ประกาศกรมพินิจและคุ้มครองเด็กและเยาวชน
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมพินิจและคุ้มครองเด็กและเยาวชน

ด้วยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ประกอบด้วย พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ดังนั้น เพื่อให้การดำเนินการใด ๆ มีความมั่นคงปลอดภัย มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ กรมพินิจและคุ้มครองเด็กและเยาวชน เห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ใช้เป็นแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมพินิจและคุ้มครองเด็กและเยาวชน เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓ ประกาศนี้ให้กรมพินิจและคุ้มครองเด็กและเยาวชน ดำเนินการให้ผู้ที่เกี่ยวข้องและผู้ใช้งานทั้งหมด ได้รับทราบโดยทั่วกันผ่านทาง https://www.djop.go.th ของกรมพินิจและคุ้มครองเด็กและเยาวชน

ข้อ ๔ ให้ใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน ที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๖ พฤศจิกายน พ.ศ. ๒๕๖๗

พันตำรวจโท
(ประวุธ วงศ์สีนิล)
อธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชน

แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศและข้อมูลส่วนบุคคล ของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ. 2568

0 2141 6484

it_information@djop.mail.go.th

http://portal.djop.go.th/itinformation/home

เอกสารแนบท้ายประกาศ
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมพินิจและคุ้มครองเด็กและเยาวชน

สารบัญ

หน้า

คำนิยาม

“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

“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 หรือบุคคลที่กรมพินิจและคุ้มครองเด็กและเยาวชนกำหนดให้ดูแลและบริหารจัดการระบบระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชน

“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 หรือใช้งานระบบคอมพิวเตอร์ทั้งทางอิเล็กทรอนิกส์ของกรมพินิจและคุ้มครองเด็กและเยาวชน

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

“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 ให้อยู่ในรูปแบบที่มีความหมาย เพื่อนำไปใช้ประโยชน์ในงานของกรมพินิจและคุ้มครองเด็กและเยาวชน

“ข่าวสารอิเล็กทรอนิกส์” หมายถึง เรื่องราว หรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของข้อความ เสียง และภาพ 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

“ระบบคอมพิวเตอร์” หมายถึง เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ (Hardware) โปรแกรม ชุดคำสั่ง (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

“ขอมูลสวนบุคคล” หมายความวา ขอมูลใด ๆ ที่สามารถระบุตัวบุคคลนั้นได (ระบุไปถึงเจาของข้อมูล) ไมวาจะเปนทางตรงหรือทางออมก็ตาม แตจะไมรวมไปถึงขอมูลของผูที่เสียชีวิตแลว หรือขอมูลของนิติบุคคล

“เจ้าของข้อมูล” หมายถึง ส่วนงานที่มีหน้าที่รวบรวม ใช้ และเปิดเผยข้อมูลที่เกี่ยวข้องกับการดำเนินงานตามภารกิจที่รับผิดชอบ

“ผู้ควบคุมข้อมูล” หมายถึง เจ้าหน้าที่ในส่วนงานที่รับผิดชอบจัดเก็บข้อมูลส่วนบุคคลตั้งแต่ ๑ คนขึ้นไป ที่ได้รับมอบหมายจากส่วนงานให้เป็นผู้รับผิดชอบ ควบคุม ดูแลข้อมูล

“เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” หมายถึง ผู้ที่ได้รับมอบหมายในการกำกับดูแล ตรวจสอบ ให้คำแนะนำเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทั้งหมดของหน่วยงาน เพื่อให้เป็นไปตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

“คณะกรรมการเทคโนโลยีสารสนเทศ” หมายถึง คณะเจ้าหน้าที่ซึ่งได้รับมอบหมายให้ดำเนินการ ตามอำนาจหน้าที่เกี่ยวกับการบริหารเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

“คณะกรรมการธรรมภิบาลข้อมูล (Data Governance Council)” หมายถึง คณะเจ้าหน้าที่ซึ่งได้รับ มอบหมายให้ดำเนินการตามอำนาจหน้าที่เกี่ยวกับการจัดทำธรรมาภิบาลข้อมูลของหน่วยงาน

“ผู้บริหารเทคโนโลยีสารสนเทศและการสื่อสารระดับสูง (DCIO)” หมายถึง ผู้บริหารสูงสุดด้านเทคโนโลยี สารสนเทศ เพื่อบริหาร กำกับ ดูแลงานด้านเทคโนโลยีสารสนเทศ กำหนดแผน และนโยบายรวมทั้งทิศทาง การดำเนินงานด้านเทคโนโลยีสารสนเทศของกรมพินิจและคุ้มครองเด็กแลเยาวชน

“ระบบงานคอมพิวเตอร์” หมายถึง ระบบงานที่กรมพินิจและคุ้มครองเด็กและเยาวชน ใช้ในการพัฒนาขึ้นแล้ว หรือจัดให้มีเพื่อใช้ในการปฏิบัติงานของกรมพินิจและคุ้มครองเด็กและเยาวชน

“ระบบรับ-ส่งหนังสือ และข่าวสารทางอิเล็กทรอนิกส์” หมายถึง

(๑) ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ ใช้สำหรับ สร้าง ส่ง และรับหนังสือหรือ ข่าวสารอิเล็กทรอนิกส์

(๒) ระบบจัดเก็บเอกสารอิเล็กทรอนิกส์ ใช้สำหรับ สร้าง ส่ง รับ และจัดเก็บ หนังสือ หรือ ข่าวสารอิเล็กทรอนิกส์

“ระบบลงลายมือชื่ออิเล็กทรอนิกส์” หมายถึง ระบบสนเทศของกรมพินิจและคุ้มครองเด็ก และเยาวชนที่สามารถลงลายมือชื่ออิเล็กทรอนิกส์ได้ และเป็นไปตามมาตรฐานที่สำนักงานพัฒนาธุรกรรม อิเล็กทรอนิกส์กำหนด

“ระบบเครือข่ายสื่อสาร” หมายถึง การติดต่อระหว่างคอมพิวเตอร์ระบบหนึ่งไปยังคอมพิวเตอร์อีกระบบหนึ่ง โดยผ่านสื่อที่เป็นสายเคเบิลหรือสื่อไร้สายและอุปกรณ์เครือข่ายสื่อสาร เป็นตัวเชื่อมโยงระหว่างกัน เพื่อให้ผู้ใช้ สามารถที่จะใช้งานข้ามระบบคอมพิวเตอร์ระหว่างกันได้ และติดต่อระหว่างผู้ใช้ได้อย่างกว้างขวางมากขึ้น

“ระบบเครือข่ายภายในกรม (Intranet)” หมายถึง ระบบเครือข่ายที่กำหนดให้มีการติดต่อ สื่อสารระหว่างผู้ใช้เฉพาะภายในหน่วยงานของกรมพินิจและคุ้มครองเด็กและเยาวชนเท่านั้น

“ระบบเครือข่ายอินเทอร์เน็ต (Internet)” หมายถึง ระบบเครือข่ายที่ให้บริการข้อมูลข่าวสารและ สารสนเทศ รวมถึงการติดต่อสื่อสารระหว่างผู้ใช้ภายในกรมพินิจและคุ้มครองเด็กและเยาวชนกับผู้ใช้ภายนอก กรมพินิจและคุ้มครองเด็กและเยาวชน

“ระบบเครือข่ายเอกซ์ทราเน็ต (Extranet)” หมายถึง ระบบเครือข่ายที่กำหนดเฉพาะ ให้มีการติดต่อสื่อสารระหว่างกรมพินิจและคุ้มครองเด็กและเยาวชนกับหน่วยงานภายนอกทั้งภาคราชการ หรือเอกชน เช่น ระบบ DXC เป็นต้น

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

“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 ข้อมูลการเข้าถึงเว็บไซต์ หรือข้อมูลส่วนบุคคลของเราที่ได้มีการลงทะเบียนกับเว็บไซต์นั้นๆ

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

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

“After Action Review (AAR)” หรือชื่อภาษาไทยว่า การทบทวนหลังการปฏิบัติงาน หมายถึง เป็นเทคนิค/วิธีการ/ขั้นตอนหนึ่งในการทำงานเป็นการทบทวนวิธีการทำงานทั้งด้านความสำเร็จและปัญหาที่เกิดขึ้น

ส่วนที่ ๑
นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงาน

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับหน่วยงานรับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๓. เพื่อให้การปฏิบัติงานเป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ผู้รับผิดชอบ

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO)

๒. คณะกรรมการเทคโนโลยีสารสนเทศ

๓. คณะกรรมการธรรมภิบาลข้อมูล (Data Governance Council)

๔. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

๕. ผู้อำนวยศูนย์เทคโนโลยีสารสนเทศ

๖. ผู้ดูแลเทคโนโลยีสารสนเทศที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Access Control)

เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลให้มีความมั่นคงปลอดภัย โดยมีแนวปฏิบัติดังนี้

๑.๑ สำหรับผู้ดูแลระบบสารสนเทศ

(๑) จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน ซึ่งจะจำแนกกลุ่มทรัพยากรของระบบและการทำงาน โดยกำหนดกลุ่มผู้ใช้งานและสิทธิของผู้ใช้งาน

(๒) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๒.๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

(๒.๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้ และ/หรือให้ระงับสิทธิการใช้งานภายหลังจากได้รับการแจ้งจากหน่วยงานที่เกี่ยวข้องเป็นลายลักษณ์อักษร

(๓) ต้องจัดให้ใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(๓.๑) ควบคุมการเข้าถึงสารสนเทศ โดยกำหนดการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(๓.๒) ปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๑.๒ สำหรับผู้ใช้งานระบบสารสนเทศที่ได้รับมอบหมาย จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้มีอำนาจหรือผู้ที่ได้รับมอบหมายเพื่อขอสิทธิการใช้งาน

๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทของข้อมูลออกเป็น

(๑.๑) ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี ข้อมูลด้านสถิติ เป็นต้น

(๑.๒) ข้อมูลสารสนเทศด้านการให้สนับสนุนการปฏิบัติงานสำหรับเจ้าหน้าที่ เช่น ข้อมูลบริหารการฝึกอบรม ข้อมูลรายงานการตรวจราชการ ข้อมูลการจองรถยนต์ ข้อมูลอาคารสถานที่ ข้อมูลเด็กรายวัน ข้อมูลสาธารณูปโภค ข้อมูลเครือข่ายเด็กและเยาวชน ข้อมูลคดีอาญา ข้อมูลคดีครอบครัว ข้อมูลกำกับการปกครอง เป็นต้น

(๑.๓) ข้อมูลสารสนเทศด้านการให้บริการประชาชน (E-Service) เช่น ข้อมูลการขอเยี่ยมเด็ก การข้อขึ้นทะเบียนเครือข่ายผู้ติดตามเด็กและเยาวชนหลังปล่อย การขอมีบัตรประชาชนกรรมการสงเคราะห์ เป็นต้น

(๑.๔) ข้อมูลการเชื่อมโยงระหว่างหน่วยงาน

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับคือ

(๒.๑) ข้อมูลที่มีระดับความสำคัญมากที่สุด

(๒.๒) ข้อมูลที่มีระดับความสำคัญปานกลาง

(๒.๓) ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

(๓.๑) ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างน้อยร้ายแรงที่สุด

(๓.๒) ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างน้อยร้ายแรง

(๓.๓) ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

(๓.๑) ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔) จัดแบ่งระดับชั้นการเข้าถึง

(๔.๑) ระดับชั้นสำหรับผู้บริหาร สามารถเข้าถึงข้อมูลทุกลำดับชั้นความลับของข้อมูล

(๔.๒) ระดับชั้นสำหรับผู้ใช้งานทั่วไป สามารถเข้าถึงลำดับชั้นข้อมูลทั่วไปเท่านั้น

(๔.๓) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย สามารถเข้าถึงลำดับชั้นข้อมูลทั่วไป โดยข้อมูลลับที่สุด ข้อมูลลับมาก และข้อมูลลับ ต้องได้รับอนุญาตจากผู้บริหาร

(๕) การกำหนดเวลาเข้าถึงระบบสารสนเทศและระบบเครือข่าย ดังนี้

(๕.๑) ข้อมูลสารสนเทศด้านบริหารต้องกำหนดให้มีการตรวจสอบการดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์โดยผู้ดูแลระบบประจำกรมพินิจและคุ้มครองเด็กและเยาวชนตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญต่อกรมพินิจและคุ้มครองเด็กและเยาวชน เพื่อป้องกันการเข้าถึงที่ไม่ถูกต้องและเหมาะสม

(๕.๒) ข้อมูลสารสนเทศสำหรับบริการประชาชนสามารถเข้าถึงได้ ๒๔ ชั่วโมง

(๖) ช่องทางที่สามารถเข้าถึงระบบเครือข่ายและระบบสารสนเทศของหน่วยงานมี ดังนี้

(๖.๑) ผ่านช่องทางเครือข่ายมีสาย (Wired LAN) และช่องทางเครือย่ายไร้สาย (Wireless LAN) โดยมีการจัดเก็บ Log การเข้าถึงเครือข่ายตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

(๖.๒) ผ่านหน้าเว็บไซต์หลักและเว็บไซต์ Portal โดยตรวจสอบสิทธิเข้าใช้งานด้วยระบบรหัสผู้ใช้งานและรหัสผ่าน

๒. การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต โดยมีการกำหนดขั้นตอนปฏิบัติ ต่อไปนี้

๒.๑ การลงทะเบียนบุคลากรและบุคคลที่ปฏิบัติงานให้กับหน่วยงาน ให้ผู้ดูแลระบบกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น ทั้งขั้นตอนปฏิบัติสำหรับการยกเลิก และการเปลี่ยนแปลงการใช้งาน ดังนี้

(๑) มีแบบฟอร์มขอใช้ระบบสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๒) ระบุชื่อบัญชีผู้ใช้งานแยกเป็นรายบุคคล และไม่ซ้ำกัน

(๓) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

(๔) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(๕) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

(๖) มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(๗) มีการตรวจสอบข้อมูลสิทธิและหน้าที่ที่เกี่ยวข้องของผู้ขอใช้งานระบบสารสนเทศโดยผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เป็นผู้พิจารณา

๒.๒ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการดูแลและจำกัดสิทธเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) ผู้ใช้งานต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องดำเนินการตามขั้นตอนการลงทะเบียนการเข้าถึงและใช้งานระบบสารสเทศ

(๒) จัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

(๒.๑) มีการจัดเก็บเอกสารการร้องขอและการกำหนดสิทธิ

(๒.๒) มีระบบจัดเก็บผู้ใช้งาน และสิทธิของผู้ใช้งาน

๒.๓ กำหนดการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว ต้องยากต่อการคาดเดาและมความแตกต่าง

(๓) ผู้ดูแลระบบต้องกำหนดวันหมดอายุรหัสผ่านอย่างน้อยทุก ๓ เดือน สำหรับรหัสผ่านของผู้ใช้งานทุกคน

(๔) ผู้ดูแลระบบต้องส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่น ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันทีหลังกจากได้รับรหัสผ่าน

(๕) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และต้องเปลี่ยนรหัสผ่านให้ยากต่อการดาดเดา

(๖) การเปลี่ยนรหัสผ่านในการเข้าใช้งานระบบสารสนเทศ ต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนจึงจะอนุญาตให้เปลี่ยนรหัสใหม่ได้

(๗) ในกรณีที่ผู้ใช้งานมีความจำเป็นต้องการใช้งานนอกเหนือจากสิทธิที่ได้รับ ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของตน และได้รับการอนุญาตจากผู้ดูแลระบบโดยมีการกำหนดระยะเวลาการเริ่มต้นใช้งาน และสิ้นสุดการใช้งาน ทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือร้นจากหน้าที่ความรับผิดชอบ

๒.๔ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยทุก ๓ เดือน หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง โดยมีการดำเนินการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsivilities) เพื่อให้ผู้ใช้งานทั้งส่วนกลางและส่วนภูมิภาค ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์ และระบบเครือข่าย อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ ดังนี้

๓.๑ ผู้ใช้งานต้องไม่ใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่ายของหน่วยงานในทางที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๓.๒ ผู้ใช้งานต้องใช้ระบบคอมพิวเตอร์อย่างปลอดภัย ดังนี้

(๑) ต้องดูแลเครื่องคอมพิวเตอร์และโปรแกรมชุดคำสั่งที่อยู่ในความรับผิดชอบให้มีความปลอดภัย จากการติดไวรัสคอมพิวเตอร์และภัยคุกคามในรูปแบบต่าง ๆ ตรวจสอบการป้องกันช่องโหว่ของโปรแกรมระบบปฏิบัติการและโปรแกรมอื่น ๆ ที่ติดตั้งในเครื่องคอมพิวเตอร์ให้เป็นปัจจุบันอยู่เสมอ และเมื่อพบความผิดปกติของอุปกรณ์คอมพิวเตอร์ให้รีบดำเนินการแก้ไขหรือแจ้งเจ้าหน้าที่ดูแลระบบความมั่นคงปลอดภัยสารสนเทศหรือเจ้าหน้าที่บริหารระบบความมั่นคงปลอดภัยสารสนเทศทราบโดยเร็ว

(๒) ห้ามนำเครื่องคอมพิวเตอร์ที่ยังไม่ได้รับการติดตั้งโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ที่เป็นปัจจุบันเชื่อมต่อกับระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชน

(๓) ห้ามใช้บริการที่ส่งผลกระทบต่อการใช้งานเครือข่ายสื่อสารและความปลอดภัย เช่น การดูภาพยนตร์ ฟังเพลง เล่นเกมส์ และบริการที่ให้ความบันเทิงต่าง ๆ

(๔) ห้ามติดตั้งโปรแกรมชุดคำสั่งที่มีผลกระทบต่อระบบความปลอดภัยของกรมพินิจและคุ้มครองเด็กและเยาวชน

(๕) ห้ามดาวน์โหลดโปรแกรมแจกฟรีในลักษณะ Freeware หรือ Shareware ที่ไม่มีให้บริการสำหรับดาวน์โหลดภายในเครือข่ายภายในกรม (Intranet)

(๖) ห้ามพัฒนาโปรแกรมไวรัสคอมพิวเตอร์ขึ้นเอง ห้ามทดสอบโปรแกรมไวรัสคอมพิวเตอร์และโปรแกรมในลักษณะที่ไม่ประสงค์ดีอื่น ๆ ที่อาจก่อให้เกิดความเสี่ยงและเป็นอันตรายต่อระบบคอมพิวเตอร์

(๗) ผู้ใช้งานที่ได้รับการจัดสรรเครื่องคอมพิวเตอร์ หรือผู้ดูแลการใช้เครื่องคอมพิวเตอร์จะต้องดูแลเครื่องคอมพิวเตอร์ให้อยู่ในสภาพดี ติดตั้งใช้งานอยู่ในสถานที่ที่ปลอดภัย มีการควบคุมผู้มีสิทธิในการเข้าใช้เครื่องคอมพิวเตอร์ มีการเก็บรักษาข้อมูลให้เป็นความลับ ใช้ความระมัดระวังในการเปิดเผยข้อมูลและเครื่องคอมพิวเตอร์ต้องมีความพร้อมในการใช้งานอยู่เสมอ

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

๓.๓ ผู้ใช้งานต้องดำเนินการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ดังนี้

(๑) กรณีที่มีการนำอุปกรณ์คอมพิวเตอร์และระบบสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนไปปฏิบัติงานภายนอกสำนักงาน เช่น ที่บ้าน เป็นต้น ผู้ใช้งานจะต้องปกปิดระบบสารสนเทศให้เป็นความลับและไม่เปิดเผยแก่บุคคลภายนอก พร้อมทั้งต้องดูแลรักษาอุปกรณ์คอมพิวเตอร์และระบบสารสนเทศให้มีความปลอดภัยตลอดเวลา

(๒) กรณีที่มีการนำอุปกรณ์คอมพิวเตอร์และระบบสารสนเทศเข้ามาใช้ภายในสำนักงาน จะต้องมีการตรวจสอบโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ให้เป็นปัจจุบัน รวมทั้งสื่อต่าง ๆ ที่จะนำกลับเข้ามาใช้งานให้ปลอดภัยก่อนการเชื่อมต่อกับระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชน

๓.๔ การป้องกันไวรัสคอมพิวเตอร์และปิดช่องโหว่ของซอฟต์แวร์ (Preventing Malware)

(๑) เครื่องคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่อกับเครือข่ายสื่อสาร ของกรมพินิจและคุ้มครองเด็กและเยาวชนจะต้องติดตั้งโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ (Antivirus) ที่เป็นลิขสิทธิ์ของกรมพินิจและคุ้มครองเด็กและเยาวชน รวมทั้งโปรแกรมการปิดช่องโหว่ (Patch) หรือเครื่องมือด้านความปลอดภัยอื่นๆ เพื่อความปลอดภัยในการใช้งาน

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

(๓) ผู้ดูแลระบบต้องตรวจสอบช่องโหว่ของระบบงาน และต้องปรับปรุงแก้ไขช่องโหว่เป็นประจำ เพื่อป้องกันการถูกบุกรุกหรือโจมตีระบบงาน

(๔) เมื่อพบว่าเครื่องคอมพิวเตอร์ติดไวรัสคอมพิวเตอร์ ให้หยุดการใช้งานโปรแกรมทั้งหมดและให้กำจัดไวรัสฯ รวมทั้งปรับปรุงโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Virus Definition File) และโปรแกรมการปิดช่องโหว่ให้เป็นปัจจุบันอยู่เสมอ หากไม่สามารถกำจัดไวรัสคอมพิวเตอร์ได้ ให้ตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ออกจากระบบเครือข่ายสื่อสาร (ดึงสาย UTP ออกจาก Port) และแจ้งเจ้าหน้าที่ดูแลระบบความปลอดภัยสารสนเทศให้ดำเนินการกำจัดไวรัสคอมพิวเตอร์โดยเร็ว พร้อมทั้งควรตรวจสอบการใช้สื่อบันทึกข้อมูลอื่นๆ ให้ปลอดภัยจากไวรัสคอมพิวเตอร์ก่อนการใช้งานเสมอ

(๕) ผู้ดูแลระบบและผู้ใช้งานระบบคอมพิวเตอร์จะต้องทำการสำรองข้อมูลให้เป็นปัจจุบันอยู่เสมอ และจัดเก็บไว้ในที่ปลอดภัย เพื่อสามารถนำกลับคืนมาใช้งานในกรณีที่มีการสูญเสียข้อมูลจากการติดไวรัสคอมพิวเตอร์

(๖) ติดตามข่าวสารด้านความปลอดภัยสารสนเทศ ตลอดจนปฏิบัติตามคำแนะนำเกี่ยวกับการป้องกันและกำจัดไวรัสคอมพิวเตอร์ รวมทั้งทำความเข้าใจกับภัยคุกคามและโทษของภัยคุกคามในรูปแบบต่างๆ ให้เป็นปัจจุบันอยู่เสมอ

(๗) ผู้ใช้ต้องมีความตระหนักและความระมัดระวัง (Awareness) ในการใช้ระบบสารสนเทศอย่างปลอดภัย

๓.๕ การใช้งานรหัสผ่าน (Password User)

(๑) การตั้งรหัสผ่าน (Password) ควรใช้รหัสผ่านที่คาดเดาได้ยาก รหัสผ่านควรมีความยาวไม่น้อยกว่า ๘ หลัก ประกอบด้วยตัวอักษรพิมพ์เล็ก ตัวอักษรพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์พิเศษ มีการแปลงคำที่ใช้ด้วยวิธีเฉพาะ เช่น การใช้ตัวเลขกับตำแหน่งต่างๆ ของคำ นำสัญลักษณ์พิเศษเข้ามาใช้ร่วมกับตัวเลขในคำที่กำหนด สร้างคำจากชื่อย่อของเพลง คำกลอนหรือลำดับในคำ กำหนดคำที่เจตนาพิมพ์ผิด ไม่ควรกำหนดค่าใดๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น หมายเลขบัตรต่างๆ ชื่อคู่สมรส หรือที่อยู่ รหัสผ่านที่กำหนดต้องไม่เป็นชื่อเดียวกันกับรหัสผู้ใช้งาน (User ID) ไม่ใช้รหัสผ่านที่ซ้ำกับรหัสผ่านเดิมก่อนหน้านี้ และรหัสผ่านที่กำหนดต้องไม่มีคำในพจนานุกรมหรือเป็นส่วนของคำพูด เช่น ชื่อเฉพาะ ชื่อสถานที่ คำศัพท์ด้านเทคนิค และคำหยาบ ไม่สร้างรหัสผ่านที่มีการพิมพ์เรียงตามลำดับตัวอักษร เช่น ๑๒๓๔๕ หรือ abcdef เป็นต้น ถ้าต้องการกำหนดรหัสผ่านเป็นวันเดือนปีจะต้องมีส่วนประกอบอื่นๆ เพิ่มเติม เช่น ๑๑๑๐๒๐๑๕@Mypass

(๒) ต้องเปลี่ยนรหัสผ่าน (Password) ในกรณีที่ได้รับสิทธิการเข้าใช้ระบบงานในครั้งแรก

(๓) ต้องเก็บรักษารหัสผ่าน (Password) ให้เป็นความลับโดยไม่เปิดเผยรหัสผ่านให้กับบุคคลอื่นๆ ทราบการกระทำใดๆ ภายใต้รหัสผู้ใช้ ถือเป็นความรับผิดชอบของเจ้าของรหัสผู้ใช้นั้น

(๔) ให้เปลี่ยนรหัสผ่านทันทีที่สงสัยว่ารหัสผ่านถูกใช้จากบุคคลที่ไม่ได้รับอนุญาต หรือถูกขโมย และให้เปลี่ยนรหัสผ่าน (Password) เป็นประจำทุกๆ ๖๐ วัน

(๕) ไม่เขียนรหัสผ่าน (Password) ในที่ใดที่หนึ่งที่บุคคลอื่นเข้าถึงได้ ไม่จัดเก็บรหัสผ่านในไฟล์ Batch file หรือ Script ที่ทำงานอัตโนมัติได้ และเมื่อไม่มีกิจกรรมใดๆ บนเครื่องคอมพิวเตอร์ ต้องกำหนดให้ล็อคหน้าจอ เมื่อกลับมาใช้งานใหม่ต้องระบุรหัสผ่านที่ถูกต้องก่อน โดยกำหนดค่าเวลาในการล็อคหน้าจอให้มีความปลอดภัย ตามความเหมาะสม

(๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่าย

(๗) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

(๘) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ระบบคอมพิวเตอร์ ของกรมพินิจและคุ้มครองเด็กและเยาวชน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล็อค หรือเกิดจากความผิดพลาดใดๆ 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

๓.๖ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน เพื่อป้องกันผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

(๑) ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีเมื่อเสร็จสิ้นการใช้งาน

(๒) ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๑๐ นาที และกำหนดให้ใส่รหัสผ่านจึงจะสามารถเปิดหน้าจอได้

(๓) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๓.๗ การควบคุมทรัพย์สินสารสนเทศ และการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ไม่ให้สินทรัพย์สารสนเทศ โดยเฉพาะเอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

(๑) ข้อปฏิบัติในการป้องกัน และควบคุมไม่ให้มีการทิ้งหรือปล่อยสินทรัพย์สารสนเทศให้อยู่ในสถานที่ที่ไม่ปลอดภัย ดังนี้

- จำกัดการเข้าถึงสินทรัพย์สารสนเทศที่สำคัญให้กำหนดสิทธิเฉพาะบุคคลที่เกี่ยวข้อง
- การจัดบริเวณการเข้าถึงบุคคลภายนอก
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- ล็อกคอมพิวเตอร์เมื่อไม่ได้ใช้งาน
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องแสกนเอกสาร
- ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน
- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
- ทำลายสื่ออิเล็กทรอนิกส์ เพื่อป้องกันการนำกลับมาใช้ใหม่ ดังนี้

อุปกรณ์สำหรับจัดเก็บ	วิธีทำลายข้อมูล
๑. แผ่นดิสก์	ใช้วิธีการหั่นด้วยเครื่องทำลายเอกสาร
๒. เทป	ใช้วิธีการทุบ หรือบดให้เสียหาย หรือเผาทำลาย
๓. กระดาษ	ใช้วิธีการหั่นด้วยเครื่องทำลายเอกสาร
๔. แผ่น CD/DVD	ใช้วิธีการทุบ หรือบดให้เสียหาย หรือเผาทำลาย
๕. ฮาร์ดดิสก์	ใช้วิธีการ Fotmat ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)
๖. Flash Drive	ใช้วิธีการทุบ หรือบดให้เสียหาย หรือเผาทำลาย
๗. ข้อมูลดิจิทัล	ใช้วิธีการทำลายสนามแม่เหล็ก โดยใช้เครื่องที่ผ่านการรับรองตามมาตรฐานสากล

(๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ
- วัฒนธรรมองค์กร

(๓) การป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกในการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

(๔) ผู้ใช้งานต้องนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม และระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ ๒) พ.ศ. ๒๕๖๑ ดังนี้

- ต้องแสดงหลักฐานในการกำหนดเรื่องข้อมูลลับ หรือข้อมูลที่สำคัญ
- มีเอกสารหรือหนังสืออย่างเป็นทางการว่าเป็นข้อมูลลับ
- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ แจ้งมาตรฐานข้อปฏิบัติการพัฒนาโปรแกรมและการกำหนดสิทธิข้อมูลที่เป็นความลับ

(๕) ข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับ หรือข้อมูลสำคัญ

- มีเอกสารหรือหนังสืออนุญาตอย่างเป็นทางการจากผู้ที่รับผิดชอบข้อมูลลับนั้น

(๖) ข้อปฏิบัติเบื้องต้นในการเข้ารหัสข้อมูลกรณีที่ไม่มีการบันทึกข้อมูลลงระบบฐานข้อมูลให้ดำเนินการดังนี้

- ข้อมูลประเภท Soft file ที่มีชั้นความลับ จะต้องใช้ซอฟต์แวร์ประเภทบีบอัดข้อมูลร่วมกับการเข้ารหัส เช่น ๗zip, winzip หรือ winrar เป็นต้น โดยระบุรหัสผ่านไม่น้อยกว่า ๘ ตัวอักษร ประกอบด้วยตัวอักษร ตัวเลข และอักขระพิเศษ ซึ่งยากต่อการคาดเดา
- กรณีต้องการกลับมาใช้งานข้อมูลที่ถูกบีบอัดที่ได้กำหนดรหัสผ่านไว้ ต้องใส่รหัสผ่านให้ตรงตามที่กำหนดไว้ในกระบวนการบีบอัดข้อมูลข้างต้น
- รหัสที่ใช้ในการบีบอัดและแตกไฟล์ดังกล่าว จะต้องไม่ถูกจัดเก็บไว้ในที่เดียวกับที่อยู่ของไฟล์ใน media เดียวกัน

(๗) ข้อปฏิบัติเบื้องต้นในการเข้ารหัสข้อมูลในกรณีที่ข้อมูลความลับอยู่บนระบบฐานข้อมูล

- ในขั้นตอนการดำเนินการจัดทำระบบฐานข้อมูล จะต้องดำเนินการพัฒนาระบบให้รองรับการเข้ารหัสข้อมูลชนิดที่มีใบรับรอง Certificated SSL เป็นอย่างน้อย ทั้งนี้เพื่อป้องกันการถูกดักจับข้อมูลระหว่างทางการส่งข้อมูล
- ให้ผู้ใช้งานนำการเข้ารหัส (Encryption) มาใช้กับข้อมูลที่เป็นความลับ โดยจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๓.๘ การใช้งานสื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) ได้แก่ (Optical Discs (Blu-Ray discs, DVDS, CD-ROMs), Memory Cards (Compact Flash card, Secure Digital card, Memory Stick), Zip Disks/ Floppy disks, USB flash drives, External hard drives (DE, EIDE, SCSSI, and SSD), Digital cameras, Smart phones, Other external/dockable devices which contain removable media capabilities) อย่างปลอดภัย มีแนวปฏิบัติดังนี้

(๑) สแกนสื่อเก็บข้อมูลแบบถอดได้ทุกครั้งก่อนใช้งาน ด้วยซอฟต์แวร์แอนตี้ไวรัสที่เชื่อถือได้ เพื่อตรวจหามัลแวร์หรือไวรัสที่อาจจะซ่อนอยู่ การสแกนเป็นขั้นตอนที่ไม่ควรละเลย เพราะช่วยลดความเสี่ยงในการนำไวรัสเข้าสู่ระบบคอมพิวเตอร์ของคุณ

(๒) ไม่เชื่อมต่อสื่อเก็บข้อมูลแบบถอดได้กับเครื่องคอมพิวเตอร์ที่ไม่รู้จักหรือที่ไม่แน่ใจว่ามีความปลอดภัยหรือไม่

(๓) ห้ามเปิดเผยรหัสผ่านที่ใช้กับสื่อหรืออุปกรณ์แบบถอดได้แก่ผู้อื่นหรือผู้ที่ไม่ได้รับอนุญาต

(๔) ปิดการใช้งานคุณสมบัติการทำงานแบบอัตโนมัติ (AutoRun) คือฟีเจอร์ที่ทำให้สื่อเก็บข้อมูลแบบถอดได้ทำงานอัตโนมัติเมื่อเสียบเข้ากับคอมพิวเตอร์ ซึ่งเป็นช่องทางที่มัลแวร์สามารถรันได้ทันที ควรปิดการทำงานของ AutoRun เพื่อป้องกันการรันไฟล์ที่อาจจะเป็นอันตรายต่อระบบคอมพิวเตอร์

(๕) สำรองข้อมูลสำคัญเสมอ ในกรณีที่ข้อมูลที่อยู่ในสื่อเก็บข้อมูลแบบถอดได้ ได้รับความเสียหายจากมัลแวร์ การสำรองข้อมูลเป็นวิธีที่ดีที่สุดในการป้องกันความสูญเสีย จัดเก็บข้อมูลสำคัญในหลาย ๆ แหล่ง เช่น บนคลาวด์หรือในฮาร์ดไดร์ฟภายนอก เพื่อให้มั่นใจว่าข้อมูลจะไม่สูญหายแม้สื่อเก็บข้อมูลแบบถอดของคุณจะเสียหาย

(๖) ติดตั้งระบบ Encryption เพื่อเข้ารหัสสื่อเก็บข้อมูลแบบถอดได้ ให้เปิดได้เฉพาะเครื่องที่อนุญาต

- เข้ารหัสไฟล์ก่อนการสำเนาข้อมูล
- เข้ารหัส สื่อเก็บข้อมูลแบบถอดได้ทั้งหมด เพื่อป้องกันการนำไปเปิดกับเครื่องที่ไม่อนุญาต

(๗) หากมีการถ่ายโอนข้อมูลที่ละเอียดอ่อนจากสื่อหรืออุปกรณ์แบบถอดได้เสร็จแล้ว ควรลบข้อมูลดังกล่าวออกจากอุปกรณ์นั้น

(๘) ควรเปลี่ยนรหัสผ่านใหม่ทุกครั้งก่อนและหลังการถ่ายโอนข้อมูลทุกครั้ง

๓.๙ การแบ่งปันข้อมูล (Information Sharing)

(๑) แนวปฏิบัติการแบ่งปันข้อมูลส่วนบุคคล

(๑.๑) ผู้ขอใช้บริการข้อมูล ต้องเป็นหน่วยงานหรือบุคคลที่ได้รับสิทธิ์การเข้าถึงข้อมูลจากกรมพินิจและคุ้มครองเด็กและเยาวชน เท่านั้น

(๑.๒) ผู้ขอใช้บริการต้องทำหนังสือขอรับ Token Key จากทางกรมพินิจและคุ้มครองเด็กและเยาวชน เพื่อเรียกใช้บริการข้อมูล ซึ่ง Token Key มีอายุใช้งานเป็นระยะเวลา ๑ ปี เท่านั้น

(๑.๓) ในกรณีที่ผู้ขอใช้บริการไม่ทำหนังสือขอต่ออายุการใช้งาน Token Key มายังกรมพินิจและคุ้มครองเด็กและเยาวชน ภายในระยะเวลาที่กำหนด กรมพินิจและคุ้มครองเด็กและเยาวชน ขอสงวนสิทธิ์ในการหยุดให้บริการ API ดังกล่าวทันที

(๑.๔) ผู้ขอใช้บริการจะต้องเก็บรักษา Token key ไว้เป็นอย่างดี ห้ามเปิดเผยแก่ผู้อื่น

(๑.๕) หากมีข้อมูลรั่วไหลของข้อมูลอันเกิดจากการใช้งานผ่าน Token key ดังกล่าว ผู้ขอใช้บริการจะต้องเป็นผู้รับผิดชอบต่อความเสียหายทุกกรณี

(๒) แนวปฏิบัติการแบ่งปันข้อมูลทั่วไป ผู้ใช้งานทุกระดับสามารถเข้าถึงบริการได้ โดยไม่ต้องมีการเข้ารหัสข้อมูล เช่น ข้อมูลสถิติ เป็นต้น

๔. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operation System Access Control) แบ่งออกเป็นระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์ลูกข่ายประเภทที่ใช้ช่องสัญญาณมีสาย (Wired LAN) ระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์ลูกข่ายประเภทที่ใช้ช่องสัญญาณไร้สาย (Wireless LAN) และระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่าย โดยมีรายละเอียด ดังนี้

๔.๑ สำหรับผู้ดูแลระบบ

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

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

(๓) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธียืนยันตัวตนที่มั่นคงปลอดภัย โดยมีข้อกำหนดดังนี้

(๓.๑) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการคาดเดารหัสผ่าน จากเครื่องปลายทาง

(๓.๒) ดำเนินการปิดการเชื่อมต่อโดยตรงผ่านทาง Command Line เพื่อป้องกันการสูญเสียที่อาจจะเกิดขึ้นได้

(๓.๓) ดำเนินการปิดการเข้าสู่การตั้งค่าต่างๆ ในระบบปฏิบัติการของระบบคอมพิวเตอร์ลูกข่ายที่ได้เชื่อมต่อเข้าสู่ระบบเครือข่ายแบบมีสาย

(๔) การเข้าถึงระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย โดยใช้สิทธิในการติดตั้งโปรแกรมต่างๆ จะต้องเข้าถึงและดำเนินการโดยผู้ดูแลระบบในระดับของกรมเท่านั้น

(๕) การใช้งานโปรแกรมอรรถประโยชน์ (user of system utilities) ต้องจำกัด และควบคุมการใช้งานโปรแกรมดังกล่าวในเครื่องคอมพิวเตอร์ที่มีข้อมูล หรือใช้ในงานสำคัญ เนื่องจากโปรแกรมอรรถประโยชน์บางชนิด สามารถทำให้ผู้ใช้งานหลีกเลี่ยงจากการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ ดังนั้นเพื่อป้องกันการละเมิดหรือหลีกเลี่ยงจากการตรวจสอบ ให้เจ้าหน้าที่ที่ได้รับมอบหมายดำเนินการ ดังนี้

(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

๔.๒ สำหรับผู้ใช้งานทั่วไป

(๑) ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ซึ่งสามารถระบุตัวตนของผู้ใช้งาน หรืออาจมีระบบความปลอดภัยอื่น ๆ เช่น Token, Smart Card, Finger Print ที่นำมาใช้ร่วมกันเพื่อพิสูจน์ตัวตนของผู้ใช้งาน (Multi Factors Authentication) 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 เมื่อได้ดำเนินการติดตั้งระบบเสร็จสิ้นแล้วให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้กำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที เพื่อป้องกันการเข้าติดตั้งโปรแกรมในระบบปฏิบัติการโดยผู้ใช้งานทั่วไป ทั้งนี้เพื่อป้องกันการติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์

(๔) ผู้ใช้งานทั่วไปไม่สามารถติดตั้งโปรแกรมต่าง ๆ บนระบบปฏิบัติการของเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่ายประเภทมีสายด้วยตัวเองได้ ทั้งนี้เพื่อป้องกันการติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์

(๕) เมื่อมีการเว้นจากการใช้งานระยะหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

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

(๕.๒) เมื่อไม่มีการใช้งานระบบต้องทำการยกเลิกการใช้โปรแกรมประยุกต์ และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๖) การเข้าถึงระบบปฏิบัติการของเครื่องคอมพิวเตอร์ลูกข่ายประเภทไร้สาย สามารถเข้าถึงได้โดยผู้ใช้งานทั่วไป แต่จะถูกจำกัดสิทธิการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด ซึ่งหมายถึงมีระดับสิทธิเสมือนเป็นผู้ใช้งานที่เป็นบุคคลภายนอกเท่านั้น

(๗) ผู้ใช้งานทั่วไปไม่สามารถเข้าใช้งานระบบปฏิบัติการที่ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายของกรมพินิจและคุ้มครองเด็กและเยาวชน

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

๕. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ (Application and information access control)

๕.๑ สำหรับผู้ดูแลระบบ

(๑) ดำเนินการจำกัดการเข้าถึงสารสนเทศ (information access restriction) โดยการควบคุมผู้ใช้งาน และบุคลากรฝ่ายสนับสนุน ที่มีการเข้าใช้งานระบบสารสนเทศ โปรแกรมประยุกต์ หรือแอพพลิเคชัน ดังนี้

(๑.๑) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของหน่วยงานตามข้อกำหนดการลงทะเบียนผู้ใช้งานหรือการบริหารจัดการสิทธิ์ของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิ์การเข้าถึงระบบสารสนเทศและข้อมูลต่างๆ

(๑.๒) ต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่าง ๆ และหากไม่มีการใช้งานเกินระยะเวลาที่กำหนด หรือยกเลิกการเชื่อมต่อระบบ

(๑.๓) ผู้ให้บริการภายนอก (Outsource) ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลหน่วยงาน

(๑.๔) ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิ์การเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

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

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อกรมพินิจและคุ้มครองเด็กและเยาวชน จะต้องดำเนินการ ดังนี้

(๒.๑) ต้องมีการระบุความสำคัญของระบบงานซึ่งไวต่อการรบกวน หรือมีผลกระทบสูงต่อหน่วยงาน

(๒.๒) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ

(๒.๓) มีการประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกัน ระหว่างระบบงานที่มีความสำคัญสูงกับระบบงานอื่นๆ ที่มีความสำคัญน้อยกว่า

(๒.๔) ต้องควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ ได้แก่การตรวจสอบและดูแลสภาพแวดล้อมภายในบริเวณพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในพื้นที่รับผิดชอบของกรมพินิจและคุ้มครองเด็กและเยาวชน

(๒.๕) มีการสำรองและทดสอบการกู้คืนระบบ ตามนโยบายระบบสารสนเทศและระบบสำรองสารสนเทศ

(๒.๖) ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

(๒.๗) ทำการควบคุมเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกตามข้อกำหนดที่ตั้งค่าไว้ใน Firewall หรืออุปกรณ์ระบุเส้นทางบนเครือข่าย (Routing)

๕.๒ สำหรับผู้ใช้งานทั่วไป

การเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศด้วยอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ (Mobile Computing) จะต้องมีการควบคุมการใช้งาน โดยมีขั้นตอนการควบคุม ดังนี้

(๑) ผู้ที่จะใช้งานผ่านอุปกรณ์เคลื่อนที่ดังกล่าว จะต้องกรอกแบบฟอร์มตามรูปแบบที่เจ้าหน้าที่ผู้รับชอบดูแลระบบกำหนดไว้

(๒) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ พิจารณาอนุญาตเป็นรายกรณีเมื่อผ่านการพิจารณาและจะส่งต่อให้ผู้ดูแลระบบประจำกรมพินิจและคุ้มครองเด็กและเยาวชนตรวจสอบและดำเนินการกำหนดสิทธิ์การใช้งาน และแจ้งกลับบุคคลดังกล่าวทราบ เป็นลายลักษณ์อักษรหรือผ่านช่องทางจดหมายอิเล็กทรอนิกส์

(๓) ผู้ใช้งานทั่วไปที่ใช้อุปกรณ์สื่อสารเคลื่อนที่ในการเข้าถึงระบบเครือข่ายของหน่วยงานจะไม่สามารถเข้าถึงระบบเครือข่ายที่จัดทำขึ้นเพื่อใช้สำหรับเป็นช่องทางเฉพาะ เว้นแต่ได้รับสิทธิ์พร้อมทั้งมีการยืนยันตัวบุคคลจากรหัสผู้ใช้งานและรหัสผ่าน ก่อนการเข้าใช้งานระบบแล้วเท่านั้น

(๔) การเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงานต้องใช้งานตามสิทธิ์ที่ตนเองได้รับ หากมีการส่งมอบรหัสผู้ใช้งานและรหัสผ่านของตนเองให้บุคคลอื่นดำเนินการต่าง ๆ ในระบบสารสนเทศแทนตนเองแล้วและหากเกิดความเสียหายขึ้น ผู้ส่งมอบรหัสผ่านจะต้องรับผิดชอบต่อความเสียหายนั้นในทุกกรณี

๕.๓ สำหรับผู้ดำเนินการจากภายนอก (Out Source) ตามโครงการที่มีการจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์แม่ข่ายและระบบงานสารสนเทศ หรือโครงการในลักษณะที่มีการจัดจ้างดำเนินการอื่นๆ ที่มีความเกี่ยวข้องกับข้อมูลสารสนเทศหรือระบบเครือข่ายของหน่วยงาน มีข้อปฏิบัติที่ต้องดำเนินการ ดังนี้

(๑) พิสูจน์ตัวตนก่อนเข้าดำเนินการบำรุงรักษาระบบสารสนเทศ

(๒) ดำเนินการทดสอบการใช้งานของระบบสารสนเทศตามรอบระยะเวลาที่เหมาะสม

(๓) หากพบปัญหาในระหว่างดำเนินการบำรุงรักษาระบบงาน จะต้องแจ้งต่อผู้ดูแลระบบทราบในทันทีพร้อมดำเนินการแก้ไขให้แล้วเสร็จตามข้อกำหนดในสัญญาว่าจ้าง หรือระยะเวลาที่เหมาะสม และจัดทำรายงานสรุปผล และข้อเสนอข้อแก้ไขดังกล่าว

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

(๕) การเข้าถึงและใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงาน จะต้องใช้งานตามสิทธิ์ที่ตนเองได้รับ ซึ่งหากมีการส่งมอบรหัสผู้ใช้งานและรหัสผ่านของตนเองให้บุคคลอื่น ๆ ดำเนินการต่างๆ ในระบบสารสนเทศแทนตนเอง และเกิดความเสียหายขึ้น ผู้ส่งมอบรหัสผ่านจะต้องรับผิดชอบต่อความเสียหายนั้นในทุกกรณี

(๖) ผู้ดำเนินการจากหน่วยงานภายนอก ต้องยอมรับในข้อกำหนดการรักษาความลับของข้อมูลสารสนเทศ ข้อมูลระบบเครือข่าย และข้อมูลระบบรักษาความปลอดภัยต่างๆ ที่เกี่ยวข้องต่อความมั่นคงปลอดภัยด้านข้อมูลและสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน

๖. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

๖.๑ ผู้ดูแลระบบประจำกรมพินิจและคุ้มครองเด็กและเยาวชน ต้องมีการออกแบบระบบเครือข่ายให้ชัดเจนและรัดกุม เพื่อทำให้การควบคุมและป้องกันการบุกรุกเป็นไปอย่างมีประสิทธิภาพ

๖.๒ ผู้ดูแลระบบประจำกรมพินิจและคุ้มครองเด็กและเยาวชน ต้องกำหนดวิธีในการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถ ใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น ดังนี้

(๑) มีการกำหนดการเข้าถึงระบบสารสนเทศ โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้ โดยการใช้รหัสผู้ใช้งาน และรหัสผ่านในการยืนยันตัวบุคคล โดยภายหลังระบุตัวตนแล้วจะสามารถเข้าถึงระบบเครือข่ายตามระดับการควบคุม ดังนี้

- ระดับการควบคุมการเข้าถึงระบบเครือข่าย แบ่งเป็นระบบเครือข่ายสำหรับผู้แลระบบ
- ระดับกรม ผู้ดูแลระบบระดับหน่วยงาน และสำหรับผู้ใช้งานทั่วไป ระดับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงาน โดยแบ่งเป็นผู้ดูแลระบบสารสนเทศระดับกรม ผู้ดูแลระบบสารสนเทศ และผู้ใช้งานทั่วไปที่มีสิทธิ์เข้าถึงระบบ
- ควบคุมการเข้าถึงระบบปฏิบัติการ โปรแกรมประยุกต์หรือแอพพลิเคชันต่างๆ แบ่งเป็นผู้ดูแลระบบระดับหน่วยงาน และผู้ใช้งานทั่วไป

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

(๓) กรณีที่มีการเปลี่ยนแปลงผู้ใช้งาน หรือพ้นสภาพจาการปฏิบัติงานของกรมพินิจและคุ้มครองเด็กและเยาวชน หน่วยงานต้นสังกัดของผู้ใช้งานดังกล่าว จะต้องแจ้งศูนย์เทคโนโลยีสารสนเทศทราบเป็นลายลักษณ์อักษร ภายใน ๗ วันทำการ หรือในกรณีที่เป็นผู้ใช้งานจากหน่วยงานภายนอกให้เป็นไปตามที่ผู้ดูแลระบบกำหนด

๖.๓ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องดำเนินการตามข้อปฏิบัติหรือกระบวนการเพื่อยืนยันบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

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

(๒) การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต จะต้องกำหนดให้มีการตรวจสอบสิทธิผู้ใช้งานด้วยทุกครั้ง โดยตรวจสอบสิทธิเพื่อพิสูจน์ตัวตน

(๓) เข้าใช้งานโปรแกรมควบคุมเครื่องจากระยะไกล (VPN) เพื่อใช้งานระบบภายในกรมพินิจและคุ้มครองเด็กและเยาวชน จะต้องประสานผู้รับผิดชอบดูเครือข่ายของกรมพินิจและคุ้มครองเด็กและเยาวชน ซึ่งผู้ใช้งานจำเป็นต้องปฏิบัติงานทุกครั้ง

(๔) บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ผู้ดูแลระบบต้องเป็นผู้รับผิดชอบและต้องจัดเจ้าหน้าที่อยู่เฝ้าระวังความปลอดภัยอย่างใกล้ชิดตลอดเวลาจนแล้วเสร็จ หากมีปัญหาหรือข้อสงสัยด้านความปลอดภัยให้ปรึกษาหรือสอบถามจากเจ้าหน้าที่บริหารระบบความปลอดภัยสารสนเทศ

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

(๖) ผู้ใช้งานจะเข้าถึงระบบสารสนเทศเพื่อการปฏิบัติงานได้เฉพาะในส่วนที่ได้รับอนุญาตตามการกำหนดสิทธิจากผู้ดูแลระบบคอมพิวเตอร์เท่านั้น

(๗) การเข้าถึงระบบสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนจากภายนอกหน่วยงานจะต้องใช้งานผ่านระบบ ตามที่กรมพินิจและคุ้มครองเด็กและเยาวชนอนุญาตเท่านั้น

(๘) การทิ้งทำลายสื่อบันทึกข้อมูลที่อาจมีข้อมูลสำคัญหรือชั้นความลับ เช่น กระดาษจดรหัสผ่าน รายงานสารสนเทศที่เป็นความลับจะต้องผ่านกระบวนการทำลาย เช่น การตัดย่อยกระดาษ การเผาทำลาย

(๙) ผู้ใช้งานที่ต้องการได้รับสิทธิในการเข้าใช้ระบบงาน ต้องขออนุญาตผู้มีอำนาจของหน่วยงานและส่งให้ผู้ดูแลระบบเพื่อดำเนินการกำหนดสิทธิในการเข้าใช้งานต่อไป

(๑๐) การเปลี่ยนแปลงสิทธิการเข้าใช้งานระบบงาน ผู้มีอำนาจจะต้องดำเนินการตรวจสอบเจ้าหน้าที่ว่ามีสิทธิการใช้ระบบงานในระบบนั้น ๆ และแจ้งต่อผู้ดูแลระบบงานเพื่อเปลี่ยนแปลงสิทธิการเข้าใช้งานระบบงาน

(๑๑) ห้ามผู้ใช้งานเข้าใช้งาน พิมพ์ หรือสำรองข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล

๖.๔ ผู้ดูแลประจำกรมพินิจและคุ้มครองเด็กและเยาวชน เป็นผู้พิจารณาและกำหนดช่องทาง/เส้นทางการเข้าถึงเครือข่าย โดยควบคุมการเข้าถึงการใช้งาน ให้สอดคล้องกับแนวปฏิบัติ ดังนี้

(๑) มีการตรวจสอบการเชื่อมต่อเครือข่าย และกำหนดสิทธิตามสิทธิผู้ใช้งาน

(๒) มีระบบป้องกันการบุกรุกระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๓) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

๖.๕ ผู้ดูแลระบบประจำกรมพินิจและคุ้มครองเด็กและเยาวชน จะต้องกำหนดการใช้เส้นทางบนเครือข่ายจากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้

๖.๖ ต้องมีการมอบหมายบุคคลที่รับผิดชอบในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน

๖.๗ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานให้เชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก เช่น ผ่านอุปกรณ์ Firewall

๖.๘ 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) ให้ผู้ดูแลระบบเครือข่ายสื่อสารดำเนินการกำหนดเลขที่อยู่ไอพี (IP Address) และให้ดำเนินการลงทะเบียนเลขที่อยู่ไอพีเข้าระบบแจกจ่ายเลขที่อยู่ไอพีอัตโนมัติ

(๖) กรณีต้องการยกเลิกใช้งานเลขที่อยู่ไอพี (IP Address) ที่ได้รับจากศูนย์เทคโนโลยีสารสนเทศให้ดำเนินการแจ้งยกเลิกการใช้งานกับศูนย์เทคโนโลยีสารสนเทศ เพื่อให้ผู้ดูแลระบบเครือข่ายสื่อสารดำเนินการยกเลิกการใช้งานเลขที่อยู่ไอพี

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

(๘) การเชื่อมต่อระบบเครือข่ายสื่อสารกับเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่เกี่ยวข้องให้ใช้เฉพาะเลขที่อยู่ไอพี (IP Address) ที่ได้ลงทะเบียนไว้แล้วเท่านั้น

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

๖.๑๐ ในกรณีที่หน่วยงานต้องการจัดทำวง LAN หรือปรับปรุงจุดติดตั้งภายในหน่วยงานให้ขออนุมัติต่อศูนย์เทคโนโลยีสารสนเทศก่อนดำเนินการ โดยข้อมูลที่ใช้ประกอบการจัดทำวง LAN ได้แก่

- วัตถุประสงค์ของการจัดทำวง LAN
- ผังการเชื่อมต่ออุปกรณ์เครือข่ายสื่อสาร
- จำนวนจุดติดตั้ง

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

๖.๑๒ การเผยแพร่ข้อมูลโครงสร้างหรือแผนภาพ (Diagram) ของระบบเครือข่ายสื่อสารให้เผยแพร่ได้เฉพาะที่ผู้ดูแลระบบเครือข่ายสื่อสารได้จัดเตรียมไว้สำหรับเผยแพร่เท่านั้น

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

๖.๑๔ ในกรณีที่จำเป็นต้องนำเครื่องคอมพิวเตอร์ที่มีการใช้ Air Card หรือการเชื่อมต่อ Internet ไร้สายด้วยวิธีการอื่นใดก็ตามมาใช้ภายในหน่วยงานของกรมพินิจและคุ้มครองเด็กและเยาวชน ไม่อนุญาตให้นำเครื่องคอมพิวเตอร์เชื่อมต่อเข้ากับระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชนโดยเด็ดขาด

๖.๑๕ ห้ามผู้ใช้งานกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ หรือกระทำด้วยประการใดเพื่อให้การทำงานของคอมพิวเตอร์ของผู้อื่นถูกระงับ เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานได้ตามปกติ

๖.๑๖ ผู้ใช้งานต้องรายงานการล่วงละเมิดการใช้งานระบบเครือข่ายสื่อสารหรือการใช้งานที่ผิดปกติให้แก่ผู้ดูแลระบบเครือข่ายสื่อสารทราบโดยทันที

๖.๑๗ ห้ามจัดตั้งหรือใช้งานอุปกรณ์หรือโปรแกรมใด ๆ เพื่อทำการเปลี่ยนกลุ่มเลขที่อยู่ไอพี Proxy หรือเปลี่ยน Port ที่ให้บริการ Tunnel เพื่อเชื่อมต่อกับระบบเครือข่ายสื่อสาร ทั้งระบบเครือข่ายภายในกรม และระบบเครือข่ายอินเทอร์เน็ต

๖.๑๘ ห้ามผู้ใช้งานจัดตั้งระบบที่ใช้สำหรับการกำหนดเลขที่อยู่ไอพี (IP Address) อัตโนมัติแก่เครื่องคอมพิวเตอร์ที่ติดตั้งอยู่บนระบบเครือข่ายสื่อสาร

๖.๑๙ ห้ามผู้ใช้งานเข้าถึงอุปกรณ์เครือข่ายเพื่อทำการแก้ไขหรือตรวจสอบค่า Configuration ของอุปกรณ์เครือข่ายสื่อสาร

๖.๒๐ ผู้ดูแลระบบเครือข่ายสื่อสารมีหน้าที่กำหนดการแบ่งแยกระบบเครือข่ายสื่อสาร (Segregation In Networks) ต้องทำการแบ่งแยกเครือข่ายสื่อสารตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบงาน และดำเนินการแบ่งแยกระบบเครือข่ายสื่อสารเฉพาะที่ไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงของกรมพินิจและคุ้มครองเด็กและเยาวชน

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

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

๖.๒๓ ผู้ดูแลระบบเครือข่ายสื่อสารมีสิทธิตรวจสอบข้อมูลที่อยู่ระหว่างการรับ-ส่งข้อมูลในระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชน เพื่อการวิเคราะห์และแก้ไขปัญหาต่าง ๆ

๖.๒๔ ผู้ดูแลระบบเครือข่ายสื่อสารต้องเฝ้าดูแล (Monitor) ระบบเฝ้าระวังเครือข่ายสื่อสาร (Network Monitoring Tools) ตลอดเวลาเพื่อการแจ้งปัญหาอุปสรรค ความผิดปกติของระบบเครือข่ายสื่อสารที่เกิดขึ้นให้หัวหน้าหน่วยงาน หรือผู้มีอำนาจทราบโดยเร็ว

๖.๒๕ ในกรณีฉุกเฉินและมีความจำเป็นเร่งด่วนหากล่าช้าอาจเกิดผลเสียต่อราชการได้ ผู้มีอำนาจสามารถอนุญาตผู้ดูแลระบบเครือข่ายสื่อสาร ดำเนินการแก้ปัญหาก่อนได้ และผู้ดูแลระบบเครือข่ายสื่อสาร จะต้องจัดทำเอกสารการขออนุญาตดำเนินการเป็นลายลักษณ์อักษรในภายหลังโดยเร็ว ทั้งนี้ ต้องไม่เกินวันทำการถัดไป

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

๖.๒๗ ห้ามเปิดเผยหรือส่งมอบข้อมูลโครงสร้างระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชนให้แก่บุคคลใดที่ไม่เกี่ยวข้องก่อนได้รับการอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

๖.๒๘ ห้ามเปิดเผยข้อมูลที่ได้จากการตรวจสอบข้อมูลที่อยู่ระหว่างการรับส่งในระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชน ให้แก่บุคคลใดที่ไม่เกี่ยวข้องก่อนได้รับการอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

๖.๒๙ ต้องจัดให้มีระบบสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและต้องจัดทำแผนรองรับความเสี่ยง (Risk Plan) หรือแผนถอยกลับไปที่ระบบงานก่อนการเปลี่ยนแปลง (Fall Back Procedure) และทดสอบแผนงานดังกล่าวให้สามารถปฏิบัติได้จริง

๖.๓๐ การพัฒนาโปรแกรมที่มีการติดต่อสื่อสารระหว่างหน่วยงาน ให้แจ้งหมายเลข Port ที่ให้บริการในโปรแกรมนั้นๆ ต่อผู้ดูแลระบบเครือข่ายสื่อสารเพื่อพิจารณาความเหมาะสมในการเปิด Port ให้บริการก่อนนำโปรแกรมขึ้นใช้งาน

๗. การเข้าถึงการปฏิบัติงานบนเครือข่ายอินเทอร์เน็ต และเครือข่ายภายในกรม

๗.๑ 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) 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 หรือมีจำนวนมากให้บีบอัดหรือแบ่งแฟ้มข้อมูลให้มีขนาดเล็กลง

(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) ต้องดำเนินการให้เป็นไปตามมาตรฐานเว็บเพจที่กรมพินิจ และคุ้มครองเด็กและเยาวชนกำหนด

(๙) การใช้งานสังคมออนไลน์ (Social Network) ผ่านระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชนให้ปฏิบัติตามแนวปฏิบัติ ดังนี้

(๙.๑) อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

(๙.๒) ผู้ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัย รวมถึงพฤติกรรมที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์

(๙.๓) หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ ที่อ่าจมีผลกระทบกับหน่วยงานผู้ใช้งานต้องแจ้งศูนย์เทคโนโลยีสารสนเทศโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

(๙.๔) ห้ามใช้จดหมายอิเล็กทรอนิกส์ (e-Mail) ของกรมพินิจและคุ้มครองเด็กและเยาวชนในการสมัครใช้งานสังคมออนไลน์ (Social Network)

๘. การควบคุมการใช้งานระบบรับ-ส่งหนังสือ ข่าวสารทางอิเล็กทรอนิกส์ และระบบจดหมายอิเล็กทรอนิกส์ (e-mail)

๘.๑ 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 หรือหัวหน้าส่วนราชการหรือผู้รักษาราชการแทน 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) ระบบการจองห้องประชุม การจองห้องประชุมอาคารกรมพินิจและคุ้มครองเด็กและเยาวชน เพื่อการประชุมปกติ ผู้ที่มีสิทธิใช้งาน ได้แก่ ผู้ที่มีบัญชีผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์

(๗) ให้ผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์เปลี่ยนรหัสผ่านของตนเป็นประจำครั้งละไม่เกิน ๖๐ วัน หรือให้ทำการเปลี่ยนรหัสผ่านของตนทันทีหากพบว่ามีผู้ทราบรหัสผ่านดังกล่าว

(๘) ห้ามผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ เปิดเผยรหัสผ่านของตนเองให้ผู้อื่นทราบ

(๙) การเปลี่ยนบัญชีผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ส่วนบุคคลให้ผู้ใช้ส่วนบุคคลยื่นคำร้องขอเปลี่ยนที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (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

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

๘.๓ ผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ต้องรับผิดชอบต่อข่าวสารอิเล็กทรอนิกส์ที่มีอยู่ในความรับผิดชอบของตนเองในทุกกรณี

๘.๔ ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์เป็นทรัพย์สินของกรมพินิจและคุ้มครองเด็กและเยาวชนมีไว้เพื่อใช้ในการปฏิบัติราชการเท่านั้น ผู้ใช้ระบบงานจะต้องไม่กระทำการอย่างหนึ่งอย่างใด ต่อไปนี้

(๑) กระทำการก่อให้เกิดความเสียหายต่อกรมพินิจและคุ้มครองเด็กและเยาวชน หรือละเมิดสิทธิหรือก่อให้เกิดความเดือดร้อนรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และแสวงหาผลประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาประโยชน์ในเชิงธุรกิจจากการใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์

(๒) ส่งจดหมายลูกโซ่

(๓) ภาพลามกอนาจาร

(๔) ส่งข้อความหยาบคาย ดูหมิ่นผ่านระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์

(๕) ปลอมแปลงบัญชีผู้ใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์

(๖) ตัดต่อ เติม หรือดัดแปลงภาพของผู้อื่น ด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่จะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย หากตรวจพบจะดำเนินการยกเลิกการใช้งานของผู้นั้นทันที และดำเนินการตามกฎหมายที่เกี่ยวข้อง ทั้งนี้ผู้ดูแลระบบข่าวสารทางอิเล็กทรอนิกส์ขอสงวนสิทธิ ในการตรวจสอบ แก้ไขเปลี่ยนแปลงยกเลิกการใช้ระบบรับ-ส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์โดยไม่ต้องแจ้งให้ผู้ใช้ระบบงานทราบล่วงหน้า

๙. การบริหารจัดการการเข้าถึงข้อมูลตามลำดับชั้นความลับ (Management of Confidential Data Access)

๙.๑ การรักษาความปลอดภัยข้อมูล แบ่งออกเป็น ๒ ประเภท คือ

(๑) ข้อมูลลับที่สุด ข้อมูลลับมาก ข้อมูลลับ ได้แก่ ข้อมูลที่ถูกกำหนดชั้นความลับตามหลักเกณฑ์เกี่ยวกับการรักษาความปลอดภัยของบุคคลและเอกสารที่กรมพินิจและคุ้มครองเด็กและเยาวชนกำหนดหรือถือปฏิบัติอยู่ในเวลานั้น

(๒) ข้อมูลทั่วไป ได้แก่ ข้อมูลที่ไม่ถูกกำหนดชั้นความลับ

๙.๒ เพื่อประโยชน์ในการรักษาความปลอดภัยข้อมูล ให้ศูนย์เทคโนโลยีสารสนเทศดำเนินการดังต่อไปนี้

(๑) กำหนดวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน เพื่อป้องกันการลักลอบเข้าถึงข้อมูล

(๒) กำหนดวิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภท เพื่อป้องกันการลักลอบดูข้อมูลและแก้ไขข้อมูล

(๓) กำหนดวิธีปฏิบัติในการรับส่งข้อมูลแต่ละประเภท เพื่อป้องกันการลักลอบดูข้อมูลหรือสร้างความเสียหายให้กับข้อมูลในระหว่างการรับส่ง

(๔) กำหนดวิธีปฏิบัติในการทำลายข้อมูลแต่ละประเภท เมื่อข้อมูลหมดอายุการใช้งานหรือมีความจำเป็นต้องทำลาย เพื่อป้องกันการลักลอบดูข้อมูลที่ค้างในอุปกรณ์เฉพาะสำหรับจัดเก็บ

(๕) กำหนดวิธีปฏิบัติในการสำรองข้อมูลแต่ละประเภทให้เหมาะสมกับจำนวนครั้งในการเปลี่ยนแปลงข้อมูล เพื่อใช้กู้คืนในกรณีที่ข้อมูลได้รับความเสียหาย และให้เก็บสื่อที่ใช้สำรองข้อมูลในอุปกรณ์เฉพาะสำหรับจัดเก็บที่มีความปลอดภัย

๙.๓ เจ้าของข้อมูล ต้องทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๙.๔ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

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

๙.๖ ให้หน่วยงานในสังกัดกรมพินิจและคุ้มครองเด็กและเยาวชน มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน ต้องมีการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกข้อมูลก่อน เป็นต้น

๙.๗ วิธีปฏิบัติที่เกี่ยวข้องกับข้อมูลลับบนอุปกรณ์คอมพิวเตอร์ ให้ถือปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

(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) การทำลายข้อมูลลับให้เป็นไปตามคำสั่ง เรื่อง การรักษาความปลอดภัยเกี่ยวกับบุคคลและข้อมูลข่าวสารลับ โดยวิธีการทำลายข้อมูลลับให้ปฏิบัติตามวิธีปฏิบัติ ดังนี้

(๒.๒) การทำลายเอกสาร (Destruction) แบ่งตามชั้นความลับของเอกสาร ดังนี้

(๒.๒.๑) ลับที่สุด ให้ทำลายเอกสารโดยใช้เครื่องย่อยเอกสาร และเผาทำลายเศษเอกสาร ที่ได้จากการย่อย

(๒.๒.๒) ลับมาก ให้ทำลายเอกสารโดยใช้เครื่องย่อยเอกสาร และเผาทำลายเศษเอกสารที่ได้จากการย่อย

(๒.๒.๓) ลับ ให้ทำลายเอกสารโดยใช้เครื่องย่อยเอกสาร

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

(๒.๓.๑) ลับที่สุด ให้ลบข้อมูลโดยใช้โปรแกรมประยุกต์ประเภทที่ไม่สามารถกู้คืนข้อมูลได้(Secure Erase)

(๒.๓.๒) ลับมาก ให้ลบข้อมูลโดยใช้โปรแกรมประยุกต์ประเภทที่ไม่สามารถกู้คืนข้อมูลได้ (Secure Erase)

(๒.๓.๓) ลับ ให้ลบข้อมูลโดยใช้โปรแกรมประยุกต์ประเภทที่ไม่สามารถกู้คืนข้อมูลได้ (Secure Erase)

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

(๔) ในการสำรองข้อมูลลับ ให้ปฏิบัติ ดังนี้

- สำรองข้อมูลตามระยะเวลาหรือเมื่อได้รับแจ้งจากเจ้าของข้อมูลว่าข้อมูลมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
- จัดเก็บสื่อที่ใช้สำรองข้อมูล ในอุปกรณ์เฉพาะสำหรับเก็บรักษาที่ปิดล็อคได้
- ตรวจสอบความครบถ้วนของข้อมูลที่สำรองทุกครั้ง

๙.๘ การควบคุมการเข้าถึงข้อมูลทั่วไป ให้หน่วยงานในสังกัดกรมพินิจและคุ้มครองเด็กและเยาวชนกำหนดให้เจ้าของข้อมูล หรือผู้ได้รับมอบหมายทำหน้าที่บริหารความปลอดภัยของข้อมูลดังนี้

(๑) เจ้าของไฟล์ข้อมูลสามารถอ่านและเขียนไฟล์ข้อมูล และบุคคลทั่วไปสามารถอ่านไฟล์ข้อมูลได้เท่านั้น

(๒) กรณีข้อมูลที่จัดเก็บข้อมูลในฐานข้อมูล ควรกำหนดให้ผู้ใช้งานสามารถเข้าถึงข้อมูลในฐานข้อมูลผ่านระบบงานเท่านั้น ไม่ควรเข้าถึงข้อมูลในฐานข้อมูลโดยตรง

(๓) วิธีการทำลายข้อมูลทั่วไป ควรปฏิบัติตาม ข้อ ๙.๗

(๔) การสำรองข้อมูลทั่วไป ให้หน่วยงานในสังกัดกรมพินิจและคุ้มครองเด็กและเยาวชน เจ้าของข้อมูล หรือหน่วยงานอื่นที่ได้รับมอบหมายจากเจ้าของข้อมูลให้ทำหน้าที่บริหารความปลอดภัยของข้อมูล ให้ปฏิบัติดังนี้

- สำรองข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อยหรือเมื่อได้รับแจ้งจากเจ้าของข้อมูลว่ามีการเปลี่ยนแปลงจากเดิมอย่างเป็นนัยสำคัญ
- ควรจัดเก็บสื่อที่ใช้สำรองข้อมูลตามความเหมาะสมของหน่วยงาน
- ควรตรวจสอบความครบถ้วนของข้อมูลที่สำรองทุกครั้ง

๑๐. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๑๐.๑ การบริหารจัดการเครื่องคอมพิวเตอร์อุปกรณ์คอมพิวเตอร์ อุปกรณ์ด้านระบบรักษาความปลอดภัยและอุปกรณ์ด้านระบบเครือข่ายสื่อสาร

๑๐.๑.๑ การลงทะเบียนควบคุมดูแลเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์

(๑) ให้ฝ่ายบริหารงานทั่วไป/งานธุรการ ของแต่ละหน่วยงาน ดำเนินการ ดังนี้

(๑.๑) ให้ตรวจสอบหมายเลขเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์กับเอกสารใบส่งของให้ถูกต้อง ไม่ว่าจะได้รับการจัดสรร จัดซื้อจัดหาเอง หรือได้รับบริจาค

(๑.๒) ให้บันทึก/ปรับปรุงข้อมูลเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ลงในระบบจัดเก็บข้อมูลที่กรมพินิจและคุ้มครองเด็กและเยาวชนกำหนด ได้แก่ ระบบรายงานครุภัณฑ์คอมพิวเตอร์ในแต่ละกรณี ดังนี้

(๑.๒.๑) ได้รับเครื่องคอมพิวเตอร์ และ/หรือ อุปกรณ์คอมพิวเตอร์จากการจัดสรรใหม่จากการบริจาค หรือการจัดซื้อจัดหาเอง

(๑.๒.๒) การปรับปรุง หรือการเพิ่มประสิทธิภาพเครื่องคอมพิวเตอร์และ/หรืออุปกรณ์คอมพิวเตอร์ เช่น เพิ่มขนาดหน่วยความจำ (Ram) เปลี่ยนขนาดฮาร์ดดิสก์ เป็นต้น

(๑.๒.๓) การโยกย้าย สับเปลี่ยน หรือการจำหน่ายเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์

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

(๓) การนำอุปกรณ์คอมพิวเตอร์เข้าหรือออกนอกหน่วยงานของกรมพินิจและคุ้มครองเด็กและเยาวชน จะต้องได้รับอนุมัติจากหัวหน้าหน่วยงานหรือผู้ได้รับมอบหมาย และผู้ใช้งานต้องรับผิดชอบต่อความปลอดภัยของอุปกรณ์คอมพิวเตอร์ และความปลอดภัยของข้อมูลที่อยู่ภายในเครื่องคอมพิวเตอร์นั้น

(๔) ห้ามถอดและ/หรือประกอบชิ้นส่วนใดๆ ของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ เว้นแต่จะได้รับอนุมัติจากหัวหน้าหน่วยงานหรือผู้ได้รับมอบหมาย และให้ดำเนินการตามข้อ (๑.๒)

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

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

๑๐.๑.๒ การบำรุงดูแลรักษาเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์

(๑) ให้ศูนย์เทคโนโลยีสารสนเทศ ตรวจสอบดูแลและควบคุมสัญญาการบำรุงรักษาระบบคอมพิวเตอร์ ตลอดทั้งอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องกับระบบคอมพิวเตอร์ทุกชนิดให้เป็นไปตามสัญญา เช่น การจัดทำโครงการจัดจ้าง บำรุงรักษาซ่อมแซมแก้ไข และแจ้งให้หน่วยงานที่เกี่ยวข้องทุกแห่งทราบกำหนดเวลาการบำรุงรักษาซ่อมแซม แก้ไขตามสัญญาที่กรมพินิจและคุ้มครองเด็กและเยาวชนทำไว้กับผู้รับจ้าง

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

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

๑๐.๒ การปฏิบัติงานภายในห้องเครื่องคอมพิวเตอร์แม่ข่าย

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

๑๐.๒.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิในการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานและสอดคล้องกับหน้าที่ความรับผิดชอบ รวมทั้งให้มีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๑๐.๒.๓ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น (Administrator) ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลสารสนเทศได้

๑๐.๒.๔ ผู้ดูแลระบบจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเครือข่ายกรมพินิจและคุ้มครองเด็กและเยาวชน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญอย่างสม่ำเสมอและต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบต่างๆ และการผ่านเข้าออก สถานที่ตั้งระบบเครือข่ายทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๑๑. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ให้ปฏิบัติดังต่อไปนี้

๑๑.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้อง แท้จริง ระบุตัวตนที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

๑๑.๒ ห้ามแก้ไขข้อมูลจราจรทางคอมพิวเตอร์ (Log)

๑๑.๓ หากต้องการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ (Log) ต้องได้รัยการอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO)

๑๑.๔ ให้ทำการเก็บรักษา Log File ของการประมวลผล โดยมีระยะเวลาในการเก็บรักษาข้อมูลไว้ไม่น้อยกว่า ๙๐ วันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

๑๑.๕ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๑๑.๖ เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลระบบเก็บข้อมูลจราจร (Log) ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้นและค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

๑๒. การบริหารระบบรักษาความปลอดภัยไฟร์วอลล์ (Firewall)

เพื่อควบคุมการสื่อสารระหว่างเครือข่ายภายในกรมฯ กับเครือข่ายภายนอกกรมฯ โดยการตั้งค่าของไฟร์วอลล์ และอุปกรณ์ที่อนุญาตให้เชื่อมโยงภายในกรมให้มีประสิทธิภาพในการทำงานรวมทั้งต้องทบทวนสิทธิของผู้ใช้งานอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบไฟร์วอลล์

แนวปฏิบัติ

(๑) ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการระบบรักษาความปลอดภัยไฟร์วอลล์ทั้งหมด

(๒) ผู้ดูแลระบบต้องกำหนดนโยบาย (Policy) การใช้งานไฟร์วอลล์

(๓) ผู้ดูแลระบบต้องกำหนดค่า (Configuration) หรือกำหนดนโยบาย (Policy) เพื่อกลั่นกรองข้อมูลและระบบความปลอดภัยของระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ของกรมฯ การป้องกันการบุกรุกไวรัส รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์

(๔) ผู้ดูแลระบบต้องกำหนดขั้นตอนหรือวิธีการปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอ์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะผิดปกติต้องดำเนินการแก้ไขและรายงานผู้บังคับบัญชาโดยทันที่

(๕) ผู้ดูแลระบบต้องเปิดใช้งานไฟร์วอลล์ตลอดเวลา

(๖) การเปิดใช้บริการ Service ต้องรับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ผู้ดูแลระบบต้องกำหนดมาตรการป้องกันเพิ่มเติม

(๗) ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ ค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาตต้องบันทึกการเปลี่ยนแปลงทุกครั้ง

(๘) การเข้าถึงกระบวนการไฟร์วอลล์ต้องเข้าได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

(๙) ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้า – ออกอุปกรณ์ไฟร์วอลล์ ต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ และต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๖๐ วัน

(๑๐) การกำหนดค่าการบริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่ใช้งานเท่านั้น

(๑๑) ต้องสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ และทุกครั้งที่มีการเปลี่ยนแปลงค่า

(๑๒) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ ต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยกำหนดเป็นกรณีไป

(๑๓) ผู้ดูแลระบบมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

(๑๔) การเชื่อมต่อในลักษณะของการ Remote login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน ต้องทำการผ่าน VPN เท่านั้น

(๑๕) ผู้ละเมิดนโยบายความปลอดภัยของไฟร์วอลล์ ต้องถูกระงับการใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ทันที

(๑๖) ผู้ขอใช้งานต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศโดยระบบข้อมูล ดังนี้

- หมายเลข Port ที่ต้องการเปิด
- หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร
- วัตถุประสงค์หรือ Application ที่ต้องการใช้งานผ่าน Port นั้นๆ
- วันที่เริ่มใช้และวันที่สิ้นสุดการใช้งาน

(๑๗) ในการขอใช้งาน หากพบว่าขัดต่อนโยบาย ประกาศ ระเบียบของกรมหรือกฎหมาย หรืออาจเกิดช่องโหว่ด้านความปลอดภัยของระบบสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศจะไม่อนุญาตให้ใช้งาน

(๑๘) ภายหลังการอนุญาตให้ใช้งานพบว่ามีการใช้งานขัดต่อนโยบาย ประกาศ ระเบียบของกรมฯ หรือกฎหมาย หรืออาจเกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศต้องยกเลิกการให้บริการทันที

๑๓. การรับส่งข้อมูลสารสนเทศ (Information Transfer)

เพื่อจัดทำข้อตกลงในการรับส่งข้อมูลสารสนเทศและซอฟต์แวร์ระหว่างกรมกับหน่วยงานภายนอกอย่างเป็นลายลักษณ์อักษร เพื่อสร้างความมั่นคงปลอดภัยการรับส่งข้อมูลสารสนเทศ

แนวปฏิบัติ

(๑) ในการรับส่งข้อมูลสารสนเทศและซอฟต์แวร์ของกรมกับหน่วยงานภายนอกต้องได้รับการอนุมัติจาก DCIO

(๒) DCIO ต้องจัดให้มีการทำข้อตกลงหรือสัญญากับหน่วยงานภายนอกหรือมีหนังสือการขอความอนุเคราะห์ข้อมูล (หากเป็นข้อมูลส่วนบุคคลต้องมีการระบุให้มีการดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลด้วย) โดยต้องพิจารณาข้อกำหนดหรือเงื่อนไขอย่างเหมาะสมอย่างน้อยดังต่อไปนี้

- การรักษาความลับของสารสนเทศและซอฟต์แวร์
- ข้อตกลงในการฝากข้อมูลหรือ Source Code ไว้ที่หน่วยงานภายนอกซึ่งไม่ใช่คู่สัญญาเพื่อให้หน่วยงานงานสามารถเข้าถึงข้อมูลดังกล่าวได้ในกรณีที่หน่วยงานคู่สัญญาหรือหน่วยงานที่ได้รับการว่าจ้างให้พัฒนาซอฟต์แวร์ไม่สามารถให้บริการได้ (Escrow Agreement)
- หน้าที่ความรับผิดชอบของหน่วยงาน และคู่สัญญาในการควบคุมสารสนเทศและซอฟต์แวร์ระหว่างการส่งผ่าน (Transmission) การกระจายต่อ (Dispatch) และการได้รับ (Receipt) สารสนเทศ
- ความรับผิดชอบ และการใช้เมื่อสารสนเทศสูญหาย ถูกแก้ไข หรือถูกเปิดเผยโดยมิชอบ
- กรรมสิทธิ์ การป้องกันสิทธิและทรัพย์สินทางปัญญาของสารสนเทศและซอฟต์แวร์
- กำหนดข้อตกลงร่วมกันในการจัดทำป้ายชื่อ ตามระดับความมั่นคงปลอดภัยของสารสนเทศ เพื่อให้มีความเข้าใจตรงกันและสามารถดำเนินการป้องกันได้อย่างเหมาะสม
- มาตรฐานทางเทคนิคอื่นๆ สำหรับรูปแบบของข้อมูล การจัดเก็บ การประมวลผล และการส่งสารสนเทศที่มีการรับส่งข้อมูล
- ขั้นตอนปฏิบัติงานสำหรับการรับส่งข้อมูลสารสนเทศ
- กระบวนการติดตาม (Traceability) และป้องกันการปฏิเสธความรับผิด (Non-Repudiation)
- ใช้โปรโตคอลในการถ่ายโอนข้อมูลที่มีความมั่นคงปลอดภัย หรือใช้ VPN เวอร์ชันล่าสุด

(๓) ผู้รับผิดชอบกระบวนการ

- DCIO
- ผู้ดูแลระบบ

๑๔. การปฏิบัติงานจากภายนอกสำนักงาน

๑๔.๑ ผู้ใช้งานต้องขออนุญาตจากผู้มีอำนาจหรือผู้ที่ได้รับมอบหมายเพื่อขอสิทธิการใช้งานสำหรับการปฏิบัติงานจากภายนอกสำนักงาน

๑๔.๒ ผู้ใช้งานต้องไม่นำสิทธิที่ได้ไปให้บุคคลอื่นใช้งาน

๑๔.๓ ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์จากการปฏิบัติงานจากภายนอกสำนักงาน

๑๔.๔ การปฏิบัติงานจากภายนอกสำนักงาน ให้คำนึงถึงความมั่นคงปลอดภัยด้านสารสนเทศ

๑๔.๕ ศูนย์เทคโนโลยีสารสนเทศไม่อนุญาตให้คอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ที่กำลังปฏิบัติงานจากภายนอกสำนักงานเข้าเชื่อมต่อระบบเครือข่ายสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชน หากมีเหตุอันน่าสงสัยว่าคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์นั้นไม่ปลอดภัยต่อระบบคอมพิวเตอร์กรมพินิจและคุ้มครองเด็กและเยาวชน

๑๔.๖ ผู้ใช้งานต้องใช้ระบบเครือข่ายภายในกรม (Intranet) และระบบงานเพื่อการปฏิบัติงานของราชการเท่านั้น

๑๕. การควบคุมผู้ให้บริการภายนอกที่กรมพินิจและคุ้มครองเด็กและเยาวชนทำสัญญาว่าจ้าง (Outsource)

๑๕.๑ ผู้ให้บริการภายนอกที่กรมพินิจและคุ้มครองเด็กและเยาวชนทำสัญญาว่าจ้าง (Outsource) ที่เข้ามาดำเนินกิจกรรมภายในกรมพินิจและคุ้มครองเด็กและเยาวชนในงานด้านความมั่นคงปลอดภัยสารสนเทศในสัญญาจ้างจะต้องมีตกลงการไม่เปิดเผยความลับ (Non-Disclosure Agreement) หรือข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ (Security in Third Party Agreements) หรือจะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรก่อน จึงจะสามารถเข้ามาปฏิบัติงานในกรมพินิจและคุ้มครองเด็กและเยาวชนได้

๑๕.๒ มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่กรมพินิจและคุ้มครองเด็กและเยาวชน ปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ ระดับการให้บริการ ลิขสิทธิ์และกฎหมายที่เกี่ยวข้อง เช่น กฎหมายลิขสิทธิ์และทรัพย์สินทางปัญญา เป็นต้น

๑๕.๓ มีการติดตามตรวจสอบรายงาน หรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอ

๑๕.๔ เมื่อสิ้นสุดการจ้างงาน หรือเปลี่ยนลักษณะการจ้างงาน ผู้ให้บริการภายนอกที่กรมพินิจและคุ้มครองเด็กและเยาวชนทำสัญญาจ้าง (Outsource) ต้องคืนทรัพย์สินของกรมพินิจและคุ้มครองเด็กและเยาวชนที่อยู่ในความครอบครองของตน

๑๕.๕ ต้องทำการถอดถอนสิทธิในการเข้าถึงระบบสารสนเทศและทรัพย์สินของเจ้าหน้าที่ที่กรมพินิจและคุ้มครองเด็กและเยาวชนสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน

๑๖. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

แนวปฏิบัติ

(๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นทรัพย์สินของหน่วยงาน และอนุญาตให้ใช้งาน และผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพและด้วยความระมัดระวัง

(๒) โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย ห้ามคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งที่เครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

(๔) การเคลื่อนย้ายคอมพิวเตอร์ส่วนบุคคลไปติดตั้ง ณ สถานที่อื่นใดภายในกรมต้องดำเนินการโดยเจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมายหรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับกรม

(๕) ในการส่งซ่อมเครื่องคอมพิวเตอร์ส่วนบุคคล ต้องได้รับความเห็นชอบจากและได้รับอนุญาตจากหัวหน้าหน่วยงานก่อน

(๖) ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

(๗) ผู้ใช้งานต้องตรวจสอบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ และทำการตรวจสอบจัดเรียงข้อมูลภายในฮาร์ดดิสก์ (Defragment) ของเครื่องคอมพิวเตอร์เป็นประจำ เพื่อเพิ่มประสิทธิภาพในการทำงาน

(๘) ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสก่อนการใช้งานสื่อบันทึกข้อมูลชนิดพกพาต่างๆ

(๙) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลทุกครั้งเมื่อใช้งานประจำวันเสร็จสิ้น

(๑๐) ผู้ใช้งานต้องตั้งค่าหน้าจอให้มีการล็อกหน้าจอเมื่อไม่มีการใช้งาน และตั้งค่ารหัสผ่านให้เครื่องคอมพิวเตอร์ก่อนการเข้าใช้งาน

๑๗. การใช้งานเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารชนิดพกพา (Mobile Device)

แนวปฏิบัติ

(๑) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นทรัพย์สินของหน่วยงาน และอนุญาตให้ใช้งาน และผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพและด้วยความระมัดระวัง

(๒) โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์พกพาต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย ห้ามคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งที่เครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(๔) ไม่ดัดแปลงและแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์แบบพกพาและรักษาสภาพให้มีสภาพเดิม

(๕) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

(๖) หลีกเลี่ยงการใช้ของแข็ง เช่น ปลายปากกากดสัมผัสหน้าจอให้เป็นลอยขีดข่วน หรือทำให้จอคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๗) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๘) การเช็คทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือ และเช็คไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีลอยขีดข่วนได้

(๙) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องเพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๑๐) การเคลื่อนย้ายเครื่องขณะที่เครื่องใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

(๑๑) ห้ามนำเครื่องคอมพิวเตอร์แบบพกพาส่วนตัวมาใช้กับระบบเครือข่ายของหน่วยงาน ยกเว้นได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งานหรือได้รับอนุญาตจากหัวน้าหน่วยงาน หากมีการตรวจสอบพบความเสียหายต่อหน่วยงาน ถือว่าเป็นความผิดหัวหน้าหน่วยงานและผู้ใช้งานจะต้องรับผิดชอบร่วมกัน รวมถึงการส่งข้อมูลผ่านทางผู้ให้บริการขนส่งที่น่าเชื่อถือ

(๑๒) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๑๓) ผู้ใช้งานไม่เก็บหรือใช้งานเครื่องคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน ความชื้น ฝุ่นละอองสูง และระวังป้องกันการตกกระทบ

(๑๔) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

(๑๕) ผู้ใช้งานต้องทำการออกจากระบบ (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๑๘. การตรวจจับการบุกรุก (Intrusion Detection System/Intrusion Prevention System: IDS/IPS)

แนวปฏิบัติ

(๑) หน่วยงานควรติดตั้ง ระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในหน่วยงาน ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่ายพร้อมกับบทบาทความรับผิดชอบที่เกี่ยวข้อง

(๒) หน่วยงานควรติดตั้ง IDS/IPS ให้ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของหน่วยงาน และระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ต

(๓) ระบบ IDS/IPS ต้องมีการตรวจสอบและ Update Patch เป็นประจำ

(๔) หน่วยงานมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบโดยไม่ต้องแจ้งผู้ใช้งานล่วงหน้า

๑๙. การเข้ารหัสข้อมูล มาตรการการเข้ารหัสข้อมูล

แนวปฏิบัติ

๑.๑ มาตรการการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)

(๑) การแปลงรูปแบบของข้อมูลที่รับเข้ามาไม่ว่าขนาดเท่าใดก็ตาม ให้อยู่ในอีกรูปแบบหนึ่งที่มีขนาดคงที่ และไม่สามารถถอดรหัสข้อมูลได้ (Decrypt) ทำได้เพียงตรวจสอบว่าข้อมูลที่ส่งแต่ละครั้งเหมือนกันหรือไม่ ความปลอดภัยจึงค่อนข้างสูง เช่น การเก็บรหัสผ่านผู้ใช้งานในฐานข้อมูล ได้แก่ การใช้ฟังก์ชั่น MD๕ หรือ SHA๑ เป็นต้น

(๒) อัลกอริทึมที่เรียกใช้ต้องรองรับซอฟต์แวร์ประยุกต์ที่นำไปใช้งานได้ เช่น PGP (Pretty Good Privacy), SSL (Secure Socket Layer), TLS (Tranport Layer Security) เป็นต้น

(๓) ความยาวของคีย์ (Key) ในการเข้ารหัสต้องไม่น้อยกว่า ๔๘ บิต (bit) สำหรับการเข้ารหัสแบบสมมาตร (Sysmetric) และแบบไม่สมมาตร (Asymmetric) ต้องมีความยาวไม่น้อยกว่าตามที่ตกลงกันไว้

(๔) เจ้าของข้อมูลต้องมีการทบทวนมาตรฐานคีย์ (Key) ที่เข้ารหัสทุกๆ ปี เพื่อให้สอดคล้องกับความปลอดภัยและประสิทธิภาพของเครื่องคอมพิวเตอร์ลูกข่าย

(๕) กรณีไม่ทราบหรือต้องการทราบข้อมูลเกี่ยวกับการเข้ารหัสเพิ่มเติมให้ติดต่อหน่วยงานที่รับผิดชอบ

๑.๒ การบริหารจัดการกุญแจ (Key Management)

(๑) ข้อมูลที่มีการเข้ารหัส (Encrypt) ต้องจัดให้มีกระบวนการในการบริหารจัดการกุญแจ (Key Management) ที่มีประสิทธิภาพโดยการดำเนินการ เช่น การสร้าง การจัดเก็บ การจัดส่งและการเปลี่ยน ควรกระทำอย่างปลอดภัยและมีการที่ควบคุมที่เหมาะสม

(๑.๑) กรณีที่กุญแจ (Key) มีการกำหนดวันหมดอายุ ดำเนินการดังนี้

๑) ผู้ใช้งานดำเนินการร้องขอมายังศูนย์เทคโนโลยีสารสนเทศ

๒) ผู้ดูแลระบบกำหนดกุญแจ (Key) ซึ่งเป็นการเข้ารหัสข้อมูลแบบมาตรฐานการเข้ารหัสลับขั้นสูง (Avanced Encyption Standard : AES) โดยกำหนดวันที่และระยะเวลาในการใช้กุญแจ (Key)

๓) กุญแจ (Key) จะถูกเปลี่ยนทุกครั้งที่ใช้งาน ไม่สามารถทำซ้ำได้

(๑.๒) กรณีที่กุญแจ (Key) ไม่กำหนดวันหมดอายุ ดำเนินการดังนี้

๑) ผู้ใช้งานดำเนินการร้องขอผ่านระบบอัตโนมัติเพียงครั้งเดียว

๒) ระบบอัตโนมัติกำหนดกุญแจ (Key) ให้กับผู้ร้องขอ โดยการแปลงรูปแบบของข้อมูลที่รับไม่ว่าขนาดใดก็ตาม ให้อยู่ในอีกรูปแบบหนึ่งที่มีขนาดคงที่ และไม่สามารถถอดรหัสข้อมูลได้ (Decrypt) เช่น การเก็บรหัสผู้ใช้งานในฐานข้อมูล ได้แก่ การใช้ฟังก์ชัน MD๕ หรือ SHA๑ เป็นต้น

๓) ผู้ใช้งานสามารถใช้งานได้ตลอดไม่มีวันหมดอายุ เนื่องจากมีผลต่อความสามารถในการพิมพ์รายงานบนระบบงาน

(๒) กุญแจส่วนตัว (Private key) ที่ใช้ในการเข้ารหัสข้อมูลต้องถูกจัดเก็บให้เป็นความลับและมั่นคงปลอดภัย

(๓) การส่งกุญแจ (Key) ถึงผู้รับ ต้องส่งผ่านในช่องทางที่มีความปลอดภัย

(๔) กุญแจ (Key) ต้องได้รับการเพิกถอนทันที เมื่อทราบว่ามีความเสี่ยงที่จะก่อนให้เกิดการล่วงละเมินทางด้านความมั่นคงปลอดภัย เช่น กุญแจส่วนตัว (Private key) รั่วไหลไปยังบุคคลอื่น เป็นต้น

(๕) การเพิกถอนการใช้งานกุญแจ (Key) ต้องแจ้งให้ผู้รับผิดชอบและผู้ใช้งานทราบ รวมถึงต้องแจ้งเหตุการเพิกถอน วันที่และเวลาที่กุญแจ (Key) ถูกเพิกถอน

(๖) การจัดเก็บกุญแจ (Archive) เมื่อไม่มีการใช้งานเป็นระยะเวลานาน ต้องมีวิธีการเก็บด้วยวิธีที่มีความปลอดภัยด้วยการเข้ารหัส (Encrypt)

(๗) การทำลายกุญแจ (Key) ต้องทำด้วยความระมัดระวัง โดยใช้วิธีการทำลายกุญแจอย่างปลอดภัยและถาวร (Secure Deletion) และตรวจสอบว่าจะไม่มีการนำกลับมาใช้งานซ้ำอีก

(๘) การกระทำใดๆ ที่เกี่ยวข้องกับกุญแจ (Key) ต้องมีการจัดเก็บข้อมูลการดำเนินการย้อนหลัง (Log) สม่ำเสมอ เพื่อให้สามารถตรวจสอบการทำงานได้ในภายหลัง

ส่วนที่ ๒
นโยบายระบบสารสนเทศและระบบสำรองสารสนเทศและข้อมูลส่วนบุคคล

วัตถุประสงค์

๑. เพื่อให้ผู้ใช้งานระบบสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน ได้รับทราบถึงข้อห้ามและข้อปฏิบัติที่จะส่งผลให้เกิดความมั่นคงปลอดภัยต่อระบบสารสนเทศ และเกิดการใช้งานตรงตามวัตถุประสงค์การใช้งานระบบสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน รวมทั้งไม่ละเมิดระเบียบ กฎหมาย หือทำให้เกิดความเสียหายในการปฏิบัติงาน

๒. เพื่อให้ระบบสารสนเทศของหน่วยงาน ให้บริการได้อย่างต่อเนื่อง

๓. เพื่อเป็นมาตรฐานแนวทางปฏิบัติ และความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานเป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO)

๒. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

๓. ผู้อำนวยศูนย์เทคโนโลยีสารสนเทศ

๔. ผู้ดูแลเทคโนโลยีสารสนเทศที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. ทบทวนและคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

๑.๑ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน และกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรองข้อมูล พร้อมกับซ้อมตามแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑.๒ 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

๒. จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในเหตุการณ์ที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยดำเนินการปรับปรุงแผนดังกล่าวให้สามารถใช้การได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ มีแนวทางปฏิบัติต่อไปนี้

๒.๑ กำหนดให้มีการจัดทำและทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีกาทางอิเล็กทรอนิกส์ (BCM)

๒.๒ ในกรณีที่ไม่สามารถดำเนินการโดยระบบสารเทศได้ในช่วงเวลาหนึ่ง หน่วยงานจะต้องจัดเตรียมกระบวนการทำงานในช่องทางอื่นทดแทน ดังนี้

(๑) ระบบงานที่เกี่ยวข้องกับประชาชนทั่วๆไป ตามภารกิจหน่วยงานเจ้าหน้าที่ผู้รับเรื่องจะต้องดำเนินการตามแบบฟอร์มที่กำหนดไปพลางก่อน โดยภายหลังจากที่ระบบสารสนเทศกลับมาใช้งานได้ดังเดิม เจ้าหน้าที่ผู้รับเรื่องดังกล่าว จะต้องดำเนินการบันทึกข้อมูลเข้าสู่ระบบสารสนเทศที่เกี่ยวข้องในทันที

(๒) ระบบงานสารบรรณอิเล็กทรอนิกส์ (ระบบงานที่ใช้จัดส่งเอกสารทางราชการ) เจ้าหน้าที่ที่เกี่ยวข้องกับงานสารบรรณ ประจำสำนัก/กอง/กลุ่มงาน จะต้องดำเนินการจดบันทึกลำดับเลขที่หนังสือล่าสุดที่เกี่ยวข้องกับหน่วยงานของตนเอง ได้แก่ เลขที่หนังสือภายใน และเลขที่หนังสือภายนอก ก่อนที่ผู้ดูแลระบบงานสารบรรณจะดำเนินการปิดระบบสารสนเทศ ทั้งนี้เพื่อให้สามารถดำเนินการออกหนังสือด้วยวิธีนับมือหรือใช้กระดาษไปพลางก่อนและเมื่อระบบงานสารบรรรณอิเล็กทรอนิกส์ สามารถกลับเข้าใช้งานได้ตามปกติ เจ้าหน้าที่งานสารบรรณดังกล่าว จะต้องดำเนินการบันทึกข้อมูลย้อนหลังโดยทันที

(๓) ระบบงานอื่นๆ ภายในหน่วยงาน ผู้รับผิดชอบหลังของระบบงานแต่ละระบบจะต้องรับผิดชอบในการดำเนินการบันทึกข้อมูลในภายหลังเมื่อระบบงานดังกล่าวกลับมาใช้งานได้ตามปกติ

(๔) มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. แต่งตั้งบุคลากรที่ได้กำหนดหน้าที่และความรับผิดชอบ

ในการดำเนินการตามแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีอิเล็กทรอนิกส์ ดังนี้

๓.๑ ระดับนโยบาย ได้แก่

(๑) ผู้บริหารสูงสุด (CEO)

(๒) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO)

(๓) ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO)

(๔) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

(๕) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

<u>รับผิดชอบ</u> ในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนกำกับ ติดตาม ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

๓.๒ ระดับอำนวยการ ได้แก่ ผู่อำนวยการศูนย์เทคโนโลยีสารสนเทศ

<u>รับผิดชอบ</u>

- เป็นผู้บังคับบัญชาสูงสุดในการควบคุมและปฏิบัติการฉุกเฉินระบบสารสนเทศ
- มีอำนาจสั่งการให้ทุกหน่วยหยุดหรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ กรมพินิจและคุ้มครองเด็กและเยาวชน
- กำหนดจุดปลอดภัยสำหรับบุคคล และวัสดุอุปกรณ์ต่างๆ ในสถานที่ที่เหมาะสม
- ประชุมหารือกับผู้จัดการฐานข้อมูล
- ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผน ตามความเหมาะสม
- รายงานข้อมูลและผลการปฏิบัติงานให้ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Department Chief Information Office : DCIO) ทราบ

๓.๓ ระดับประสานงานเหตุฉุกเฉิน ได้แก่ หัวหน้าฝ่ายเทคโนโลยีเครือข่ายและคอมพิวเตอร์

<u>รับผิดชอบ</u>

- วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ
- มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้น จนกว่าผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ จะมาถึงที่เกิดเหตุ
- มีอำนาจสั่งการแทนผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ในกรณีที่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศไม่สามารถสั่งการได้
- สั่งการให้เจ้าหน้าที่ผู้เกี่ยวข้องมาปฏิบัติการตามแผนฯ
- พิจารณาขั้นตอนและวิธีการป้องกันชีวิต ทรัพย์สิน ให้เสียหายน้อยที่สุด
- กำหนดอัตรากำลังพล วัสดุอุปรกรณ์ และเครื่องมือจำเป็นต้องขอเพิ่มเติมในอนาคต

๓.๔ ระดับบหัวหน้าสั่งการ ได้แก่

(๑) หัวหน้าฝ่ายเทคโนโลยีเครือข่ายและคอมพิวเตอร์

(๒) หัวหน้าฝ่ายบริหารฐานข้อมูลสารสนเทศ

<u>รับผิดชอบ</u>

- กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษา ทบทวน วางแผนติดตาม การบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ
- แจ้งเหตุฉุกเฉิน และเคลื่อนย้ายตนเอง ผู้อื่น ตลอดจนทรัพย์สินออกจากที่เกิดเหตุไปเก็บรักษา ณ จุดปลอดภัยโดยเร็ว
- ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และเจ้าหน้าที่ประสานงานรักษาความปลอดภัยทราบ
- นำทรัยพ์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพ และรายงานเสนอผู้บังคับบัญชาตามลำดับชั้น

๓.๕ ระดับทีมที่เกี่ยวข้องกับแผน

(๑) ทีมรับผิดชอบดูแลบำรุงรักษาข้อมูลสารสนเทศ คือ พนักงานราชการ ลูกจ้าง และบริษัทคู่สัญญาตามโครงการฯ ที่ได้รับมอบหมาย มีหน้าที่เฝ้าระวังและตรวจสอบบำรุงรักษา แก้ไขข้อบกพร่องต่างๆ ของข้อมูลพื้นฐาน รวมทั้งการทำสำเนาและกู้คืนข้อมูลพื้นฐาน โดยมี หัวหน้าฝ่ายบริหารฐานข้อมูลสารสนเทศรับผิดชอบกำกับดูแล

(๒) ทีมรับผิดชอบดูแลระบบโปรแกรมสารสนเทศ คือ พนักงานราชการ ลูกจ้าง และบริษัทคู่สัญญาตามโครงการฯมอบหมาย มีหน้าที่เฝ้าระวังและตรวจสอบบำรุงรักษา แก้ไขข้อบกพร่องต่างๆ ของระบบโปรแกรมสารสนเทศ รวมทั้งทำสำเนาและกู้คืนฐายข้อมูลสารสนเทศ โดยมี หัวหน้าฝ่ายบริหารฐานข้อมูลสารสนเทศ รับผิดชอบกำกับดูแล

(๓) ทีมรับผิดชอบดูแลระบบเทคโนโลยีคอมพิวเตอร์ คือ พนักงานราชการ ลูกจ้าง และบริษัทคู่สัญญาตามโครงการฯ ที่ได้รับมอบหมาย มีหน้าที่เฝ้าระวังและตรวจสอบ บำรุงรักษา แก้ไขข้อบกพร่องต่างๆ ของระบบเทคโนโลยีคอมพิวเตอร์ รวมทั้งดำเนินตามแผนรองรับสถานการณ์ฉุกเฉิน โดยมี หัวหน้าฝ่ายเทคโนโลยีเครือข่ายและคอมพิวเตอร์ รับผิดชอบกำกับดูแล

(๔) ทีมรับผิดชอบดูแลระบบเครือข่าย คือ พนักงานราชการ ลูกจ้าง และบริษัทคู่สัญญาตามโครงการฯ ที่ได้รับมอบหมาย มีหน้าที่เฝ้าระวังและตรวจสอบ บำรุงรักษา แก้ไขข้อบกพร่องต่างๆ ของระบบเครือข่าย รวมทั้งการทำสำเนาและกู้คืนฐานข้อมูลบนระบบคอมพิวเตอร์แม่ข่าย โดยมี หัวหน้าฝ่ายเทคโนโลยีเครือข่ายและคอมพิวเตอร์ รับผิดชอบกำกับดูแล

๔. มีการทดสอบและทบทวนสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองข้อมูล และแผนเตรียมความพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓

นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (IT Risk Management) และข้อมูลส่วนบุคคล

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO)

๒. ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO)

๓. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

๔. คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)

๕. ผู้อำนวยศูนย์เทคโนโลยีสารสนเทศ

๖. ผู้ดูแลเทคโนโลยีสารสนเทศที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้เชี่ยวชาญจากโครงการบำรุงรักษาระบบคอมพิวเตอร์แม่ข่ายและระบบงานสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงาน ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒. แนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้

๒.๑ ทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๒.๒ ทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสเนทศ อย่างน้อยปีละ ๑ ครั้ง

๒.๓ ตรวจสอบและประเมินความเสี่ยงความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อการธำรงไว้ซึ่งความลับ (Condidentiality) ความถูกต้อง (Integrity) ความพร้อมใช้ (Availability) และให้จัดทำรายงานพร้อมข้อเสนอแนะต่อผู้บริหาร อย่างน้อยปีละ ๑ ครั้ง

๒.๔ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) กำหนดให้ระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๔) เฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Log) แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ จัดเก็บข้อมูลตามข้อ ๑๑

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

๓. ข้อกำหนดการแจ้งเหตุด้านความมั่นคงปลอดภัย ให้ปฏิบัติดังนี้

๓.๑ การกระทำที่ขัดต่อกฎหมายว่าด้วยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓.๒ การกระทำที่ขัดต่อความมั่นคงของชาติ

๓.๓ การใช้ทรัพยากรสารสเทศของหน่วยงานไม่เหมาะสม ผิดวัตถุประสงค์

๓.๔ หน้าเว็บไซต์หลัก หรือระบบงานของหน่วยงานถูกเปลี่ยนแปลงโดยผู้ไม่ประสงค์ดี

๓.๕ ข้อมูลเว็บไซต์หลัก หรือระบบงานของหน่วยงานไม่ถูกต้อง หรือคลาดเคลื่อนจากความเป็นจริง

๓.๖ ข้อมูลสารสนเทศสำคัญของหน่วยงานหรือส่วนตัวถูกเปิดเผย เปลี่ยนแปลง ลบ หรือสูญหาย โดยไม่ได้รับอนุญาต

๓.๗ มีการนำข้อมูลสารสนเทศสำคัญของหน่วยงานไปใช้ผิดวัตถุประสงค์

๓.๘ ทรัพยากรสารสนเทศถูกขโมย

๓.๙ มีบุคคลภายนอกเข้าใช้งานระบบสารสนเทศของหน่วยงานโดยไม่ได้รับอนุญาต

๓.๑๐ มีการแอบติดตั้งอุปกรณ์ หรือโปรแกรมเพื่อดักขโมยข้อมูล หรือดักฟัง ดักดูข้อมูลในระบบเครือข่ายของหน่วยงาน

๓.๑๑ การใช้อำนาจของสิทธิการเป็นผู้ดูแลระบบอย่างไม่เหมาะสม

๓.๑๒ มีการบุกรุกระบบฐานข้อมูลสารสนเทศ และเครือข่ายคอมพิวเตอร์

๓.๑๓ มีการบุกรุกหรือการใช้โปรแกรมของผู้ไม่ประสงค์ดี

๓.๑๔ เหตุการณ์อื่นๆ ที่เป็นการละเมิดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

ส่วนที่ ๔

นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์และข้อมูลส่วนบุคคล

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของกรมพินิจและคุ้มครองเด็กและเยาวชน

๒. เพื่อเป็นการป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน

๓. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO)

๒. ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO)

๓. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

๔. คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)

๕. ผู้อำนวยศูนย์เทคโนโลยีสารสนเทศ

๖. ผู้ดูแลเทคโนโลยีสารสนเทศที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. จัดฝึกอบรมการใช้งานระบบสารสนเทศและข้อมูลส่วนบุคคลของหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๒. จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน

๓. จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

๔. ประชาสัมพันธ์ เผยแพร่แนวนโยบายและแนวปฏิบัติ เกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness)

ส่วนที่ ๕
การทบทวนหลังการปฏิบัติงาน (After Action Review : AAR)

วัตถุประสงค์

เพื่อเป็นเครื่องมือที่นำมาใช้ในกระบวนการทำงาน ทบทวนวิธีการทำงานทั้งด้านความสำเร็จและปัญหาที่เกิดขึ้น ทั้งนี้ไม่ใช่การค้นหาคนที่ทำผิดพลาดไม่ใช่การกล่าวโทษ แต่เป็นการทบทวนเพื่อร่วมกันสะท้อน และทบทวนกระบวนการต่าง ๆ นำบทเรียนที่ได้จากความสำเร็จและปัญหาที่เกิดขึ้น มาจัดทำและพัฒนากระบวนการทำงานให้มีประสิทธิภาพและประสิทธิผลมากขึ้น โดยมีการแลกเปลี่ยนประสบการณ์การทำงาน

ผู้รับผิดชอบ

๑. ผู้อำนวยศูนย์เทคโนโลยีสารสนเทศ

๒. ผู้ดูแลเทคโนโลยีสารสนเทศที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. เตรียมจัดประชุม AAR ทันทีหลังจบงานนั้นๆ

๒. กระตุ้นและตั้งคำถาม

๓. สมาชิกร่วมกันตอบคำถาม

๔. วิเคราะห์และสรุปผล AAR

๕. จัดทำแบบบันทึกการทบทวนหลังการปฏิบัติงาน (AAR) โดยมีรายละเอียดในการบันทึกดังนี้

(๕.๑) หน่วยงาน หมายถึง ชื่อหน่วยงานที่ดำเนินการทบทวนหลังการปฏิบัติงาน

(๕.๒) เรียน หมายถึง ผู้บังคับบัญชาของหน่วยงาน

(๕.๓) ชื่องาน หมายถึง ชื่อกิจกรรมที่ดำเนินการทบทวนหลังการปฏิบัติงาน

(๕.๔) AAR ครั้งที่..... หมายถึง การดำเนินการสรุปผลการทบทวนหลังการปฏิบัติงาน ครั้งที่.....

(๕.๕) วัน/เวลาที่เริ่มปฏิบัติงาน หมายถึง ระยะเวลาเริ่มต้นการปฏิบัติงาน

(๕.๖) วัน/เวลาสิ้นสุดการปฏิบัติงาน หมายถึง ระยะเวลาสิ้นสุดการปฏิบัติงาน

(๕.๗) วันที่ทำ AAR หมายถึง วันที่ดำเนินการทบทวนหลังการปฏิบัติงาน

(๕.๘) เวลาเริ่ม-สิ้นสุด หมายถึง เวลาที่เริ่มดำเนินการทบทวนหลังการปฏิบัติงานจนถึงสิ้นสุดในแต่ละครั้ง

(๕.๙) ผู้ร่วม AAR หมายถึง ผู้ร่วมกิจกรรมการทบทวนหลังการปฏิบัติงาน

(๕.๑๐) เป้าหมายของงาน หมายถึง การตั้งเป้าหมายในการดำเนินงานในแต่ละงาน/โครงการ

(๕.๑๑) ผลการปฏิบัติ/ผลลัพธ์ที่เกิดขึ้นจริง หมายถึง การรายงานสภาพผลที่เกิดขึ้นจากการดำเนินงานทั้งจุดเด่นของงาน ผลที่ได้รับ และด้านที่เป็นปัญหาอุปสรรค

(๕.๑๒) งาน/กิจกรรม/ขั้นตอนที่ทำได้ดี หมายถึง การรายงานการปฏิบัติงาน/กิจกรรม/ขั้นตอนที่ผู้ปฏิบัติงานประสบความสำเร็จ มีผลงานเป็นที่ประจักษ์

(๕.๑๓) งาน/กิจกรรม/ขั้นตอนที่ทำได้ไม่ดี หมายถึง การรายงานการปฏิบัติงาน/กิจกรรม/ขั้นตอนที่ผู้ปฏิบัติงานไม่ประสบความสำเร็จ/เกิดปัญหา อุปสรรค ไม่เกิดผลงานเป็นที่ประจักษ์

(๕.๑๔) อุปสรรค/ข้อจำกัด/ข้อขัดข้อง หมายถึง ในระหว่างการปฏิบัติงาน มีปัญหา ข้อจำกัดที่เกิดขึ้น หรือไม่ได้รับความร่วมมือในระหว่างที่ปฏิบัติงาน ทำให้ผลการดำเนินงาน ไม่ประสบความสำเร็จ หรือทำให้ผลการดำเนินงานไม่ต่อเนื่อง

(๕.๑๕) ประเด็นที่ได้เรียนรู้ หมายถึง การสรุปประเด็นที่ผู้ปฏิบัติงานได้รับความรู้ ได้รับประสบการณ์ในการเรียนรู้จากการปฏิบัติงาน/จัดกิจกรรมที่ได้รับจากการปฏิบัติงาน

(๕.๑๖) ข้อปฏิบัติในการทำงานครั้งต่อไป หมายถึง การนำผลจากประเด็นที่ได้เรียนรู้มาพัฒนาต่อเนื่องและสามารถนำประเด็นที่เกิดปัญหามาพิจารณาร่วมกันกำหนดแนวทางในการพัฒนาหรือปรับปรุงงานใหม่ให้ดีขึ้น

ส่วนที่ ๖
นโยบายและแนวปฏิบัติด้านดารรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

วัตถุประสงค์

เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อการใช้บริการคลาวด์สาธารณะให้กับกรมพินิจและคุ้มครองเด็กและเยาวชน

ผู้รับผิดชอบ

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO)
๒. ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO)
๓. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
๔. คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)
๕. ผู้อำนวยศูนย์เทคโนโลยีสารสนเทศ
๖. ผู้ดูแลเทคโนโลยีสารสนเทศที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. ข้อกำหนดขั้นต่ำและการตรวจรับรองสำหรับผู้ใช้ริการคลาวด์และผู้ให้บริการคลาวด์

ตารางข้อกำหนดขั้นต่ำและการตรวจรับรองสำหรับผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์

ประเภทของข้อมูลหรือ ระบบสารสนเทศ	การตรวจรับรอง สำหรับผู้ใช้บริการคลาวด์	การตรวจรับรองสำหรับ ผู้ให้บริการคลาวด์
ผลกระทบระดับต่ำ	ประเมินตนเอง (Self - assessment) พร้อมแนบหลักฐานและขออนุมัติไปยังผู้บริหารสูงสุดของหน่วยงานโดยเก็บรักษาไว้ที่หน่วยงานและส่งสำนักงานด้วย	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC ๒๗๐๐๑ Certification และ CSA STAR Lavel ๑/CCM Lite เป็นอย่างน้อย
ผลกระทบระดับกลาง	ได้รับการรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation) หรือ ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจจำรวจในปีที่ ๒ และ ๓	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสำรวจ

ประเภทของข้อมูลหรือ ระบบสารสนเทศ	การตรวจรับรอง สำหรับผู้ใช้บริการคลาวด์	การตรวจรับรองสำหรับ ผู้ให้บริการคลาวด์
		ในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน CSA STAR Lavel ๒/CCM และ ISO/IEC ๒๗๐๐๑ Certification เป็นอย่างน้อย
ผลกระทบระดับสูง	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC ๒๗๐๐๑ Certification เป็นอย่างน้อย หรือ CSA STAR Lavel ๒/CCM และ ISO/IEC ๒๗๐๑๘ Certification และ ISO/IEC ๒๗๗๐๑ Certification เป็นอย่างน้อย

๒. แนวปฏิบัติการนำระบบงานไปติดตั้งบนคลาวด์ (Cloud Computing)

๒.๑ การวางแผนการนำระบบงานไปติดตั้งบนคลาวด์

(๑) คัดเลือกผู้ใช้บริการคลาวด์ที่มีความน่าเชื่อถือด้านความมั่นคงปลอดภัย

(๒) การจัดการส่วนที่เกี่ยวข้องกับเขตอำนาจรัฐ รัฐบาลประเทศไทย และกฎหมายระหว่างประเทศ (ที่เกี่ยวข้อง)

(๓) ระบุระบบงานและข้อมูลของระบบงานที่จะนำขึ้นคลาวด์

(๔) ระบุชั้นความลับและเจ้าของข้อมูลว่าสอดคล้องกับนโยบายการนำระบบงานและข้อมูลไปติดตั้งบนคลาวด์ที่องค์กรกำหนดไว้หรือไม่

(๕) ดำเนินการจัดการกับข้อมูลตามชั้นความลับของข้อมูล

(๖) จัดทำบัญชีทรัพย์สินขององค์ประกอบของระบบที่จะนำขึ้นคลาวด์

(๗) ประเมินความเสี่ยงกับระบบและจัดทำแผนการลดความเสี่ยง

(๘) กำหนดความต้องการด้านความมั่งคงปลอดภัยของระบบงาน

(๙) กำหนดข้อตกลงการควบคุมการเชื่อมต่อระบบ (The Agreed and Finalized Interface Control Document : ICD)

๒.๒ การวิเคราะห์และออกแบบความมั่นคงปลอดภัยทางเครือข่าย

(๑) ออกแบบและจัดทำผังเครือข่ายของระบบ

(๒) แบ่งแยกเครือข่ายตามผังเครือข่ายที่กำหนด

(๓) แยกเครื่องคอมพิวเตอร์แม่ข่ายเสมือนสำหรับการทดสอบไว้ในเครือข่ายที่แยกต่างหากจากเครื่องคอมพิวเตอร์แม่ข่ายเสมือนสำหรับการให้บริการจริง

(๔) ศึกษาการจราจร (Traffic) ที่เข้าออกเครื่อข่ายทั้งหมด เพื่อกำหนดเป็น Traffic ที่อนุญาต และไม่อนุญาต ซึ่งเป็นการกำหนดการไหลของข้อมูลในเครือข่าย

(๕) กำหนดนโยบาย (Policy) ไฟร์วอลล์ (Firewall) เพื่อจำกัด Traffic ที่เข้า - ออกเครือข่าย

(๖) ติดตั้งไฟร์วอลและกำหนด Rule บนไฟร์วอลล์ตามนโยบายไฟร์วอลล์ที่กำหนดไว้

(๗) ติดตั้งระบบป้องกันการบุกรุก

(๘) ติดตั้งระบบป้องกันไวรัส

(๙) ติดตั้งระบบ VPN สำหรับผู้ดูแลระบบใช้งาน

(๑๐) ติดตั้งระบบตั้งสัญญาณนาฬิกาให้ตรง

๒.๓ การวิเคราะห์และออกแบบระบบงานด้านความมั่นคงปลอดภัย

(๑) กำหนดความต้องการด้านความมั่นคงปลอดภัยของระบบงานอย่างน้อย ดังต่อไปนี้

๑.๑ ด้านการรวจสอบข้อมูลนำเข้าและออกจากระบบงาน

๑.๒ ด้านการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่สำคัญและอาจจำเป็นต้องตรวจสอบในภายหลัง

๑.๓ ด้านกลุ่มผู้ใช้งาน บทบาท และสิทธิ์การเข้าถึงระบบงาน

๑.๔ ด้านการลงทะเบียนและถอดถอนหการเข้าถึงระบบงาน

๑.๕ ด้านการตัดหรือหมดเวลาเข้าใช้งาน

๑.๖ ด้านการระบุและพิสูจนัวตนที่มีความมั่นคงปลอดภัย

๑.๗ ด้านหน้าจอการล็อคอิน (login) ที่มีความมั่นคงปลอดภัย

๑.๘) ด้านการติดตามปริมาณการใช้ระบบและขีดความสามารถหรือประสิทธิภาพของระบบ

๑.๙ ด้านการป้องกันข้อมูลรหัสผ่าน (Password) ของผู้ใช้งาน

๑.๑๐ ด้านการป้องกันข้อมูลสำคัญที่จัดเก็บไว้ในระบบงาน

๑.๑๑ ด้านการป้องกันข้อมูลสำคัญที่มีการส่งผ่านเครือข่าย

๑.๑๒ ด้านการเข้ารหัสข้อมูลและการลงลายมือชื่อดิเล็กทรอนิกส์

๑.๑๓ ด้านการวิเคราะห์จุดอ่อนของซอร์สโค้ด (Source Code)

๑.๑๔ ด้านการกู้คืนระบบ

(๒) ดำเนินการวิเคราะห์และออกแบบระบบด้านความมั่นคงปลอดภัย

๒.๔ การทดสอบระบบ

(๑) ทดสอบระบบบให้ครอบคลุมตามความต้องการด้านความมั่นคงปลอดภัยของระบบงานที่กำหนดไว้ (Security Test)

(๒) ป้องกันข้อมูลสำคัญ (Data Masking Technique) ก่อนนำไปทดสอบกับระบบ

๒.๑ เจ้าของข้อมูล้องลบข้อมูลส่วนที่สามารถบ่งชี้ตัวบุคคลทิ้งไปก่อนทดสอบกับระบบ

๒.๒ เจ้าของข้อมูลต้องลบข้อมูลส่วนตัวที่เป็นความลับทิ้งไปก่อนนำไปทดสอบกับระบบ

(๓) ทดสอบโดยการป้อนอินพุท (Input) ที่จะทำให้ระบบทำงานผิดพลาด ไม่ถูกต้อง ทำให้ระบบล่ม หรือถึงขั้นระบบถูกบุกรุกได้ (Fuzzing Tecnique)

(๔) ทดสอบและรับรองระบบ (User Acceptance Test)

๒.๕ การติดตั้งระบบ

(๑) จัดทำแผนการติดตั้งระบบงาน

(๒) ติดตั้งโปรแกรมแก้ไขช่องโหว่ต่าง ๆ ที่เกี่ยวข้องกับระบบงานให้แล้วเสร็จ ก่อนที่จะติดตั้งระบบงาน

(๓) ปิดบริการ (Service) ที่ไม่มีความจำเป็นต้องใช้งานในระบบงาน

(๔) จัดทำพื้นฐานด้สนความปลอดภัยในการใช้งาน (Security Baseline) ของระบบที่จะทำการติดตั้ง

(๕) ปรับแต่งค่าพารามิเตอร์ต่าง ๆ ที่มีผลต่อความมั่นคงปลอดภัยของระบบงานตาม Security Baseline ของระบบที่ได้กำหนดไว้

(๖) จำกัดการเข้าถึงซอร์สโค้ด (Source Code) ของระบบงาน หลีกเลี่ยงการติดตั้งซอร์สโค้ดของระบบงานบนเครื่องให้บริการ (ยกเว้นในกรณีที่ระบบงานต้องเรียกใช้โดยตรงในขณะที่ทำงาน)

(๗) ตรวจสอบและปิดช่องโหว่ในระบบที่ทำการติดตั้ง

(๘) ติดตั้งโปรแกรมเพื่อติดตามและตรวจสอบการเปลี่ยนแปลงแก้ไขไฟล์ต่าง ๆ ของระบบโดยไม่ได้รับอนุญาต

(๙) ทำแผนการตรวจสอบและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Log) บนเครื่องคอมพิวเตอร์แม่ข่ายสำหรับให้บริการระบบงานที่ทำการติดตั้ง

(๑๐) ทำแผนการสำรองข้อมูลของระบบงานและดำเนินการตามแผน

(๑๑) ทำแผนการตรวจสอบและติดตามสภาพความพร้อมใช้ของระบบงานและดำเนินการตามแผน

(๑๒) ทำแผนการตรวจสอบและติดตามทรัพยากรของระบบงานและดำเนินการตามแผน

(๑๓) ทำแผนการกู้คืนระบบงานและดำเนินการทดสอบปีละครั้ง

๓. แนวปฏิบัติการใช้คลาวด์ส่วนบุคคล (Private Cloud)

๓.๑ กรมพินิจและคุ้มครองเด็กและเยาวชนอนุญาตให้ใช้คลาวด์ส่วนบุคคล (Private Cloud) เช่น Google drive,dropbox ในเครื่องคอมพิวเตอร์ของกรม และระบบเครือข่ายของกรมได้เฉพาะในกรณีที่เป็นข้อมูลส่วนบุคคลเท่านั้นไม่เกี่ยวข้องกับงานตามภารกิจของกรม

๓.๒ งานตามภารกิจของกรมอนุญาตให้ใช้ได้เฉพาะ drive ที่กรมกำหนดให้เท่านั้น

(๑) กรณีเป็นข้อมูลที่ต้องจำกัดผู้รับรู้ หรือมีชั้นความลับ ให้มีการตั้งค่า drive กลางของกรมให้เข้าถึงได้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

(๒) เมื่อสิ้นสุดระยะเวลาดำเนินการต้องดำเนินการยกเลิกสิทธิการเข้าถึงของคลาวด์ drive ของกรม

๓.๓ เจ้าหน้าที่ที่ได้รับมอบหมาย ทำการสุ่มตรวจการใช้คลาวด์ส่วนบุคคล อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๗
หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อให้บุคคลากรที่เกี่ยวข้องทราบหน้าที่และแนวปฏิบัติในการดำเนินงานตามระเบียบนี้

๑. หน้าที่ความรับผิดชอบของเจ้าหน้าที่ดูแลระบบความปลอดภัยสารสนเทศ

แนวปฏิบัติ

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

๑.๒ ดูแลการรับแจ้งและแก้ไขปัญหาจากผู้ใช้งาน (Incident Response) รวมทั้ง เฝ้าระวังความปลอดภัยระบบคอมพิวเตอร์

๑.๓ ให้ความรู้ (Education) สร้างความตระหนักและความระมัดระวัง (Awareness) ในการใช้บริการระบบสารสนเทศอย่างปลอดภัย

๑.๔ ตรวจสอบการใช้อุปกรณ์คอมพิวเตอร์ให้มีความปลอดภัยและสามารถใช้งานได้อย่างต่อเนื่องตลอดเวลา

๑.๕ รายงานผู้ใช้งานที่ฝ่าฝืน ละเลย ไม่ปฏิบัติ ตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ. ๒๕๖๖ ต่อเจ้าหน้าที่บริหารระบบความปลอดภัยสารสนเทศ

๑.๖ ประสานงานกับเจ้าหน้าที่บริหารระบบความปลอดภัยสารสนเทศของหน่วยงานสำหรับให้เจ้าหน้าที่ดูแลระบบความปลอดภัยสารสนเทศประสานงานกับเจ้าหน้าที่ดูแลระบบความปลอดภัยสารสนเทศของหน่วยงานที่อยู่ในความรับผิดชอบ

๒. หน้าที่ความรับผิดชอบของเจ้าหน้าที่บริหารระบบความปลอดภัยสารสนเทศ

แนวปฏิบัติ

๒.๑ บริหาร จัดการ ควบคุม และดูแลผู้ใช้งานให้มีการใช้ระบบคอมพิวเตอร์ อย่างปลอดภัย

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

๒.๓ รายงานผู้ใช้งานที่ฝ่าฝืน ละเลย ไม่ปฏิบัติตามระเบียบกรมพินิจและคุ้มครองเด็กและเยาวชนว่าด้วยการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมพินิจและคุ้มครองเด็กและเยาวชนอย่างปลอดภัย พ.ศ. ๒๕๖๖ ต่อหัวหน้าหน่วยงาน

๒.๔ ให้ความร่วมมือในการดำเนินการตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit) ของกรมพินิจและคุ้มครองเด็กและเยาวชน เพื่อการปรับปรุงประสิทธิภาพการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนอย่างต่อเนื่อง

๒.๕ ศูนย์เทคโนโลยีสารสนเทศ ต้องกำหนดหน้าที่ความรับผิดชอบ และขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณ์ ด้านความมั่นคงปลอดภัย และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

๓. หน้าที่ความรับผิดชอบของเจ้าหน้าที่ในหน่วยงานสังกัดกรมพินิจและคุ้มครองเด็กและเยาวชน

๓.๑ ผู้ใช้งานต้องปฏิบัติตามระเบียบฯ อย่างเคร่งครัดและต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง หากผู้ใดละเมิด ฝ่าฝืน ละเลย ไม่ปฏิบัติตามระเบียบนี้ และก่อให้เกิดความเสียหายแก่กรมพินิจและคุ้มครองเด็กและเยาวชนหรือบุคคลใดบุคคลหนึ่ง หัวหน้าหน่วยงานต้องพิจารณาดำเนินการทางวินัยและทางกฎหมาย แก่เจ้าหน้าที่ที่ละเมิด หรือฝ่าฝืนที่ก่อให้เกิดความเสียหาย ตามความเหมาะสมเป็นกรณีไป

๓.๒ ให้หัวหน้าหน่วยงานมีหน้าที่ควบคุมดูแลการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารตามระเบียบนี้อย่างเคร่งครัดหากพบการไม่ปฏิบัติตามระเบียบนี้ให้แจ้งรายงานการละเมิดต่อกรมพินิจและคุ้มครองเด็กและเยาวชน ตามสายการบังคับบัญชา

๓.๓ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่กรมพินิจและคุ้มครองเด็กและเยาวชน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือ ฝ่าฝืนการปฏิบัติตามระเบียบนี้ให้ผู้บริหารสูงสุด (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้น

๓.๔ ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติงานตามระเบียบนี้ หรือมิได้กำหนดแนวทางปฏิบัติไว้ให้ผู้ใช้ระบบงานแจ้งต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อเสนออธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชนวินิจฉัยสั่งการต่อไป

๓.๕ ให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ รักษาการตามระเบียบนี้

๓.๖ ระเบียบใดที่ขัดหรือแย้งกับระเบียบนี้ ให้ถือปฏิบัติตามระเบียบนี้