ประกาศสถาบันนิติวิทยาศาสตร์

เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

พ.ศ. ๒๕๖๓

โดยที่เป็นการสมควรปรับปรุง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันนิติวิทยาศาสตร์ พ.ศ. ๒๕๖๒ ให้สอดคล้องกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. ๒๕๕๓ และแก้ไขเพิ่มเติม เพื่อให้ทำธุรกรรมทางอิเล็กทรอนิกส์ของสถาบันนิติวิทยาศาสตร์มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ ผู้อำนวยการสถาบันนิติวิทยาศาสตร์โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศสถาบันนิติวิทยาศาสตร์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๓"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ให้ยกเลิก แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันนิติวิทยาศาสตร์ พ.ศ. ๒๕๖๒

ข้อ ๔ นิยาม

"สถาบัน" หมายความว่า สถาบันนิติวิทยาศาสตร์

"หน่วยงาน" หมายความว่า หน่วยงานในสังกัดสถาบันนิติวิทยาศาสตร์

"ผู้ใช้งาน" หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบของสถาบันนิติวิทยาศาสตร์ ผู้บริหาร ผู้รับบริการ ผู้รับจ้างทำของ และผู้ใช้งานที่ใช้บริการระบบเทคโนโลยีสารสนเทศของสถาบันนิติวิทยาศาสตร์

"บัญชีผู้ใช้งาน" หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของสถาบันสถาบันนิติวิทยาศาสตร์

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

/"สินทรัพย์"...

"สินทรัพย์" หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามที่มีคุณค่าสำหรับหน่วยงาน

"สินทรัพย์คอมพิวเตอร์" หมายความว่า โปรแกรมคอมพิวเตอร์ เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และให้หมายความรวมถึงอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้องด้วย

"ข้อมูลอิเล็กทรอนิกส์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"สารสนเทศ" หมายความว่า การอนุญาต ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และเพื่อประโยชน์อื่นใด

"เครือข่าย" หมายความว่า ระบบการสื่อสารที่เป็นการเชื่อมต่อคอมพิวเตอร์ ตั้งแต่ ๒ เครื่องขึ้นไปเข้าด้วยกัน เพื่อสะดวกต่อการร่วมใช้ข้อมูล โปรแกรม หรือเครื่องพิมพ์ และอำนวยความสะดวกในการติดต่อแลกเปลี่ยนข้อมูลระหว่างเครื่องได้ตลอดเวลา

"ความมั่นคงปลอดภัยด้านสารสนเทศ" (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย" (Information Security Event) หมายความว่า การเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของสถาบันนิติวิทยาศาสตร์ ถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"นโยบาย" หมายความว่า หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมอิเล็กทรอนิกส์ซึ่งสถาบันนิติวิยาศาสตร์ จัดไว้ให้บริการประชาชน ซึ่งสถาบันสถาบันนิติวิทยาศาสตร์ประกาศไว้เพื่อให้เจ้าหน้าที่และผู้ปฏิบัติงานของสถาบันนิติวิทยาศาสตร์ ที่ต้องเกี่ยวข้องกับการดำเนินงานดังกล่าวได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกันและเพื่อให้มีการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับประกาศแนบท้ายพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

/"แนวปฏิบัติ"...

"แนวปฏิบัติ" หมายความว่า ขั้นตอนวิธีการที่สถาบัน ได้กำหนดไว้โดยภาพรวม สำหรับการปฏิบัติงาน ของเจ้าหน้าที่และผู้ปฏิบัติงานของสถาบัน ที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยมีจุดมุ่งหมาย เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์นั้น มีวิธีการที่มั่นคงปลอดภัย ทั้งนี้แต่ละหน่วยงานในสังกัดสถาบันนิติวิทยาศาสตร์ สามารถประกาศแนวปฏิบัติที่เฉพาะเจาะจงหรือเพิ่มเติมของตนได้ แต่ต้องไม่ขัดกับนโยบายและแนวปฏิบัติ ตามประกาศนี้

"ผู้บริหาร" หมายความว่า ผู้อำนวยการ รองผู้อำนวยการซึ่งผู้อำนวยการมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของสถาบันนิติวิทยาศาสตร์

"ผู้บริหารระดับสูงสุด" หมายความว่า ผู้อำนวยการซึ่งเป็นผู้รับผิดชอบการสั่งการตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันนิติวิทยาศาสตร์

ข้อ ๕ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันนิติวิทยาศาสตร์ มี ๒ ส่วน ดังนี้

(๑) นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(๒) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ข้อ ๖ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันนิติวิทยาศาสตร์ มี ๒ ส่วน ดังนี้

(๑) การกำหนดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ โดยมีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ ดังนี้

(ก) การเข้าถึงระบบสารสนเทศ ให้มีมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศของสถาบันนิติวิทยาศาสตร์ รวมถึงข้อมูลที่จัดเก็บรักษาในระดับชั้นความลับเพื่อป้องกันการเปิดเผย การล่วงรู้ หรือ การลักลอบทำสำเนาข้อมูล และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

(ข) การเข้าถึงระบบเครือข่าย ให้ผู้ดูแลระบบต้องกำหนดมาตรการรักษาความปลอดภัยเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ด้วยช่องทางต่าง ๆ ตามโครงสร้างระบบเครือข่ายที่ได้ออกแบบไว้ รวมทั้งจัดทำทะเบียนของอุปกรณ์เพื่อประโยชน์ในการบริหารจัดการการเข้าถึงได้อย่างเหมาะสม

(ค) การเข้าถึงระบบปฏิบัติการ ให้ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบปฏิบัติการ โดยให้ผู้ใช้งานยืนยันตัวตนด้วยรหัสผ่านที่มีคุณภาพและต้องบริหารจัดการการใช้งานโปรแกรมอรรถประโยชน์ให้ถูกต้องตามลิขสิทธิ์ที่สถาบัน มีอยู่ รวมทั้งควบคุมเวลาที่สามารถเข้าถึงระบบปฏิบัติการที่มีความเสี่ยง

/(ง) การเข้าถึง...

(ง) การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ ให้ผู้ดูแลระบบต้องจำกัดการเข้าถึงโปรแกรมประยุกต์ ให้เป็นไปตามหน้าที่ความรับผิดชอบของผู้ใช้งาน โดยมีการแยกกลุ่มระบบสารสนเทศที่มีความไวต่อการรบกวน ออกจากระบบอื่น ๆ รวมถึง ควบคุมการเข้าใช้งานระบบสารสนเทศจากเครือข่ายภายนอกสถาบันนิติวิทยาศาสตร์ ให้มีความปลอดภัย

(๒) การจัดระบบสารสนเทศและระบบสำรองของสารสนเทศ ให้อยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยกำหนดให้มีการตรวจสอบและควบคุมคุณภาพระบบงานเทคโนโลยีสารสนเทศ ดำเนินการตรวจประเมินระบบรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสถาบันนิติวิทยาศาสตร์ อย่างน้อยปีละ ๑ ครั้ง

(๔) การสร้างความรู้ความเข้าใจให้กับผู้ใช้งานของสถาบันนิติวิทยาศาสตร์ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ด้วยวิธีการ ดังนี้

(ก) เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์สถาบันนิติวิทยาศาสตร์ ให้แก่ผู้ใช้งานและบุคคลทั่วไปสามารถเข้าถึงได้

(ข) จัดอบรมให้ความรู้ความเข้าใจแก่ผู้ใช้งานในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training)

ข้อ ๗ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานนิติวิทยาศาสตร์ กระทรวงยุติธรรม พ.ศ. ๒๕๖๓ ที่กำหนดไว้ท้ายประกาศนี้

ข้อ ๘ การกำหนดชั้นความลับของสารสนเทศให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ และในกรณีที่มีการแก้ไขปรับปรุงกฎหมาย กฎ และระเบียบที่เกี่ยวข้อง ให้ถือปฏิบัติตามกฎหมาย กฎ และระเบียบที่ได้มี การแก้ไขปรับปรุงใหม่

ข้อ ๙ ต้องทบทวนและปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้มีความทันสมัย เป็นปัจจุบันและเป็นมาตรฐานที่ยอมรับได้ อย่างสม่ำเสมออย่างน้อยทุก ๑ ปี

/ข้อ ๑๐ กำหนด...

ข้อ ๑๐ กำหนดให้ผู้บริหารระดับสูงสุดเป็นผู้รับผิดชอบ ต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายอื่นใด ๆ แก่สถาบันนิติวิทยาศาสตร์ หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

รองผู้อำนวยการสถาบันนิติวิทยาศาสตร์ ในตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) เป็นผู้รับผิดชอบต่อนโยบาย ในฐานะกำกับดูแล ติดตาม ทบทวนแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันนิติวิทยาศาสตร์

ประกาศ ณ วันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๒

พันตำรวจโท

(ไพศิษฎ์ สังคหะพงศ์)

รองผู้อำนวยการสถาบันนิติวิทยาศาสตร์

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง CIO

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สถาบันนิติวิทยาศาสตร์

พ.ศ. ๒๕๖๓

กองสารสนเทศนิติวิทยาศาสตร์

กันยายน ๒๕๖๒

คำนำ

ตามที่สถาบันนิติวิทยาศาสตร์ ได้จัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้มีแนว ทางการรักษาความมั่นคงปลอดภัยสารสนเทศในการให้บริการอิเล็กทรอนิกส์ภาครัฐและเพื่อให้สอดคล้องตามพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

กองสารสนเทศนิติวิทยาศาสตร์ จึงจัดทำแนวปฏิบัติที่มีความสอดคล้องกับนโยบายดังกล่าว โดยเนื้อหาสาระโดยสังเขป ได้แก่ การอนุญาตการเข้าถึงสารสนเทศที่มีระดับชั้นความลับต่างกัน วิธีการเข้าถึงระบบสารสนเทศตามหน้าที่รับผิดชอบ วิธีการป้องกันการเข้าถึงทางเครือข่าย การบริหารจัดการสิทธิการเข้าถึง เป็นต้น รวมถึงการระบุหน้าที่รับผิดชอบของผู้ใช้งาน ผู้ปฏิบัติงานที่เกี่ยวข้อง ทั้งในด้านของผู้ที่ทำหน้าที่เป็นผู้ดูแลระบบ ผู้ดูแลเครือข่าย ผู้ดูแลฐานข้อมูล เป็นต้น

แนวปฏิบัติต่าง ๆ เหล่านี้จึงเป็นสิ่งสำคัญที่ผู้ปฏิบัติงานต้องถือปฏิบัติเพื่อให้เกิดความมั่นคง ปลอดภัยในการให้บริการต่าง ๆ ตามภารกิจของสถาบัน ผ่านการทำธุรกรรมอิเล็กทรอนิกส์ เพื่อสร้างความเชื่อมั่นให้กับประชาชนผู้ใช้บริการและสร้างความน่าเชื่อถือให้กับองค์กรต่อไป

แนวปฏิบัตินี้ จึงแบ่งเป็นหมวดเพื่อให้ง่ายต่อการอ้างอิงไปปฏิบัติ ประกอบด้วย

หมวด ๑ แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

หมวด ๒ แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

หมวด ๓ แนวปฏิบัติและหน้าที่ของผู้ดูแลระบบ/ผู้ดูแลเครือข่าย

หมวด ๔ แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย

หมวด ๕ แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

หมวด ๖ แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

หมวด ๗ แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

หมวด ๘ แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

หมวด ๙ แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

หมวด ๑๐ แนวปฏิบัติในการจัดซื้อจัดจ้างระบบเทคโนโลยีสารสนเทศ

หมวด ๑๑ แนวปฏิบัติในการเผยแพร่ข้อมูลสาธารณะ

สารบัญ

		หน้า
คำนิยาม		๑
หมวด ๑	แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ	๔
หมวด ๒	แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน	๑๔
หมวด ๓	แนวปฏิบัติและหน้าที่ของผู้ดูแลระบบ/ผู้ดูแลเครือข่าย	๒๐
หมวด ๔	แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย	๒๒
หมวด ๕	แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ	๒๖
หมวด ๖	แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันหรือสารสนเทศ	๒๘
หมวด ๗	แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน	๓๑
หมวด ๘	แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	๓๓
หมวด ๙	แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย	๓๔
หมวด ๑๐	แนวปฏิบัติในการจัดซื้อจัดจ้างระบบเทคโนโลยีสารสนเทศ	๓๗
หมวด ๑๑	แนวปฏิบัติในการเผยแพร่ข้อมูลสาธารณะ	๓๘

คำนิยาม

"สถาบัน" หมายถึง สถาบันนิติวิทยาศาสตร์

"หน่วยงาน" หมายถึง สำนักงาน กอง หรือที่เรียกชื่ออย่างอื่นในสังกัดสถาบัน

"สารสนเทศ" หมายความว่า ข้อมูลในรูปแบบต่าง ๆ ที่ได้จากการนำเข้าข้อมูลผ่านการประมวลผล ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและตามภารกิจของสถาบัน

"ระบบเทคโนโลยีสารสนเทศ" หมายความว่า ระบบงานของสถาบัน ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่สถาบัน สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร หารสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายความว่า ความมั่นคงปลอดภัยในบริบทของ การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) สภาพความพร้อมใช้งาน (Availability) ของสารสนเทศ สำหรับระบบเทคโนโลยีสารสนเทศของสถาบัน รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้าม ปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางการปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบเครือข่าย" หมายความว่า โครงข่ายคอมพิวเตอร์ที่เชื่อมโยงคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่าง ๆ เข้าด้วยกัน ซึ่งทำให้การสื่อสารข้อมูลระหว่างคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทั้งที่อยู่ภายในและภายนอก ทำให้สถาบัน สามารถติดต่อสื่อสารและแลกเปลี่ยนข้อมูลกันได้

"ระบบอินเทอร์เน็ต" หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของสถาบัน เข้ากับเครือข่ายคอมพิวเตอร์สากลเข้าด้วยกันโดยอาศัยเครือข่ายโทรคมนาคมเป็นตัวเชื่อมโยง

"ระบบอินทราเน็ต" หมายความว่า ระบบที่มีการเชื่อมต่อกับระบบเครือข่ายที่ให้บริการเฉพาะภายในสถาบันเท่านั้น

"เครื่องคอมพิวเตอร์" หมายความว่า เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพา

"อุปกรณ์คอมพิวเตอร์" หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อหรือทำงานเป็นส่วนหนึ่งของระบบคอมพิวเตอร์โดยอาจใช้ทำหน้าที่ เป็นอุปกรณ์สื่อสาร บันทึกข้อมูล หรือประมวลผลเป็นต้น

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจจะประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายด้วยธุรกรรมทางอิเล็กทรอนิกส์

"คอมพิวเตอร์ส่วนตัว" หมายความว่าเครื่องคอมพิวเตอร์ที่ไม่ใช่ทรัพย์สินของสถาบัน ซึ่งผู้ใช้งานนำมาใช้ภายในสถาบัน

"สื่อบันทึกพกพา" หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้งานการบันทึกหรือจัดเก็บข้อมูลชนิดพกพา ได้แก่ Flash Drive หรือ Handy Drive หรือ Thump Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น

"ผู้บริหารระดับสูง" หมายความว่า ผู้อำนวยการสถาบันนิติวิทยาศาสตร์ และรองผู้อำนวยการสถาบันนิติวิทยาศาสตร์

"ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง" หมายความว่า ผู้บริหารระดับสูงที่ได้รับการแต่งตั้งให้เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ CIO ของสถาบัน

"ผู้บังคับบัญชา" หมายความว่า หัวหน้าหน่วยงานของผู้ปฏิบัติหน้าที่ในระบบเทคโนโลยีสารสนเทศของสถาบัน

"ผู้ใช้งาน" หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างเหมาบริการในสังกัดสถาบันนิติวิทยาศาสตร์ และให้ความหมายรวมถึงบุคคลในสถาบัน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของสถาบัน

"ผู้ดูแลระบบ" หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลหรือบริหารจัดการระบบเทคโนโลยีสารสนเทศของสถาบัน

"ผู้ดูแลเครือข่าย" หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลหรือบริหารจัดการระบบเครือข่ายของสถาบัน

"ผู้ดูแลฐานข้อมูล" หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลหรือบริหารจัดการระบบฐานข้อมูลของสถาบัน

"หน่วยงานภายนอก" หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

"สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของสถาบัน

"บัญชีผู้ใช้บริการ" หมายความว่า รายชื่อผู้มีสิทธิใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของหน่วยงาน

"รหัสผ่าน" หมายความว่า ตัวอักษรหรืออักขระตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัย ของข้อมูลและระบบเทคโนโลยีสารสนเทศ

"สื่อลามกอนาจาร" หมายความว่า สื่อประเภทอันเป็นที่น่ารังเกียจ น่าอับอาย นอกรีต นอกแบบผิดปกติไปจากศีลธรรมอันดีของประชาชน

"เหตุฉุกเฉิน" หมายความว่า เหตุที่ก่อให้เกิดเป็นปัญหาการทำงานของระบบและนำมาซึ่งการหยุดชะงัก ของระบบ

"เหตุวิบัติภัย" หมายความว่า เหตุที่ทำให้เกิดความเสียหายและก่อให้เกิดการหยุดชะงักต่อกระบวนการสำคัญทางนิติวิทยาศาสตร์ของสถาบัน ได้แก่ ไฟไหม้ การถูกปิดล้อม ไฟฟ้าดับ การก่อวินาศกรรม เป็นต้น

"โปรแกรมมาตรฐาน" หมายความว่า โปรแกรมที่สถาบัน กำหนดให้เป็นโปรแกรม มาตรฐานสำหรับให้ผู้ใช้งานใช้งานได้ตามปกติ

"โปรแกรมประสงค์ร้าย" หมายความว่า โปรแกรมคอมพิวเตอร์ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาเพื่อวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่ายเช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spy ware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือ ฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

"ลิขสิทธิ์" หมายความว่า สิทธิที่ได้รับแต่เพียงผู้เดียวตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๗ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น

"จดหมายอิเล็กทรอนิกส์" หมายความว่า การส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเทคโนโลยี สารสนเทศ ซึ่งมีความหมายตรงกับคำภาษาอังกฤษว่า Electronic Mail หรือ E-mail

หมวด ๑
แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

ผู้รับผิดชอบ

๑. กองสารสนเทศนิติวิทยาศาสตร์

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ ๑ การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล

๑. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องจัดการควบคุมการเข้าถึงระบบสารสนเทศของสถาบัน ดังนี้

๑.๑. ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ตนต้องใช้งานได้ก็ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบข้อมูล และ/หรือ ผู้รับผิดชอบระบบสารสนเทศตามความจำเป็นต่อการใช้งานแล้วเท่านั้น

๑.๒. ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบ กล่าวคือ ในการขออนุญาตเข้าระบบสารสนเทศนั้น ผู้ใช้จะต้องมีการทำเป็นบันทึกและกรอกแบบเอกสารที่สถาบัน กำหนดเพื่อขออนุญาตเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดย ผู้บังคับบัญชาหรือผู้รับมอบอำนาจจากผู้บังคับบัญชาเพื่อการจัดเก็บไว้เป็นหลักฐาน จากนั้นผู้ดูแลระบบจะสร้างบัญชีสำหรับการเข้าถึงโดยอนุญาตเฉพาะในส่วนที่จำเป็น และโดยคำนึงถึงประเภทข้อมูล และชั้นความลับ

๑.๓. ผู้ดูแลระบบ ต้องกำหนดไม่ให้ผู้ใช้งานเข้าสู่ระบบได้ หากผู้ใช้งานใส่รหัสผ่านเข้าระบบผิด ๓ ครั้ง จนกว่าจะยื่นเรื่องพร้อมหลักฐานแสดงความเป็นตัวตนต่อเจ้าหน้าที่ดูแลระบบ เพื่อขอรหัสใหม่อีกครั้ง

๑.๔. ผู้ดูแลระบบ ต้องกำหนดให้การ Log-in เพื่อเข้าใช้ระบบสารสนเทศใด ๆ จะต้องมีการตรวจจับการเปิดระบบสารสนเทศไว้ เมื่อไม่มีการใช้งาน จะทำการ Log-Out ระบบให้อัตโนมัติ ในระยะเวลาที่เหมาะสม

๑.๕. ผู้รับผิดชอบข้อมูลและผู้รับผิดชอบระบบสารสนเทศต้องอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบสารสนเทศต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๑.๖. กำหนดระยะเวลาการเข้าถึงระบบสารสนเทศของสถาบัน ได้ตลอด ๒๔ ชั่วโมง

๒. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องจัดการรักษาความปลอดภัยทางกายภาพ (Physical Security Management) ดังนี้

๒.๑. กำหนดระดับความสำคัญของพื้นที่ หรือจำแนกพื้นที่ที่ใช้งานกับพื้นที่ที่มีการควบคุม

๒.๒. ดำเนินการทดสอบระบบควบคุมการเข้าถึงพื้นที่ทางกายภาพเพื่อตรวจสอบยังใช้งานได้ตามปกติ หรือไม่

๒.๓. ผู้ปฏิบัติงานต้องปิดประตูและหน้าต่างให้ล็อคอยู่เสมอ

๓. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องจัดการควบคุมการเข้า-ออกพื้นที่ควบคุม (Restricted Area) ได้แก่ ห้องคอมพิวเตอร์แม่ข่าย (Server Room) ของกองสารสนเทศนิติวิทยาศาสตร์และกองสารพันธุกรรม ดังนี้

๓.๑. ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาเยือน

๓.๒. ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญ จนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๓.๓. จัดให้มีกลไกการอนุญาตการเข้าถึงพื้นที่ หรือบริเวณที่มีความสำคัญของสถาบัน โดยบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๓.๔. มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๓.๕. ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

๓.๖. มีการพิสูจน์ตัวตน ด้วยวิธีต่อไปนี้อย่างใดอย่างหนึ่ง ได้แก่ การแสดงบัตรผ่านเพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ

๓.๗. จัดเก็บบันทึกการเข้า-ออก สำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๓.๘. บุคคลภายนอกที่มิใช่ ข้าราชการ และพนักงานราชการสังกัด ต้องติดบัตรให้สามารถสังเกตเห็นได้ชัดเจนตลอดระยะเวลาการทำงาน

๓.๙. ต้องจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๓.๑๐. จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๓.๑๑. ต้องติดตั้งกล้องวงจรปิดในพื้นที่ควบคุม พร้อมจัดเก็บบันทึกดังกล่าวเป็นเวลาอย่างน้อย ๑ ปี

๔. ผู้รับผิดชอบระบบสารสนเทศ ต้องกำหนดการจัดวางและการป้องกันฮาร์ดแวร์และอุปกรณ์ต่าง ๆ ดังนี้

๔.๑. จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงของบุคคลภายนอก

๔.๒. อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่มีความมั่นคงปลอดภัยเพียงพอ

๔.๓. ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในศูนย์คอมพิวเตอร์ (Data Center) ของสถาบัน

๔.๔. ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว ได้แก่ การตรวจสอบ ระดับอุณหภูมิ ความชื้น ให้อยู่ในระดับปกติอย่างสม่ำเสมอ

๕. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องกำหนดระบบและอุปกรณ์สนับสนุนการทำงาน ดังนี้

๕.๑. มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

๕.๑.๑. ระบบสำรองกระแสไฟฟ้า (UPS) สำหรับศูนย์คอมพิวเตอร์ของสถาบัน (Data Center)

๕.๑.๒. ระบบระบายอากาศ

๕.๑.๓. ระบบปรับอากาศ

๕.๒. ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากความล้มเหลวในการทำงานของระบบ

๕.๓. ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในศูนย์คอมพิวเตอร์ของสถาบัน ทำงานผิดปกติหรือหยุดการทำงาน

๖. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องกำหนดการบำรุงรักษาอุปกรณ์ ดังนี้

๖.๑. ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

๖.๒. ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๖.๓. จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๖.๔. จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ ดังกล่าว

๖.๕. ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วย

๖.๖. จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๗. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องควบคุมการนำอุปกรณ์คอมพิวเตอร์ของสถาบัน ออกนอกหน่วยงาน ดังนี้

๗.๑. ให้มีการขออนุญาตก่อนนำสิ่งอุปกรณ์หรือทรัพย์สินออกนอกหน่วยงาน

๗.๒. บันทึกข้อมูลการนำสิ่งอุปกรณ์ของสถาบัน ออกนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๘. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องจัดการป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน

๘.๑. กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์คอมพิวเตอร์ของสถาบัน ออกไปใช้งานนอกสถานที่

๘.๒. ห้ามผู้ใช้งานละทิ้งอุปกรณ์คอมพิวเตอร์ของสถาบัน ไว้โดยลำพังในที่สาธารณะ

๘.๓. ให้ผู้ใช้งานรับผิดชอบดูแลอุปกรณ์คอมพิวเตอร์ของสถาบัน เสมือนเป็นทรัพย์สินของตนเอง

๙. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องควบคุมการจำหน่ายอุปกรณ์คอมพิวเตอร์หรือ การนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง ดังนี้

๙.๑. ให้ทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะแทงจำหน่ายอุปกรณ์ดังกล่าว โดยปฏิบัติตามแนวปฏิบัติฯ หมวด ๒ ข้อ ๓.๕

๙.๒. มีมาตรการหรือเทคนิค ในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญ ในอุปกรณ์สำหรับจัดเก็บข้อมูล ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

ส่วนที่ ๒ การบริหารจัดการสิทธิการเข้าถึง

๑. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องปฏิบัติเพื่อจัดเก็บข้อมูล ดังนี้

๑.๑. จัดประเภทของข้อมูล ออกเป็น

๑.๑.๑. ข้อมูลทั่วไป คือ ข้อมูลเกี่ยวกับสถาบัน ข้อมูลสถิติการตรวจพิสูจน์ ข้อมูลสถิติทั่วไป ข้อมูลประชาสัมพันธ์ ข้อมูลยุทธศาสตร์และแผนปฏิบัติงาน ข้อมูลประกาศจัดซื้อจัดจ้าง

๑.๑.๒. ข้อมูลสารสนเทศด้านกฎหมาย คือ ระเบียบ ข้อบังคับ นโยบาย แนวปฏิบัติ และกฎหมายต่าง ๆ

๑.๑.๓. ข้อมูลสารสนเทศด้านการบริหารจัดการ คือ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำร้อง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี ข้อมูลพัสดุ ข้อมูลเอกสารคุณภาพ ข้อมูลเกี่ยวกับอุปกรณ์เครือข่ายและโครงสร้างเครือข่าย

๑.๑.๔. ข้อมูลสารสนเทศด้านนิติวิทยาศาสตร์ คือ ข้อมูลการตรวจพิสูจน์ทางด้านนิติวิทยาศาสตร์ ข้อมูลรายงานผลการตรวจพิสูจน์ ข้อมูลเอกสารสำเนารายงานผลการตรวจพิสูจน์

๑.๒. จัดแบ่งระดับชั้นการเข้าถึง

๑.๒.๑. ระดับชั้นสำหรับผู้บริหาร

๑.๒.๒. ระดับชั้นสำหรับผู้ใช้งานทั่วไป

๑.๒.๓. ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๑.๓. การกำหนดเวลาที่เข้าถึงได้ ผู้ดูแลระบบจะต้องกำหนดเวลาให้ผู้ใช้งานสามารถเข้าถึงระบบงานสารสนเทศ ตามความเหมาะสมในการปฏิบัติงานของผู้ใช้งาน ดังนี้

๑.๓.๑. ตลอดเวลา (๒๔ ชั่วโมง)

๑.๓.๒. ภายในเวลาราชการ (๘.๓๐ - ๑๖.๓๐ นาฬิกา)

๑.๓.๓. นอกเวลาราชการ (๑๖.๓๑ - ๘.๒๙ นาฬิกา)

๑.๓.๔. อื่น ๆ ตามภารกิจที่สถาบัน มอบหมาย

๑.๔. การกำหนดช่องทางที่สามารถเข้าถึงได้ ผู้ดูแลระบบจะต้องบริหารจัดการให้มีการรักษาความปลอดภัยอย่างเหมาะสมสำหรับการเข้าถึงระบบงานสารสนเทศด้วยช่องทาง ดังนี้

๑.๔.๑. ทางการเชื่อมต่อด้วยสายสัญญาณ (Wired Access)

๑.๔.๒. ทางการเข้าถึงตรงที่เครื่องแม่ข่าย (Local Access)

๑.๔.๓. ทางการเชื่อมต่อผ่านทางอินเทอร์เน็ต (Internet Access)

๒. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องจัดให้มีการลงทะเบียนผู้ใช้งาน (User Registration) โดยกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาต

๓. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน ดังนี้

๓.๑. ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานภายในสถาบัน จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาและผู้ดูแลระบบที่ได้รับมอบหมาย จากนั้นจึงส่งเอกสารดังกล่าวมายังกองสารสนเทศนิติวิทยาศาสตร์ เพื่อดำเนินการเพิ่มสิทธิการเข้าถึงของระบบดังกล่าว

๓.๒. กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชา และผู้ดูแลระบบที่ได้รับมอบหมายเป็นลายลักษณ์อักษร จากนั้นจึงส่งเอกสารดังกล่าวมายังกองสารสนเทศนิติวิทยาศาสตร์ เพื่อดำเนินการกำหนดสิทธิรวม ทั้งนี้ต้องมีการทบทวนการกำหนดสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๓.๓. กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ โดยกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้

๓.๓.๑. อ่านอย่างเดียว

๓.๓.๒. สร้างข้อมูล

๓.๓.๓. ป้อนข้อมูล

๓.๓.๔. แก้ไข

๓.๓.๕. อนุมัติ

๓.๓.๖. ไม่มีสิทธิ

๓.๔. กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยผู้ร้องขอใช้สิทธิพิเศษนั้นจะต้องส่งคำขอเป็นลายลักษณ์อักษร เพื่อใช้เป็นปัจจัยในประกอบการพิจารณาเพื่อขอความเห็นชอบและอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาสูงสุดของสถาบัน

๓.๔.๑. ควบคุมการใช้งานอย่างเข้มงวด โดยมีการกำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๓.๔.๒. กำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๓.๔.๓. มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดเมื่อหมดความจำเป็นในการใช้งานทุกครั้ง หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน

๔. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องบริหารจัดการบัญชีผู้ใช้บริการ (User Account) และรหัสผ่านของผู้ใช้งาน ดังนี้

๔.๑. กำหนดบัญชีชื่อผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน ไม่อนุญาตให้ผู้ร้องขอใช้ระบบงานสารสนเทศเข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้น

๔.๒. จัดเก็บข้อมูลการลงทะเบียนของผู้ที่ร้องขอใช้ระบบไว้เพื่อเอาไว้ใช้อ้างอิงหรือตรวจสอบในภายหลัง

๔.๓. ทบทวนบัญชีผู้ใช้งานทั้งหมดอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้งเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทางดังนี้

๔.๓.๑. พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงานภายในของสถาบัน

๔.๓.๒. จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานภายในสถาบัน เพื่อดำเนินการทบทวนว่ามีรายชื่อที่ออกไปแล้ว หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้มีการแก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่

๔.๓.๓. ผู้บังคับบัญชาของหน่วยงานภายในสถาบัน แจ้งกลับว่ามีรายชื่อใดที่ต้องดำเนินการแก้ไขให้ถูกต้อง

๔.๓.๔. ดำเนินการแก้ไขข้อมูลสิทธิให้ถูกต้องตามที่ได้รับแจ้ง

๕. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องจัดให้มีการพิสูจน์ตัวตน เพื่อเข้าใช้ระบบสารสนเทศสำคัญ สำหรับผู้ใช้ที่อยู่ภายนอก ดังนี้

๕.๑. การแสดงตัวตนด้วยชื่อบัญชีผู้ใช้งาน

๕.๒. การพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน

๕.๓. การเข้าสู่ระบบสารสนเทศสำคัญของสถาบัน ผ่านเครือข่ายอินเทอร์เน็ตนั้น จะมีการตรวจสอบผู้ใช้งานด้วย

๕.๔. เพื่อเพิ่มความปลอดภัยในการเข้าสู่ระบบสารสนเทศสำคัญของสถาบันจากระยะไกล จะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน โดยการใช้รหัสผ่าน และการเข้ารหัสช่องทางการสื่อสาร

๖. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องมีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

๖.๑. มีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับผู้ใช้งานระบบ

๖.๒. ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้น

ระยะเวลา ดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าขึ้นได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานปกติ

๗. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องควบคุมการใช้งานรหัสผ่านของผู้ใช้งานระบบตามแนวทางปฏิบัติ ดังนี้

๗.๑. ต้องกำหนดข้อปฏิบัติสำหรับการใช้งานรหัสผ่านของผู้ใช้งานระบบให้มีความมั่นคงปลอดภัย

๗.๒. ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๗.๓. เมื่อผู้ใช้งานระบบลาออกหรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิการใช้งานให้หน่วยงานแจ้งผู้รับผิดชอบระบบสารสนเทศโดยทันที เพื่อเปลี่ยนสิทธิหรือถอดถอนสิทธิของผู้ที่ลาออกออกจากระบบทันทีที่ได้รับแจ้ง

๗.๔. เมื่อผู้ใช้งานได้รับรหัสผ่านจากระบบสารสนเทศหรือผู้ดูแลระบบ ให้ผู้ใช้งานทำการเปลี่ยนรหัสผ่านทันที เมื่อเข้าใช้งานครั้งแรก และควรทำการเปลี่ยนรหัสผ่านทุก ๓ เดือน หรือเปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่ารหัสผ่านนั้นอาจรั่วไหล

๗.๕. การส่งมอบรหัสผ่านให้กับเจ้าหน้าที่ต้องเป็นไปอย่างปลอดภัยโดยใส่ซองปิดผนึกและส่งไปยังผู้ใช้งานรวมทั้งแจ้งให้ผู้ใช้งานเก็บรักษารหัสผ่านเป็นความลับและเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดผู้ใช้งานจะต้องเก็บรักษารหัสผ่านที่ได้มาโดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผย หรือกระทำใดให้ผู้อื่นทราบ โดยมิได้รับอนุญาตจากผู้บังคับบัญชา

ส่วนที่ ๓ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

ผู้บังคับบัญชาหน่วยงานภายในสถาบัน ต้องจัดให้มีวิธีการจัดการ การเข้าถึงข้อมูลตามระดับชั้นความลับ ซึ่ง เบื้องต้น สถาบัน ใช้แนวทางตาม "พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐" และระเบียบที่ เกี่ยวข้อง ในการกำหนดชั้นความลับของข้อมูล จึงกำหนดให้มีแนวทางปฏิบัติ ดังนี้

๑. ประเภทของข้อมูล แบ่งออกเป็น ๒ ประเภท ดังนี้
   - ๑.๑. ข้อมูลประเภทเอกสาร ได้แก่ ข้อมูลที่มีการเขียนหรือพิมพ์ลงบนกระดาษ
   - ๑.๒. ข้อมูลประเภทอิเล็กทรอนิกส์ ได้แก่ ไฟล์ข้อมูลต่าง ๆ
๒. ลำดับความสำคัญ หรือ ลำดับชั้นความลับของข้อมูล แบ่งออกเป็น ๔ ระดับ ดังนี้
   - ๒.๑. ลับ (Top Secret / Secret / Confidential)
   - ๒.๒. ใช้ภายในเท่านั้น (Internal Use)
   - ๒.๓. ส่วนบุคคล (Personal)
   - ๒.๔. เปิดเผยได้ (Public)
๓. ระดับชั้นการเข้าถึง แบ่งออกเป็น ๓ ระดับ ดังนี้
   - ๓.๑. ระดับชั้นสำหรับผู้บริหาร
   - ๓.๒. ระดับชั้นสำหรับผู้ดูแลระบบ หรือ ผู้ที่ได้รับมอบหมาย
   - ๓.๓. ระดับชั้นสำหรับผู้ใช้งานทั่วไป
๔. เวลาที่ได้เข้าถึง การกำหนดเวลาที่ได้เข้าถึงสารสนเทศของสถาบัน ได้กำหนดให้สามารถเข้าถึงระบบสารสนเทศได้ตลอดเวลา ๒๔ ชั่วโมง ไม่เว้นวันหยุดราชการ หรือวันหยุดนักขัตฤกษ์
๕. ช่องทางการเข้าถึง การกำหนดจำนวนช่องทางในการเข้าถึงระบบสารสนเทศของสถาบัน ต้องกำหนดให้เข้าถึง ได้ทั้งภายในและภายนอก โดยเชื่อมต่อผ่าน Intranet Internet การติดต่อด้วยตนเอง โทรศัพท์ โทรสาร หนังสือ บันทึกข้อความ จดหมายอิเล็กทรอนิกส์ (E-mail)
๖. ผู้ใช้งาน ปฏิบัติตามแนวทางกำหนดชั้นความลับของข้อมูลตาม "ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔"
๗. ในการจัดการกับไฟล์ข้อมูลลับ ให้ปฏิบัติดังนี้
   - ๗.๑. จัดหมวดหมู่ข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือที่มีระดับความสำคัญสูงไว้ต่างหาก และป้องกันให้มีความปลอดภัยอย่างพอเพียงต่อการเข้าถึงและต้องแสดงชั้นความลับบนไฟล์ข้อมูลลับ ด้วยวิธีการ ทำลายน้ำ หรือวิธีอื่น ๆ โดยต้องแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว
   - ๗.๒. การสำเนาข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูงต้องได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูล

๗.๓. ระมัดระวังการกระจาย หรือแจกจ่ายข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับของสถาบัน ไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

๗.๔. ผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ต้องตรวจสอบความถูกต้องของข้อมูลอิเล็กทรอนิกส์ก่อนนำไปใช้งาน

๗.๕. ห้ามผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือที่มีระดับความสำคัญสูง ส่งข้อมูลดังกล่าวไปทางไปรษณีย์ เว้นแต่จะได้ใช้วิธีเข้ารหัสที่สถาบัน กำหนดไว้

๗.๖. ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยคำนึงถึงการป้องกันด้วยวิธีต่าง ๆ ได้แก่

๗.๖.๑. การใช้รหัสผ่านที่มีความมั่นคงปลอดภัย

๗.๖.๒. การอัพเดทข้อมูลในระบบป้องกันไวรัสอย่างสม่ำเสมอ

๗.๖.๓. การติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์

๗.๗. ห้ามแชร์ไฟล์ข้อมูลลับบนเครือข่ายของสถาบัน เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการแชร์ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้

๗.๘. ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

๗.๙. ต้องทำลายข้อมูลอิเล็กทรอนิกส์บนฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์ที่ถูกยกเลิกการใช้งาน

หมวด ๒
แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

ผู้รับผิดชอบ

๑. กองสารสนเทศนิติวิทยาศาสตร์

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องมีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements For Access Control) โดยแบ่งการจัดทำข้อปฏิบัติ เป็น ๒ ส่วนคือ

๑.๑. มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และ สิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

๑.๒. มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของสถาบัน ในขณะที่ไม่มีผู้ดูแล ดังนี้

๒.๑. ต้องจัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ไว้ในห้องเก็บครุภัณฑ์ที่มีการรักษาความปลอดภัยเพื่อป้องกันการสูญหาย

๒.๒. ผู้ใช้งานต้องไม่ทิ้งเครื่องคอมพิวเตอร์และอุปกรณ์ไว้โดยไม่มีผู้ดูแล

๒.๓. เข้ารับการฝึกอบรมที่มีเนื้อหาเกี่ยวกับการให้ความรู้ ความตระหนัก ด้านการรักษาความมั่งคงปลอดภัยสารสนเทศที่สถาบัน จัดขึ้นอย่างสม่ำเสมอ

๒.๔. ต้องออกจากระบบสารสนเทศ (Log Off) ทันทีที่เสร็จสิ้นการใช้งาน

๒.๕. ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลาตามที่เหมาะสม และต้องใส่รหัสผ่านให้ ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๓. การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk And Clear Screen Policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

๓.๑. มีการกำหนดมาตรการป้องกันทรัพย์สินขององค์กร และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องต่าง ๆ ได้แก่

๓.๑.๑ ต้องจัดเก็บคอมพิวเตอร์และอุปกรณ์ให้อยู่บริเวณที่ปลอดภัย โดยไม่วางในบริเวณที่เสี่ยงต่อการสูญหาย

๓.๑.๒ ในกรณีที่มีบุคคลภายนอกเข้ามาติดต่องานหรือปฏิบัติงาน ให้ปฏิบัติตามแนวปฏิบัติฯ หมวด ๑ ส่วนที่ ๑ ข้อ ๓

๓.๑.๓ ต้องไม่เปิดระบบสารสนเทศที่ใช้งานอยู่ทิ้งไว้โดยไม่มีผู้ดูแล

๓.๑.๔ ต้องไม่วางอุปกรณ์คอมพิวเตอร์ไว้ในบริเวณที่สามารถหยิบฉวยได้โดยง่าย

๓.๑.๕ ต้องไม่วางเอกสารสำคัญไว้ในบริเวณที่เสี่ยงต่อการสูญหาย หรือ ลักลอบอ่านได้ง่าย

๓.๒. การป้องกันต้องมีความสอดคล้องกับเรื่องต่าง ๆ ดังนี้

๓.๒.๑ แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ

๓.๒.๒ กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ

๓.๒.๓ วัฒนธรรมองค์กร

๓.๓. มีการป้องกันเครื่องคอมพิวเตอร์ โดยให้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

๓.๔. มีการกำหนดขอบเขตการป้องกัน ดังนี้

๓.๔.๑ ทุกคนต้องตระหนักและปฏิบัติการใด ๆ เพื่อป้องกันทรัพย์สินของสถาบัน

๓.๔.๒ ออกจากระบบ (Log Off) ทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

๓.๔.๓ จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย

๓.๔.๔ ล็อกหน้าจอเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน

๓.๔.๕ ป้องกันตู้ หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์ และเอกสารภายในสถาบัน

๓.๔.๖ ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ของหน่วยงานภายในสถาบัน โดยไม่ได้รับอนุญาต

๓.๔.๗ นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๓.๕. กองสารสนเทศนิติวิทยาศาสตร์เป็นผู้รับผิดชอบในการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่าง ๆ ของสถาบัน

๔. ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตาม “ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔” ดังนี้

๔.๑. ต้องแสดงหลักเกณฑ์ในการกำหนดเรื่องข้อมูล หรือข้อมูลที่สำคัญยิ่งยวด

๔.๒. ต้องแสดงข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด

๕. การใช้งานรหัสผ่าน ต้องปฏิบัติตาม แนวปฏิบัติฯ หมวดที่ ๑ ส่วนที่ ๒ ข้อ ๗

๖. การใช้คอมพิวเตอร์ของสถาบัน ให้เจ้าหน้าที่ปฏิบัติดังต่อไปนี้

๖.๑. ห้ามใช้คอมพิวเตอร์จนกว่าจะได้รับการอนุมัติให้ใช้ได้โดยผ่านการลงทะเบียนและต้องสแกนไวรัสก่อนการใช้งานทุกครั้ง

๖.๒. ต้องตรวจสอบว่าโปรแกรมป้องกันไวรัส ยังทำงานตามปกติและมีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ หากพบว่าโปรแกรมดังกล่าวทำงานผิดปกติ ให้รีบแจ้งกองสารสนเทศนิติวิทยาศาสตร์เพื่อดำเนินการแก้ไขโดยเร็ว

๖.๓. เครื่องคอมพิวเตอร์ที่ใช้ในสถาบัน ให้ติดตั้งโปรแกรมมาตรฐานตามที่กำหนดโดยสถาบัน การเปลี่ยนแปลงหรือติดตั้งโปรแกรมเพิ่มเติมต้องได้รับความเห็นชอบจากผู้บังคับบัญชา หรือผู้ที่ได้รับมอบหมาย ยกเว้นการติดตั้งโปรแกรมเพื่อการทดลองใช้งานโดยกองสารสนเทศนิติวิทยาศาสตร์ หรือผู้ที่ได้รับการว่าจ้างให้มาจัดทำหรือดูแลระบบเทคโนโลยีสารสนเทศของสถาบัน

๖.๔. ห้ามติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์เพื่อให้บุคคลภายนอกสามารถใช้งานเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของสถาบัน ได้

๖.๕. ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกจากโปรแกรมมาตรฐานที่กำหนดไว้โดยสถาบัน

๖.๖. ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น

๖.๗. ห้ามเปลี่ยนแปลงหรือแก้ไขซอฟท์แวร์ที่มีลิขสิทธิ์ถูกต้องของสถาบัน

๖.๘. ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย

๖.๙. ต้องระมัดระวังการใช้งานและดูแลคอมพิวเตอร์ รวมทั้งระบบเครือข่ายตามที่วิญญูชนทั่วไปจะพึงปฏิบัติ

๖.๑๐. เอกสารหรือข้อมูลต่าง ๆ ไม่ว่าจะอยู่ในรูปแบบใดก็ตามที่ได้มีการกำหนดเงื่อนไขการใช้งานไว้ต้องใช้งานด้วยความระมัดระวัง และต้องปฏิบัติตามเงื่อนไขอย่างเคร่งครัด เพื่อป้องกันมิให้เกิดการละเมิดตามกฎหมาย

๖.๑๑. ต้องลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากคอมพิวเตอร์เพื่อประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

๖.๑๒. ต้องออกจากระบบ (Log Off) ทุกครั้งที่มิได้ปฏิบัติงานอยู่หน้าคอมพิวเตอร์ รวมทั้งปิดคอมพิวเตอร์เมื่อใช้งานประจำวันเสร็จสิ้น

๖.๑๓. การยืมเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต้องได้รับอนุมัติจากกองสารสนเทศนิติวิทยาศาสตร์เป็นลายลักษณ์อักษร

๗. การใช้คอมพิวเตอร์แบบพกพาของสถาบัน นอกจากต้องปฏิบัติตามที่กำหนดไว้ในข้างต้นแล้ว ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๗.๑. ต้องตรวจสอบคอมพิวเตอร์แบบพกพาที่นำไปใช้ว่าได้ติดตั้งโปรแกรมมาตรฐาน ที่กำหนดไว้แล้วหรือไม่ หากพบว่ายังไม่ได้ติดตั้งให้แจ้งกองสารสนเทศนิติวิทยาศาสตร์เพื่อขอรับการติดตั้งก่อนการใช้งาน

๗.๒. ต้องระมัดระวังไม่ให้บุคคลภายนอกมองเห็นหรือคัดลอกข้อมูลจากคอมพิวเตอร์แบบพกพาที่นำไปใช้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

๗.๓. เมื่อหมดความจำเป็นต้องใช้คอมพิวเตอร์แบบพกพาแล้ว ให้รีบนำส่งคืนผู้รับผิดชอบของสถาบันทันที ทั้งนี้ให้ผู้รับผิดชอบในการรับคืนตรวจสอบสภาพความพร้อมในการใช้งานของคอมพิวเตอร์ที่รับคืนไว้ดังกล่าวด้วย

๘. ในกรณีที่เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนคอมพิวเตอร์แบบพกพา ตรวจพบความเสียหายให้แจ้งผู้ส่งคืนผู้บังคับบัญชา และกองสารสนเทศนิติวิทยาศาสตร์ทราบโดยเร็ว และหากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทเลินเล่ออย่างร้ายแรงของผู้นำไปใช้ ต้องให้ผู้นำไปใช้รับผิดชอบต่อความเสียหายที่เกิดขึ้นดังกล่าว

๙. การใช้คอมพิวเตอร์เพื่อประโยชน์ส่วนตัวของเจ้าหน้าที่อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่และความรับผิดชอบของผู้ใช้อื่น ๆ

๑๐. การเข้าถึงระบบสารสนเทศ ผู้ใช้งานต้องปฏิบัติตามข้อกำหนด ดังต่อไปนี้

๑๐.๑. กรอกแบบเพื่อขออนุมัติใช้งานระบบสารสนเทศและนำเสนอต่อผู้บังคับบัญชาเพื่อขออนุมัติ

๑๐.๒. ต้องไม่เข้าถึงระบบสารสนเทศอื่นที่ตนไม่ได้รับอนุมัติให้ใช้งาน

๑๐.๓. ต้องออกจากระบบสารสนเทศโดยทันทีที่ใช้งานเสร็จ

๑๑. การใช้งานอินเทอร์เน็ต ผู้ใช้งานต้องปฏิบัติตามข้อกำหนด ดังต่อไปนี้

๑๑.๑. ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้

๑๑.๑.๑ การพนัน

๑๑.๑.๒ การประมูล

๑๑.๑.๓ วิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และพระมหากษัตริย์

๑๑.๑.๔ ลามก อนาจาร

๑๑.๑.๕ อื่น ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือผิดศีลธรรม จริยธรรม

๑๑.๒. ห้ามใช้โปรแกรมสนทนาที่สถาบันได้ประกาศห้ามไว้

๑๑.๓. ห้ามเล่น หรือดาวน์โหลดเกมส์ ภาพยนตร์ เพลง หรือสื่อลามกอนาจารผ่านทางอินเทอร์เน็ต

๑๑.๔. ห้ามใช้อินเทอร์เน็ตเพื่อส่ง กระจาย หรือแจกจ่าย ดังต่อไปนี้

๑๑.๔.๑ ข้อมูลที่ส่งผลกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

๑๑.๔.๒ ข้อมูลที่เป็นความลับของสถาบัน ไปยังบุคคลที่ไม่ได้รับอนุญาต

๑๑.๔.๓ ข้อมูลที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๑๑.๔.๔ ข้อมูลประเภทสื่อลามก อนาจาร

๑๑.๔.๕ สื่อสิ่งพิมพ์อิเล็กทรอนิกส์ที่เป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของ

๑๑.๔.๖ ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

๑๑.๔.๗ ข้อมูลปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลอันเป็นเท็จ โดยจะเกิดความเสียหายต่อผู้อื่น

๑๑.๔.๘ ข้อมูลที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติมหรือดัดแปลงด้วยวิธีทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชังหรือได้รับความอับอาย

๑๑.๕. ห้ามใช้งานข้อมูลที่ได้รับโดยผ่านทางอินเทอร์เน็ตที่มีลักษณะเป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของข้อมูลนั้น

๑๑.๖. ห้ามใช้อินเทอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์ หรือชื่อเสียงของสถาบัน

๑๒. การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องปฏิบัติตาม ข้อกำหนด ดังต่อไปนี้

๑๒.๑. ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ตามที่สถาบัน กำหนดเท่านั้น

๑๒.๒. ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ที่สถาบัน กำหนดให้ลงทะเบียนตามเว็บไซต์ที่ไม่เกี่ยวข้องกับงานของสถาบัน

๑๒.๓. ห้ามดู ใช้ หรือเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ของบุคคลอื่นโดยไม่ได้รับอนุญาต

๑๒.๔. ห้ามปลอมแปลง รับหรือส่งจดหมายอิเล็กทรอนิกส์ของบุคคลอื่นโดยไม่ได้รับอนุญาต

๑๒.๕. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะ ดังต่อไปนี้

๑๒.๕.๑ จดหมายขยะ (Spam Mail)

๑๒.๕.๒ จดหมายลูกโซ่ (Chain Letter)

๑๒.๕.๓ จดหมายที่ละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น

๑๒.๕.๔ จดหมายที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

๑๒.๖. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีขนาดใหญ่เกินกว่าที่สถาบัน กำหนด

๑๒.๗. ต้องระบุชื่อเรื่อง (Subject) และชื่อผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป

๑๒.๘. ต้องใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับจดหมายอิเล็กทรอนิกส์เท่าที่มีความจำเป็นต้องรับรู้เท่านั้น

๑๒.๙. ต้องใช้คำที่สุภาพในการส่งจดหมายอิเล็กทรอนิกส์

๑๒.๑๐. ต้องสำรองข้อมูลที่อยู่จุดหมายอิเล็กทรอนิกส์ตามความจำเป็นอย่างสม่ำเสมอ

๑๓. ห้ามมิให้ผู้ใช้งานระบบเทคโนโลยีสารสนเทศของสถาบัน กระทำการในลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้

๑๓.๑. กระทำผิดกฎหมาย หรือก่อให้เกิดความเสียหายแก่บุคคลอื่น หรือขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือละเมิดทรัพย์สินทางปัญญาของสถาบัน และของบุคคลอื่น

๑๓.๒. เปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงาน ทั้งที่เป็นข้อมูลของสถาบัน หรือบุคคลภายนอก

๑๓.๓. การเข้าถึงข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาต

๑๓.๔. ขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของสถาบัน หรือผู้ใช้งานอื่น ๆ ของสถาบัน

๑๓.๕. แสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับสถาบัน ไปยังที่อยู่เว็บไซต์ (Website) ใด ๆ ในลักษณะ ที่ก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง และก่อให้เกิดความเสียหายแก่สถาบัน

๑๓.๖. กระทำการอื่นใดที่อาจขัดต่อการดำเนินงานตามอำนาจหน้าที่ของสถาบัน หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่สถาบัน

๑๔. เอกสารที่เป็นความลับหรือมีระดับความสำคัญซึ่งพิมพ์ออกมาจากเครื่องพิมพ์ ผู้ใช้งานต้องปฏิบัติให้เป็นไปตาม “ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔” ดังต่อไปนี้

๑๔.๑. จัดหมวดหมู่เอกสารที่เป็นความลับ หรือที่มีระดับความสำคัญสูงไว้ต่างหาก

๑๔.๒. จัดเก็บและกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างเพียงพอ

๑๔.๓. การสำเนาเอกสารที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูง ต้องได้รับอนุญาตจากผู้เป็นเจ้าของ

๑๔.๔. ระมัดระวังการกระจาย หรือแจกจ่ายเอกสารที่เป็นความลับของสถาบัน ไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

๑๔.๕. ตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน

๑๔.๖. ให้ทำลายเอกสารที่เป็นความลับ หรือมีระดับความสำคัญสูงเมื่อหมดความจำเป็นในการใช้งาน

๑๕. การจัดการข้อมูลที่เป็นความลับที่อยู่ในรูปอิเล็กทรอนิกส์ ผู้ใช้งานปฏิบัติตามแนวทางปฏิบัติในการจัดการกับข้อมูลลับในข้อข้างต้น

หมวด ๓
แนวปฏิบัติและหน้าที่ของผู้ดูแลระบบ/ผู้ดูแลเครือข่าย

ผู้รับผิดชอบ

๑. กองสารสนเทศนิติวิทยาศาสตร์

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่ายของหน่วยงาน ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจาการใช้งานของผู้ใช้บริการที่ไม่เป็นไปตามนโยบายนี้ให้รีบแจ้งผู้ใช้บริการผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่เกิดขึ้นแก่หน่วยงานให้ ผู้ดูแลระบบ (System Administrator) พิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้บริการดังกล่าวได้ทันที

๒. ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์ และระบบบนเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

๓. ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย

๔. ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

๕. ดูแลรักษาและปรับปรุงบัญชีผู้ใช้งานระบบสารสนเทศ ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ ตามอำนาจหน้าที่ที่ได้รับผิดชอบ

๖. บริหารจัดการระบบสารสนเทศ และระบบเครือข่ายตามอำนาจหน้าที่ที่ได้รับผิดชอบ

๗. บริหารและจัดการระบบสารสนเทศ หรือควบคุมโดยเจ้าหน้าที่ผู้ดูแลระบบที่ได้รับมอบหมายจากผู้อำนวยการกองสารสนเทศนิติวิทยาศาสตร์ ทั้งนี้ต้องเป็นไปตามอำนาจหน้าที่ที่ได้รับการอนุมัติและเท่านั้น

๘. ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

๙. ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือข้อมูลส่วนบุคคลของผู้ใช้บริการที่ ที่มีการจัดเก็บหรือใช้งานบน ระบบคอมพิวเตอร์ ระบบสารสนเทศ และระบบเครือข่าย โดยไม่มีเหตุผลอันสมควร

๑๐. ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๑๑. เก็บรักษา ข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของผู้ใช้งานเท่าที่จำเป็น เช่น ระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Log) และระบบป้องกันการบุกรุก ให้มีความถูกต้องและสามารถระบุถึงตัวบุคคลผู้ใช้งาน ป้องกันการแก้ไขเปลี่ยนแปลง มีการจำกัดสิทธิการเข้าถึงบันทึกให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น และต้องเก็บรักษาไว้เป็นเวลาอย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

หมวด ๔
แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย

ผู้รับผิดชอบ

๑. กองสารสนเทศนิติวิทยาศาสตร์

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. กำหนดมาตรการทางเครือข่ายสื่อสารข้อมูลเพื่อป้องกันข้อมูลในเครือข่าย ระบบสารสนเทศหรือบริการต่าง ๆ จากการถูกเข้าถึงหรือถูกทำลายโดยไม่ได้รับอนุญาต ดังต่อไปนี้

๑.๑. กำหนดบุคลากรผู้มีหน้าที่รับผิดชอบ ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล

๑.๒. กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการบัญชีผู้ใช้งานที่อนุญาตให้สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศจากระยะไกล

๑.๓. กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ ได้แก่ เครือข่ายอินเทอร์เน็ต เครือข่ายไร้สาย

๑.๔. กำหนดมาตรการเพื่อป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

๑.๕. กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่าง ๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

๑.๖. มีการบันทึกข้อมูลพฤติกรรมการใช้งานเก็บ Log ของอุปกรณ์เครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๒. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ผู้รับผิดชอบต้องปฏิบัติตาม ข้อกำหนดดังต่อไปนี้

๒.๑. ผู้ดูแลระบบ ต้องมีการออกแบบแบ่งระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ และการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เพื่อเป็นการควบคุม และ ป้องกันการบุกรุกได้อย่างเป็นระบบ โดยแบ่งเป็น ๒ เครือข่าย คือ เครือข่ายภายในและเครือข่ายภายนอก

๒.๒. การเข้าสู่ระบบเครือข่ายภายในของสถาบัน โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา ก่อนที่จะสามารถใช้งานได้ในทุกกรณี

๒.๓. ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๒.๓.๑. ผู้ดูแลระบบต้องควบคุมไม่ให้ผู้ใช้งานภายนอกสามารถเข้าถึงระบบสารสนเทศภายในได้

๒.๓.๒. มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับ อนุญาตให้เข้าถึงเท่านั้น

๒.๓.๓. ผู้ดูแลระบบต้องกำหนดการใช้งานระบบสารสนเทศที่สำคัญสำหรับผู้ใช้งาน โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรเท่านั้น

๒.๔. ผู้ดูแลระบบ ต้องมีการควบคุมการเชื่อมต่อทางเครือข่าย และ การจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และ การส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง หรือ การประยุกต์ใช้งานตามภารกิจ ดังนี้

๒.๔.๑. กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย โดยอนุญาตให้แต่ละเส้นทางเครือข่ายของหน่วยงานภายในสามารถเชื่อมต่อกันได้เท่าที่จำเป็น

๒.๔.๒. ในการเข้าใช้งานเครือข่ายอินเทอร์เน็ตจากภายในสถาบัน ผู้ดูแลระบบต้องกำหนดเส้นทางให้ ผู้ใช้งาน สามารถใช้เส้นทางออกไปยัง อินเทอร์เน็ตได้เพียงช่องทางเดียว เพื่อให้สามารถกำกับดูแลได้อย่างมีประสิทธิภาพ

๒.๔.๓. ควบคุมไม่ให้มีการเปิดเผยแผนผังเครือข่ายภายในสถาบัน

๒.๔.๔. กำหนดให้มีการแปลงหมายเลขเครือข่ายเพื่อ แยกเครือข่ายย่อยภายในสถาบันให้ปลอดภัยจากการเข้าถึงจากเครือข่าย อินเทอร์เน็ตภายนอกสถาบัน

๒.๕. ผู้ดูแลระบบ ต้องกำหนดการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบโดยต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับ ตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย ดังนี้

๒.๕.๑. จำกัดการเข้าถึง พอร์ตที่ใช้สำหรับตรวจสอบ และพอร์ตสำหรับปรับแต่งระบบให้สามารถเข้าถึงได้เฉพาะ IP Address ที่ผู้ดูแลระบบกำหนดเท่านั้น

๒.๕.๒. ปิดพอร์ตที่ไม่ได้มีการใช้งานทั้งหมด

๒.๕.๓. ป้องกันการเชื่อมต่อที่ Console Port ของอุปกรณ์

๒.๖. ผู้ดูแลระบบ ต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย โดยกำหนดให้การเชื่อมต่อจากเครื่องคอมพิวเตอร์ใช้งาน ไปยังเครื่องคอมพิวเตอร์สำหรับให้บริการ สามารถทำได้เฉพาะชุด IP Address ที่ผู้ดูแลระบบอนุญาตเท่านั้น

๒.๗. ผู้ดูแลระบบต้องควบคุมการแก้ไข หรือเปลี่ยนแปลงค่าตัวแปรต่าง ๆ ของระบบเครือข่าย และอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่าย

๒.๘. ระบบเครือข่ายทั้งหมดของสถาบัน ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสถาบัน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก โดยใช้ Firewall หรือ Hardware อื่น ๆ

๒.๙. มีการติดตั้งระบบตรวจจับและป้องกันการบุกรุก เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๒.๑๐. การเข้าสู่ระบบเครือข่ายภายในหน่วย ผ่านทางอินเทอร์เน็ตต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตนเพื่อตรวจสอบความถูกต้อง

๒.๑๑. ข้อมูลหมายเลขชุดอินเทอร์เน็ตของคอมพิวเตอร์ที่เชื่อมต่อเครือข่ายภายในสถาบัน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของสถาบัน ได้โดยง่าย

๒.๑๒. จัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๑๓. จัดให้มีการใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้รับมอบอำนาจ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒.๑๔. การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องได้รับการอนุญาตการดำเนินการโดยเจ้าหน้าที่กองสารสนเทศนิติวิทยาศาสตร์เท่านั้น

๒.๑๕. การบริหารจัดการการบันทึกและตรวจสอบ กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึก ดังกล่าวไว้อย่างน้อยกว่า ๓ เดือน หรือไม่ต่ำกว่า ๙๐ วัน

๒.๑๖. มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๓. ผู้ดูแลระบบสารสนเทศของสถาบัน ต้องควบคุมการเข้าใช้งานระบบจากภายนอก โดยมีรายละเอียดดังนี้

๓.๑. การเข้าสู่ระบบจากระยะไกลสู่ระบบเครือข่ายคอมพิวเตอร์ของสถาบัน

๓.๑.๑. ผู้ใช้งานที่มีความประสงค์จะเข้าสู่ระบบจากระยะไกล ต้องขออนุญาตจากผู้บริหารระดับสูง หรือ ผู้ที่ได้รับการมอบอำนาจก่อน

๓.๑.๒. ผู้ดูแลระบบเครือข่าย ต้องเปิดช่องทางให้กับผู้ใช้งาน ตามที่ได้รับอนุมัติ เท่านั้น

๓.๑.๓. ผู้ใช้งานต้องยืนยันตัวตนด้วย User และ Password ที่ได้รับอนุมัติ ก่อนเข้าใช้งานเครือข่าย

๓.๑.๔. ผู้ใช้งานต้องเข้าสู่ระบบสารสนเทศที่ได้รับอนุญาตให้เข้าใช้ได้เท่านั้น

๓.๑.๕. ผู้ดูแลระบบต้องควบคุมให้มีการบันทึกประวัติการเข้าสู่ระบบจากระยะไกลเพื่อเป็นหลักฐานอ้างอิงในกรณีที่จำเป็นต้องใช้

๓.๒. การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น

หมวด ๕
แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

ผู้รับผิดชอบ

๑. กองสารสนเทศนิติวิทยาศาสตร์

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยการเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ดังนี้

๑.๑. เครื่องคอมพิวเตอร์ทุกเครื่องของสถาบัน ต้องกำหนดชื่อผู้ใช้งานและรหัสผ่าน เพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสถาบันตามข้อกำหนดของกองสารสนเทศนิติวิทยาศาสตร์

๑.๒. ผู้ดูแลระบบต้องตั้งค่าให้ระบบปฏิบัติการ ส่วนของหน้าจอล็อกอินไม่ให้แสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่ผู้ใช้งานจะล็อกอินเข้าสู่ระบบ

๑.๓. ผู้ใช้งานต้องลงทะเบียนขอใช้เครื่องคอมพิวเตอร์โดยยื่นเอกสารตามแบบฟอร์มของกองสารสนเทศนิติวิทยาศาสตร์เพื่อขออนุมัติ

๑.๔. หลังจากที่ผู้ใช้งานได้รับอนุญาตให้ใช้งานเครื่องคอมพิวเตอร์ ต้องปฏิบัติตาม แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

๒. แนวปฏิบัติในการใช้งานบัญชีผู้ใช้บริการ (Account/Username)

๒.๑. ผู้ใช้บริการที่เป็นเจ้าของบัญชีผู้ใช้บริการ ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการของตนเอง จากเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่พิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๒.๒. ผู้ใช้บริการจะต้องเก็บรักษาบัญชีผู้ใช้บริการไว้เป็นความลับและห้ามเปิดเผยต่อผู้บุคคลอื่น ห้ามโอน จำหน่ายจ่ายแจก ให้กับผู้อื่นและไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่าน ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของสถาบันร่วมกัน

๒.๓. ผู้ใช้บริการจะต้องลงบันทึกการเข้าใช้ (Login) โดยบัญชีผู้ใช้บริการของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดงานชั่วคราว

๓. แนวปฏิบัติการกำหนดรหัสผ่านการเปลี่ยนรหัสผ่าน และการใช้งานรหัสผ่านของการเข้าถึงระบบปฏิบัติการให้ดำเนินการตามแนวปฏิบัติฯ หมวด ๑ ส่วนที่ ๒ ข้อ ๖ และ ข้อ ๗

๔. การใช้งานโปรแกรมอรรถประโยชน์ โปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ ควรจำกัดและควบคุมการใช้งาน เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการ ดังนี้

๔.๑. กำหนดให้ใช้โปรแกรมที่มีลิขสิทธิ์ของสถาบันเท่านั้น

๔.๒. ผู้ดูแลระบบ ต้องมีการจัดทำทะเบียนซอฟต์แวร์ลิขสิทธิ์ของสถาบัน และ มีการควบคุมการนำซอฟต์แวร์ไปใช้งาน เพื่อป้องกันการละเมิดลิขสิทธิ์

๔.๓. ผู้ดูแลระบบ ต้องไม่อนุญาตให้ผู้ใช้งานติดตั้งโปรแกรมได้ด้วยตนเอง หากผู้ใช้งานต้องการใช้งานโปรแกรมอื่น ๆ เพิ่มเติม ต้องแจ้งกับผู้ดูแลระบบ

๔.๔. ผู้ใช้งาน ต้องไม่ติดตั้งซอฟต์แวร์ระบบปฏิบัติการด้วยตนเอง

๔.๕. หากผู้ใช้งานเรียกใช้งานโปรแกรมอื่นใด นอกเหนือไปจากที่ติดตั้งไว้ในคอมพิวเตอร์ของสถาบัน ให้ถือว่า ผู้ใช้งานต้องเป็นผู้รับผิดชอบในความเสียหายที่อาจเกิดขึ้นได้

๕. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศเมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น

๕.๑. ตั้งค่าให้เครื่องคอมพิวเตอร์ของผู้ใช้งานทั่วไป ล็อกหน้าจอโดยอัตโนมัติ เมื่อไม่มีการใช้นานต่อเนื่องเป็นระยะเวลาที่กำหนด

๕.๒. ยุติการใช้งานระบบสารสนเทศ กรณีมีการว่างเว้นจากการใช้งานเกินกว่าเวลาที่กำหนด

๖. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศ หรือโปรแกรม ที่มีความเสี่ยงหรือมีความสำคัญสูง

๖.๑. ผู้ดูแลระบบ ต้องควบคุมการเข้าถึง ระบบปฏิบัติการของระบบสารสนเทศ หรือ แอปพลิเคชันที่มี ความเสี่ยงหรือมีความสำคัญสูง โดยกำหนดให้การเข้าถึงระบบต่อครั้ง โดยมีผู้ดูแลระบบกำกับดูแลอยู่ด้วย

๖.๒. ในการเข้าถึงระบบปฏิบัติการของระบบสารสนเทศหรือ แอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูงจากเครือข่ายภายนอกสถาบัน ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บังคับบัญชาเท่านั้น

หมวด ๖

แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันหรือสารสนเทศ

ผู้รับผิดชอบ

๑. กองสารสนเทศนิติวิทยาศาสตร์

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ดังนี้

๑.๑. ผู้ดูแลระบบต้องกำหนดมาตรการควบคุมการเข้าใช้งานของผู้ใช้งาน ดังนี้

๑.๑.๑. ผู้ใช้งานต้องลงทะเบียนขออนุญาตเป็นลายลักษณ์อักษรด้วยแบบฟอร์มที่กำหนดเพื่อขอรับสิทธิการเข้าใช้งานจากผู้บังคับบัญชาหน่วยงานเจ้าของระบบ โดยผ่านความเห็นชอบจากผู้บังคับบัญชาของผู้ใช้งาน

๑.๑.๒. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงตามคำร้องขอ เพิ่มเติม/เปลี่ยนแปลง/ยกเลิก สิทธิของผู้ใช้งาน ภายใน ๓ วัน หลังจากได้รับอนุมัติจากหัวหน้าหน่วยงานของผู้ใช้งาน หรือตามคำสั่งเปลี่ยนแปลงหน้าที่ความรับผิดชอบของบุคลากรสถาบัน

๑.๑.๓. ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

๑.๑.๔. ผู้ดูแลระบบต้องจดบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๑.๑.๕. ผู้ดูแลระบบต้องบริหารจัดการรหัสผ่านและสิทธิการใช้งานระบบสารสนเทศของบุคลากร ดังต่อไปนี้

๑.๑.๕.๑. กำหนดรหัสผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานเริ่มต้นเป็นแบบรหัสผ่านชั่วคราว (Temporary Password)

๑.๑.๕.๒. ส่งมอบรหัสผ่านชั่วคราว (Temporary Password) ให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๑.๑.๕.๓. เมื่อมีการส่งมอบรหัสผ่านตามข้อ ๑.๑.๕.๒ ให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน และกำหนดและแจ้งผู้ใช้งานให้ทำการเปลี่ยนรหัสผ่านใหม่

๑.๑.๕.๔. กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๑.๑.๕.๕. แจ้งผู้ใช้งาน ไม่ให้ทำการบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๑.๑.๕.๖. ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๑.๑.๕.๗. กำหนดให้ระบบแจ้งเตือนให้ผู้ใช้งานทำการเปลี่ยนรหัสผ่านทุก ๆ ๓ เดือน

๑.๑.๕.๘. กำหนดระยะเวลาการใช้งานระบบสารสนเทศภายในของสถาบัน โดยผู้ใช้งานต้องใช้งานระบบสารสนเทศอย่างต่อเนื่อง หากว่างเว้นจากการใช้งานระบบสารสนเทศมากกว่าเวลาที่กำหนดต้องกำหนดให้โปรแกรมปิดการทำงาน และกำหนดให้ผู้ใช้งานกรอกรหัสผู้ใช้งานและรหัสผ่านเพื่อเข้าสู่ระบบสารสนเทศใหม่อีกครั้ง

๑.๑.๖. มีการทบทวนสิทธิการเข้าถึงระบบงานสารสนเทศ ปีละ ๑ ครั้ง

๑.๒. กรณีมีการจ้างเหมาดำเนินงาน พัฒนาระบบและบำรุงรักษาระบบ ผู้ดูแลระบบต้องมีการควบคุมการเข้าถึงของผู้ให้บริการภายนอก (Outsource) ดังนี้

๑.๒.๑. ผู้ให้บริการที่ต้องการสิทธิ ในการเข้าถึงระบบสารสนเทศ ต้องขออนุญาตเป็นลายลักษณ์อักษร เพื่อให้ผู้อำนวยการสถาบัน

๑.๒.๒. อนุมัติ ให้มีการกำหนดสิทธิที่สอดคล้องกับที่กำหนดไว้ในขอบข่ายหน้าที่ตามสัญญาจ้าง

๑.๒.๓. ดำเนินการเปิดสิทธิการเข้าถึงระบบฯ ให้แก่ผู้ให้บริการภายนอก ตามที่ได้รับอนุมัติ

๑.๒.๔. ดำเนินการเพิกถอน ลบ หรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการที่สิ้นสุดการว่าจ้าง หรือเปลี่ยนการจ้างงานโดยทันที หรือภายในระยะเวลาที่กำหนดไว้

๑.๒.๕. กำหนดให้ผู้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบสารสนเทศ (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อป้องกันผลกระทบต่องานให้บริการของสถาบัน

๑.๒.๖. การอนุญาตให้ผู้ให้บริการเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางเชื่อมต่อ (Port) และ อุปกรณ์เชื่อมต่อระยะไกล (Modem) ทิ้งเอาไว้โดยไม่จำเป็น โดยผู้ดูแลระบบต้องควบคุมการใช้งานช่องทางดังกล่าวเท่าที่จำเป็น เท่านั้น

๒. ระบบสารสนเทศที่มีความไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อองค์กรต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร ดังนี้

๒.๑. แบ่งแยกเครือข่ายด้วยอุปกรณ์ป้องกันการบุกรุก (Firewall) โดยเฉพาะในส่วนของระบบฐานข้อมูล และระบบโปรแกรมประยุกต์ (Application) ด้วยพอร์ตการใช้งานเฉพาะ

๒.๒. กำหนดกลุ่มของเครือข่ายเสมือน (VLAN) เพื่อแบ่งแยก

๒.๒.๑. ผู้ใช้งานระหว่างกลุ่มหรือหน่วยงานหรือพื้นที่การใช้งาน

๒.๒.๒. กลุ่มผู้ใช้งานกับระบบสารสนเทศหลัก

๒.๒.๓. ระบบสารสนเทศหลักกับเครือข่ายภายนอก

หมวด ๗
แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

ผู้รับผิดชอบ

๑. กองสารสนเทศนิติวิทยาศาสตร์

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. สถาบันมีการกำหนดระบบสารสนเทศที่มีความสำคัญ และจัดหมวดหมู่ของข้อมูลพร้อมกำหนดระดับความสำคัญของข้อมูล เพื่อจัดทำระบบสำรองโดยมีทบทวนระดับความสำคัญของระบบสารสนเทศและหมวดหมู่ของข้อมูลที่มีความสำคัญ อย่างน้อยปีละ ๑ ครั้ง

๒. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบัน ต้องกำหนดแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูล เมื่อมีระบบสารสนเทศใหม่ เกิดข้อมูลใหม่ หรือข้อมูลที่มีการเปลี่ยนแปลงใหม่ ควรกำหนดให้ใช้แนวทางการสำรองและกู้คืนข้อมูล โดยคำนึงถึงสภาพความเสี่ยงที่สถาบันยอมรับได้ ดังนี้

๒.๑. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง โดยต้องมีการทบทวน อย่างน้อยปีละ ๑ ครั้ง

๒.๒. ต้องจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ โดยต้องมีการทบทวน อย่างน้อยปีละ ๑ ครั้ง

๒.๓. กำหนดผู้รับผิดชอบในการสำรองข้อมูล โดยมีการปรับปรุงรายชื่อผู้รับผิดชอบ อย่างน้อยปีละ ๑ ครั้ง

๒.๔. กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อยต้องประกอบด้วยข้อมูลใน ฐานข้อมูลของระบ ข้อมูลสำหรับตัวระบบ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่น ๆ ที่เกี่ยวข้อง

๒.๕. กำหนดความถี่ในการสำรองข้อมูลของระบบสารสนเทศ

๒.๖. กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์ที่ใช้ในการสำรองข้อมูล

๒.๗. ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ และข้อมูลที่สำรองไว้จะต้องได้รับการป้องกันทั้งทางกายภาพและสภาพแวดล้อมที่เหมาะสม

๒.๘. ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้นสำเร็จครบถ้วนหรือไม่

๒.๙. ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบสารสนเทศทั้งหมดสามารถใช้งานได้หรือไม่

๒.๑๐. จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนด แผนควรมีรายละเอียดอย่างน้อย ดังต่อไปนี้

๒.๑๐.๑. กำหนดหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด

๒.๑๐.๒. ประเมินความเสี่ยงสำหรับระบบสารสนเทศที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น

๒.๑๐.๓. กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๒.๑๐.๔. กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

๒.๑๐.๕. กำหนดช่องทางในการติดต่อสื่อสารกับผู้ให้บริการภายนอกที่เกี่ยวข้อง สำหรับติดต่อเมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อในกรณีเกิดเหตุฉุกเฉินต่าง ๆ

๒.๑๑. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่าง เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง และแจ้งข้อมูลแก่ผู้ที่เกี่ยวข้อง

๒.๑๒. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

หมวด ๘
แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ผู้รับผิดชอบ

๑. กองสารสนเทศนิติวิทยาศาสตร์
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง ร่วมกับกลุ่มงานตรวจสอบภายใน เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของสถาบัน
๒. จัดทำร่างแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เสนอผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เห็นชอบ / ลงนาม และประกาศนโยบายและแนวปฏิบัติฯ
๓. ทบทวนปรับปรุงนโยบายและแนวปฏิบัติฯ ทุก ๑ ปี ให้เป็นปัจจุบันและเป็นมาตรฐานที่ยอมรับได้อยู่เสมอ กรณีมีการเปลี่ยนแปลงหรือปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องเสนอแนวนโยบายและแนวปฏิบัติฯ ที่มีการเปลี่ยนแปลงให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ลงนามหรือให้ความเห็นชอบ
๔. ติดตามประเมินผลการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน

หมวด ๙
แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. กองสารสนเทศนิติวิทยาศาสตร์

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การจัดการระบบสารสนเทศกรณีพบเหตุละเมิดความมั่นคงปลอดภัยหรือสงสัยว่าจะเกิดเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ

๑.๑. ให้เจ้าหน้าที่หรือผู้ปฏิบัติงานแจ้งไปยังผู้ดูแลระบบทันทีที่พบเห็นเหตุการณ์ที่อาจเป็นปัญหาต่อความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของสถาบัน

๑.๒. เมื่อผู้ดูแลระบบได้รับแจ้งเหตุให้ดำเนินการ ดังนี้

๑.๒.๑. สำรวจความเสียหายที่เกิดจากเหตุละเมิดการรักษาความมั่นคงปลอดภัย

๑.๒.๒. วิเคราะห์ประเภทการละเมิดการรักษาความมั่นคงปลอดภัย

๑.๒.๓. ตรวจสอบสาเหตุและจุดอ่อนหรือข้อบกพร่องที่ก่อให้เกิดการละเมิดการรักษาความมั่นคงปลอดภัย

๑.๓. ผู้ดูแลระบบรายงานให้บุคคลและหน่วยงานที่เกี่ยวข้องรับทราบทันที

๑.๔. ผู้ดูแลระบบปฏิบัติการตามวิธีรับมือกับเหตุละเมิดตามความเหมาะสม ในกรณีนี้อาจได้แก่ การเปลี่ยนแปลงรหัสผ่าน การแยกระบบที่มีปัญหาออก การปิดบริการที่สงสัย การปิดเส้นทางการเข้าสู่ระบบสารสนเทศ การยกเลิกบัญชีผู้ใช้งานที่ถูกใช้ในการเข้าถึงระบบโดยมิได้รับอนุญาต ในบางกรณีเจ้าหน้าที่ที่เกี่ยวข้องจะต้องค้นหาและจับกุมผู้ก่อเหตุละเมิด

๑.๕. ผู้ดูแลระบบและเจ้าหน้าที่ที่เกี่ยวข้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษรและรวบรวมหลักฐาน

๑.๖. ผู้ดูแลระบบตรวจสอบว่าวิธีการรับมือที่ใช้ได้ผลหรือมีประสิทธิภาพหรือไม่ แล้วเพิ่มเติมมาตรการเพื่อลดช่องโหว่หรือถอดแยกส่วนของระบบสารสนเทศที่มีปัญหาออก

๑.๗. ผู้ดูแลระบบกู้คืนระบบสารสนเทศสู่สภาพเดิม และทำรายงานแจ้งผู้ที่เกี่ยวข้อง

๑.๘. ผู้ดูแลระบบทำรายงานและทบทวนมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้อง เสนอผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เพื่อพิจารณา

๒. การป้องกันการละเมิดจากผู้ไม่พึงประสงค์ทั้งภายในและภายนอกองค์กร

๒.๑. กำหนดหน้าที่ความรับผิดชอบรวมถึงโทษของผู้ใช้งาน ในการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีการกำหนดดังนี้

๒.๑.๑. ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่านและการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๒.๑.๒. ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๒.๑.๓. ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ยังไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน โดยการบันทึกประวัติการซ่อมบำรุงทรัพย์สินเทคโนโลยีสารสนเทศ โดยเก็บข้อมูล วันและเวลาที่ซ่อม ชื่อผู้ซ่อม ชื่อผู้ร่วมงาน รายละเอียดการซ่อม และรายการอุปกรณ์ที่เปลี่ยนหรือเอาออกเป็นอย่างน้อย

๒.๑.๔. กำหนดบทลงโทษผู้ใช้งาน กรณีที่ผู้ใช้งานการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต เปิดเผย ล่วงรู้ ลักลอบทำสำเนาข้อมูลสารสนเทศ และลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ให้เป็นไปตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๕๔

๒.๒. การพัฒนาหรือปรับปรุงซอฟต์แวร์ระบบสารสนเทศใหม่ ทั้งที่ว่าจ้างให้หน่วยงานภายนอกเป็นผู้จัดทำหรือให้หน่วยงานของสถาบันจัดทำขึ้นเอง ให้นำมาตรการสำหรับการพัฒนาซอฟต์แวร์เป็นส่วนหนึ่งของข้อกำหนดของระบบ ในทุกขั้นตอนตั้งแต่การออกแบบจนถึงการส่งมอบ สำหรับ การพัฒนาระบบสารสนเทศโดยหน่วยงานภายใน จะต้องจัดให้มีระบบสำหรับการพัฒนา และการทดสอบโดยเฉพาะ ห้ามใช้หรือเชื่อมต่อกับระบบที่ใช้งานจริง

๒.๓. กำหนดวิธีการทดสอบประสิทธิภาพและทดสอบภาระสูงสุดของระบบ และให้วิธีดังกล่าวเป็นส่วนหนึ่งของเกณฑ์การตรวจรับระบบสารสนเทศใหม่รวมทั้งการปรับปรุงระบบสารสนเทศ บำรุงรักษาหรือซ่อมแซมเครื่องมือหรืออุปกรณ์สารสนเทศต้องทำโดยบุคลากร ที่ได้รับอนุญาตจากสถาบันเท่านั้น

๒.๔. กรณีที่การซ่อมแซมหรือบำรุงรักษาระบบสารสนเทศทำโดยหน่วยงานภายนอก บุคลากรของหน่วยงานภายนอกจะต้องได้รับการกลั่นกรองในเรื่องการเข้าถึงความลับตามความเหมาะสมจาก เจ้าหน้าที่กองสารสนเทศ ที่รับผิดชอบ

๒.๕. กำหนดวิธีการและความถี่การสำรองข้อมูล การเข้ารหัส และดำเนินการสำรองข้อมูล ให้ถูกต้องและสมบูรณ์ รวมทั้งระบุวิธีการนำข้อมูลกลับคืน

๒.๖. ทดสอบแผนการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อหาช่องโหว่ของระบบเป็นระยะทั้งด้วยระบบอัตโนมัติและด้วยบุคคล

๓. เจ้าหน้าที่หรือผู้ใช้บริการที่ละเมิดความมั่นคงปลอดภัยระบบสารสนเทศ และบุกรุกทรัพย์สินทางราชการหรืออื่น ๆ แล้วแต่กรณีจะถูกดำเนินการทางวินัยฐานฝ่าฝืนระเบียบวินัยทางราชการ

หมวด ๑๐
แนวปฏิบัติในการจัดซื้อจัดจ้างระบบเทคโนโลยีสารสนเทศ

ผู้รับผิดชอบ

๑. กองสารสนเทศนิติวิทยาศาสตร์
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. คณะกรรมการที่เกี่ยวข้อง โดยได้รับการแต่งตั้งจากสถาบัน

แนวปฏิบัติ

๑. การจัดซื้อจัดจ้างที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ หรือจัดซื้อเครื่องคอมพิวเตอร์ หรือวัสดุอุปกรณ์ อื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ต้องผ่านการพิจารณากลั่นกรองความเหมาะสม ความคุ้มค่า ประโยชน์ที่จะได้รับและความสอดคล้องกับโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศของสถาบัน จากกองสารสนเทศนิติวิทยาศาสตร์ก่อนนำเสนอ ผู้อำนวยการสถาบัน หรือผู้ซึ่งผู้อำนวยการสถาบัน มอบหมายพิจารณาอนุมัติจัดซื้อจัดจ้าง

๒. การจัดซื้อจัดจ้างที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ หรือจัดซื้อเครื่องคอมพิวเตอร์ หรือวัสดุอุปกรณ์ อื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ จะต้องมีการกำหนดความต้องการที่ชัดเจนในข้อกำหนดของผู้ว่าจ้าง (Term of Reference: TOR) ให้ชัดเจน รวมถึงมีการกำหนดเรื่องการจะไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) ลงในข้อกำหนดของผู้ว่าจ้างอย่างชัดเจน

๓. กำหนดวิธีการทดสอบประสิทธิภาพและทดสอบภาระสูงสุดของระบบ และให้วิธีดังกล่าวเป็นส่วนหนึ่งของเกณฑ์การตรวจรับระบบสารสนเทศใหม่รวมทั้งการปรับปรุงระบบสารสนเทศบำรุงรักษาหรือซ่อมแซมเครื่องมือหรืออุปกรณ์สารสนเทศต้องทำโดยบุคลากร ที่ได้รับอนุญาตจากสถาบัน เท่านั้น

๔. การคัดเลือกผู้พัฒนาซอฟต์แวร์จากภายนอกจะต้องมีการตรวจสอบความไว้ใจได้ของบุคลากรในคณะปฏิบัติงานในการเข้าถึงเอกสารราชการในระดับลับ การทำสัญญาจะต้องระบุความรับผิดชอบของผู้พัฒนาและคณะปฏิบัติงานในการปกปิด และรักษาความลับ ทั้งระหว่างการพัฒนาและหลังการส่งมอบซอฟต์แวร์

๕. ผู้พัฒนาซอฟต์แวร์ต้องพัฒนาซอฟต์แวร์ตามหลักวิชาการที่ยอมรับโดยทั่วไป และยินยอมให้ทำการตรวจสอบได้ตลอดเวลา รวมทั้งแสดงรายละเอียดที่จำเป็นไว้ในซอร์สโค้ด

๖. ผู้พัฒนาซอฟต์แวร์ทั้งที่เป็นบุคลากรทางคอมพิวเตอร์ของสถาบัน และบุคคลภายนอกที่รับจัดทำซอฟต์แวร์ให้สถาบัน ต้องคำนึงถึงความมั่นคงปลอดภัยระบบสารสนเทศในทุกขั้นตอนของการพัฒนาซอฟต์แวร์ รวมทั้งปฏิบัติต่อเอกสารหรือคู่มือระหว่างการพัฒนาซอฟต์แวร์โดยถือเป็นเอกสารระดับลับ

๗. การเข้าถึงระบบสารสนเทศของสถาบัน จากภายในและภายนอกสถานที่ทำการของสถาบัน ผู้พัฒนาซอฟต์แวร์ต้องเข้าถึงโดยจำกัดและจะต้องแจ้งให้ผู้ดูแลระบบทราบทุกครั้ง

หมวด ๑๑

แนวปฏิบัติในการเผยแพร่ข้อมูลสาธารณะ

ผู้รับผิดชอบ

๑. กองสารสนเทศนิติวิทยาศาสตร์

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การเผยแพร่ข้อมูลในความรับผิดชอบของสถาบันสู่สาธารณะโดยผ่านระบบเทคโนโลยีสารสนเทศของสถาบัน หน่วยงานเจ้าของข้อมูลจะต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำออกเผยแพร่ และจะต้องได้รับความเห็นชอบจากผู้อำนวยการสถาบัน หรือ ผู้ซึ่งผู้อำนวยการสถาบันมอบหมาย ก่อนนำออกเผยแพร่ ในกรณีที่ข้อมูลที่นำออกเผยแพร่มีความผิดพลาดและมีความเสียหายเกิดขึ้น โดยความเสียหายนั้นเกิดจากความจงใจหรือประมาทเลินเล่ออย่างร้ายแรง ให้เป็นความรับผิดของเจ้าหน้าที่ที่นำข้อมูลดังกล่าวออกเผยแพร่

๒. การเผยแพร่ข้อมูลสู่สาธารณะโดยผ่านระบบเทคโนโลยีสารสนเทศของสถาบัน ให้ดำเนินการโดยหน่วยงานเจ้าของข้อมูล เว้นแต่กรณีที่ผู้อำนวยการสถาบันหรือผู้ซึ่งผู้อำนวยการสถาบันมอบหมายได้สั่งการหรือเห็นชอบไว้เป็นอย่างอื่น