ประกาศกรมแผนที่ทหาร
เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กรมแผนที่ทหาร
พ.ศ.๒๕๖๑

เพื่อให้การรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกรมแผนที่ทหาร เป็นไปอย่างเหมาะสม มีประสิทธิภาพและประสิทธิผล และมีความมั่นคงปลอดภัยสอดคล้องกับระเบียบกรมแผนที่ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๑ โดยคำนึงถึงหลักการพื้นฐานของการรักษาความลับ การรักษาความถูกต้องครบถ้วน และการรักษาสภาพความพร้อมใช้งาน ต่อระบบสารสนเทศ สินทรัพย์สารสนเทศ และข้อมูลสำคัญในการปฏิบัติภารกิจ อันเป็นการลดความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศ และลดความเสียหายต่างๆ ที่เกิดขึ้นจากเหตุละเมิดความมั่นคงปลอดภัย และรักษาไว้ซึ่งความสามารถในการปฏิบัติภารกิจได้อย่างต่อเนื่อง รวมทั้งสอดคล้องกับกฎหมาย และระเบียบที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศและด้านการประกอบธุรกรรมทางอิเล็กทรอนิกส์ กรมแผนที่ทหาร มีความจำเป็นอย่างยิ่งที่จะต้องมีนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อกำหนดขอบเขตและข้อกำหนดในการรักษาความปลอดภัยระบบสารสนเทศให้กับหน่วยขึ้นตรง ตลอดจนผู้ใช้งานระบบเทคโนโลยีสารสนเทศของ กรมแผนที่ทหาร จึงกำหนดนโยบาย ดังนี้

๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

๑.๑ กรมแผนที่ทหาร จัดให้มีนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Information Technology Security Policy) เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของ กรมแผนที่ทหาร ให้สอดคล้องกับข้อกำหนด การบริหารราชการ กฎหมายเทคโนโลยีสารสนเทศและกฎระเบียบที่เกี่ยวข้องและประกาศใช้อย่างเป็นลายลักษณ์อักษร และลงนามอนุมัติโดยเจ้ากรมแผนที่ทหาร รวมทั้งประกาศและเผยแพร่ ให้กำลังพลและผู้เกี่ยวข้องรับทราบและถือปฏิบัติรวมทั้งส่วนราชการในกรมแผนที่ทหาร สามารถจัดทำนโยบายเป็นของตนเองได้ โดยไม่ขัดต่อนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กรมแผนที่ทหาร

๑.๒ เจ้ากรมแผนที่ทหาร ในฐานะผู้บริหารระดับสูง (Chief Executive Officer : CEO) กรมแผนที่ทหาร เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ เกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้ใดอันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามระเบียบ กรมแผนที่ทหาร ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ

๑.๓ รองเจ้ากรมแผนที่ทหาร ในฐานะผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) กรมแผนที่ทหาร เป็นผู้รับผิดชอบด้านสารสนเทศในภาพรวมของกรมแผนที่ทหาร

๑.๔ ผู้อำนวยการกองแผนและโครงการ กองบัญชาการ กรมแผนที่ทหาร ในฐานะผู้บริหารจัดการข้อมูล (Information Management Officer : IMO) มีหน้าที่รับผิดชอบร่างกลยุทธการดำเนินงานด้านสารสนเทศของกรมแผนที่ทหาร บริหารการเก็บรักษาข้อมูลสารสนเทศทั้งรูปแบบเอกสารหรือแบบอื่น ๆ รวมทั้งกำหนดชั้นความลับ และสิทธิการเข้าถึงข้

/๑.๕ ผู้อำนวยการ...

๑.๕ ผู้อำนวยการศูนย์ข้อมูลทางแผนที่ กรมแผนที่ทหาร มีหน้าที่รับผิดชอบในการดำเนินการจัดทำและทบทวนปรับปรุงนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ รวมถึงแนวนโยบาย และ/หรือ แนวปฏิบัติที่เกี่ยวข้องให้เป็นปัจจุบันอยู่เสมอ และการประกาศให้บุคลากรและผู้เกี่ยวข้องทั้งหมดทราบ ให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามแนวนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กองบัญชาการกองทัพไทย ได้

๒. การจัดโครงสร้างส่วนราชการ เพื่อรักษาความปลอดภัยสารสนเทศ (Security Organization) เพื่อการบริหารจัดการควบคุมและกำหนดรูปแบบการติดตั้งและใช้งานระบบการรักษาความปลอดภัยสารสนเทศ ให้ครอบคลุมและมีประสิทธิภาพ ดังนี้

๒.๑ ต้องกำหนดนิยามและกระบวนการต่าง ๆ ในการรักษาความปลอดภัยที่ชัดเจน รวมถึงต้องประสานงานกับส่วนราชการที่มีส่วนเกี่ยวข้องตามแผนนโยบายรักษาความปลอดภัยของ กรมแผนที่ทหาร

๒.๒ ต้องจัดตั้งคณะหรือกลุ่มผู้ทำงานหลักเพื่อบริหารและจัดการความปลอดภัยสำหรับสารสนเทศของส่วนราชการ

๒.๓ ต้องกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานทางด้านความปลอดภัยสารสนเทศของส่วนราชการไว้อย่างชัดเจน

๒.๔ ต้องกำหนดสิทธิการใช้งานระบบสารสนเทศทั้งระบบปัจจุบันที่มีอยู่แล้วและที่จะนำเข้ามาใช้งานใหม่

๒.๕ ต้องระบุลักษณะของการเข้าใช้งานผ่านทางเครือข่าย การใช้งานในสำนักงานโดยตรง

๒.๖ ต้องระบุเหตุความจำเป็นในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศอย่างชัดเจน

๒.๗ ต้องควบคุมหน่วยงานภายนอกที่ปฏิบัติงานอยู่ในสำนักงานของส่วนราชการในการใช้งานระบบสารสนเทศและทรัพยากรสารสนเทศอื่น ๆ ให้เป็นไปอย่างปลอดภัย (รวมทั้งในสัญญาที่ทำไว้กับหน่วยงานนั้นจะต้องระบุข้อกำหนดในการใช้งานไว้อย่างชัดเจน)

๓. การสร้างความมั่นคงปลอดภัยด้านควบคุมการเข้าถึงและการใช้งานสินทรัพย์สารสนเทศ

๓.๑ ต้องบริหารจัดการสินทรัพย์สารสนเทศ (Asset Management) โดยระบุประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลหรือสารสนเทศ รวมทั้งการระบุความเป็นเจ้าของหรือผู้ดูแลสินทรัพย์สารสนเทศ

๓.๒ ต้องมีมาตรการ แนวนโยบาย และ/หรือ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านควบคุมการเข้าถึงและการใช้งานสินทรัพย์สารสนเทศ (Access Control Policy) กำหนดการเข้าถึงและควบคุมการเข้าถึงดังต่อไปนี้

๓.๒.๑ ข้อกำหนดการใช้งานตามภารกิจ

๓.๒.๒ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

๓.๒.๓ การควบคุมการเข้าถึงเครือข่าย

๓.๒.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๒.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ

๓.๒.๖ การควบคุมการเข้าถึงการใช้งานจากภายนอก

๓.๒.๗ การควบคุมการใช้งานสารสนเทศ

/๓.๒.๘ จัดให้มี...

๓.๒.๘ จัดให้มีมาตรการ แนวนโยบาย และ/หรือ แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy or Privacy Policy) ในกรณีที่ดำเนินการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม

๔. การสร้างความมั่นคงปลอดภัยด้านบุคลากร

๔.๑ ต้องกำหนดคุณสมบัติ และหน้าที่ความรับผิดชอบของบุคลากรด้านเทคโนโลยีสารสนเทศ

๔.๒ ต้องจัดอบรมให้ความรู้วิธีปฏิบัติแก่บุคลากร ความตระหนักรู้ เพื่อสร้างความปลอดภัยให้กับระบบสารสนเทศและเครือข่ายของส่วนราชการ ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของส่วนราชการด้วย

๔.๓ ต้องพิจารณาลงโทษทางวินัยและดำเนินการตามกฎหมาย ในกรณีที่มีการฝ่าฝืน หรือละเมิดนโยบายความปลอดภัยหรือระเบียบปฏิบัติเพื่อความปลอดภัยของส่วนราชการ

๕. ความปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) มาตรการ และ/หรือ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security) สำหรับพื้นที่ควบคุมและสถานที่สำคัญในการให้บริการสารสนเทศ ศูนย์ข้อมูล ศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงาน ให้ยึดถือตามแนวปฏิบัติในการควบคุมการเข้าถึงและใช้งานสารสนเทศ รวมทั้งการรักษาความมั่นคงปลอดภัยสำหรับระบบสารสนเทศและอุปกรณ์ในการให้บริการสารสนเทศ

๖. การสร้างความมั่นคงปลอดภัยด้านการปฏิบัติงาน

๖.๑ ต้องมีมาตรการ แนวนโยบาย และ/หรือ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการบริหารจัดการด้านการสื่อสารและการปฏิบัติงาน (Communications and Operations Management) ของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๖.๒ ต้องมีมาตรการ แนวนโยบาย และ/หรือ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (Information System Acquisition, Development and Maintenance)

๖.๓ ต้องมีมาตรการ แนวนโยบาย และ/หรือ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ (Information Security Incident Management) การสร้างความมั่นคงปลอดภัยด้านการบริหารความต่อเนื่องในการปฏิบัติภารกิจ

๖.๔ ต้องมีระบบสำรอง ศูนย์ข้อมูลสำรองหรือศูนย์คอมพิวเตอร์สำรอง ที่เหมาะสมสำหรับหน่วยงานและให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสมต่อภารกิจหลักของหน่วยงาน รวมทั้งนโยบายการสำรองข้อมูล (Back up Policy) เพื่อรองรับการดำเนินการตามภารกิจในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์หรือในกรณีที่ระบบหลักหรือศูนย์ข้อมูลหลักหรือศูนย์คอมพิวเตอร์หลักไม่สามารถให้บริการในระยะเวลาที่เหมาะสมต่อความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๖.๕ ต้องจัดการการบริหารความต่อเนื่องในการปฏิบัติภารกิจของหน่วยงาน (Business Continuity Management : BCM) โดยมีเนื้อหาครอบคลุม ดังนี้

/๖.๕.๑ ต้องจัดทำ...

๖.๕.๑ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ประกอบด้วยแผนรองรับการดำเนินงานอย่างต่อเนื่อง (Business Continuity Plan : BCP) และแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ (IT Contingency Plan : ITCP) ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๖.๕.๒ ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๖.๕.๓ ต้องทดสอบสภาพความพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ รวมถึงการทบทวนและปรับปรุงแผนเตรียมพร้อมกรณีฉุกเฉิน โดยความถี่ของการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อย ๑ ครั้งต่อปี

๗. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบายและข้อกำหนดความมั่นคงปลอดภัยด้านสารสนเทศ

๗.๑ ต้องประเมินความเสี่ยงด้านสารสนเทศ (Information Security Risk Assessment) และทบทวนการประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ ตามรอบระยะเวลาที่หน่วยงานกำหนด หรือ อย่างน้อยปีละ ๒ ครั้ง โดยอ้างอิงหลักเกณฑ์การประเมินความเสี่ยงที่เหมาะสมหรือที่หน่วยงานจัดทำขึ้น ซึ่งครอบคลุมปัจจัยเสี่ยงทั้งปัจจัยภายในและภายนอก ตามกระบวนงานที่สำคัญของภารกิจหลักและสินทรัพย์สารสนเทศที่เกี่ยวข้อง

๗.๒ ต้องตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนด (Compliance) อย่างสม่ำเสมอ รวมถึงการตรวจสอบด้านความมั่นคงปลอดภัยระบบสารสนเทศที่สำคัญต่อการปฏิบัติภารกิจหลัก (Information System / Information Security Audit) โดยการตรวจสอบของผู้ตรวจสอบภายในหน่วยงาน (Internal Auditor) ทั้งนี้จะตรวจสอบจากผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เฉพาะในกรณีที่จำเป็นเท่านั้น เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๗.๓ ต้องประเมินตนเองด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Self - Assessment) ของหน่วยงานสม่ำเสมอตามแนวปฏิบัติและในการรักษาความมั่นคงปลอดภัย และกระบวนงานที่สำคัญตามภารกิจของหน่วยงานต่อสภาพความเสี่ยงที่ยอมรับได้ของหน่วยงานโดยครอบคลุมหัวข้ออย่างน้อยตามกฎระเบียบที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง

๘. การปฏิบัติการตามข้อกำหนดทางด้านกฎหมาย คำสั่ง นโยบาย และระเบียบการรักษาความปลอดภัยสารสนเทศ (Compliance) เพื่อให้หัวหน้างานสารสนเทศ และนายทหารพระธรรมนูญ คำนึงถึงการปฏิบัติตามข้อกำหนดทางกฎหมาย เพื่อป้องกันการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญาและข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ โดยมีแนวนโยบาย ให้ดำเนินการให้สอดคล้องให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และมาตรฐานการรักษาความปลอดภัย

/๙. รายละเอียด...

๙. รายละเอียดเพิ่มเติม

ข้อแนะนำและแนวปฏิบัติในการดำเนินการตามรายละเอียดเพิ่มเติม มีวัตถุประสงค์เพื่อให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กรมแผนที่ทหาร และระเบียบกรมแผนที่ทหาร ว่าด้วยนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ปีพ.ศ.๒๕๖๑ เป็นมาตรการและแนวทางในการรักษาความปลอดภัยด้านสารสนเทศให้อยู่ในระดับที่มีความมั่นคงปลอดภัยสูงสุด ให้ข้าราชการลูกจ้าง และพนักงานราชการที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของ กรมแผนที่ทหาร ยึดถือและปฏิบัติอย่างเคร่งครัด หากดำเนินการแก้ไขปรับปรุงแนวปฏิบัติอื่น ๆ ให้สามารถเพิ่มเป็นภาคผนวกได้

ประกาศ ณ วันที่ ๒๖ เมษายน พ.ศ.๒๕๖๑

พลโท

(หัสฎี วงศ์อิศเรศ)
เจ้ากรมแผนที่ทหาร

ศูนย์ข้อมูลทางแผนที่ กรมแผนที่ทหาร