แนวทางปฏิบัติ
เพื่อป้องกันการกระทำความผิด
เกี่ยวกับคอมพิวเตอร์

เอกสารความรู้ สดร.
ลำดับที่ ๒ / ปีงบประมาณ ๒๕๕๕
สถาบันดำรงราชานุภาพ
สำนักงานปลัดกระทรวงมหาดไทย

แนวทางปฏิบัติ
เพื่อป้องกันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

วิไลภรณ์ ศรีไพศาล[๑]

เนื่องจากเทคโนโลยีด้านการสื่อสารและโทรคมนาคมขยายตัวมากขึ้น คอมพิวเตอร์ถูกออกแบบให้มีความหลากหลายรูปแบบ เพื่อให้ตอบสนองความต้องการของผู้ใช้หลากหลายลักษณะ จึงทำให้เกิดการใช้งานแพร่หลายมากยิ่งขึ้น และการใช้งานผ่านเครือข่ายอินเทอร์เน็ต ทำให้เราสามารถค้นหาและเข้าถึงข้อมูลได้อย่างไม่จำกัดระยะเวลา และสถานที่ ดังนั้นจึงมีการกระจายข้อมูลข่าวสารแบบทุกทิศทาง มีการสื่อสารแบบสองทิศทางที่มีตอบสนองอย่างรวดเร็ว ช่วยลดอุปสรรคเรื่องสถานที่และเวลาในการดำเนินกิจกรรมต่างๆ ด้วยเหตุนี้จึงส่งผลกระทบต่อการเปลี่ยนแปลงทางด้านเศรษฐกิจ การเมือง และสังคมอย่างรวดเร็วและกว้างขวาง

---

[๑] นักวิชาการคอมพิวเตอร์ ชำนาญการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย

เมื่อคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตกลายเป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิต หากมีผู้กระทำการใดๆ ที่เกี่ยวข้องกับการใช้คอมพิวเตอร์และทำให้ผู้เสียหายได้รับความเสียหาย หรือผู้กระทำความผิดได้รับผลประโยชน์ เช่น การบิดเบือนข้อมูล การฟอกเงิน การฉ้อโกง การเผยแพร่รูปลามกอนาจาร การขโมยข้อมูลของผู้อื่น การถอดรหัสโปรแกรมคอมพิวเตอร์โดยไม่ได้รับอนุญาตแล้วเผยแพร่ให้ผู้อื่นดาวน์โหลดได้ การนำภาพไปตัดต่อเข้าสู่ระบบคอมพิวเตอร์ทำให้ผู้อื่นเสียหาย การปลอมแปลงเอกสาร เป็นต้น สิ่งเหล่านี้ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน จึงได้กำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว โดยตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ ๑๘ กรกฎาคม ๒๕๕๐

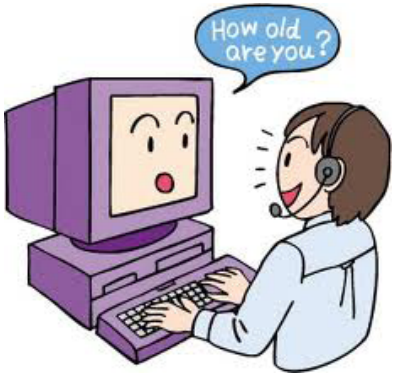
๑. แนวทางปฏิบัติเพื่อป้องกันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

เมื่อมีการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ประชาชนและหน่วยงานทุกภาคส่วนต้องปฏิบัติตาม ดังนั้น จึงจำเป็นที่จะต้องทำความเข้าใจในสาระสำคัญของพระราชบัญญัติฉบับนี้ เพื่อนำมาเป็นแนวทางในการปฏิบัติตามกฎหมาย และป้องการกระทำผิดกฎหมาย โดยมีลักษณะความผิดดังนี้

๑.๑ การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ เช่น การเจาะระบบคอมพิวเตอร์หรือการบุกรุกทางคอมพิวเตอร์โดยที่เจ้าของไม่รู้ตัว การใช้บัญชีผู้ใช้ (Log In) และรหัสผ่าน (Password) ของผู้อื่น

๑.๒ การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ไม่ว่าจะได้มาโดยชอบ เช่น Log In และ Password ของหน่วยงานที่มีหน้าที่ดูแลอยู่ หรือการได้มาโดยไม่ชอบ เช่น การแอบบันทึกการกด Password ของผู้อื่น แล้วนำไปเปิดเผยให้บุคคลที่สามรู้

๑.๓ การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ เช่น การเข้าถึงแฟ้มข้อมูลที่มีชั้นความลับโดยไม่ได้รับอนุญาต การเข้าไปดูข้อมูลในเครื่องคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต รวมถึงการนำแผ่นซีดี หรือแผ่นดิสก์มาเก็บหรือส่งข้อมูลผ่านระบบคอมพิวเตอร์



๑.๔ การดักรับข้อมูลโดยมิชอบเพื่อลักลอบดักฟัง ตรวจสอบหรือติดตามเนื้อหาสาระของข่าวสารที่สื่อสารถึงกันระหว่างบุคคล (ไม่ใช่สาธารณะ) เพื่อให้ได้มาซึ่งเนื้อหาของข้อมูลโดยตรง หรือโดยทางอ้อมด้วยการแอบบันทึกข้อมูลสื่อสารถึงกันด้วยอุปกรณ์อิเล็กทรอนิกส์ ไม่ว่าอุปกรณ์อิเล็กทรอนิกส์ที่ใช้บันทึกข้อมูลดังกล่าวจะเชื่อมต่อเข้ากับสายสัญญาณสำหรับส่งผ่านข้อมูล หรือโดยใช้เทคโนโลยีไร้สาย (Wireless LAN) ก็ตาม นอกจากนี้ยังรวมถึงกรณีใช้ซอฟต์แวร์หรือรหัสผ่านต่างๆ เพื่อทำการแอบบันทึกข้อมูลที่ส่งผ่านถึงกันด้วย

๑.๕ การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลงข้อมูลคอมพิวเตอร์ เช่น การแพร่กระจายไวรัส (Virus) การติดตั้งโปรแกรมไม่ประสงค์ดี เช่น สแปมเมล (Spam Mail) ม้าโทรจัน (Trojan Horse)

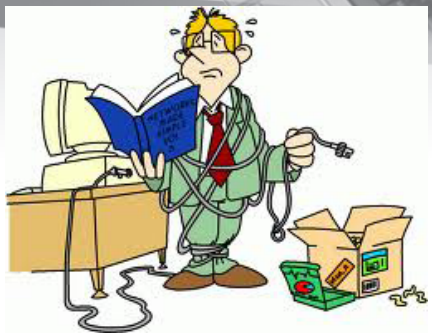
๑.๖ การทำให้ระบบไม่สามารถทำงานได้ตามปกติ แม้จะยังทำงานได้ แต่ถ้าไม่สามารถทำงานได้อย่างสมบูรณ์ เช่น การแพร่กระจายไวรัส (Virus) ทำให้ระบบคอมพิวเตอร์ทำงานได้ช้าลง การวินาศกรรมเพื่อให้มีผลการทำลายการทำงานของระบบคอมพิวเตอร์

๑.๗ สแปมเมล (Spam Mail) คือ การส่งอีเมลจำนวนมากๆ ในครั้งหนึ่ง หรือทยอยส่งเพื่อวัตถุประสงค์ในการโฆษณาสินค้า การโจมตีระบบการกลั่นแกล้งให้รำคาญ ฯลฯ

๑.๘ การกระทำซึ่งก่อให้เกิดผลกระทบต่อความมั่นคง เช่น การเจาะเข้าไปในระบบคอมพิวเตอร์และลักลอบเติมหรือทำลายข้อมูลคอมพิวเตอร์ที่ก่อให้เกิดความเสียหายต่อประเทศชาติหรือสร้างความตื่นตระหนกแก่ประชาชนในวงกว้าง กรณีเป็นเหตุให้ผู้อื่นถึงแก่ความตายนั้น หากผู้กระทำมีเจตนาฆ่า ต้องมีความผิดตามประมวลกฎหมายอาญา ซึ่งมีอัตราโทษจำคุกสูงสุด คือ ประหารชีวิต หากกระทำโดยประมาท ก็ต้องถือว่าเป็นกรรมเดียวผิดกฎหมายหลายบท ก็ต้องรับโทษตามกฎหมายฉบับที่มีบทลงโทษหนักที่สุด

๑.๙ การจำหน่าย/เผยแพร่ชุดคำสั่ง หรือโปรแกรมคอมพิวเตอร์ที่นำไปใช้เป็นเครื่องมือในการกระทำความผิด

๑.๑๐ การนำเข้า/เผยแพร่เนื้อหาอันไม่เหมาะสม เช่น ในกระดานข่าว (Web Board) หรือการส่งต่ออีเมล (E-mail) ที่มีข้อความ เนื้อหา หรือรูปภาพไม่เหมาะสม เป็นเท็จ กระทบความมั่นคง หรือลามกอนาจาร



๑.๑๑ ความรับผิดชอบของผู้ให้บริการ เช่น เจ้าของเว็บบอร์ดหรือเว็บไซต์ ซึ่งมีการพิจารณาว่าควรต้องมีหน้าที่ลบเนื้อหาอันไม่เหมาะสมด้วย หากทราบว่ากระทำผิดแล้วปล่อยให้มีการกระทำผิดแสดงว่าให้การสนับสนุนให้ข้อมูลคอมพิวเตอร์นั้นอยู่ในระบบคอมพิวเตอร์ของตน หรือยินยอมให้มีการกระทำความผิด จึงมีความผิดและต้องรับโทษเช่นเดียวกับผู้กระทำความผิด

ตารางสรุปลักษณะความผิดและบทกำหนดโทษ

ลักษณะความผิด	โทษจำคุก	โทษปรับ
มาตรา ๕ การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ	ไม่เกิน ๖ เดือน	ไม่เกิน ๑๐,๐๐๐ บาท
มาตรา ๖ การเปิดเผยมาตรการป้องกัน	ไม่เกิน ๑ ปี	ไม่เกิน ๒๐,๐๐๐ บาท
มาตรา ๗ การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ	ไม่เกิน ๒ ปี	ไม่เกิน ๔๐,๐๐๐ บาท
มาตรา ๘ การดักข้อมูลคอมพิวเตอร์โดยมิชอบ	ไม่เกิน ๓ ปี	ไม่เกิน ๖๐,๐๐๐ บาท
มาตรา ๙ การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๐ การทำให้ระบบไม่สามารถทำงานได้ตามปกติ	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท

ลักษณะความผิด	โทษจำคุก	โทษปรับ
มาตรา ๑๑ สแปมเมล์ (Spam Mail)	ไม่มี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๒ กระทำผิดมาตรา ๙ หรือมาตรา ๑๐ (๑) ก่อให้เกิดความเสียหายแก่ประชาชน (๒) กระทบต่อความมั่นคงของประเทศ/เศรษฐกิจ วรรคท้าย เป็นเหตุให้ผู้อื่นถึงแก่ชีวิต	ไม่เกิน ๑๐ ปี ๓ ปี ถึง ๑๕ ปี ๑๐ ปี ถึง ๒๐ ปี -	ไม่เกิน ๒๐๐,๐๐๐ บาท ๖๐,๐๐๐-๓๐๐,๐๐๐ บาท ไม่มี -
มาตรา ๑๓ การจำหน่าย/เผยแพร่ชุดคำสั่ง	ไม่เกิน ๑ ปี	ไม่เกิน ๒๐,๐๐๐ บาท
มาตรา ๑๔ การเผยแพร่เนื้อหาอันไม่เหมาะสม	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๕ ความรับผิดชอบของผู้ให้บริการ	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๖ การตัดต่อภาพผู้อื่น	ไม่เกิน ๓ ปี	ไม่เกิน ๖๐,๐๐๐ บาท
มาตรา ๑๗ การกระทำความผิดนอกราชอาณาจักร	-	-
มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน	-	ไม่เกิน ๕๐๐,๐๐๐ บาท

๑.๑๒ การเผยแพร่ภาพซึ่งตัดต่อในลักษณะหมิ่นประมาท และนำไปเผยแพร่ในระบบคอมพิวเตอร์โดยเจตนา เช่น เผยแพร่บนเว็บบอร์ด เว็บไซต์ อีเมล

๑.๑๓ การกระทำความผิดนอกราชอาณาจักรที่ต้องรับโทษในราชอาณาจักร ไม่ว่าจะเป็นการเข้าถึง (Access) การเข้าแทรกแซง ทำลาย การนำ

เข้าสู่ระบบคอมพิวเตอร์ แม้ว่าจะไม่ได้กระทำในประเทศไทย แต่ถ้า ผู้รับข้อมูลสามารถเปิดรับข้อมูลคอมพิวเตอร์นั้นในประเทศไทยได้ ย่อมถือว่าการกระทำความผิดนั้นได้กระทำในประเทศไทยด้วย

๑.๑๔ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้บริการเท่าที่จำเป็น เพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง ตัวอย่างเช่น ข้อมูลเกี่ยวกับวันและเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ ข้อมูลหมายเลขชุดอินเทอร์เน็ต (IP Address) ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Facebook, Yahoo, Hotmail, MSN

๒. ข้อปฏิบัติการใช้งานระบบสารสนเทศของสำนักงานปลัดกระทรวงมหาดไทย

๒.๑ คำนิยาม

๒.๑.๑ “สำนักงาน” หมายความว่า สำนักงานปลัดกระทรวงมหาดไทย

๒.๑.๒ “หน่วยงานในสังกัด” หมายความว่า ส่วนราชการและหน่วยงานในสังกัดสำนักงานปลัดกระทรวงมหาดไทย ระดับสำนัก สถาบัน ศูนย์หรือกองหรือเทียบเท่า

๒.๑.๓ “ระบบเทคโนโลยีสารสนเทศ”หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ระบบสารสนเทศ ชุดคำสั่งงานคอมพิวเตอร์สำหรับการบันทึกประมวลผล เรียกดู พิมพ์ออก รายงานในระบบของสำนักงาน และโปรแกรมการใช้งานที่เจ้าหน้าที่ทำการติดตั้งประจำเครื่องคอมพิวเตอร์

๒.๑.๔ “ข้อมูล” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใดๆ ไม่ว่าการสื่อสารความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยการผ่านวิธีการใดๆ และได้จัดทำไว้ในรูปแบบเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม ภาพเคลื่อนไหว เสียงการบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีการอื่นใดที่ทำให้สิ่งที่ทำการบันทึกไว้ปรากฏได้

๒.๑.๕ “เครื่องคอมพิวเตอร์” หมายความว่า เครื่องคอมพิวเตอร์แม่ข่าย (Server) และรวมถึงเครื่องคอมพิวเตอร์ลูกข่าย (Client) ชนิดตั้งโต๊ะ (Personal Computer) และชนิดพกพา (Notebook, Palm, PDA)

๒.๑.๖ “เครือข่ายคอมพิวเตอร์” หมายความว่า เครือข่ายคอมพิวเตอร์และการสื่อสารของสำนักงานปลัดกระทรวงมหาดไทย

๒.๑.๗ “เจ้าหน้าที่” หมายความว่า ผู้ซึ่งได้รับมอบหมายให้ดูแลการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงมหาดไทย

๒.๑.๘ “ผู้ใช้งาน” หมายความว่า ข้าราชการ พนักงาน และลูกจ้างของสำนักงานปลัดกระทรวงมหาดไทย

๒.๒ การใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๒.๑ ผู้ใช้งานมีสิทธิใช้ระบบเทคโนโลยีสารสนเทศของสำนักงานได้ภายใต้ข้อปฏิบัติการใช้งานนี้รวมทั้งต้องปฏิบัติตามแนวทางหรือหลักเกณฑ์อื่นใดจะออกต่อไป

๒.๒.๒ การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงของสำนักงานให้ปฏิบัติดังนี้

(๑) ให้ใช้งานเพื่อภารกิจของสำนักงานเท่านั้น

(๒) หน่วยงานในสังกัดต้องจัดให้มีเจ้าหน้าที่ผู้ดูแลรับผิดชอบเป็นผู้ประสานการปฏิบัติด้านระบบเทคโนโลยีสารสนเทศ การจัดทำระเบียนครุภัณฑ์เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงรวมถึงการติดตามปรับปรุงและแก้ไขทะเบียนครุภัณฑ์อย่างต่อเนื่อง

(๓) ห้ามนำเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงของสำนักงานไปใช้งานนอกสถานที่เว้นแต่จะนำไปใช้งานภารกิจของสำนักงาน โดยจะต้องได้รับอนุญาตเป็นหนังสือจากหัวหน้าหน่วยงานในสังกัดที่ผู้ใช้งานสังกัด

(๔) ห้ามผู้ใช้งานและบุคคลภายนอกนำเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงจากภายนอกสำนักงานเข้ามาเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ของสำนักงาน เว้นแต่จะได้รับความเห็นชอบจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ที่ได้รับมอบหมาย

(๕) ห้ามผู้ใช้งานทำการติดต่อเพิ่ม ลบ แก้ไข หรือเปลี่ยนแปลงโปรแกรมใดๆ บนเครื่องคอมพิวเตอร์ของสำนักงานนอกเหนือจากที่เจ้าหน้าที่ได้ทำการติดตั้งและใช้งานไว้แล้ว

(๖) ต้องจัดวางเครื่องคอมพิวเตอร์และอุปกรณ์ไว้ในสถานที่ที่ปลอดภัย ห้ามเปิดฝา ถอด เพิ่ม หรือเปลี่ยนชิ้นส่วน เครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วง เว้นแต่เป็นการดำเนินการเพื่อซ่อมแซมบำรุงรักษาโดยเจ้าหน้าที่

(๗) ห้ามผู้ใช้งานแก้ไข เปลี่ยนแปลง หรือปรับค่าต่างๆ ที่กำหนดไว้ในเครื่องคอมพิวเตอร์ เพื่อให้ทำงานได้ในระบบเครือข่าย (Network Configuration/IP Address) เว้นแต่เป็นการดำเนินการโดยเจ้าหน้าที่

(๘) กรณีมีการย้ายจุดติดตั้งเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วง ผู้ใช้งานต้องได้รับความเห็นชอบจากผู้บังคับบัญชาระดับหัวหน้าหน่วยงานในสังกัด และแจ้งให้ศูนย์เทคโนโลยีสารสนเทศแลกสื่อสารทราบเป็นหนังสือ

(๙) ห้ามผู้ใช้งานติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อใช้งานในระบบเครือข่ายคอมพิวเตอร์ของสำนักงาน หรือเปิดการใช้แฟ้มข้อมูลร่วมกัน (Share File/ Directory) ให้ผู้อื่นสามารถเข้าถึง (Access) ข้อมูลที่ไม่ใช้เพื่อประโยชน์ หรือภารกิจในการปฏิบัติงาน

(๑๐) ให้ปิดเครื่องคอมพิวเตอร์และอุปกรณ์ทุกครั้งที่เลิกใช้งาน หรือเมื่อไม่ได้ใช้งาน เครื่องคอมพิวเตอร์เกินกว่า ๑ ชั่วโมง

๒.๒.๓ ผู้ใช้งานพึงใช้ทรัพยากรเครือข่ายคอมพิวเตอร์ให้เกิดประสิทธิภาพและประโยชน์ในการปฏิบัติงานส่วนรวม โดยให้ปฏิบัติ ดังนี้

(๑) ไม่ใช้เครือข่ายคอมพิวเตอร์โดยมีวัตถุประสงค์ต่อไปนี้

- กระทำผิดกฎหมายหรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น
- กระทำขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
- เพื่อการพาณิชย์
- เปิดเผยข้อมูลที่เป็นความลับซึ่งได้จากการปฏิบัติงาน
- เป็นการละเมิดทรัพย์สินทางปัญญา
- รับหรือส่งข้อมูลซึ่งก่อให้เกิดความเสียหายแก่สำนักงาน เช่น การรับหรือส่งจดหมายที่มีลักษณะเป็นจดหมายลูกโซ่

- ขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของผู้ใช้งานอื่น หรือเพื่อให้เครือข่ายคอมพิวเตอร์ของสำนักงานไม่สามารถใช้งานได้ตามปกติ

- รับรู้ รับทราบข้อมูล ส่งต่อ ประกาศ หรือแสดงความคิดเห็นในเรื่องที่ไม่เกี่ยวข้องกับการดำเนินงานของศาลและสำนักงานในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

(๒) ไม่ถ่ายโอนข้อมูลที่มีขนาดใหญ่ที่ไม่เกี่ยวข้องกับการปฏิบัติงานโดยไม่จำเป็น และไม่ควรปฏิบัติในระหว่างเวลาทำงาน

(๓) ไม่นำเครื่องคอมพิวเตอร์ของสำนักงาน ไปติดตั้งหรือเชื่อมโยงกับเครือข่ายคอมพิวเตอร์ภายนอกโดยผ่านทางช่องทางโทรศัพท์หรือช่องทางอื่นที่สำนักงานไม่ได้กำหนดไว้

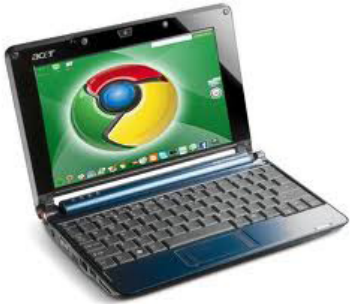
(๔) ไม่ควรติดตั้งและใช้งานโปรแกรมการสนทนาผ่านเครือข่ายคอมพิวเตอร์ เช่น โปรแกรม IRC, ICQ, MSN เป็นต้น

๒.๓ การรักษาความปลอดภัยของข้อมูล

เพื่อความปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของสำนักงาน ให้ผู้ใช้ปฏิบัติงานดังนี้

๒.๓.๑ สำรวจแฟ้มข้อมูลต่างๆ ที่ได้บันทึกไว้ในแผ่นบันทึกข้อมูลเครื่องคอมพิวเตอร์ (Hard Disk) อย่างสม่ำเสมอและลบแฟ้มข้อมูลหรือข้อมูลที่ไม่จำเป็นออกไปเพื่อให้มีเนื้อที่ในการบันทึกข้อมูลอื่นๆ เพิ่มมากขึ้น และเป็นการเพิ่มสมรรถนะในการประมวลผลข้อมูลของเครื่องคอมพิวเตอร์ให้เร็วยิ่งขึ้นได้

๒.๓.๒ ข้อมูลที่เป็นความลับ หรือข้อมูลที่ไม่พึงเปิดเผย ให้บันทึกข้อมูลลงในแผ่นบันทึกข้อมูลที่สามารถแยกเก็บไว้ต่างหากในที่ปลอดภัย กรณีมีข้อมูลที่มีความสำคัญให้สำรองของมูล (Back Up) และจัดเก็บแยกต่างหากในที่ที่ปลอดภัย



๒.๓.๓ กรณีมีความจำเป็นต้องนำข้อมูลจากแหล่งจัดเก็บข้อมูลภายนอกมาใช้งานกับเครื่องคอมพิวเตอร์ของสำนักงาน ให้ตรวจไวรัสคอมพิวเตอร์ก่อนทุกครั้งโดยใช้โปรแกรมตรวจสอบไวรัสคอมพิวเตอร์ที่เจ้าหน้าที่ได้ติดตั้งไว้กับเครื่องคอมพิวเตอร์นั้น และหากตรวจพบไวรัสคอมพิวเตอร์ฝังอยู่ในข้อมูลส่วนใดจะต้องรีบจัดการทำลายไวรัสหรือข้อมูลนั้นโดยเร็วที่สุด

๒.๓.๔ ลงทะเบียนการใช้งานระบบงานสารสนเทศของสำนักงาน โดยหัวหน้าหน่วยงานในสังกัดที่ผู้ใช้งานสังกัดอยู่เป็นผู้พิจารณา

๒.๓.๕ กรณีผู้ใช้งานโอนย้าย เปลี่ยนแปลงหน้าที่ หรือไม่มีความจำเป็นในการใช้งานระบบงานสารสนเทศใด ให้หัวหน้าหน่วยงานในสังกัดแจ้งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ เพื่อปรับปรุงเปลี่ยนแปลงสิทธิหรือยกเลิกชื่อหรือรหัสของผู้ใช้งานนั้นต่อไป

๒.๓.๖ ในการใช้งานระบบสารสนเทศของสำนักงาน ผู้ใช้จะต้องใส่ชื่อผู้ใช้งาน (Log In Name) และกำหนดรหัสผ่าน (Password) เพื่อเชื่อมต่อเข้าสู่ระบบงานสารสนเทศ และเมื่อเสร็จสิ้นการใช้งานให้ปิดระบบ (Exit) ทันที

๒.๓.๗ ดูแล และใช้รหัสผ่านที่ได้รับ ความระมัดระวังและรักษาเป็นความลับ มิให้แจ้งรหัสผ่านของตนเองให้กับบุคคลภายนอกหรือบุคคลอื่นที่ไม่เกี่ยวข้องกับการปฏิบัติงานเพื่อป้องกันมิให้ผู้อื่นนำชื่อรหัสผ่านไปใช้งานในระบบงานสารสนเทศของสำนักงาน ซึ่งอาจก่อให้เกิดความเสียหายขึ้นได้

๒.๓.๘ ไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลที่สำคัญไว้ในที่ที่สามารถพบเห็นได้ง่าย โดยให้มีการจัดเก็บไว้ในที่ปลอดภัย

๒.๓.๙ ต้องป้องกันข้อมูลและอุปกรณ์ที่อยู่ในเครื่องคอมพิวเตอร์ชนิดพกพาเมื่อปฏิบัติงานนอกสถานที่ เช่น การใส่รหัสผ่านป้องกันการเข้าถึงหน้าจอ การใช้กุญแจล็อกเครื่องคอมพิวเตอร์ชนิดพกพา หรือการเข้ารหัสแฟ้มข้อมูลที่สำคัญ

๒.๓.๑๐ กรณีที่ตรวจสอบหรือพบเห็นเหตุการณ์หรือการกระทำอื่นใดที่เป็นผลเสียต่อการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานรวมถึงการตรวจพบจุดอ่อนหรือภัยที่พบในระบบงานสารสนเทศที่ใช้งานอยู่ ให้รายงานให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบเพื่อป้องกันแก้ไขต่อไปโดยเร็ว

๒.๓.๑๑ กรณีพบปัญหา หรือข้อบกพร่องของระบบงานสารสนเทศของสำนักงาน ผู้ใช้งานรายงานปัญหาหรือข้อบกพร่องที่พบให้สำนักเทคโนโลยีสารสนเทศทราบ เพื่อแก้ปัญหาโดยเร็วที่สุด

๒.๔ การดูแล บำรุงรักษา และการปฏิบัติของเจ้าหน้าที่

เจ้าหน้าที่ต้องดูแล บำรุงรักษา ระบบเทคโนโลยีสารสนเทศให้ใช้งานได้ดีอยู่เสมอ และจะต้องตรวจสอบดูแลการใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นไปตามข้อปฏิบัติ ดังนี้

๒.๔.๑ เจ้าหน้าที่ต้องดำเนินการจัดเก็บข้อมูลจลาจลคอมพิวเตอร์ (Log File) ตามที่กฎหมายกำหนดไว้

๒.๔.๒ เจ้าหน้าที่ต้องไม่ใช้สิทธิหรืออำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น เว้นแต่กรณีที่ได้รับมอบหมายให้ดำเนินการเพื่อแก้ไขปัญหาที่เกี่ยวข้อง และจะต้องไม่เปิดเผยหรือเผยแพร่ข้อมูลที่ได้รับจากการปฏิบัติหน้าที่

๒.๔.๓ เจ้าหน้าที่ต้องจัดให้มีวิธีการป้องกันข้อมูลส่วนตัวของผู้ใช้งาน เช่น ข้อมูลในระบบไปรษณีย์อิเล็กทรอนิกส์ ข้อมูลในระบบบริหารงานบุคคล

๒.๔.๔ เจ้าหน้าที่ต้องบันทึกเหตุการณ์ที่มีการละเมิดความมั่นคงปลอดภัย จุดอ่อน ภัยคุกคาม หรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไขปัญหาที่เกิดขึ้น

๒.๔.๕ เจ้าหน้าที่ต้องติดตั้งซอฟต์แวร์หรืออุปกรณ์ป้องกันไวรัสคอมพิวเตอร์ และตรวจสอบไวรัสคอมพิวเตอร์ที่อาจบุกรุกเข้ามาทางเครือข่ายคอมพิวเตอร์อย่างสม่ำเสมอหากตรวจพบต้องรีบจัดการทำลายไวรัสคอมพิวเตอร์นั้นโดยเร็วที่สุด

๒.๔.๖ เจ้าหน้าที่ต้องสำรองข้อมูลในระบบสารสนเทศ โดยต้องมีข้อมูลการสำรองข้อมูลและจัดทำบันทึกรายละเอียดการสำรองข้อมูล รวมถึงการรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้นและวิธีการแก้ไขปัญหาที่เกิดขึ้น

๒.๔.๗ เจ้าหน้าที่ต้องจัดการให้มีระบบการบริหารจัดการเกี่ยวกับการกำหนดสิทธิ์การใช้งานระบบงานสารสนเทศและทำการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบงานสารสนเทศแต่ละระบบ

๒.๔.๘ เจ้าหน้าที่ต้องจัดให้มีการควบคุมการใช้งานของชุดคำสั่งงานคอมพิวเตอร์ (Program source library) ไม่เก็บซอร์สโค้ด (source code) ไว้ในเครื่องที่ใช้ปฏิบัติงานระบบงานสารสนเทศ ไม่เก็บซอร์สโค้ดที่อยู่ระหว่างทำการทดสอบรวมไว้กับไลบรารีที่ใช้งานได้จริงแล้ว และต้องเก็บซอร์สโค้ดไว้ในที่ที่ปลอดภัย

เจ้าหน้าที่หรือผู้ใช้งานฝ่าฝืนหรือไม่ปฏิบัติตามข้อปฏิบัตินี้ และก่อหรืออาจก่อให้เกิดความเสียหายแก่สำนักงานหรือบุคคลหนึ่งบุคคลใด สำนักงานปลัดจะพิจารณาระงับสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ

๓. นโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศของสำนักงานปลัดกระทรวงมหาดไทย

๓.๑ นโยบายการใช้งานอย่างถูกต้อง (Acceptable Use Policy Solution) ได้กำหนดข้อปฏิบัติการใช้งานระบบเทคโนโลยีสารสนเทศ ๓ ด้าน คือ

๑) การใช้งานระบบเทคโนโลยีสารสนเทศ
๒) การรักษาความปลอดภัยของข้อมูล
๓) การดูแล บำรุงรักษา และการปฏิบัติของเจ้าหน้าที่

๓.๒ นโยบายด้าน การเชื่อมโยงเครือข่ายแบบไร้สาย (Wireless Policy)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป. ผู้ให้บริการระบบสารสนเทศของสำนักงานปลัดกระทรวงมหาดไทย มีการให้บริการเชื่อมโยงเครือข่ายแบบไร้สายในบางจุดที่การให้บริการเชื่อมโยงแบบ ใช้สาย (LAN) ไม่เหมาะสม โดยมีข้อกำหนดในการให้บริการแบบไร้สาย (Wireless LAN) ดังนี้

ข้อ ๑ มีการควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๒ มีการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

ข้อ ๓ มีการกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ ๔ มีการใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ ๕ มีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ ๖ มีการใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

ข้อ ๗ การควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่าย ไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

๓.๓ นโยบายด้าน Firewall (Firewall Policy)

ในการป้องกันและรักษาความปลอดภัยของข้อมูล สำนักงานปลัดกระทรวงมหาดไทย มีนโยบายในการกำหนดสิทธิการใช้งานเครื่องแม่ข่ายระบบงาน Application Server และเครื่องแม่ข่ายฐานข้อมูล Database Server ที่ติดตั้ง ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป. ทำหน้าที่

ข้อ ๑ การบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

ข้อ ๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

ข้อ ๓ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

ข้อ ๔ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

ข้อ ๕ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๖ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๗ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางสำนักงานปลัดกระทรวงมหาดไทยอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความความยินยอมจากสำนักงานปลัดกระทรวงมหาดไทย

ข้อ ๘ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ ๙ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกเดือน หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ ๑๐ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๑ สำนักงานปลัดกระทรวงมหาดไทย มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ ๑๒ การเชื่อมต่อในลักษณะของการ Remote Log In จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจาก สำนักงานปลัดกระทรวงมหาดไทยก่อน

ข้อ ๑๓ ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานในระบบการสืบค้นข้อมูลสารสนเทศทันที

๓.๔ นโยบายด้านการใช้จดหมายอิเล็กทรอนิกส์ (E-mail Policy)

การติดต่อราชการในสำนักงานปลัดกระทรวงมหาดไทยทางจดหมายอิเล็กทรอนิกส์ (E-mail) ให้ใช้อีเมลของกระทรวงมหาดไทยคือ username@moi.go.th ซึ่งข้าราชการ ลูกจ้างประจำ และพนักงานราชการในสังกัดสำนักงานปลัดกระทรวงมหาดไทย มีสิทธิในการใช้งานโดยลงทะเบียนขอใช้งานได้ที่ http://mail.moi.go.th/newmail.php และสร้างรหัสผ่านด้วยตนเอง หลังจากนั้น ผู้ดูแลระบบเมล คือ ส่วนเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จะเป็นผู้ตรวจสอบ และอนุมัติการเข้าใช้งาน พร้อมกำหนดพื้นที่ให้จำนวน ๑ Gigabyte ในการจัดเก็บจดหมาย โดยผู้ใช้ต้องบริหารจัดการพื้นที่ใช้งาน และเปลี่ยนรหัสผ่านของตนเองได้ด้วยตนเอง และกำหนดให้การส่งจดหมายถึงผู้รับได้ครั้งละไม่เกิน ๑๐๐ ฉบับ

๓.๕ นโยบายด้านการใช้อินเทอร์เน็ต (Internet Security Policy)

ข้อ ๑ ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงานเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบ

กระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๒ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๓ ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การดาวน์โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๔ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Web Board) ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ ๕ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

ข้อ ๖ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราเซอร์ (Web Browser) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ข้อ ๗ ผู้ใช้งานใหม่จะต้องลงทะเบียนขอใช้บริการอินเทอร์เน็ตผ่านหน้าเว็บไซต์ส่งให้ผู้ดูแลระบบจัดทำบัญชีผู้ใช้ และต้องพิมพ์หน้าจอที่ได้ลงทะเบียนไว้ให้หัวหน้าหน่วยงานลงนามรับรองบุคคล พร้อมบันทึกนำส่งอย่างเป็นทางการหลังได้รับการอนุมัติให้ใช้บริการอินเทอร์เน็ตแล้ว ผู้ดูแลระบบจึงเปิดสิทธิ์ให้ผู้ใช้รายนั้นใช้งานได้ โดยกำหนดหมายเลขประจำตัวประชาชน ๑๓ หลักเป็นรหัสผู้ใช้

ข้อ ๘ ก่อนการเรียกใช้ทุกครั้งจะต้องมีการใส่รหัสผู้ใช้และรหัสผ่านที่ได้ลงทะเบียนไว้กับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อจัดเก็บประวัติการใช้ไว้ ๙๐ วันตามพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ ๙ เมื่อผู้ใช้งานรายใดไม่ได้เป็นข้าราชการ ลูกจ้าง พนักงานราชการ เจ้าหน้าที่บริษัทตามสัญญาต่างๆ ที่เข้ามาทำงานในเครือข่ายมหาดไทย หรือเป็นนักศึกษาฝึกงานของสำนักงานปลัดกระทรวงมหาดไทยที่หมดช่วงระยะเวลาฝึกงานกับสำนักงานปลัดกระทรวงมหาดไทยจะหมดสิทธิ์ในการใช้บริการอินเทอร์เน็ตทันที

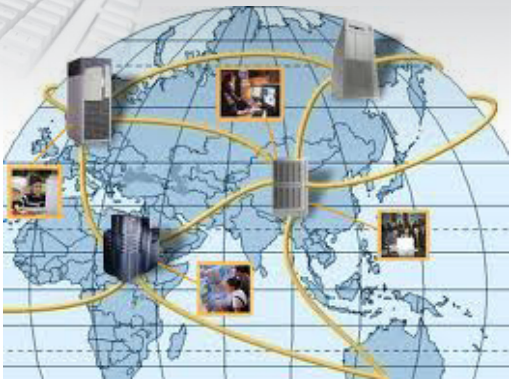
ข้อ ๑๐ ไม่อนุญาตให้เปิดเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์เกี่ยวกับลามกอนาจาร การพนัน และจำกัดเวลาการใช้งานเว็บที่ทำให้ระบบการสืบค้นข้อมูลสารสนเทศแออัดล่าช้า เช่น การใช้งาน MSN, IRC, ICQ, MSN เป็นต้น

ข้อ ๑๑ ไม่อนุญาตให้เปิดเว็บที่มีการมีการส่งผ่านข้อมูลปริมาณมากๆ เช่น การ download ภาพยนตร์ วิดีโอต่างๆ

๓.๖ นโยบายด้านการเข้าถึงข้อมูลการใช้เครื่องแม่ข่าย และการใช้เครือข่าย (Access Control Policy)

ข้อ ๑ สำนักงานปลัดกระทรวงมหาดไทยกำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

ข้อ ๒ ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากสำนักงานปลัดกระทรวงมหาดไทย และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด



ข้อ ๓ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อสำนักงานปลัดกระทรวงมหาดไทย และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่นๆ

ข้อ ๔ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

ข้อ ๕ มีการควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

- ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

- ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

- ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้

- ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

- ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

- การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Log In) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

- เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

- ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

- การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ข้อ ๖ มีการบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๗ สำนักงานปลัดกระทรวงมหาดไทยกำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

- ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

- ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

- ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

- ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ข้อ ๘ สำนักงานปลัดกระทรวงมหาดไทยกำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

- บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากสำนักงานปลัดกระทรวงมหาดไทย

- มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

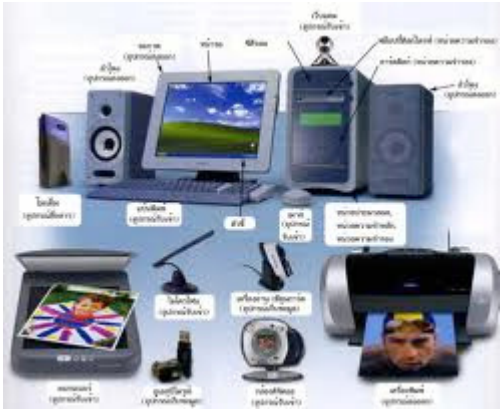
- วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากสำนักงานปลัดกระทรวงมหาดไทย

- การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็น ในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

- การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

ข้อ ๙ เครื่องแม่ข่ายทุกระบบงานจะอยู่ภายในห้องเครื่องแม่ข่าย ซึ่งมีระบบรักษาความปลอดภัยคือมีระบบตรวจสอบการเข้าออกห้อง ต้องมีการตรวจสอบก่อนว่ามีสิทธิ์ในการเข้าห้องหรือไม่ โดยมีประกาศเงื่อนไขการเข้าใช้ห้องติดไว้ที่หน้าห้องเครื่อง แม่ข่ายให้ทุกคนทราบ

๓.๗ นโยบายด้านการป้องกันการบุกรุกเครือข่าย (Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) Policy)



ข้อ ๑ IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในสำนักงานปลัดกระทรวงมหาดไทยให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ ๒ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของสำนักงานปลัดกระทรวงมหาดไทยและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๓ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ ๔ ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๕ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ ๖ มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

ข้อ ๗ มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำโดยผู้ดูแลระบบ

ข้อ ๘ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๙ เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลอย่างน้อยสัปดาห์ละ ๑ ครั้ง

ข้อ ๑๐ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จจะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

ข้อ ๑๑ พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบ

ข้อ ๑๒ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๓ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ ๑๔ สำนักงานปลัดกระทรวงมหาดไทยมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ ๑๕ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของสำนักงานปลัดกระทรวงมหาดไทย การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ **พระราชบัญญัติว่า**ด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของสำนักงานปลัดกระทรวงมหาดไทยจะต้องถูกดำเนินคดี ตามขั้นตอนของกฎหมาย

๓.๘ นโยบายด้านการป้องกันไวรัสแบบองค์การ

สำนักงานปลัดกระทรวงมหาดไทยมีการติดตั้งเครื่องแม่ข่ายป้องกันไวรัส ทำหน้าที่ Update signature หรือตัวป้องกันและทำลายไวรัสชนิดใหม่โดยจะทำการ update ฐานข้อมูลไวรัสตลอดเวลาที่มีการเปลี่ยนแปลงข้อมูลสำหรับเครื่องลูกข่ายที่อยู่ที่ส่วนกลางที่มีการติดตั้งโปรแกรมป้องกันไวรัสโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จะมีการกำหนดค่าของโปรแกรมให้ทำการ update ฐานข้อมูลไวรัสของเครื่องลูกข่ายทุกครั้งที่เปิดเครื่องจากเครื่องแม่ข่ายที่กำหนดไว้ สำหรับจังหวัดต่างๆ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีการติดตั้งเครื่องแม่ข่ายป้องกันไวรัสคอมพิวเตอร์ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเขต ๑-๑๒ เครื่องลูกข่ายของจังหวัด

ที่อยู่ภายใต้การดูแลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเขตใดก็จะติดต่อกับเครื่อง แม่ข่ายเขตนั้น โดยจะทำการ update ฐานข้อมูลไวรัสของเครื่องลูกข่ายทุกครั้งที่เปิดและเวลาเที่ยงวัน (๑๒.๐๐ น) จะทำการตรวจสอบ (scan) หาไวรัสคอมพิวเตอร์ในเครื่องลูกข่ายโดยอัตโนมัติ และโปรแกรมป้องกันไวรัสจะฆ่าไวรัสที่ติดในเครื่อง รวมทั้งป้องกันและตรวจจับไวรัสที่มากับระบบอินเทอร์เน็ตด้วย

นอกจากนี้ สำนักงานปลัดกระทรวงมหาดไทยมีการมอบหมายเจ้าหน้าที่รับผิดชอบในการแก้ไขปัญหาจากความเสี่ยง รวมทั้งผู้ทำหน้าที่ Backup and Recovery ทุกระบบ

เอกสารอ้างอิง

๑. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

๒. สำนักกำกับการใช้เทคโนโลยีสารสนเทศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. ๒๕๕๑. คู่มือการปฏิบัติแนวทางการป้องกันเพื่อหลีกเลี่ยงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, กรุงเทพฯ.

๓. นายพรเพชร วิชิตชลชัย. คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐. (๒๖ สิงหาคม ๒๕๕๔). http://www.mict.go.th/download/law/38_.pdf

๔. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย. ๒๕๕๔. ระบบการบริหารความเสี่ยงระบบสารสนเทศ สำนักงานปลัดกระทรวงมหาดไทย. กระทรวงมหาดไทย, กรุงเทพฯ.

คณะผู้จัดทำ

บรรณาธิการบริหาร

นายทรรศนะ วิชัยธนพัฒน์ ผู้อำนวยการสถาบันดำรงราชานุภาพ

ที่ปรึกษากองบรรณาธิการ

นายสงวน ธีระกุล ผู้เชี่ยวชาญเฉพาะด้านนโยบายและแผน

หัวหน้ากองบรรณาธิการ

นางณิทฐา แสวงทอง ผู้อำนวยการส่วนพัฒนาและบริหารจัดการความรู้

กองบรรณาธิการ

นางวันเพ็ญ ทรงวิวัฒน์ นางณิรมล เกิดแก้ว

น.ส.สุพัตรา บุญถึง นางกาญจนา แจ่มมินทร์

ศิลปกรรม/จัดทำรูปเล่ม

นางสาวอัจนา เตชะพันธุ์

ส่วนพัฒนาและบริหารจัดการความรู้ สถาบันดำรงราชานุภาพ
สำนักงานปลัดกระทรวงมหาดไทย โทร. ๐-๒๒๒๑-๕๙๕๘, ๕๐๕๕๖ (สื่อสาร สป.มท.)

พิมพ์ที่ บริษัท บพิธการพิมพ์ จำกัด 70 ถ.ราชบพิธ แขวงวัดราชบพิธ เขตพระนคร กทม. 10200
โทร. 0-2222-5555, 0-221-9781 โทรสาร 0-2221-6433 นายยอดยิ่ง โสภณ ผู้พิมพ์ผู้โฆษณา พ.ศ. 2555
E-mail Address : borpitt@hotmail.co.th