ประกาศกรมทรัพย์สินทางปัญญา

เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมทรัพย์สินทางปัญญาเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถทำงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องหรือการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กรมทรัพย์สินทางปัญญาหรือเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และกฎหมายอื่นที่เกี่ยวข้อง

อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ ๕) พ.ศ. ๒๕๔๕ ประกอบมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ อธิบดีกรมทรัพย์สินทางปัญญาจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมทรัพย์สินทางปัญญา เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของสารสนเทศ”

ข้อ ๒ การรักษาความมั่นคงปลอดภัยของสารสนเทศให้เป็นไปตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของสารสนเทศที่กำหนดไว้ท้ายประกาศนี้

ข้อ ๓ ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม (Department Chief Information Officer: DCIO) เป็นผู้รับผิดชอบต่อความเสี่ยงและความเสียหายต่อระบบสารสนเทศของกรมทรัพย์สินทางปัญญา อันเนื่องมาจากความบกพร่อง ละเลย หรือละเว้นการควบคุมตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของสารสนเทศ

ข้อ ๔ ให้มีการทบทวนและปรับปรุงนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของสารสนเทศ พร้อมทั้งตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ ตั้งแต่วันที่ เป็นต้นไป

ประกาศ ณ วันที่ ๑๖ มีนาคม ๒๕๖๔

(นายวุฒิไกร สีวีระพันธุ์)
อธิบดีกรมทรัพย์สินทางปัญญา

๙๔/๒๕๖๔

แนบท้ายประกาศกรมทรัพย์สินทางปัญญา
เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของสารสนเทศ

นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของสารสนเทศ

นโยบายนี้จัดทำขึ้นโดยอาศัยกรอบตามมาตรฐานสากลด้านความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013 เพื่อใช้เป็นกรอบและแนวทางปฏิบัติในการป้องกันและรักษาทรัพย์สินของสารสนเทศของกรมทรัพย์สินทางปัญญา

วัตถุประสงค์

๑. เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศของกรมทรัพย์สินทางปัญญา ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒. เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับของกรมทรัพย์สินทางปัญญาได้รับทราบและถือปฏิบัติตามนโยบายและแนวทางปฏิบัติอย่างเคร่งครัด

๓. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีการปฏิบัติให้กับผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมทรัพย์สินทางปัญญา ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมทรัพย์สินทางปัญญาในการดำเนินงานและต้องปฏิบัติตามอย่างเคร่งครัด

๔. เพื่อกำหนดให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ มีการจัดเตรียมความพร้อมสำหรับกรณีฉุกเฉิน และระบบสามารถให้บริการได้อย่างต่อเนื่อง สอดคล้องตามภารกิจของกรมทรัพย์สินทางปัญญา

คำนิยาม

“ศูนย์คอมพิวเตอร์ (Data Center)” หมายความว่า สถานที่สำหรับจัดวางเครื่องคอมพิวเตอร์แม่ข่าย (Computer Server) และอุปกรณ์เครือข่าย (Network Equipment) และจัดเก็บข้อมูลสารสนเทศของกรมทรัพย์สินทางปัญญา ซึ่งประกอบด้วยศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง

“ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม (Department Chief Information Officer: DCIO)” หมายความว่า อธิบดีหรือผู้บริหารระดับสูงที่ได้รับการแต่งตั้งจากอธิบดีกรมทรัพย์สินทางปัญญาให้ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมทรัพย์สินทางปัญญา

“ระบบสารสนเทศ” หมายความว่า ระบบงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์มาช่วยในการสร้างระบบสารสนเทศ เพื่อนำมาใช้ประโยชน์ในการวางแผนการบริหารจัดการ และการสนับสนุนการให้บริการของกรมทรัพย์สินทางปัญญา

“ผู้ใช้งาน” หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างตามสัญญาจ้างตามหน่วยงาน บุคคลภายนอก และผู้ให้บริการภายนอก ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ และเข้าถึงข้อมูลสารสนเทศของกรมทรัพย์สินทางปัญญา

“ผู้พัฒนาระบบ” หมายความว่า ผู้ที่มีหน้าที่และความรับผิดชอบในการพัฒนาและดูแลระบบสารสนเทศของกรมทรัพย์สินทางปัญญา

“ผู้ดูแลระบบ” หมายความว่า ผู้ที่มีหน้าที่และความรับผิดชอบในการดูแลรักษาระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ ฐานข้อมูล หรือจดหมายอิเล็กทรอนิกส์ (E-mail) ซึ่งได้รับมอบหมายจากผู้บังคับบัญชา เพื่อการบริหารจัดการระบบสารสนเทศของกรมทรัพย์สินทางปัญญา

“ผู้บังคับบัญชา” หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมทรัพย์สินทางปัญญา

“เจ้าของระบบงาน” หมายความว่า หน่วยงานที่มีหน้าที่และความรับผิดชอบในการควบคุมดูแลระบบสารสนเทศและอนุญาตให้เจ้าหน้าที่หรือบุคคลใด ๆ เข้าใช้งานระบบสารสนเทศดังกล่าวได้

“หน่วยงานภายนอก” หมายความว่า องค์กรหรือผู้มีส่วนได้ส่วนเสียที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงระบบสารสนเทศหรือข้อมูลของกรมทรัพย์สินทางปัญญา โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาข้อมูลไว้เป็นความลับ

“ผู้ให้บริการภายนอก” หมายความว่า องค์กรหรือบริษัทที่ให้บริการแก่กรมทรัพย์สินทางปัญญาในด้านต่าง ๆ เพื่อสนับสนุนการดำเนินการตามภารกิจของกรมทรัพย์สินทางปัญญา

“ทรัพย์สิน” หมายความว่า ทรัพย์สินหรือสิ่งอื่นใดอันมีมูลค่าหรือคุณค่าต่อกรมทรัพย์สินทางปัญญา

“อุปกรณ์สื่อสารพกพา (Mobile Device)” หมายความว่า โทรศัพท์มือถือสมาร์ทโฟน (Smartphone) หรือแท็บเล็ต (Tablet)

“โปรแกรมอรรถประโยชน์ (Utility Program)” หมายความว่า โปรแกรมจัดการงานพื้นฐานและบริการต่าง ๆ ซึ่งอำนวยความสะดวกให้กับผู้พัฒนาระบบและผู้ดูแลระบบในการดูแลระบบสารสนเทศของกรมทรัพย์สินทางปัญญา

“ระบบวิศวกรรมความมั่นคงปลอดภัย” หมายความว่า กรอบวิธีการออกแบบ การสร้างและดำเนินการอย่างมั่นคงปลอดภัย

“ความมั่นคงปลอดภัยของสารสนเทศ (Information Security)” หมายความว่า การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Information Security Event)” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ ที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบสารสนเทศของกรมทรัพย์สินทางปัญญาถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

องค์ประกอบของนโยบาย

แบ่งเป็น ๑๔ หมวด ประกอบด้วย

๑. นโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยของสารสนเทศ (Information Security Policy)

๒. นโยบายและแนวทางปฏิบัติการจัดโครงสร้างความมั่นคงปลอดภัยของสารสนเทศ (Organization of Information Security Policy)

๓. นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศด้านบุคลากร (Human Resource Security Policy)

๔. นโยบายและแนวทางปฏิบัติด้านการบริหารจัดการทรัพย์สิน (Asset Management Policy)

๕. นโยบายและแนวทางปฏิบัติด้านการควบคุมการเข้าถึง (Access Control Policy)

๖. นโยบายและแนวทางปฏิบัติด้านการเข้ารหัสข้อมูล (Cryptography Policy)

๗. นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security Policy)

๘. นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operation Security Policy)

๙. นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศด้านการสื่อสาร (Communications Security Policy)

๑๐. นโยบายและแนวทางปฏิบัติด้านการจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance Policy)

๑๑. นโยบายและแนวทางปฏิบัติด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships Policy)

๑๒. นโยบายและแนวทางปฏิบัติการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Information Security Event Management Policy)

๑๓. นโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยของสารสนเทศเกี่ยวกับการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management Policy)

๑๔. นโยบายและแนวทางปฏิบัติในการปฏิบัติตามข้อกำหนด (Compliance Policy)

นโยบายที่ ๑
นโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยของสารสนเทศ
(Information Security Policy)

วัตถุประสงค์

๑. เพื่อกำหนดทิศทางและแนวทางปฏิบัติในการดำเนินการด้านความมั่นคงปลอดภัยของสารสนเทศของกรมทรัพย์สินทางปัญญา

๒. เพื่อให้สอดคล้องกับข้อกำหนดทางกฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

๓. เพื่อผลักดันให้มีการควบคุมภายในของสารสนเทศที่รัดกุมตามแนววิเคราะห์ความเสี่ยงที่สอดคล้องกับมาตรฐานสากล

๔. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับกรมฯ ได้รับทราบ และตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ

ผู้รับผิดชอบ

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม

๒. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และส่วนงานที่เกี่ยวข้อง

แนวทางปฏิบัติ

๑. จัดทำเอกสารนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของสารสนเทศเป็นลายลักษณ์อักษรโดยต้องได้รับอนุมัติจากกรมทรัพย์สินทางปัญญาพร้อมทั้งเผยแพร่นโยบายฯ ให้ผู้ใช้งานได้รับทราบ

๒. จัดตั้งคณะกรรมการด้านความมั่นคงปลอดภัยสารสนเทศของกรมฯ โดยให้มีตัวแทนจากกองต่าง ๆ ร่วมเป็นสมาชิกในคณะกรรมการ

๓. ทบทวนและปรับปรุงนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของสารสนเทศอย่างสม่ำเสมอและทันเหตุการณ์ โดยทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีเหตุการณ์ที่สำคัญ

๔. จัดให้มีทรัพยากร ด้านงบประมาณ ทรัพยากรบุคคล การบริหารจัดการเทคโนโลยีสารสนเทศที่เพียงพอต่อการบริหารจัดการด้านความมั่นคงปลอดภัย

นโยบายที่ ๒
นโยบายและแนวทางปฏิบัติการจัดโครงสร้างความมั่นคงปลอดภัยของสารสนเทศ
(Organization of Information Security Policy)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม กำกับ และติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศ และเพื่อเป็นแนวทางการควบคุมอุปกรณ์ประมวลผลสารสนเทศของกรมทรัพย์สินทางปัญญาที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารเพื่อปฏิบัติงานจากภายนอก

การจัดโครงสร้างภายในองค์กร

ผู้รับผิดชอบ

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม

๒. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

แนวทางปฏิบัติ

๑. กำหนดบทบาทหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ

๒. กำหนดรายละเอียดหน้าที่และความรับผิดชอบของแต่ละกลุ่มงานอย่างชัดเจน และให้มีการสอบทานระหว่างกันได้

๓. จัดทำโครงสร้างการสั่งการและการอนุมัติตามสายงาน และเผยแพร่ให้ผู้ที่เกี่ยวข้องได้รับทราบและถือปฏิบัติ

๔. สร้างความตระหนักให้กับผู้ปฏิบัติงานในการใช้งานอุปกรณ์ประมวลผล อุปกรณ์ประมวลผลเคลื่อนที่ หรือ อุปกรณ์สื่อสารพกพาอย่างมั่นคงปลอดภัย

๕. จัดทำและปรับปรุงรายชื่อผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยให้เป็นปัจจุบันอยู่เสมอ

๖. ระบุรายละเอียดด้านความมั่นคงปลอดภัยของสารสนเทศในการบริหารจัดการโครงการที่เกี่ยวข้องกับระบบสารสนเทศของกรมฯ

การควบคุมอุปกรณ์ประมวลผล

ผู้รับผิดชอบ

ผู้ใช้งานและผู้ที่เกี่ยวข้อง

แนวทางปฏิบัติ

๑. อุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของกรมฯ ถือเป็นทรัพย์สินของกรมฯ โดยใช้เพื่อการดำเนินงานของกรมฯ เท่านั้น

๒. ผู้ใช้งานต้องไม่แก้ไข ปรับแต่ง เปลี่ยนแปลง หรือติดตั้งโปรแกรมต่างๆ บนเครื่องคอมพิวเตอร์และ/หรืออุปกรณ์เคลื่อนที่ของกรมฯ เว้นแต่ได้รับความเห็นชอบจากผู้บังคับบัญชา

๓. การคืน หรือส่งซ่อมอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของกรมฯ ให้ลบข้อมูลตามขั้นตอนการปฏิบัติการทำลายสื่อ

๔. เมื่อพบความผิดปกติบนเครื่องคอมพิวเตอร์หรือซอฟต์แวร์ที่ใช้งานหรือสงสัยว่ามีการติดไวรัสคอมพิวเตอร์ มัลแวร์ แรนซัมแวร์ หรือพบข้อมูลภัยคุกคาม ผู้ใช้งานต้องยุติการเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายและแจ้งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบโดยทันที

๕. ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย หากอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของกรมฯ สูญหาย จะต้องแจ้งให้กลุ่มบริหารงานพัสดุและศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบโดยทันที

๖. ผู้ใช้งานต้องปฏิบัติตามนโยบายการสำรองข้อมูล (Back up Policy)

๗. ต้องตรวจสอบหาไวรัส มัลแวร์ แรมซั่มแวร์ จากอุปกรณ์สื่อบันทึกพกพา อีเมล์ หรือไฟล์ที่ดาวน์โหลดจากอินเทอร์เน็ตด้วยโปรแกรมที่กรมฯ กำหนดเสมอ

๘. ไม่ติดตั้งโปรแกรมที่สุ่มเสี่ยงการกระทำผิดกฎหมาย และละเมิดลิขสิทธิ์ในอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของกรมฯ

๙. การใช้งานอุปกรณ์ประมวลผล อุปกรณ์ประมวลผลเคลื่อนที่ หรือ อุปกรณ์สื่อสารพกพา ส่วนบุคคลในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ของกรมฯ จะต้องได้รับการอนุญาตจากผู้บังคับบัญชา โดยต้องลงทะเบียนกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และต้องปฏิบัติตามขั้นตอนที่กรมฯ กำหนด กรณีที่ก่อให้เกิดความเสียหายกับระบบสารสนเทศของกรมฯ ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

การปฏิบัติงานจากภายนอก (Teleworking)

ผู้รับผิดชอบ

ผู้ใช้งานและผู้ที่เกี่ยวข้อง

แนวทางปฏิบัติ

๑. การใช้อุปกรณ์ประมวลผล อุปกรณ์ประมวลผลเคลื่อนที่ หรือ อุปกรณ์สื่อสารพกพา ส่วนบุคคลเพื่อปฏิบัติงานจากภายนอกกรมฯ ต้องปฏิบัติตามแนวทางปฏิบัติการปฏิบัติงานจากภายนอก (Teleworking) และจะต้องเชื่อมต่อเข้ากับระบบสารสนเทศของกรมฯ โดยใช้ช่องทางที่กรมฯ จัดเตรียมไว้เท่านั้น

๒. ผู้ที่สามารถเข้าถึงจากระยะไกล ต้องหลีกเลี่ยงการใช้เครือข่ายคอมพิวเตอร์สาธารณะแบบไร้สาย (Free Wi-Fi) ในการเชื่อมต่อเข้าระบบสารสนเทศของกรมฯ

๓. สิทธิ์การใช้งานเพื่อปฏิบัติงานจากภายนอก ไม่สามารถถ่ายโอนกันได้

๔. ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น กรณีที่มีความเสียหายต่อระบบที่เกิดจากการปฏิบัติงานจากภายนอกกรมฯ

นโยบายที่ ๓
นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศด้านบุคลากร
(Human Resource Security Policy)

วัตถุประสงค์

๑. เพื่อสร้างความมั่นคงปลอดภัยทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และสิ้นสุดการจ้างงาน รวมถึงการเปลี่ยนแปลงตำแหน่งหรือเปลี่ยนแปลงการจ้างงานของกรมทรัพย์สินทางปัญญา

๒. เพื่อให้มีการฝึกอบรมและควบคุมการปฏิบัติงานของบุคลากรอย่างเหมาะสม

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. กลุ่มบริหารงานบุคคลและส่วนที่เกี่ยวข้อง

แนวทางปฏิบัติ

๑. กลุ่มบริหารงานบุคคลต้องตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นผู้บริหาร ข้าราชการ พนักงานราชการ ลูกจ้างประจำ หรือลูกจ้างตามสัญญาจ้างตามหน่วยงาน ให้เป็นไปตามกฎหมายที่เกี่ยวข้อง

๒. กำหนดเงื่อนไข ข้อตกลงในการปฏิบัติงาน และข้อตกลงด้านความมั่นคงปลอดภัยของสารสนเทศ พร้อมทั้งให้ผู้ใช้งานลงนามในข้อตกลงดังกล่าว

๓. จัดการฝึกอบรมให้แก่ผู้ใช้งาน เพื่อสร้างความตระหนักเรื่องความมั่นคงปลอดภัยของสารสนเทศของกรมฯ

๔. จัดการฝึกอบรมและพัฒนาความรู้ด้านความมั่นคงปลอดภัยของสารสนเทศแก่ผู้มีหน้าที่ดูแลรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

๕. จัดให้มีมาตรการดำเนินการกับผู้ฝ่าฝืนหรือละเมิดนโยบายความมั่นคงปลอดภัยของสารสนเทศของกรมฯ

๖. เมื่อสิ้นสุดการจ้างหรือเปลี่ยนแปลงลักษณะการจ้างงาน ผู้ใช้งานจะต้องคืนทรัพย์สินของกรมฯ ที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนทันที

นโยบายที่ ๔
นโยบายและแนวทางปฏิบัติด้านการบริหารจัดการทรัพย์สิน
(Asset Management Policy)

วัตถุประสงค์

๑. เพื่อระบุทรัพย์สินที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของกรมฯ

๒. เพื่อกำหนดหน้าที่ความรับผิดชอบในการดูแลทรัพย์สินจากภัยคุกคามต่าง ๆ

๓. เพื่อกำหนดระดับที่เหมาะสมของการป้องกันสารสนเทศ

๔. เพื่อกำหนดหลักเกณฑ์ที่เหมาะสมสำหรับการใช้งานทรัพย์สินของกรมฯ

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. กลุ่มบริหารงานพัสดุ

แนวทางปฏิบัติ

๑. จัดทำบัญชีรายการทรัพย์สินที่เกี่ยวข้องกับระบบสารสนเทศ พร้อมทั้งระบุผู้รับผิดชอบรายการทรัพย์สิน และต้องดำเนินการทบทวนและปรับปรุงให้เป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

๒. ใช้งานทรัพย์สินด้วยความระมัดระวัง และจัดให้มีแผนการจัดหา บำรุงรักษา และจำหน่ายทรัพย์สินให้เหมาะสม

๓. จัดประเภทข้อมูลโดยจัดระดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง ระยะเวลาการจัดเก็บ และสถานที่จัดเก็บข้อมูล เพื่อป้องกันมิให้ข้อมูลถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาตโดยปฏิบัติตามวิธีปฏิบัติการจัดระดับชั้นความลับของข้อมูล

๔. จัดเก็บสื่อบันทึกข้อมูลอย่างปลอดภัย โดยจัดให้อยู่ในสภาพแวดล้อมที่ไม่เป็นอันตรายต่อสื่อบันทึกข้อมูล

๕. ในกรณีที่ผู้ใช้งานจำเป็นต้องนำสื่อบันทึกข้อมูลออกจากกรมฯ จะต้องแจ้งให้ผู้บังคับบัญชาหรือเจ้าของสื่อบันทึกข้อมูลรับทราบ และต้องดูแลรักษาและป้องกันความเสียหายที่อาจเกิดขึ้นระหว่างการนำสื่อบันทึกข้อมูลดังกล่าวออกจากกรมฯ หรือจากการเข้าถึงของผู้ไม่มีสิทธิ โดยต้องบันทึกข้อมูลการโยกย้ายสื่อ

๖. ในกรณีที่สื่อบันทึกข้อมูลไม่ได้ถูกนำมาใช้งานแล้ว ก่อนที่จะนำออกไปจากกรมฯ ต้องมั่นใจว่าข้อมูลที่อยู่ในสื่อดังกล่าวไม่สามารถกู้คืนกลับมาใช้งานได้อีก โดยปฏิบัติตามขั้นตอนการทำลายสื่อ

๗. จัดทำวิธีการทำลายสื่อบันทึกข้อมูลที่เหมาะสมและชัดเจน และในกรณีที่มีการทำลายสื่อบันทึกข้อมูลโดยผู้ให้บริการภายนอก ต้องมีการทำข้อตกลงเกี่ยวกับการรักษาความลับของกรมฯ

นโยบายที่ ๕
นโยบายและแนวทางปฏิบัติด้านการควบคุมการเข้าถึง
(Access Control Policy)

วัตถุประสงค์

๑. เพื่อกำหนดการบริหารจัดการสิทธิการเข้าถึงระบบสารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ ระบบปฏิบัติการ และแอปพลิเคชัน (Application) ของกรมฯ

๒. เพื่อป้องกันการเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ใช้งานและผู้ที่เกี่ยวข้อง

แนวทางปฏิบัติ

๑. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึง การใช้งานระบบสารสนเทศ การกำหนดสิทธิและการมอบอำนาจการเข้าถึง โดยทบทวนความเหมาะสมอย่างน้อยปีละ ๑ ครั้ง

๒. กำหนดกระบวนการสำหรับการลงทะเบียน การปรับปรุง และการยกเลิกสิทธิผู้ใช้งาน โดยกระบวนการดังกล่าวจะต้องมีการจัดเก็บข้อมูลไว้เป็นหลักฐานเพื่อการตรวจสอบในกรณีที่มีปัญหาเกิดขึ้น ตามขั้นตอนปฏิบัติการบริหารจัดการสิทธิ (User Management Procedure)

๓. ผู้ใช้งานที่ต้องการเข้าใช้ระบบสารสนเทศนอกเหนือจากสิทธิที่กำหนดไว้ต้องได้รับการพิจารณาจากผู้มีอำนาจอนุมัติตามขั้นตอนปฏิบัติการบริหารจัดการสิทธิ (User Management Procedure) โดยมีกำหนดระยะเวลาในการใช้งาน และเมื่อพ้นกำหนดระยะเวลาดังกล่าวให้ระงับสิทธิการใช้งานโดยทันที

๔. ทบทวนและปรับปรุงสิทธิการใช้งานอย่างน้อยปีละ ๑ ครั้ง

๕. ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงระบบสารสนเทศได้

๖. ควบคุมการเข้าถึงระบบสารสนเทศผ่านระบบพิสูจน์ตัวตน (Authentication) อย่างมั่นคงปลอดภัย เช่น มีข้อความแจ้งเตือนผู้ไม่มีสิทธิเข้าถึงระบบงาน จำกัดจำนวนครั้งที่อนุญาตให้เข้าระบบผิดพลาด ไม่แสดงรหัสผ่านบนหน้าจอโดยไม่ปิดบัง ไม่เก็บรักษาหรือส่งผ่านรหัสผ่านในลักษณะ Clear text

๗. จำกัดการใช้งานโปรแกรมอรรถประโยชน์เฉพาะผู้ที่ได้รับสิทธิเท่านั้น

๘. จัดให้มีการควบคุมการเข้าถึงซอร์สโค้ด (Source Code) ของระบบสารสนเทศของกรมฯ

๙. บริหารจัดการบัญชีผู้ใช้งาน (Username account) รหัสผ่าน (Password) และสิทธิการเข้าถึงระบบแยกตามหน้าที่ความรับผิดชอบของผู้ใช้งาน โดยผู้ที่รับผิดชอบระบบสารสนเทศนั้น ๆ

๑๐. ผู้ใช้งานจะต้องกำหนดรหัสผ่านส่วนบุคคลของกรมฯ ตามวิธีการดังต่อไปนี้

(๑) กำหนดรหัสผ่านส่วนบุคคลไม่น้อยกว่า ๘ ตัวอักษร

(๒) รหัสผ่านส่วนบุคคลต้องประกอบด้วยตัวอักษรทั้งตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข หรือสัญลักษณ์พิเศษประกอบกันอย่างน้อย ๓ ชนิด

(๓) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อ นามสกุล ชื่อของบุคคลใกล้ชิด หรือคำศัพท์ในพจนานุกรม เพื่อป้องกันการคาดเดารหัสผ่านได้โดยง่าย

(๔) ไม่ใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ

(๕) ไม่เปิดเผยรหัสผ่านให้ผู้อื่นทราบหรือจดบันทึกรหัสผ่านไว้ในสถานที่ที่บุคคลอื่นสามารถเข้าถึงได้โดยง่าย

๑๑. ผู้ใช้งานต้องไม่อนุญาตให้ผู้ใช้งานอื่นใช้บัญชีผู้ใช้งานของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ และต้องออกจากระบบ (Log out) ในเวลาที่ผู้ใช้งานไม่ได้ใช้งานเครื่องคอมพิวเตอร์ เพื่อป้องกันมิให้บุคคลอื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ได้

๑๒. ผู้ดูแลระบบต้องตั้งค่าให้ผู้ใช้งานทำการเปลี่ยนรหัสผ่านตามช่วงเวลาที่เหมาะสม

๑๓. ผู้ดูแลระบบต้องดำเนินการให้เครื่องคอมพิวเตอร์สำหรับผู้ใช้งาน (PC) ทำงานร่วมกับระบบ Active Directory (AD) และบริหารจัดการให้ระบบ AD สามารถควบคุมเครื่องคอมพิวเตอร์นั้นได้ พร้อมทั้งกำหนดชื่อผู้ใช้และรหัสผ่านให้ผู้ใช้งาน

นโยบายที่ ๖
นโยบายและแนวทางปฏิบัติด้านการเข้ารหัสข้อมูล
(Cryptography Policy)

วัตถุประสงค์

เพื่อรักษาความลับและความถูกต้องของสารสนเทศจากผู้ที่ไม่ได้รับอนุญาตโดยการเข้ารหัสข้อมูลและการบริหารจัดการกุญแจเข้ารหัส

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวทางปฏิบัติ

๑. กำหนดมาตรการในการเข้ารหัสข้อมูล และแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูลให้สอดคล้องกับระดับชั้นความลับของข้อมูล

๒. กำหนดให้มีการเข้ารหัสข้อมูลโดยใช้อัลกอริทึมที่เป็นมาตรฐานสากลและใช้กุญแจการเข้ารหัสที่มีความยาวไม่น้อยกว่า ๑๒๘ บิต อีกทั้งต้องมีการทบทวนอัลกอริทึมและความยาวของกุญแจที่เข้ารหัสอย่างน้อยปีละ ๑ ครั้ง เพื่อให้ยังสามารถรักษาไว้ซึ่งความมั่นคงปลอดภัย

๓. กำหนดให้มีกระบวนการในการบริหารจัดการกุญแจโดยครอบคลุมการสร้าง การจัดเก็บ การจัดส่ง และการเปลี่ยนแปลง

นโยบายที่ ๗
นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
(Physical and Environmental Security Policy)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมและป้องกันการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. ผู้ใช้งาน และผู้ให้บริการภายนอก

แนวทางปฏิบัติ

๑. จัดสรรพื้นที่โดยกั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า - ออกของศูนย์คอมพิวเตอร์ เพื่อป้องกันการเข้าถึงระบบสารสนเทศของกรมฯ

๒. กำหนดให้การเดินสายไฟฟ้า สายสื่อสาร และสายเคเบิลอื่น ๆ ได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต จากการทำให้เกิดความเสียหายต่อการส่งสัญญาณ หรือจากการทำให้สายสัญญาณเหล่านั้นเสียหาย

๓. จัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์ (Loading Area) แก่ผู้ให้บริการภายนอกเพื่อป้องกันการเข้าถึงทรัพย์สินของกรมฯ

๔. ติดตั้งระบบป้องกันภัยต่าง ๆ ในศูนย์คอมพิวเตอร์หรือพื้นที่ควบคุมอย่างเหมาะสม เช่น ติดตั้งอุปกรณ์ดับเพลิง กล้องวงจรปิด ระบบปรับอากาศ ระบบสำรองกระแสไฟฟ้า ระบบ Access Control การควบคุมความชื้น เป็นต้น

๕. ควบคุมการเข้า - ออกของบุคคลภายนอก และเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในระหว่างปฏิบัติงานภายในกรมฯ ตามวิธีปฏิบัติการเข้า - ออกพื้นที่ศูนย์คอมพิวเตอร์

๖. กำหนด และทบทวนสิทธิการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

นโยบายที่ ๘
นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ
(Operation Security Policy)

วัตถุประสงค์

๑. เพื่อสร้างกระบวนการด้านการบริหารจัดการการรักษาความมั่นคงปลอดภัยของสารสนเทศ

๒. เพื่อป้องกันระบบสารสนเทศของกรมทรัพย์สินทางปัญญาจากการถูกบุกรุกของไวรัสคอมพิวเตอร์ (Computer Virus)

๓. เพื่อให้มีกระบวนการสำรองข้อมูล

๔. เพื่อให้มีกระบวนการจัดการ และเปลี่ยนแปลงทรัพยากร

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวทางปฏิบัติ

๑. วางแผนการใช้งานทรัพยากรสารสนเทศเพิ่มเติมในอนาคต เพื่อให้ระบบมีประสิทธิภาพที่เหมาะสมและเพียงพอต่อการใช้งาน

๒. ตั้งค่าเวลาของเครื่องคอมพิวเตอร์ทุกเครื่อง ให้ตรงกับเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการข้อมูลเวลาที่กำหนด โดยการตั้งค่าเวลาด้วย Network Time Protocol (NTP)

๓. ในกรณีที่มีการเปลี่ยนแปลงของอุปกรณ์ระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ ผู้ดูแลระบบหรือผู้พัฒนาระบบต้องดำเนินการตามขั้นตอนปฏิบัติการบริหารการเปลี่ยนแปลง (Change Management Procedure)

๔. หากผู้ดูแลระบบหรือผู้ให้บริการภายนอกต้องการใช้เครื่องมือต่างๆ (tools) เพื่อการตรวจสอบระบบเครือข่ายคอมพิวเตอร์หรือต้องการติดตั้งอุปกรณ์เครือข่ายคอมพิวเตอร์ จะต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และในกรณีการติดตั้งอุปกรณ์เครือข่ายคอมพิวเตอร์ จะต้องติดตั้งโดยผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้น

๕. ติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ในเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) พร้อมทั้งปรับปรุงให้ทันสมัยอยู่เสมอ

๖. ไม่อนุญาตให้ผู้ใช้งานครอบครองหรือพัฒนาโปรแกรมไวรัสคอมพิวเตอร์ โปรแกรมที่ก่อกวนหรือโปรแกรมที่มุ่งร้าย (Computer Worm or Trojan) ทำลายระบบสารสนเทศของกรมฯ และหน่วยงานอื่น ๆ

๗. ไม่อนุญาตให้ติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนเครื่องคอมพิวเตอร์แม่ข่ายและ อุปกรณ์ประมวลผลอุปกรณ์ประมวลผลเคลื่อนที่ หรือ อุปกรณ์สื่อสารพกพา ของกรมฯ

๘. ไม่อนุญาตให้ผู้ใช้งานคัดลอกซอฟต์แวร์อันมีลิขสิทธิ์ของกรมฯ หรือนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้บุคคลอื่นใช้งานโดยผิดกฎหมาย

๙. ติดตามและกำกับดูแล เพื่อไม่ให้ละเลยการปฏิบัติตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของสารสนเทศ

๑๐. กำหนดระยะเวลาการสิ้นสุดการใช้งานระบบสารสนเทศ (Session Timeout) เมื่อว่างเว้นจากการใช้งานมากกว่า ๑๕ นาที

๑๑. เมื่อไม่ใช้งานเครื่องคอมพิวเตอร์ ผู้ใช้งานจะต้องทำการออกจากระบบทุกครั้ง

๑๒. จัดให้มีอุปกรณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ เช่น อุปกรณ์ป้องกันเครือข่าย หรืออุปกรณ์บันทึก log อย่างเพียงพอ

๑๓. ทบทวนและปรับปรุงเวอร์ชัน (Version) ของระบบปฏิบัติการและซอฟต์แวร์ต่าง ๆ ในเครื่องคอมพิวเตอร์แม่ข่ายให้เป็นปัจจุบันอยู่เสมอ

๑๔. การติดตั้งและเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๑๕. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของกรมฯ ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑๖. จัดให้มีการบันทึกรายละเอียดการเข้าถึง และการแก้ไขเปลี่ยนแปลงสิทธิในการเข้าถึงระบบสำหรับผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบในภายหลัง

๑๗. มีการบันทึกและสอบทานการปฏิบัติงานของผู้ดูแลระบบ

๑๘. ต้องทำการสำรองข้อมูลระบบสารสนเทศ (Information Backup) ของกรมฯ ให้อยู่ในสภาพพร้อมใช้งาน อย่างน้อยเดือนละ ๑ ครั้ง

๑๙. มีการทดสอบความพร้อมใช้งานของข้อมูลระบบสารสนเทศ (Information Restore) ของกรมฯ อย่างน้อยปีละ ๑ ครั้ง

๒๐. ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้ในสื่อบันทึกอื่น ๆ และจัดเก็บสื่อสำรองข้อมูลในที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๒๑. ไม่เก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานไว้ในเครื่องคอมพิวเตอร์ หรือพื้นที่ของเครื่องแม่ข่ายที่กรมฯ จัดสรรไว้

๒๒. ต้องมีระบบประมวลผลสำรอง ระบบเครือข่ายสำรอง สำหรับข้อมูลและระบบสารสนเทศที่สำคัญของกรมฯ ให้สามารถดำเนินการได้อย่างต่อเนื่องในกรณีที่ระบบหลักทำงานไม่ได้

นโยบายที่ ๙
นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศด้านการสื่อสาร
(Communications Security Policy)

วัตถุประสงค์

๑. เพื่อบริหารจัดการการสื่อสารและระบบเครือข่ายคอมพิวเตอร์เพื่อให้ทำการส่งผ่านข้อมูลสารสนเทศทั้งภายในและภายนอกให้มีความมั่นคงปลอดภัย

๒. เพื่อป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ใช้งานและผู้เกี่ยวข้อง

แนวทางปฏิบัติ

๑. จัดระบบเครือข่ายคอมพิวเตอร์ให้เป็นสัดส่วนชัดเจน เช่น พื้นที่ส่วนระบบเครือข่ายคอมพิวเตอร์ (Network Zone) พื้นที่ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) เป็นต้น เพื่อความสะดวกในการปฏิบัติงานและการควบคุมการเข้าถึงอุปกรณ์ต่างๆ

๒. ต้องมีการปรับปรุงช่องโหว่อย่างสม่ำเสมอ และต้องมีการสำรองค่า Configuration ของเครื่องแม่ข่ายและอุปกรณ์เครือข่ายทุกครั้งที่ติดตั้ง หรือมีการเปลี่ยนแปลง หรือตามระยะเวลาที่กำหนด

๓. ต้องไม่เปิดเผย OS Version, Service Port, IP Address และ Service Patch Version ให้บุคคลที่ไม่เกี่ยวข้องทราบ

๔. ออกจากระบบทุกครั้งเมื่อเลิกใช้งาน

๕. ผู้ดูแลระบบต้องสำรองข้อมูลและระบบปฏิบัติการอย่างน้อยเดือนละ ๑ ครั้ง และทดสอบการสำรองข้อมูลอย่างน้อยปีละ ๑ ครั้ง โดยสอดคล้องกับความสำคัญของระบบ

๖. เครื่องแม่ข่ายและอุปกรณ์เครือข่ายต้องได้รับการตั้งค่าให้มีความมั่นคงปลอดภัยก่อนนำมาติดตั้งบนระบบเครือข่าย เช่น การกำหนดรหัสผ่านสำหรับบัญชีรายชื่อซึ่งใช้ในการบริการจัดการอุปกรณ์ให้มีความแข็งแกร่ง เปิด Service Port เฉพาะที่จำเป็นต้องใช้งานเท่านั้น เป็นต้น รวมทั้ง กำหนด Access Control List ของตัวอุปกรณ์สื่อสารเพื่อลดช่องโหว่ต่าง ๆ อย่างเหมาะสม

๗. กำหนดให้มีวิธีปฏิบัติในการเก็บบันทึก Log และตรวจสอบสิ่งผิดปกติต่างๆ ภายในระบบเครือข่าย

๘. การใช้งานเครื่องมือต่างๆ (Tools) เพื่อตรวจสอบระบบเครือข่าย ต้องกระทำโดยผู้ดูแลระบบเครือข่ายหรืออยู่ภายใต้การควบคุมดูแลของผู้ดูแลระบบเครือข่ายเท่านั้น และต้องได้รับการอนุมัติจากเจ้าของระบบงานที่เกี่ยวข้องก่อนทุกครั้ง โดยจะจำกัดการใช้งานเฉพาะเท่าที่จำเป็นเท่านั้น ตามที่กำหนดไว้ในนโยบายการดำเนินการของระบบเทคโนโลยีสารสนเทศ

๙. ผู้ใช้งานทุกคนจะได้รับสิทธิในการเข้าใช้งานระบบต่าง ๆ รวมถึงระบบเครือข่าย ตามหน้าที่รับผิดชอบเท่าที่จำเป็นเท่านั้น โดยผู้ใช้งานที่ต้องการเข้าถึงระบบใด ๆ ต้องดำเนินการขออนุมัติทุกครั้ง ทั้งนี้ การพิจารณาให้สิทธิในการเข้าถึงระบบจะต้องสอดคล้องตามนโยบายการควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑๐. ผู้ใช้งานต้องระบุตัวตนผ่านระบบ Active Directory (AD) ของกรมฯ ก่อนเข้าใช้งานระบบเครือข่ายของกรมฯ ทุกครั้ง

๑๑. การเชื่อมต่อเข้าสู่ระบบเครือข่ายของกรมฯ ผ่านระบบเครือข่ายไร้สายต้องได้รับการเข้ารหัสอย่างเหมาะสม

๑๒. การใช้งานเครือข่ายผู้ใช้งานต้องสามารถเข้าถึงระบบเครือข่าย ระบบเครือข่ายไร้สาย และระบบสารสนเทศได้เพียงบริการที่ได้รับอนุญาตเข้าถึงเท่านั้น

๑๓. กำหนดเกณฑ์การระงับสิทธิ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Matrix) ที่ได้กำหนดไว้

๑๔. ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่งโอนย้าย หรือสิ้นสุดการจ้าง

๑๕. สิทธิการเข้าถึงของหน่วยงานภายนอก หรือผู้ให้บริการภายนอก (Third Party) ต้องได้รับการถอดถอนเมื่อสิ้นสุดการดำเนินงาน หมดสัญญา หรือสิ้นสุดข้อตกลงทันที และต้องมีการปรับปรุงให้เป็นปัจจุบัน

๑๖. การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกกรมฯ (User Authentication for External Connections) ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (Identification) เพื่อยืนยันตัวบุคคลด้วยชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ทุกครั้ง

๑๗. ให้มีการตรวจสอบผู้ใช้งานที่อยู่ภายนอกกรมฯ ทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

๑๘. ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์ โดยมีการแสดงตัวตนด้วยชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password)

๑๙. มีการควบคุมการใช้งานอย่างเหมาะสมด้วย MAC address ของอุปกรณ์ที่กรมฯ อนุญาตให้ใช้งานได้

๒๐. จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้ผ่าน IP address ที่อนุญาตเท่านั้น

๒๑. ห้ามนำอุปกรณ์เครือข่ายมาติดตั้งกับระบบเครือข่ายของกรมฯ โดยไม่รับอนุญาต

๒๒. ห้ามผู้ใช้งานเครือข่ายกระทำการใดๆ ที่รบกวนระบบเครือข่าย โดยการเปิดใช้งาน Service DHCP เพื่อเชื่อมต่อเข้ากับระบบเครือข่ายของกรมฯ

๒๓. สายสัญญาณที่ใช้ในการเชื่อมต่อการสื่อสาร ทำการเดินในท่อนำสัญญาณอย่างเหมาะสม และมีการจัดหรือรวบสายสัญญาณให้เป็นระเบียบและจัดทำระเบียนสายสัญญาณ (Label)

๒๔. ไม่อนุญาตให้ผู้ใช้งานเปิดเผยข้อมูลหมายเลขประจำเครื่องคอมพิวเตอร์ (IP Address) แผนผังระบบเครือข่ายคอมพิวเตอร์ (Network Diagram) แผนผังระบบ (System Diagram) การตั้งค่าอุปกรณ์ (Configuration) หรือข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการเชื่อมต่อเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของกรมฯ ให้กับบุคคลอื่นที่ไม่มีสิทธิทราบ

๒๕. การใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

(๑) ไม่อนุญาตให้ส่งหรือใช้จดหมายอิเล็กทรอนิกส์ที่ผิดกฎระเบียบของกรมฯ ผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

(๒) ไม่อนุญาตให้ส่งหรือใช้จดหมายอิเล็กทรอนิกส์ที่เป็นจดหมายลูกโซ่ โดยไม่ได้รับอนุญาตจากกรมฯ

(๓) จดหมายอิเล็กทรอนิกส์จะถูกเก็บเป็นความลับ หากผู้ใช้งานใดพยายามเข้าถึงจดหมายอิเล็กทรอนิกส์ของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิในจดหมายอิเล็กทรอนิกส์ดังกล่าวจะถูกพิจารณาดำเนินการทางวินัยและทางกฎหมาย

(๔) ผู้ดูแลระบบไม่มีสิทธิเข้าถึง อ่าน หรือกระทำการอื่นใดต่อจดหมายอิเล็กทรอนิกส์ของผู้ใช้งาน

๒๖. ไม่อนุญาตให้ผู้ดูแลระบบใช้อำนาจหน้าที่ของตนไปในการเข้าถึงข้อมูลที่รับหรือส่งผ่านระบบเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และจะต้องไม่เปิดเผยข้อมูลที่ตนได้รับเนื่องจากการปฏิบัติหน้าที่ผู้ดูแลระบบ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ

๒๗. ผู้ใช้งานมีหน้าที่รักษาความปลอดภัยในการใช้ระบบเครือข่ายคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งไม่อนุญาตให้บุคคลอื่นเข้าใช้ระบบเครือข่ายคอมพิวเตอร์จากบัญชีของผู้ใช้งาน

๒๘. ผู้ใช้งานเป็นผู้รับผิดชอบต่อข้อมูลที่มีความสำคัญของตนเอง ไม่ว่าจะถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องคอมพิวเตอร์แม่ข่าย รวมทั้งรับผิดชอบต่อการส่งข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์

นโยบายที่ ๑๐
นโยบายและแนวทางปฏิบัติด้านการจัดหา การพัฒนา และการบำรุงรักษาระบบ
(System Acquisition, Development and Maintenance Policy)

วัตถุประสงค์

๑. เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศมีความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ

๒. เพื่อป้องกันความผิดพลาด การสูญหาย การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต และการใช้งานสารสนเทศผิดวัตถุประสงค์

๓. เพื่อรักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยวิธีการเข้ารหัสข้อมูล

๔. เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์ สารสนเทศ และไฟล์ต่างๆ ของระบบที่ให้บริการ

๕. เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องว่างทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้พัฒนาระบบ

แนวทางปฏิบัติ

๑. การพัฒนาระบบ การจัดหา และการบำรุงรักษาระบบสารสนเทศของกรม ฯ ต้องได้รับอนุญาตก่อนดำเนินการ

๒. แยกระบบการพัฒนาและทดสอบ และระบบให้บริการจริง (Production Server) ออกจากกันเพื่อลดความเสี่ยงในการเข้าถึงหรือการแก้ไขเปลี่ยนแปลงระบบให้บริการจริง (Production Server) โดยไม่ได้รับอนุญาต

๓. ผู้พัฒนาระบบต้องยึดหลักการด้านความมั่นคงปลอดภัยในการพัฒนาระบบสารสนเทศของกรม ฯ ดังต่อไปนี้

(๑) ให้สิทธิน้อยที่สุด (Least Privileges)

(๒) ให้สิทธิเฉพาะที่จำเป็นในการปฏิบัติงาน (Need to Know)

(๓) ออกแบบระบบให้สามารถป้องกันได้หลายชั้น (Defense in-Depth)

(๔) ออกแบบในลักษณะเปิด (Open Design)

(๕) สอดคล้องกับหลักการของระบบวิศวกรรมความมั่นคงปลอดภัย (Security Engineering Principles)

๔. ผู้พัฒนาระบบจะต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยดังต่อไปนี้

(๑) การรักษาความลับของข้อมูลสารสนเทศ (Confidentiality)

(๒) การรักษาความถูกต้องสมบูรณ์ของข้อมูลสารสนเทศ (Integrity)

(๓) ความพร้อมใช้ของข้อมูลสารสนเทศ (Availability)

(๔) การระบุตัวตนผู้ใช้งาน (Identification)

(๕) การพิสูจน์ตัวตนผู้ใช้งาน (Authentication)

(๖) การกำหนดสิทธิ (Authorization)

(๗) การบันทึกกิจกรรมต่างๆ ในระบบเพื่อการตรวจสอบ (Audit Logging)

(๘) มาตรฐานรักษาความมั่นคงปลอดภัย เช่น OWASP Top ๑๐ เป็นต้น

(๙) ความต่อเนื่องของการให้บริการระบบสารสนเทศ (Continuity)

๕. ผู้พัฒนาระบบต้องไม่ดำเนินการดังต่อไปนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกการรักษาความปลอดภัยของระบบหรือการกระทำในลักษณะที่เป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือการแกะรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(๓) พัฒนาโปรแกรมใดๆ ที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนคอมพิวเตอร์ (Worm) หรือมัลแวร์ (Malware)

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่ส่งผลเป็นการจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

(๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดทรัพย์สินทางปัญญา แสดงข้อความหรือรูปภาพที่ไม่เหมาะสม หรือขัดต่อศีลธรรมอันดีของประเทศไทย ไม่ว่าผ่านช่องทางการสื่อสารใดก็ตาม

๖. ผู้พัฒนาระบบต้องจัดทำเอกสารประกอบการจัดซื้อจัดจ้างระบบสารสนเทศของกรมฯ ดังต่อไปนี้

(๑) ระบุข้อกำหนดการไม่เปิดเผยความลับหรือข้อมูลสำคัญของกรมฯ แก่บุคคลอื่น

(๒) จัดทำเอกสารขอบเขตของงาน (Terms of Reference) โดยระบุถึงความต้องการด้านความมั่นคงปลอดภัย โดยพิจารณาคุณลักษณะที่เกี่ยวข้องอย่างใดอย่างหนึ่งดังต่อไปนี้

(๒.๑) การรักษาความลับของข้อมูลสารสนเทศ (Confidentiality)

(๒.๒) การรักษาความถูกต้องสมบูรณ์ของข้อมูลสารสนเทศ (Integrity)

(๒.๓) ความพร้อมใช้ของข้อมูลสารสนเทศ (Availability)

(๒.๔) การระบุตัวตนผู้ใช้งาน (Identification)

(๒.๕) การพิสูจน์ตัวตนผู้ใช้งาน (Authentication)

(๒.๖) การกำหนดสิทธิ (Authorization)

(๒.๗) การบันทึกกิจกรรมต่างๆ ในระบบเพื่อการตรวจสอบ (Audit Logging)

(๒.๘) มาตรฐานรักษาความมั่นคงปลอดภัย เช่น OWASP หรือ SANS Top ๒๐ เป็นต้น

(๒.๙) ความต่อเนื่องของการให้บริการระบบสารสนเทศ (Continuity)

๗. ในกรณีการพัฒนาซอฟต์แวร์ ต้องปฏิบัติตามมาตรฐานการพัฒนาเว็บแอปพลิเคชัน

๘. การเปลี่ยนแปลงของระบบภายในวงจรการพัฒนาจะต้องอาศัยกระบวนการควบคุมการเปลี่ยนแปลงที่เป็นทางการ

๙. เมื่อต้องการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวข้องกับแอปพลิเคชัน (Application) จะต้องได้รับการทดสอบก่อนการเปลี่ยนแปลง เพื่อให้มั่นใจว่าไม่มีผลกระทบต่อการดำเนินการของกรมฯ หรือต่อความมั่นคงปลอดภัย

๑๐. ในกรณีที่มีการแก้ไขเปลี่ยนแปลงชุดซอฟต์แวร์แพ็คเกจ (Software Package) จะต้องถูกป้องกันโดยจำกัดการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกควบคุมอย่างเข้มงวด

๑๑. จัดทำหลักการของระบบวิศวกรรมความมั่นคงปลอดภัยเป็นลายลักษณ์อักษร เพื่อนำมาใช้งานสำหรับการประยุกต์ใช้ระบบสารสนเทศ

๑๒. กำหนดหลักเกณฑ์ความมั่นคงปลอดภัยของสภาพแวดล้อมเพื่อการพัฒนาอย่างเหมาะสม

๑๓. การจ้างบุคคลภายนอกมาพัฒนาซอฟต์แวร์จะต้องได้รับการตรวจสอบ การกำกับดูแล และการเฝ้าระวัง โดยผู้พัฒนาระบบหรือเจ้าของระบบ

๑๔. ผู้พัฒนาระบบจะต้องดำเนินการทดสอบด้านความมั่นคงปลอดภัยในระหว่างการพัฒนาระบบ

๑๕. กำหนดหลักเกณฑ์การตรวจรับสำหรับระบบสารสนเทศใหม่ โดยต้องมีการทดสอบ การปรับปรุงและการปรับเวอร์ชัน (Version) ใหม่

๑๖. ต้องมีการควบคุมข้อมูลที่ใช้ในการทดสอบ โดยไม่ควรนำข้อมูลจากระบบงานจริงมาใช้ทดสอบ หากมีความจำเป็นที่ต้องนำข้อมูลจากระบบงานจริงมาใช้ ควรดำเนินการสร้างข้อมูลจำลองขึ้นมาโดยทำเครื่องหมายหรือแทนที่ข้อมูลเพื่อให้ไม่สามารถอ้างถึงข้อมูลจริงได้

นโยบายที่ ๑๑
นโยบายและแนวทางปฏิบัติด้านความสัมพันธ์กับผู้ให้บริการภายนอก
(Supplier Relationships Policy)

วัตถุประสงค์

๑. เพื่อกำหนดเงื่อนไขที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศสำหรับผู้ให้บริการภายนอก

๒. เพื่อประเมินผลผู้ให้บริการภายนอก

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ผู้ให้บริการภายนอก

แนวทางปฏิบัติ

๑. ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายมีอำนาจหน้าที่และความรับผิดชอบในการอนุมัติการเข้าถึงระบบสารสนเทศของกรมทรัพย์สินทางปัญญา โดยบุคคลภายนอกจะต้องทำหนังสือขออนุญาตเข้าถึงระบบสารสนเทศเป็นลายลักษณ์อักษร โดยอย่างน้อยต้องมีรายละเอียดดังต่อไปนี้

(๑) เหตุผลในการเข้าถึงระบบสารสนเทศของกรมฯ

(๒) ระยะเวลาในการเข้าถึงระบบสารสนเทศของกรมฯ

(๓) คำยินยอมจากเจ้าของระบบงานที่รับผิดชอบในการนำบุคคลภายนอกเข้ามาปฏิบัติงานภายในกรมฯ

๒. คู่สัญญาที่ปฏิบัติงานให้กับกรมฯ ไม่ว่าจะปฏิบัติงานภายในหรือภายนอกกรมฯ จะต้องลงนามในสัญญาจ้าง โดยจะต้องทำสัญญาจ้างให้เสร็จสิ้นก่อนกำหนดสิทธิให้บุคคลภายนอกนั้นเข้าถึงระบบสารสนเทศของกรมฯ

๓. คู่สัญญาที่พัฒนาระบบสารสนเทศของกรมฯ จะต้องลงนามในสัญญาให้เก็บรักษาข้อมูลไว้เป็นความลับและสรุปรายละเอียดด้านความมั่นคงปลอดภัยของสารสนเทศของผู้ให้บริการภายนอก

๔. กำหนดมาตรการควบคุมให้บุคคลภายนอกรักษาความมั่นคงปลอดภัยอย่างเคร่งครัด ทั้งด้านการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วนของข้อมูล (Integrity) และการรักษาระบบให้พร้อมใช้งานอยู่เสมอ (Availability)

๕. ควบคุมและเฝ้าระวังการปฏิบัติงานของผู้ให้บริการภายนอกให้เป็นไปตามขอบเขตที่กำหนด

๖. ในกรณีที่มีการเปลี่ยนแปลงเงื่อนไขการให้บริการ หรือรูปแบบหรือเทคโนโลยีของการให้บริการ ผู้ที่เกี่ยวข้องจะต้องประเมินความเสี่ยงที่อาจเกิดขึ้นก่อนการเปลี่ยนแปลง

๗. ผู้ให้บริการภายนอกต้องแจ้งให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายทราบทันทีหากพบว่ามีการคุกคามที่มีผลต่อความมั่นคงปลอดภัย และเจ้าของระบบงานต้องแจ้งให้คณะกรรมการบริหารจัดการรักษาความมั่นคงปลอดภัยของสารสนเทศทราบ

นโยบายที่ ๑๒
นโยบายและแนวทางปฏิบัติการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ
(Information Security Event Management Policy)

วัตถุประสงค์

๑. เพื่อให้มีกระบวนการปฏิบัติที่ถูกต้องสำหรับเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศของกรมทรัพย์สินทางปัญญาในระยะเวลาที่เหมาะสม

๒. เพื่อให้มีวิธีการที่สอดคล้องและมีประสิทธิภาพในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของกรมฯ

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวทางปฏิบัติ

๑. กำหนดหน้าที่และกระบวนการปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ เพื่อให้มั่นใจว่าการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยจะดำเนินการได้อย่างรวดเร็ว เป็นระบบ และมีประสิทธิผล

๒. จัดหาช่องทางสำหรับการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยที่เหมาะสมและรวดเร็วเท่าที่เป็นไปได้

๓. ผู้ใช้งานที่ใช้ระบบสารสนเทศต้องแจ้งให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายทราบทันทีหากพบว่ามีการคุกคามที่มีผลต่อความมั่นคงปลอดภัย และผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องแจ้งให้คณะกรรมการบริหารจัดการรักษาความมั่นคงปลอดภัยของสารสนเทศทราบ

๔. ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยและจะต้องจำแนกเหตุการณ์เหล่านั้นเป็นสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

๕. ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องทำการวิเคราะห์และแก้ไขสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

นโยบายที่ ๑๓
นโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยของสารสนเทศ เกี่ยวกับการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ
(Information Security Aspects of Business Continuity Management Policy)

วัตถุประสงค์

๑. เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่าง ๆ ทางธุรกิจ

๒. เพื่อป้องกันความล้มเหลวของระบบสารสนเทศอันอาจกระทบต่อกระบวนการทางธุรกิจที่สำคัญและสามารถกู้ระบบสารสนเทศกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวทางปฏิบัติ

๑. จัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ และจัดให้มีการซักซ้อมหรือทดสอบแผนอย่างน้อยปีละ ๑ ครั้ง

๒. ผู้ดูแลระบบต้องสำรองข้อมูลระบบงานให้เป็นไปตามผลการวิเคราะห์ผลกระทบทางธุรกิจ และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง พร้อมทั้งปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๓. ผู้ใช้งานต้องสำรองข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานของตน เพื่อให้สามารถนำมาดำเนินงานต่อไปได้ในกรณีเกิดเหตุการณ์ฉุกเฉินขึ้น

นโยบายที่ ๑๔
นโยบายและแนวทางปฏิบัติในการปฏิบัติตามข้อกำหนด
(Compliance Policy)

วัตถุประสงค์

๑. เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดด้านความมั่นคงปลอดภัยอื่นๆ

๒. เพื่อให้การตรวจประเมินระบบสารสนเทศของกรมทรัพย์สินทางปัญญาเกิดประสิทธิภาพสูงสุด และมีการแทรกแซงหรือการหยุดชะงักของกระบวนการทางธุรกิจน้อยที่สุด

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวทางปฏิบัติ

๑. ผู้ใช้งานจะต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อกำหนด ข้อบังคับ และขั้นตอนการปฏิบัติด้านความมั่นคงปลอดภัยตามหน้าที่และความรับผิดชอบของตน เพื่อให้การปฏิบัติเป็นไปตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของสารสนเทศ

๒. ผู้ใช้งานต้องระมัดระวังไม่ใช้งานซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ และกรมฯ จะไม่รับผิดชอบต่อความผิดที่เกิดจากการใช้ซอฟต์แวร์ดังกล่าว

๓. ป้องกันข้อมูลส่วนบุคคลไม่ให้ถูกเปิดเผย

๔. จัดให้มีการตรวจสอบและประเมินความเสี่ยงของสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๕. จัดทำแนวทางในการตรวจประเมินและดำเนินการตรวจประเมินความมั่นคงปลอดภัยของสารสนเทศ โดยผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) ปีละ ๑ ครั้ง

๖. ต้องปฏิบัติตามกฎหมายดังต่อไปนี้

(๑) พระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๗ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติลิขสิทธิ์ (ฉบับที่ ๒) พ.ศ.๒๕๕๘ พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ ๓) พ.ศ. ๒๕๕๘ และพระราชบัญญัติลิขสิทธิ์ (ฉบับที่ ๔) พ.ศ. ๒๕๖๑

(๒) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

(๓) ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งแก้ไขเพิ่มเติมโดยระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ ๒) พ.ศ. ๒๕๖๑

(๔) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

(๕) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

(๖) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๗) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๘) พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

(๙) พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

(๑๐) ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

(๑๑) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ซึ่งแก้ไขเพิ่มเติมโดยประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

(๑๒) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

(๑๓) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กรหรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. ๒๕๕๙

(๑๔) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕