นโยบายและแนวปฏิบัติ

ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของสำนักงานพระพุทธศาสนาแห่งชาติ

ศูนย์เทคโนโลยีสารสนเทศ
สำนักงานพระพุทธศาสนาแห่งชาติ
www.onab.go.th

นโยบายและแนวปฏิบัติ

ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของสำนักงานพระพุทธศาสนาแห่งชาติ

ศูนย์เทคโนโลยีสารสนเทศ
สำนักงานพระพุทธศาสนาแห่งชาติ
www.onab.go.th
National office of Buddhism

คำนำ

ปัจจุบันระบบเครือข่ายคอมพิวเตอร์ มีความสำคัญต่อการดำเนินงานของหน่วยงานทั้งภาครัฐและเอกชน โดยแผ่ขยายไปในส่วนต่าง ๆ ขององค์กรที่ต้องการทำให้การเข้าถึงข้อมูลมีความรวดเร็ว ถูกต้องแม่นยำ สามารถติดต่อสื่อสารได้อย่างมีประสิทธิภาพ และประหยัดต้นทุนในการดำเนินงาน ส่งผลให้การเชื่อมต่อในระบบอินเทอร์เน็ตมีความจำเป็นและใช้งานกันอย่างแพร่หลาย ทั้งนี้พบว่าการติดตั้งเครือข่ายคอมพิวเตอร์เพื่อใช้ประโยชน์ในการปฏิบัติราชการและอำนวยความสะดวกในการติดต่อสื่อสาร มีความเสี่ยงสูงที่อาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติราชการได้ ซึ่งผู้ใช้บริการ และผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงควรตระหนักถึงการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างจริงจัง

ดังนั้น สำนักงานพระพุทธศาสนาแห่งชาติ จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานพระพุทธศาสนาแห่งชาติ เพื่อใช้เป็นมาตรฐานให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ อีกทั้งเป็นไปตามกฎหมายและข้อกำหนดของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยผ่านความเห็นชอบของคณะกรรมการธุรกรรมทางอิเลคทรอนิกส์ ตามความในมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ เรียบร้อยแล้ว อย่างไรก็ตามในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นสิ่งที่ต้องได้รับความร่วมมือจากบุคลากรของสำนักงานพระพุทธศาสนาแห่งชาติและผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ ที่ต้องถือปฏิบัติอย่างเคร่งครัดและสม่ำเสมอ รวมถึงต้องปรับปรุงให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว

หวังเป็นอย่างยิ่งว่า คู่มือ “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานพระพุทธศาสนาแห่งชาติ” ฉบับนี้ จะเป็นประโยชน์แก่ผู้ใช้บริการ ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของสำนักงานพระพุทธศาสนาแห่งชาติ ในการดูแลรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ต่อไป

ศูนย์เทคโนโลยีสารสนเทศ

สำนักงานพระพุทธศาสนาแห่งชาติ

มกราคม ๒๕๕๕

ประกาศสำนักงานพระพุทธศาสนาแห่งชาติ
เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานพระพุทธศาสนาแห่งชาติ

.....

ด้วยสำนักงานพระพุทธศาสนาแห่งชาติตระหนักถึงปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศ ซึ่งอาจส่งผลกระทบต่อภาครัฐที่มีการดำเนินงานในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร ประกอบกับสำนักงานพระพุทธศาสนาแห่งชาติได้นำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ในกิจการพระพุทธศาสนา ซึ่งถือเป็นหนึ่งในสามสถาบันหลักที่สำคัญของประเทศชาติ จึงเห็นความสำคัญที่จะนำกฎหมายและข้อบังคับต่าง ๆ มาบังคับใช้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานมีความมั่นคงปลอดภัยและน่าเชื่อถือ ตลอดจนมีมาตรฐานเป็นที่ยอมรับ สำนักงานพระพุทธศาสนาแห่งชาติจึงเห็นสมควรกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเพื่อบังคับใช้ต่อไป

ฉะนั้น อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ สำนักงานพระพุทธศาสนาแห่งชาติจึงได้จัดทำประกาศฉบับนี้เพื่อเป็นนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังต่อไปนี้

ข้อ ๑. คำนิยาม

(๑) หน่วยงาน หมายความว่า สำนักงานพระพุทธศาสนาแห่งชาติ

(๒) ผู้บริหาร หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างสำนักงานพระพุทธศาสนาแห่งชาติ

(๓) ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารองค์กร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

(๔) สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิเฉพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเครือข่ายและระบบสารสนเทศของหน่วยงาน

(๕) สินทรัพย์ หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพา อุปกรณ์ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์ รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

(๖) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

(๗) ความมั่นคงปลอดภัยด้านสารสนเทศ หมายความว่า การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน ความน่าเชื่อถือ และสภาพพร้อมใช้งานของสารสนเทศ

(๘) เหตุการณ์ด้านความมั่นคงปลอดภัย หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่เป็นไปได้ว่าจะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการที่ล้มเหลว หรือเหตุการณ์อันไม่สามารถรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๙) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดซึ่งอาจทำให้ระบบสารสนเทศขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

(๑๐) ระบบเครือข่าย หมายความว่า ระบบการสื่อสารระหว่างคอมพิวเตอร์จำนวนตั้งแต่สองเครื่องเชื่อมต่อกัน แบ่งเป็น ๒ แบบ คือ ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless LAN)

ข้อ ๒. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานพระพุทธศาสนาแห่งชาติ

(๑) ข้อมูลทั้งหมดในการดำเนินงานของหน่วยงาน ที่เป็นระบบอิเล็กทรอนิกส์ นับตั้งแต่กระบวนการสร้าง การจัดเก็บ การใช้งาน รวมถึงการทำลาย ต้องได้รับการรักษาความลับอย่างเหมาะสม

(๒) ข้อมูลทั้งหมดในการดำเนินงานของหน่วยงาน ต้องมีความถูกต้อง ครบถ้วนสมบูรณ์ และเป็นปัจจุบัน

(๓) สินทรัพย์ของหน่วยงาน ทั้งระบบสารสนเทศและระบบสำรองสารสนเทศต้องอยู่ในสภาพพร้อมใช้งานอยู่เสมอ

(๔) การเข้าถึงระบบสารสนเทศ ระบบเครือข่าย ระบบปฏิบัติการ และโปรแกรมประยุกต์ของหน่วยงานต้องได้รับการป้องกันการเข้าถึงและใช้งานสารสนเทศที่ไม่ได้รับอนุญาตอย่างเหมาะสม ทั้งจากการปฏิบัติงานภายในและภายนอกหน่วยงาน

(๕) ต้องจัดให้มีการบริหารจัดการความเสี่ยงของความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานอย่างเหมาะสม

(๖) ต้องจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินทางอิเล็กทรอนิกส์ที่มีประสิทธิภาพเพื่อความมั่นคงปลอดภัยด้านสารสนเทศอย่างต่อเนื่อง

(๗) ต้องจัดให้มีระเบียบ ประกาศ คำสั่ง ข้อปฏิบัติ และเอกสารที่เกี่ยวข้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน และเผยแพร่ด้วยการปิดประกาศและผ่านระบบอิเล็กทรอนิกส์ เพื่อใช้เป็นแนวทางปฏิบัติและเป็นไปตามกฎหมายที่เกี่ยวข้อง

(๘) ผู้ใช้งานต้องปฏิบัติตามกฎหมาย นโยบาย ระเบียบ คำสั่งและข้อปฏิบัติที่เกี่ยวข้อง ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานอย่างเคร่งครัด

(๙) ให้มีการติดตามประเมินผล และทบทวน การปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ตามระยะเวลา ๑ ครั้งต่อปี

ข้อ ๓. การรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงานพระพุทธศาสนาแห่งชาติ ครอบคลุมระบบงานในด้านต่าง ๆ ดังนี้

(๑) ด้านการรักษาความมั่นคงปลอดภัยทางด้านกายภาพ

(๒) ด้านการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย

(๓) ด้านการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย

(๔) ด้านผู้ดูแลระบบ (System Administrator)

(๕) ด้านการสำรองข้อมูล

(๖) ด้านการตรวจสอบและประเมินความเสี่ยง

(๗) ด้านความรับผิดชอบต่อความเสียหายของระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศ

สำนักงานพระพุทธศาสนาแห่งชาติมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศเป็นหน่วยงานหลักในการรับผิดชอบงานด้านการรักษาความมั่นคงปลอดภัย ตามข้อ ๓ ทั้งนี้ โดยให้อยู่ในอำนาจหน้าที่ และความรับผิดชอบของผู้อำนวยการสำนักงานพระพุทธศาสนาแห่งชาติ หรือรองผู้อำนวยการสำนักงานพระพุทธศาสนาแห่งชาติที่ได้รับมอบหมาย ในฐานะผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO)

ประกาศ ณ วันที่ ๓๐ เดือน กันยายน พ.ศ. ๒๕๕๔

(นายนพรัตน์ เบญจวัฒนานันท์)
ผู้อำนวยการสำนักงานพระพุทธศาสนาแห่งชาติ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานพระพุทธศาสนาแห่งชาติ

ตามประกาศสำนักงานพระพุทธศาสนาแห่งชาติ เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานพระพุทธศาสนาแห่งชาติ กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานพระพุทธศาสนาแห่งชาติ เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานพระพุทธศาสนาแห่งชาติ เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุมคามจากภัยต่าง ๆ ซึ่งอาจจะก่อให้เกิดความเสียหายต่อสำนักงานพระพุทธศาสนาแห่งชาติ นั้น

สำนักงานพระพุทธศาสนาแห่งชาติ จึงกำหนดแนวปฏิบัติในการใช้ระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

การรักษาความมั่นคงปลอดภัยด้านกายภาพ

ให้ศูนย์เทคโนโลยีสารสนเทศ สำนักงานพระพุทธศาสนาแห่งชาติ ปฏิบัติดังนี้

(๑) กำหนดพื้นที่ใช้งาน และพื้นที่ติดตั้ง รวมทั้งพื้นที่จัดเก็บอุปกรณ์ระบบสารสนเทศและระบบเครือข่าย

(๒) กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและระบบเครือข่าย

(๓) กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศและระบบเครือข่าย

(๔) จัดให้มีการบันทึกรายละเอียดการผ่านเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) ผ่านระบบพิสูจน์ตัวตน (Authentication) รวมถึงการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ โดยมีขั้นตอน ดังนี้

(๔.๑) กำหนดสิทธิ์เฉพาะเจ้าหน้าที่ที่รับผิดชอบ

(๔.๒) จัดเก็บรายละเอียดบุคคลด้วยวิธีสแกนลายนิ้วมือลงในฐานข้อมูล

(๔.๓) ระบบจะจัดเก็บข้อมูลบุคคลผู้เข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

(๕) กำหนดให้หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์มาเพื่อใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ของศูนย์เทคโนโลยีสารสนเทศ สำนักงานพระพุทธศาสนาแห่งชาติ โดยต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

การรักษาความมั่นคงปลอดภัยด้านการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย

(๑) ด้านการใช้งานระบบคอมพิวเตอร์ ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑.๑) ไม่ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน โดยมีวัตถุประสงค์เพื่อเผยแพร่ข้อมูลที่อาจกระทบกระเทือนต่อความมั่นคงและความสงบเรียบร้อยของชาติ ศาสนา และสถาบันพระมหากษัตริย์

(๑.๒) ไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

(๑.๓) ไม่กระทำการอันอาจก่อให้เกิดความเสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลของผู้อื่นโดยมิชอบ

(๑.๔) ไม่กระทำการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

(๑.๕) ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานอย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุดแก่ทางราชการ

(๑.๖) ไม่คัดลอกโปรแกรมต่างๆ ที่หน่วยงานเป็นเจ้าของลิขสิทธิ์อย่างถูกต้องตามกฎหมาย เพื่อนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๑.๗) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย

(๑.๘) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงาน เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานได้ เว้นแต่จะได้รับอนุญาต

(๑.๙) การป้องกันจากโปรแกรมประสงค์ร้าย (Malware) เครื่องคอมพิวเตอร์ที่ใช้งานภายในหน่วยงาน ต้องติดตั้งโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้ายรวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

(๑.๑๐) ทำการปรับปรุง (Update) โปรแกรมคอมพิวเตอร์อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

(๑.๑๑) ไม่ทำการปิดหรือยกเลิกหรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้าย (Malware) ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

(๑.๑๒) หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย ห้ามเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้ายไปยังเครื่องคอมพิวเตอร์อื่น ๆ และแจ้งผู้ดูแลระบบทราบ

(๑.๑๓) กรณีส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ผู้ใช้งานต้องสำรองข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

(๑.๑๔) ผู้ใช้งานต้องมีวิธีการป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์เข้าถึง สามารถเข้าถึงทรัพย์สินสารสนเทศที่อยู่ในความรับผิดชอบของตนเองโดยไม่มีเจ้าหน้าที่ดูแลได้ เช่น เมื่อหยุดใช้งานเครื่องคอมพิวเตอร์ให้ทำการล็อคหน้าจอ หรือเมื่อออกจากห้องปฏิบัติงานให้ล็อคประตู เป็นต้น

(๑.๑๕) ทรัพย์สินสารสนเทศที่สำคัญ ไม่ว่าจะเป็นเอกสาร หรือสื่อบันทึกข้อมูล ต้องไม่อยู่ในสถานที่ที่ไม่ปลอดภัย เช่น สามารถเข้าถึงได้ทางกายภาพ หรืออยู่ในที่สาธารณะ พบเห็นได้ง่าย เป็นต้น

(๑.๑๖) เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

(๑.๑๗) ตั้งรหัสผ่าน (Password) ในการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน

(๑.๑๘) ทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งาน

(๒) ด้านการใช้งานระบบเครือข่าย ระบบสารสนเทศ และระบบอินเตอร์เน็ต ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๒.๑) ผู้ใช้งานที่มีความประสงค์จะขอใช้เลขที่อยู่ไอพีสาธารณะ (Public IP Address) จะต้องทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย

(๒.๒) ไม่ทำการเปลี่ยนแปลงเลขที่อยู่ไอพี (IP Address) ของเครื่องคอมพิวเตอร์แบบตั้งโต๊ะภายในหน่วยงาน

(๒.๓) การใช้งานระบบอินเทอร์เน็ต ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น

(๒.๔) ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของหน่วยงาน

(๒.๕) ไม่นำเข้าหรือเผยแพร่ข้อมูลใด ๆ ที่ก่อให้เกิดความเสียหายแก่ผู้อื่น

(๒.๖) ไม่นำเข้าหรือเผยแพร่ข้อมูลใด ๆ ที่มีลักษณะสื่อลามกอนาจาร

(๒.๗) ไม่นำเข้าหรือเผยแพร่ข้อมูลใด ๆ ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่จะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

(๒.๘) ไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงานเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับหน่วยงาน

(๒.๙) ไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับการดำเนินงานต่าง ๆ ของหน่วยงาน ที่ยังไม่ได้ประกาศอย่างเป็นทางการ ผ่านระบบอินเทอร์เน็ตและกระดานสนทนาอิเล็กทรอนิกส์ รวมถึงการไม่เสนอความคิดเห็นหรือข้อความผ่านระบบอินเทอร์เน็ตและกระดานสนทนาอิเล็กทรอนิกส์ ที่ก่อให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน

(๒.๑๐) ไม่กระทำการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลของผู้อื่นที่อยู่ระหว่างการส่งในระบบสารสนเทศ และข้อมูลนั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

(๒.๑๑) ในการรับส่งข้อมูลคอมพิวเตอร์ หรือสารสนเทศ (Information) ผ่านทางระบบเครือข่าย ผู้ใช้งานต้องทำการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) ก่อนการรับส่งทุกครั้ง

(๒.๑๒) ไม่ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ของบุคคลอื่น

(๒.๑๓) ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุง (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

(๒.๑๔) หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) ให้ผู้ใช้งานทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

(๒.๑๕) ไม่ควรใช้บริการบนระบบอินเทอร์เน็ต (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) จำนวนมากหรือเป็นเวลานานในระหว่างเวลาทำงาน

(๒.๑๖) การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ผู้ใช้งานที่ต้องการขอลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ของหน่วยงานให้ยื่นคำขอต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อดำเนินการกำหนดสิทธิ์บัญชีผู้ใช้บริการรายใหม่และรหัสผ่านโดยผู้ใช้บริการไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึงและควรมีการเปลี่ยนรหัสผ่านโดยกำหนดระยะที่เหมาะสม

(๒.๑๗) ผู้ใช้งานไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน และเมื่อการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นผู้ใช้งานควรทำการลงบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้บริการไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

(๒.๑๘) ในการติดต่อ รับ-ส่งข้อมูลราชการ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงานเท่านั้น

(๒.๑๙) ไม่ฝ่าฝืนการเข้าถึงระบบสารสนเทศ ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน

(๒.๒๐) ไม่นำมาตรการป้องกันการเข้าถึงระบบสารสนเทศที่หน่วยงานจัดทำขึ้นเป็นการเฉพาะไปเปิดเผยโดยมิชอบ

(๒.๒๑) ต้องปรับปรุงข้อมูลสารสนเทศของหน่วยงานให้มีความถูกต้อง ครบถ้วน สมบูรณ์ และเป็นปัจจุบัน

การรักษาความมั่นคงปลอดภัยด้านการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย

(๑) ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ให้ศูนย์เทคโนโลยีสารสนเทศ ปฏิบัติดังนี้

(๑.๑) กำหนดมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศของหน่วยงาน เพื่อดูแลรักษาความปลอดภัย

(๑.๒) กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศโดยการแบ่งระดับผู้ใช้งานให้เหมาะสมกับอำนาจหน้าที่ โดยกำหนดให้ผู้บริหารสามารถสืบค้นข้อมูลได้ทุกระบบ ส่วนผู้ใช้งานสามารถค้นหาเพิ่มเติม แก้ไข หรือลบ ตามสิทธิ์ที่ถูกกำหนดไว้ และทบทวนสิทธิ์การเข้าถึงทุก ๖ เดือน โดยการจัดส่งบัญชีรายชื่อผู้ใช้งานให้หน่วยงานในสังกัด ทำการตรวจสอบความถูกต้อง เป็นปัจจุบัน และส่งคืนศูนย์เทคโนโลยีสารสนเทศเพื่อดำเนินการ

(๑.๓) จัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน

(๑.๔) การบริหารจัดการการเข้าถึงระบบสารสนเทศ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรของหน่วยงานที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน และควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน ดังนี้

(๑.๔.๑) ผู้ใช้งานแจ้งความประสงค์ต่อผู้บังคับบัญชาระดับต้น มายังศูนย์เทคโนโลยีสารสนเทศ

(๑.๔.๒) ดำเนินการเสนอขอความเห็นชอบจากผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย

(๑.๔.๓) ผู้ดูแลระบบ (System Administrator) ดำเนินการตามผลการพิจารณา

(๑.๔.๔) แจ้งผลการดำเนินการต่อผู้ร้องขอ

(๑.๕) บริหารจัดการรหัสผ่าน (Password Management) ที่มีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ ดังต่อไปนี้

(๑.๕.๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๑.๕.๒) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(๑.๕.๓) ควรกำหนดให้ผู้ใช้งาน ตอบยืนยันการได้รับรหัสผ่าน (Password)

(๑.๕.๔) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๑.๕.๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้บริการใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

(๑.๕.๖) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(๑.๖) บริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

(๑.๖.๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๑.๖.๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๑.๖.๓) กำหนดระยะเวลาการเข้าถึงข้อมูลครั้งละไม่เกิน ๑ ชั่วโมง

(๑.๖.๔) ตั้งค่าโปรแกรมให้ยุติการใช้งาน เมื่อไม่มีการใช้งานระบบสารสนเทศเกินเวลา ๑๕ นาที

(๑.๖.๕) การรับส่งข้อมูลสาคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

(๑.๖.๖) ควรกำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสาคัญของข้อมูล

(๑.๖.๗) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน

(๑.๗) ระบบสารสนเทศที่มีความสำคัญสูงต่อหน่วยงาน ต้องทำการแยกออกจากระบบสารสนเทศอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกองค์กร

(๒) ด้านการควบคุมการเข้าถึงระบบเครือข่าย ระบบอินเตอร์เน็ต ให้ศูนย์เทคโนโลยีสารสนเทศ ปฏิบัติดังนี้

(๒.๑) บริหารจัดการการใช้งานระบบเครือข่ายที่สำคัญ เช่น จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) ระบบอินทราเน็ต (Intranet) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบจากผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

(๒.๒) การนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย และต้องปฏิบัติตามนโยบายโดยเคร่งครัด

(๒.๓) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ ซึ่งการใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(๒.๔) ควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายในการเข้าสู่ระบบอินทราเน็ต (Intranet) เครื่องคอมพิวเตอร์แม่ข่าย (Server) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

(๒.๕) ควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ด้วยการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น และต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้ โดยมีขั้นตอนดังนี้

(๒.๕.๑) จัดแบ่งกลุ่มผู้ใช้งานตามการใช้งาน

(๒.๕.๒) จัดทำกลุ่มเครือข่ายย่อย (Virtual Lan) ตามกลุ่มผู้ใช้งานข้างต้น และมีการกำหนดสิทธิ์การเข้าถึง เพื่อควบคุมการเข้าใช้งาน

(๒.๖) ผู้ดูแลระบบ (System Administrator) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมายทราบทันที

(๒.๗) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย และต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

(๒.๘) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ผู้ดูแลระบบ (System Administrator) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

(๒.๙) ทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งานผู้ดูแลระบบ (System Administrator) ต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

(๒.๑๐) ผู้ดูแลระบบ (System Administrator) ควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

(๒.๑๑) ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

(๒.๑๒) ดำเนินการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

(๒.๑๓) กำหนดมาตรการควบคุมการใช้งานระบบเครือข่าย เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยบุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่าย ของหน่วยงานจะต้องทำเรื่องขออนุญาตจากผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย เพื่อขอรับชื่อผู้ใช้ และรหัสผ่านในการเข้าใช้งานระบบ

(๒.๑๔) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบสารสนเทศที่ไวต่อการรบกวน โดยมีการบริหารจัดการเครือข่ายเสมือนส่วนตัว (Virtual Privates Network : VPN) อย่างรัดกุมเพื่อไม่ให้เกิดผลกระทบต่อหน่วยงาน

(๒.๑๕) บริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

(๒.๑๖) การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่นๆ

(๒.๑๗) การเข้าสู่ระบบเครือข่ายภายในหน่วยงานโดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ ซึ่งเลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงานจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

(๒.๑๘) กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ โดยควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

(๒.๑๙) กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง และควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ อีกทั้งต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

(๓) ด้านการใช้งานบัญชีผู้ใช้ และรหัสผ่าน ผู้ใช้งานควรปฏิบัติดังนี้

(๓.๑) ผู้ใช้งานจะต้องเก็บรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น

(๓.๒) ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานร่วมกัน มิฉะนั้นเจ้าของชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการเข้าใช้งานของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

(๓.๓) ควรทำการเปลี่ยนรหัสผ่านเพื่อใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานอย่างน้อยทุก ๖ เดือน หรือเปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

(๓.๔) ขั้นตอนปฏิบัติสำหรับการติดตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัยดังนี้

(๓.๔.๑) เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์ที่ซื้อจากผู้ผลิต

(๓.๔.๒) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่าน

(๓.๔.๓) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๓.๔.๔) การใช้รหัสผ่าน (Password) ควรมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ตัวอักขระพิเศษและสัญลักษณ์ต่างๆ ด้วย

(๓.๔.๕) ไม่ควรกำหนดรหัสผ่านจากชื่อ หรือชื่อสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์ ซึ่งการตั้งรหัสผ่านต้องยากต่อการเดา และต้องมีความแตกต่างกัน

(๓.๔.๖) ควรหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น 123 , abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน เช่น 111 , aaa เป็นต้น

(๓.๔.๗) ควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ

การรักษาความมั่นคงปลอดภัยเกี่ยวกับผู้ดูแลระบบ (System Administrator)

ให้ผู้ดูแลระบบ (System Administrator) ปฏิบัติดังนี้

(๑) ดำเนินการติดตั้ง ตรวจสอบและปรับปรุงโปรแกรมคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและถูกต้อง ทันสมัยอยู่เสมอ

(๒) ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไข ป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้น พร้อมทั้งรายงานต่อผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย ทราบในทันที

(๓) ตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้บริการให้มีการกำหนดรหัสผ่าน (Password) รวมทั้งการเก็บรักษารหัสผ่าน (Password) และไม่ใช้อำนาจหน้าที่ของผู้ดูแลระบบ (System Administrator) ในการเข้าถึงข้อมูลของผู้ใช้ที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร และไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์ หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร รวมถึงไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบโดยไม่มีเหตุผลอันสมควร

(๔) กรณีเกิดสิ่งผิดปกติขึ้นจากการใช้งานของผู้ใช้ที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่อาจจะเกิดขึ้นแก่หน่วยงาน ให้ผู้ดูแลระบบพิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้บริการดังกล่าวได้ทันที

(๕) ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที รวมถึงดูแลรักษาและปรับปรุงบัญชีผู้ใช้งาน (Account) ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิ์การใช้งานของผู้ใช้บริการที่พ้นสภาพการเป็นผู้ใช้บริการ

(๖) เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็น เพื่อให้สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ต้องใช้วิธีการที่มั่นคงปลอดภัย โดยเก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบ (System Administrator) สามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ ซึ่งในการเก็บข้อมูลจราจรนั้นต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

(๗) เมื่อผู้ดูแลระบบ (System Administrator) พ้นจากหน้าที่จะต้องคืนสินทรัพย์ของหน่วยงานที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายตรวจสอบการคืนสินทรัพย์

การรักษาความมั่นคงปลอดภัยด้านการสำรองข้อมูล

ให้ศูนย์เทคโนโลยีสารสนเทศ ปฏิบัติดังนี้

(๑) กำหนดขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

(๒) จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงาน

(๓) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูลสัปดาห์ละ ๑-๒ ครั้ง โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองทุก ๓ เดือน ถ้าพบสิ่งผิดปกติให้ผู้ดูแลระบบรายงานต่อผู้บังคับบัญชาทราบทันที

(๔) จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

การรักษาความมั่นคงปลอดภัยด้านการตรวจสอบและประเมินความเสี่ยง

ให้ศูนย์เทคโนโลยีสารสนเทศ ปฏิบัติดังนี้

(๑) จัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน เพื่อเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ซึ่งเจ้าหน้าที่และหน่วยงานภายนอกจะต้องถือปฏิบัติอย่างเคร่งครัด

(๒) ตรวจสอบความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงาน เพื่อการประเมินความเสี่ยงที่อาจจะเกิดขึ้น

(๓) กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น ซึ่งกำหนดการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง โดยผู้ตรวจสอบภายในหน่วยงานของรัฐหรือผู้ตรวจสอบอิสระ

(๔) สร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน รวมถึงอุปกรณ์คอมพิวเตอร์ โดยการจัดฝึกอบรม สัมมนา และติดตามประเมินผลอย่างน้อยปีละ ๑ ครั้ง

ด้านความรับผิดชอบต่อความเสียหายของระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศ

ให้ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) มีหน้าที่ดังนี้

(๑) ตรวจสอบหาข้อเท็จจริง กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลยหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) พิจารณาความผิดและลงโทษตามเหตุอันสมควร

ที่ ทก ๐๒๐๙.๕/๔๓๕๖

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษาฯ
๑๒๐ อาคารรัฐประศาสนภักดี ถนนแจ้งวัฒนะ
เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

๑๙ ธันวาคม ๒๕๕๔

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำนักงานพระพุทธศาสนาแห่งชาติ

เรียน ผู้อำนวยการสำนักงานพระพุทธศาสนาแห่งชาติ

อ้างถึง หนังสือสำนักงานพระพุทธศาสนาแห่งชาติ ที่ พศ ๐๐๐๗/๐๒๘๘๐ ลงวันที่ ๓๐ มีนาคม ๒๕๕๔
เรื่อง การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานพระพุทธศาสนาแห่งชาติ

ตามหนังสือที่อ้างถึง สำนักงานพระพุทธศาสนาแห่งชาติจัดส่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานพระพุทธศาสนาแห่งชาติ พร้อมแบบประเมินฯ เพื่อขอความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ตามความในมาตรา ๗ วรรค ๑ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ นั้น

สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ในฐานะฝ่ายเลขานุการของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ขอแจ้งให้ทราบว่า ในการประชุมคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ครั้งที่ ๖/๒๕๕๔ วันศุกร์ที่ ๑๖ ธันวาคม ๒๕๕๔ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ มีมติเห็นชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานพระพุทธศาสนาแห่งชาติ และขอแจ้งให้หน่วยงานทราบเพื่อสร้างความเข้าใจเพิ่มเติมว่า แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐที่ผ่านความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เป็นมาตรฐานขั้นต่ำในการลดความเสี่ยงจากภัยคุกคามของระบบสารสนเทศ เพื่อก่อให้เกิดความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ หน่วยงานจะต้องให้ความสำคัญและจัดให้มีการตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ เพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัยในทางปฏิบัติ และอาจปรับปรุงมาตรการเพื่อรักษาความมั่นคงปลอดภัยตามความเหมาะสม

จึงเรียนมาเพื่อโปรดทราบ

เรียน ผู้อำนวยการสำนักงานพระพุทธศาสนาแห่งชาติ
เพื่อโปรดทราบ และแจ้งคณะกรรมการ พศ. ทราบด้วย
ขอแสดงความนับถือ

(นายวรพัฒน์ ทิวถนอม)
รองปลัดกระทรวง ปฏิบัติราชการแทน
ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

(นายอินทพร จั่นเอี่ยม)
ผู้อำนวยการกองกลาง
๖ ธ.ค. ๒๕๕๕

(นายกนก แสนประเสริฐ)
รองผู้อำนวยการสำนักงานพระพุทธศาสนาแห่งชาติ
ปฏิบัติราชการแทนผู้อำนวยการสำนักงานพระพุทธศาสนาแห่งชาติ

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
โทรศัพท์ ๐ ๒๑๔๑ ๖๙๙๑ โทรสาร ๐ ๒๑๔๓ ๘๐๓๖

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานพระพุทธศาสนาแห่งชาติ
พิมพ์เผยแพร่ พ.ศ. ๒๕๕๕

.....

ที่ปรึกษา

นายนพรัตน์	เบญจวัฒนานันท์	ผู้อำนวยการสำนักงานพระพุทธศาสนาแห่งชาติ
นายอำนาจ	บัวศิริ	รองผู้อำนวยการสำนักงานพระพุทธศาสนาแห่งชาติ
นายพนม	ศรศิลป์	รองผู้อำนวยการสำนักงานพระพุทธศาสนาแห่งชาติ
นายกนก	แสนประเสริฐ	รองผู้อำนวยการสำนักงานพระพุทธศาสนาแห่งชาติ

คณะผู้จัดทำ

นายปราณสุวีร์	อาวอร่ามรัศมิ์	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ
นางสาวรุ้งนภา	ตันติเสาวภาพ	นักวิชาการศาสนาชำนาญการ
นายธรรมนันท์	บัวจันทร์	นักวิชาการศาสนาชำนาญการ
นางสาวพิมพ์ใจ	เริ่มวัฒนะ	เจ้าพนักงานธุรการชำนาญงาน
นายศักดิ์ดา	ภู่สีสุวรรณ	เจ้าหน้าที่การเงินและบัญชีชำนาญงาน
นางสุนัน	บุตรน้ำเพ็ชร์	เจ้าพนักงานธุรการชำนาญงาน
นางสาวอำภา	อนุวัตพาณิชย์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ