประยุกต์ประเภทที่ไม่สามารถกู้คืนข้อมูลได้ (Secure Erase)

(๓.๒) ลับมาก ให้ลบข้อมูลโดยใช้โปรแกรมประยุกต์ประเภทที่ไม่สามารถกู้คืนข้อมูลได้ (Secure Erase)

(๓.๓) ลับ ให้ลบข้อมูลโดยใช้โปรแกรมประยุกต์ประเภทที่ไม่สามารถกู้คืนข้อมูลได้ (Secure Erase)

(๔) การทำลายข้อมูลในเครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ชนิดพกพา ให้ลบข้อมูลโดยใช้โปรแกรมประยุกต์ประเภทที่ไม่สามารถกู้คืนข้อมูลได้ (Secure Erase) ก่อนที่จะจำหน่ายพัสดุ หรือบริจาคพัสดุดังกล่าว

ข้อ ๕๕ การควบคุมผู้ให้บริการภายนอกที่กรมพินิจและคุ้มครองเด็กและเยาวชนทำสัญญาว่าจ้าง (Outsource)

(๑) ผู้ให้บริการภายนอกที่กรมพินิจและคุ้มครองเด็กและเยาวชนทำสัญญาว่าจ้าง (Outsource) ที่เข้ามาดำเนินกิจกรรมภายในกรมพินิจและคุ้มครองเด็กและเยาวชนในงานด้านความมั่นคงปลอดภัยสารสนเทศ ในสัญญาจ้างจะต้องมีตกลงการไม่เปิดเผยความลับ (Non-Disclosure Agreement) หรือข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ (Security in Third Party Agreements) หรือจะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรก่อน จึงจะสามารถเข้ามาปฏิบัติงานในกรมพินิจและคุ้มครองเด็กและเยาวชนได้

(๒) มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่กรมพินิจและคุ้มครองเด็กและเยาวชน ปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ ระดับการให้บริการ ลิขสิทธิ์และกฎหมายที่เกี่ยวข้อง เช่น กฎหมายลิขสิทธิ์และทรัพย์สินทางปัญญา เป็นต้น

(๓) มีการติดตามตรวจสอบรายงาน หรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอ

(๔) เมื่อสิ้นสุดการจ้างงาน หรือเปลี่ยนลักษณะการจ้างงาน ผู้ให้บริการภายนอกที่กรมพินิจและคุ้มครองเด็กและเยาวชนทำสัญญาจ้าง (Outsource) ต้องคืนทรัพย์สินของกรมพินิจและคุ้มครองเด็กและเยาวชนที่อยู่ในความครอบครองของตน

(๕) ต้องทำการถอดถอนสิทธิในการเข้าถึงระบบสารสนเทศและทรัพย์สินของเจ้าหน้าที่ที่กรมพินิจและคุ้มครองเด็กและเยาวชนสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน

ข้อ ๕๖ ศูนย์เทคโนโลยีสารสนเทศ ต้องกำหนดหน้าที่ความรับผิดชอบ และขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณ์ ด้านความมั่นคงปลอดภัย และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

ข้อ ๕๗ เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลระบบเก็บข้อมูลจราจร (Log) ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้นและค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

ข้อ ๕๘ ผู้ใช้...

ข้อ ๕๘ ผู้ใช้ต้องนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม และระเบียบว่าด้วยการรักษาความลับของราชการ (ฉบับที่ ๒) พ.ศ. ๒๕๖๑ ดังนี้

๑. ต้องแสดงหลักฐานในการกำหนดเรื่องข้อมูลลับ หรือข้อมูลที่สำคัญ

๓. มีเอกสารหรือหนังสืออย่างเป็นทางการว่าเป็นข้อมูลลับ

๔. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ แจ้งมาตรฐานข้อปฏิบัติการพัฒนาโปรแกรมและการกำหนดสิทธิข้อมูลที่เป็นความลับ

ข้อ ๕๙ ทบทวนและคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

(๕๙.๑) จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน และกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรองข้อมูล พร้อมกับซ้อมตามแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๒ ครั้ง

(๕๙.๒) ดำเนินการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูลของระบบสารสนเทศ โดยพิจารณาตามความถี่ในการเปลี่ยนแปลงข้อมูล โดยดำเนินการดังนี้

(๑) กำหนดประเภทของข้อมูลที่ต้องการสำรองเก็บไว้ และความถี่ในการสำรอง

(๒) กำหนดรูปแบบในการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง

(๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ชื่อข้อมูลที่สำรอง วัน/เวลา ที่ได้ดำเนินการและสถานะผลการสำรองว่า สำเร็จ หรือไม่สำเร็จ

(๔) ผู้จัดเก็บสื่อบันทึกข้อมูลการสำรองข้อมูล จะต้องตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน และสำเร็จ ทุกครั้งที่สำรองข้อมูลเสร็จ

(๕) การจัดเก็บข้อมูลสำรองในสื่อเก็บข้อมูล จะต้องมีการเขียนชื่อ และวันที่สำรองข้อมูลไว้บนสื่อที่จัดเก็บอย่างชัดเจน

(๖) มีการกำหนดสถานที่เพื่อจัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ทำงาน ซึ่งระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น หรือจัดเก็บข้อมูลไว้ที่ระบบคลาวด์กลางภาครัฐ ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

(๗) มีการกำหนดการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

(๘) ทดสอบการบันทึกข้อมูลอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(๙) จัดทำข้อมูลขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(๑๐) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

ข้อ ๖๐ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในเหตุการณ์ที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยดำเนินการปรับปรุงแผนดังกล่าวให้สามารถใช้การได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ มีแนวทางปฏิบัติต่อไปนี้

(๖๐.๑) กำหนด...

(๖๐.๑) กำหนดให้มีการจัดทำและทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีกาทางอิเล็กทรอนิกส์ (BCM)

(๖๐.๒) ในกรณีที่ไม่สามารถดำเนินการโดยระบบสารเทศได้ในช่วงเวลาหนึ่ง หน่วยงานจะต้องจัดเตรียมกระบวนการทำงานในช่องทางอื่นทดแทน ดังนี้

(๑) ระบบงานที่เกี่ยวข้องกับประชาชนทั่วๆไป ตามภารกิจหน่วยงานเจ้าหน้าที่ผู้รับเรื่องจะต้องดำเนินการตามแบบฟอร์มที่กำหนดไปพลางก่อน โดยภายหลังจากที่ระบบสารสนเทศกลับมาใช้งานได้ดังเดิม เจ้าหน้าที่ผู้รับเรื่องดังกล่าว จะต้องดำเนินการบันทึกข้อมูลเข้าสู่ระบบสารสนเทศที่เกี่ยวข้องในทันที

(๒) ระบบงานสารบรรณอิเล็กทรอนิกส์ (ระบบงานที่ใช้จัดส่งเอกสารทางราชการ) เจ้าหน้าที่ที่เกี่ยวข้องกับงานสารบรรณ ประจำสำนัก/กอง/กลุ่มงาน จะต้องดำเนินการจดบันทึกลำดับเลขที่หนังสือล่าสุด ที่เกี่ยวข้องกับหน่วยงานของตนเอง ได้แก่ เลขที่หนังสือภายใน และเลขที่หนังสือภายนอก ก่อนที่ผู้ดูแลระบบงานสารบรรณจะดำเนินการปิดระบบสารสนเทศ ทั้งนี้เพื่อให้สามารถดำเนินการออกหนังสือด้วยวิธีนับมือหรือใช้กระดาษไปพลางก่อน และเมื่อระบบงานสารบรรรณอิเล็กทรอนิกส์ สามารถกลับเข้าใช้งานได้ตามปกติ เจ้าหน้าที่งานสารบรรณดังกล่าว จะต้องดำเนินการบันทึกข้อมูลย้อนหลังโดยทันที

(๓) ระบบงานอื่นๆ ภายในหน่วยงาน ผู้รับผิดชอบหลังของระบบงานแต่ละระบบจะต้องรับผิดชอบในการดำเนินการบันทึกข้อมูลในภายหลังเมื่อระบบงานดังกล่าวกลับมาใช้งานได้ตามปกติ

(๔) มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๒ ครั้ง

ข้อ ๖๑ แต่งตั้งบุคลากรที่ได้กำหนดหน้าที่และความรับผิดชอบ อย่างน้อยจำนวน ๒ คน ในการดำเนินการตามแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีอิเล็กทรอนิกส์

ข้อ ๖๒ ดำเนินการตรวจสอบสภาพพร้อมใช้งานของระบบสารสนเทศ อย่างน้อย ๓ เดือนต่อครั้ง ทดสอบสภาพพร้อมใช้งานระบบสำรองข้อมูล อย่างน้อยปีละ ๒ ครั้ง และทดสอบแผนเตรียมความพร้อมฉุกเฉิน อย่างน้อยปีละ ๒ ครั้ง

ข้อ ๖๓ มีการทดสอบระบบสารสนเทศ ระบบสำรองข้อมูล และแผนเตรียมความพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๒ ครั้ง

ข้อ ๖๔ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessments) อย่างน้อยปีละ ๒ ครั้ง

ข้อ ๖๕ ตรวจสอบและประเมินความเสี่ยง (Internal Auditor) โดยเจ้าหน้าที่กลุ่มตรวจสอบภายในและผู้เชี่ยวชาญจากโครงการบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมพินิจและคุ้มครองเด็กและเยาวชน เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศและการสื่อสารที่มีอยู่ในปัจจุบัน

หมวด ๑๐...

หมวด ๑๐
หน้าที่และความรับผิดชอบ

ข้อ ๖๖ ผู้ใช้งานต้องปฏิบัติตามระเบียบฯ อย่างเคร่งครัดและต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง หากผู้ใดละเมิด ฝ่าฝืน ละเลย ไม่ปฏิบัติตามระเบียบนี้ และก่อให้เกิดความเสียหายแก่กรมพินิจและคุ้มครองเด็กและเยาวชนหรือบุคคลใดบุคคลหนึ่ง หัวหน้าหน่วยงานต้องพิจารณาดำเนินการทางวินัยและทางกฎหมาย แก่เจ้าหน้าที่ที่ละเมิด หรือฝ่าฝืนที่ก่อให้เกิดความเสียหาย ตามความเหมาะสมเป็นกรณีไป

ข้อ ๖๗ ให้หัวหน้าหน่วยงานมีหน้าที่ควบคุมดูแลการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารตามระเบียบนี้อย่างเคร่งครัดหากพบการไม่ปฏิบัติตามระเบียบนี้ให้แจ้งรายงานการละเมิดต่อกรมพินิจและคุ้มครองเด็กและเยาวชน ตามสายการบังคับบัญชา

ข้อ ๖๘ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่กรมพินิจและคุ้มครองเด็กและเยาวชน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือ ฝ่าฝืนการปฏิบัติตามระเบียบนี้ให้ผู้บริหารสูงสุด (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๖๙ ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติงานตามระเบียบนี้ หรือมิได้กำหนดแนวทางปฏิบัติไว้ ให้ผู้ใช้ระบบงานแจ้งต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อเสนออธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชนวินิจฉัยสั่งการต่อไป

ข้อ ๗๐ ให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ รักษาการตามระเบียบนี้

ข้อ ๗๑ ระเบียบใดที่ขัดหรือแย้งกับระเบียบนี้ ให้ถือปฏิบัติตามระเบียบนี้