ระเบียบ กองบัญชาการทหารสูงสุด

ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพไทย

พ.ศ.๒๕๔๗

เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของกองทัพไทยเป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ จึงวางระเบียบไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า "ระเบียบกองบัญชาการทหารสูงสุด ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพไทย พ.ศ.๒๕๔๗"

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ บรรดาระเบียบ และคำสั่งอื่นใดในส่วนที่กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน

ข้อ ๔ ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ และลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศ ของกองบัญชาการทหารสูงสุด และเหล่าทัพ

ข้อ ๕ ในระเบียบนี้

๕.๑ ระบบสารสนเทศ (Information System) หมายความว่า ระบบข่าวสารของกองทัพไทย ที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์ และระบบสื่อสาร มาช่วยในการสร้างสารสนเทศของกองทัพไทย และสามารถนำข่าวสารมาใช้ในการวางแผน การบริหาร การพัฒนาและควบคุมซึ่งมีองค์ประกอบดังนี้

๕.๑.๑ ระบบคอมพิวเตอร์ (Computer System) หมายถึง ระบบที่ประกอบด้วยฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) และบุคลากรทางคอมพิวเตอร์ (Peopleware)

๕.๑.๒ ระบบสื่อสาร (Communication System) หมายความว่า ระบบที่ประกอบด้วยผู้รับ ผู้ส่งและสื่อกลางในระบบสื่อสารที่ใช้ในการส่งผ่านข้อมูล ทั้งระบบวงจรทางสาย และระบบไร้สาย รวมถึงอุปกรณ์ต่อพ่วงอื่น ๆ เช่น Hub, Switching, Router เป็นต้น

๕.๑.๓ สารสนเทศ (Information) ข้อเท็จจริงที่ได้จากการสกัดข้อมูลให้มีความหมายโดยผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของ ตัวเลข ข้อความหรือ

/ภาพกราฟฟิก...

ภาพกราฟฟิกที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๕.๒ เครือข่ายระบบสารสนเทศ หมายความว่า การติดต่อสื่อสาร หรือการส่งข้อมูลกันระหว่างระบบสารสนเทศภายใน บก.ทหารสูงสุด, เหล่าทัพ และการติดต่อสื่อสาร หรือการส่งข้อมูลกันระหว่าง เหล่าทัพ กับ บก.ทหารสูงสุด

ข้อ ๖ ให้ **เจ้ากรมการสนเทศทหาร กองบัญชาการทหารสูงสุด** เป็นผู้ รักษาการให้เป็นไปตามระเบียบนี้

หมวด ๑
กล่าวทั่วไป

ข้อ ๗ ความมุ่งหมายของระเบียบนี้

๗.๑ เพื่อกำหนดหลักการและมาตรการในการรักษาความปลอดภัยระบบสารสนเทศของกองทัพไทย

๗.๒ พิทักษ์รักษาและป้องกัน มิให้ข้อมูลและสิ่งที่เป็นความลับของทางราชการรั่วไหลหรือรู้ไปถึง หรือตกไปอยู่ในมือของฝ่ายตรงข้ามหรือบุคคลผู้ไม่มีอำนาจหน้าที่

๗.๓ ป้องกันการจารกรรมทั้งจากบุคคลภายในและภายนอกส่วนราชการ

๗.๔ พิทักษ์รักษาและป้องกันการก่อวินาศกรรมแก่เครื่องจักรคำนวณ อุปกรณ์เครื่องใช้ อาคาร สถานที่ และเอกสาร เป็นต้น

ข้อ ๘ หัวหน้าส่วนราชการสามารถกำหนดมาตรการรักษาความปลอดภัยให้ระบบสารสนเทศของส่วนราชการ และแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการเพิ่มเติมได้โดยให้สอดคล้องและไม่ขัด หรือแย้งกับระเบียบนี้

ข้อ ๙ เหตุผลในการประกาศใช้ระเบียบนี้ คือ วางระเบียบกองบัญชาการทหารสูงสุด ในการรักษาความปลอดภัยระบบสารสนเทศของกองทัพไทย เกี่ยวกับระบบคอมพิวเตอร์, ระบบสื่อสาร, สารสนเทศเครือข่ายระบบสารสนเทศ เพื่อให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ และลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอก ที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศ ของกองบัญชาการทหารสูงสุด และเหล่าทัพ

ข้อ ๑๐ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตาม พรบ.ข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ หรืออื่น ๆ ที่ได้ประกาศใช้ทดแทน

/หมวด ๒...

หมวด ๒

การรักษาความปลอดภัยเกี่ยวกับบุคคล

ข้อ ๑๑ ความมุ่งหมาย เพื่อเป็นการคัดเลือก ให้ได้บุคคลที่มีลักษณะเหมาะสมแก่การบรรจุ ใน อัตราที่เกี่ยวกับการปฏิบัติหน้าที่ระบบสารสนเทศ และเพื่อกำหนดระดับความไว้วางใจในการมอบหมายหน้าที่เกี่ยวกับความลับของทางราชการ ตลอดจนควบคุมบุคคลที่ไม่เกี่ยวข้องและหรือบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับระบบสารสนเทศ

ข้อ ๑๒ บุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ ให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

ข้อ ๑๓ หัวหน้าส่วนราชการ จะต้องจัดให้มีการควบคุม ดูแล และตรวจสอบสิทธิ์การเข้าถึงระบบสารสนเทศอย่างเข้มงวด โดยคำนึงถึงความปลอดภัยของระบบสารสนเทศเป็นหลัก

หมวด ๓

การรักษาความปลอดภัย สถานที่

ข้อ ๑๔ การรักษาความปลอดภัยเกี่ยวกับสถานที่ของระบบสารสนเทศให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ โดย

๑๔.๑ ส่วนราชการกำหนดมาตรการรักษาความปลอดภัยสถานที่จากการเข้าถึงโดยการได้ยิน และการมองเห็นของผู้ไม่มีอำนาจหน้าที่

๑๔.๒ ส่วนราชการกำหนดพื้นที่รักษาความปลอดภัยแบ่งเขตหวงห้ามเฉพาะเขตหวงห้ามเด็ดขาด ให้เหมาะสม

ข้อ ๑๕ ส่วนราชการจะต้องจัดทำแผนสำหรับเตรียมรับสถานการณ์ต่าง ๆ ได้แก่ แผนป้องกันระบบสารสนเทศ แผนการดำเนินการฟื้นฟูระบบคอมพิวเตอร์ แผนการเคลื่อนย้ายและแผนการทำลายระบบสารสนเทศในเวลาจำเป็นให้พร้อมที่จะปฏิบัติหน้าที่ได้ทันท่วงที และจัดให้มีการซักซ้อมความเข้าใจอย่างสม่ำเสมอ

ข้อ ๑๖ ส่วนราชการควรจัดให้มีสถานที่สำรองในการดำเนินการระบบสารสนเทศ

หมวด ๔

การรักษาความปลอดภัยระบบสารสนเทศ

ข้อ ๑๗ ส่วนราชการจะต้องจัดให้มีมาตรการรักษาความปลอดภัยระบบสารสนเทศที่เหมาะสม และดำเนินการตามมาตรการนั้นโดยเคร่งครัด เพื่อให้เกิดความปลอดภัยสูงสุดต่อระบบสารสนเทศ

/ข้อ ๑๘...

ข้อ ๑๘ ส่วนราชการต้องจัดทำระบบสำรองและการกู้คืนสภาพข้อมูลสารสนเทศตามวงรอบที่เหมาะสมและทันสมัยที่สุด

ข้อ ๑๙ ส่วนราชการต้องจัดให้มีแผนการสำรองและแผนการกู้คืนสภาพระบบสารสนเทศและทดสอบอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒๐ ต้องจัดให้มีแผนการรักษาและป้องกันความลับของข้อมูล

๒๐.๑ ต้องไม่เข้าถึงข้อมูลผู้อื่น โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล

๒๐.๒ ห้ามทำการพิมพ์หรือทำสำเนาข้อมูลที่เป็นชั้นความลับ เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๒๐.๓ ต้องมีการกำหนดผู้รับผิดชอบอุปกรณ์คอมพิวเตอร์ในระบบสารสนเทศของหน่วย

ข้อ ๒๑ การรักษาความปลอดภัยเกี่ยวกับเครือข่ายคอมพิวเตอร์

๒๑.๑ ส่วนราชการเจ้าของเรื่องสารสนเทศในเครือข่ายระบบสารสนเทศ ผู้มีสิทธิ์และอำนาจในสายงาน ที่มีการติดต่อแลกเปลี่ยนสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ เป็นผู้พิจารณาคุณสมบัติของผู้ใช้ที่ได้รับอนุญาตให้เข้าถึงและดำเนินการกับสารสนเทศดังกล่าว รวมทั้งพิจารณาระดับการป้องกันที่ต้องการ

๒๑.๒ การส่งข้อมูลที่มีชั้นความลับผ่านเครือข่ายคอมพิวเตอร์ จะต้องได้รับอนุมัติจากผู้มีสิทธิ์และอำนาจในสายงานที่กำหนดชั้นความลับนั้นก่อน แล้วจึงส่งเข้ารหัสตามมาตรฐานที่ได้รับการรับรองจากส่วนราชการ

ข้อ ๒๒ ส่วนราชการเจ้าของเรื่องสารสนเทศในเครือข่ายระบบสารสนเทศ ผู้มีสิทธิ์ และอำนาจในสายงานสามารถกำหนดระเบียบปฏิบัติของการเข้าใช้ที่สอดคล้องกับระเบียบนี้

ข้อ ๒๓ ส่วนราชการต้องจัดให้มีการรักษาความปลอดภัยฐานข้อมูล

เพื่อกำหนดมาตรการป้องกันฐานข้อมูลจากการเข้าถึง การเปลี่ยนแปลง การโอนถ่ายข้อมูล หรือการกระทำใด ๆ โดยผู้ไม่เกี่ยวข้องโดย

๒๓.๑ ข้อมูล ข่าวสาร สารสนเทศทุกประเภท ในฐานข้อมูลต้องได้รับการจัดระดับ การป้องกัน ผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

๒๓.๒ ส่วนราชการเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้และโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิ์ และจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

๒๓.๓ ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างราชการให้จัดทำข้อตกลงการใช้

/๒๓.๔ ต้องจัด...

๒๓.๔ ต้องจัดให้มีแผนการป้องกันไวรัสคอมพิวเตอร์เพื่อป้องกันฐานข้อมูลถูกทำลายโดย

๒๓.๔.๑ ห้ามเจ้าหน้าที่นำคอมพิวเตอร์ซอฟต์แวร์ หรือข้อมูลที่ไม่มั่นใจว่าติดไวรัสคอมพิวเตอร์มาติดตั้ง หรือใช้งาน เว้นแต่คอมพิวเตอร์ซอฟต์แวร์นั้นได้ผ่านการตรวจสอบจากเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการก่อน

๒๓.๔.๒ ห้ามเจ้าหน้าที่ปรับแต่ง หรือยกเลิก การทำงานของคอมพิวเตอร์ซอฟต์แวร์ป้องกันไวรัสที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ตามที่เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการจัดหามาให้

๒๓.๔.๓ กรณีที่มีการเชื่อมต่อกับระบบอินเตอร์เน็ต จะต้องจัดให้มีแผนการใช้งานคอมพิวเตอร์ ในระบบอินเตอร์เน็ต โดยคำนึงถึงความปลอดภัยของระบบสารสนเทศเป็นหลัก

ข้อ ๒๔ ส่วนราชการจะต้องจัดทำเอกสารประกอบระบบสารสนเทศให้สมบูรณ์ครบถ้วนในทุกด้าน เพื่อความสะดวกในการปรับปรุง แก้ไข และพัฒนาระบบใหม่ เมื่อมีความจำเป็น

หมวด ๕

การรักษาความปลอดภัยในการพัฒนาระบบสารสนเทศ

ข้อ ๒๕ ในการพัฒนาระบบสารสนเทศ ส่วนราชการจะต้องมีมาตรการที่เหมาะสม ในการรักษาความปลอดภัย ต่องานที่กำลังพัฒนา

ข้อ ๒๖ เมื่อพัฒนาระบบสารสนเทศแล้ว จะต้องจัดให้มีการทดสอบระบบสารสนเทศที่พัฒนาขึ้นมาอย่างละเอียดถี่ถ้วน โดยทดสอบในระบบที่แยกต่างหากจากระบบที่มีอยู่เดิมจนกว่าจะเกิดความมั่นใจในการใช้งาน จึงนำมาใช้งานจริงร่วมกัน หรือทดแทนระบบที่มีอยู่เดิม

ข้อ ๒๗ บุคคลภายนอกที่เข้ามาพัฒนาระบบสารสนเทศ ให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ โดยเคร่งครัด

หมวด ๖

การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ

ข้อ ๒๘ ความมุ่งหมาย เพื่อให้ทราบถึงสาเหตุแห่งการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ การปฏิบัติของเจ้าหน้าที่ และความรับผิดชอบของผู้บังคับบัญชาเมื่อปรากฏการละเมิด

ข้อ ๒๙ สาเหตุแห่งการละเมิดการรักษาความปลอดภัย

/การละเมิด...

การละเมิดการรักษาความปลอดภัยอันเป็นเหตุให้ความลับของทางราชการรั่วไหล เครื่องจักรคำนวณ อุปกรณ์วัสดุ และสถานที่ ถูกทำลาย หรือข้อมูลถูกลบล้าง แก้ไข จนเกิดความเสียหายขึ้น มีสาเหตุจากการขาดจิตสำนึกและวินัยในการรักษาความปลอดภัย ประมาทเลินเล่อเกียจคร้าน ไม่เคร่งครัดต่อหน้าที่ หรือเห็นแก่ประโยชน์ส่วนตัว รวมถึงการจารกรรมและและการก่อวินาศกรรมอันเกิดจากการกระทำของบุคคลภายนอก หรือข้าราชการที่ตกเป็นเครื่องมือของฝ่ายตรงข้าม

ข้อ ๓๐ การปฏิบัติเพื่อปรากฏการละเมิดการรักษาความปลอดภัย

๓๐.๑ ผู้ใดตรวจพบหรือทราบว่ามีการละเมิด หรือสงสัยว่าจะมีการละเมิดการรักษาความปลอดภัยเกิดขึ้น ต้องรีบรายงานผู้บังคับบัญชา หรือเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย หรือเจ้าหน้าที่ผู้รับผิดชอบ

๓๐.๒ เมื่อปรากฏว่าการละเมิดการรักษาความปลอดภัยได้เกิดขึ้นแล้ว เจ้าหน้าที่ที่เกี่ยวข้องหรือเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย ต้องรีบดำเนินการดังนี้

๓๐.๒.๑ รายงานผู้บังคับบัญชา และแจ้งกรมการสนเทศทหาร กองบัญชาการทหารสูงสุด เพื่อให้คำแนะนำช่วยเหลือในเรื่องดังกล่าว

๓๐.๒.๒ สำรวจความเสียหายอันเกิดจากการละเมิดการรักษาความปลอดภัย ค้นหาสาเหตุแห่งการละเมิด ตลอดจนจุดอ่อน ข้อบกพร่อง และความปลอดภัยของเครื่องจักรคำนวณและอุปกรณ์

๓๐.๒.๓ ในกรณีที่ระบบการรหัสของหน่วยสูญหาย หรือสงสัยว่ารั่วไหล ให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของหน่วย รายงานด่วนให้ผู้บังคับบัญชาตามลำดับชั้นทราบโดยเร็วที่สุด และพิจารณานำระบบรหัสสำรองที่เตรียมไว้ใช้แทน

๓๐.๒.๔ หากปรากฏหลักฐานหรือสงสัยว่า ถูกจารกรรม หรือก่อวินาศ-กรรมให้รายงานผู้บังคับบัญชา ตามลำดับชั้นทราบ เพื่อสั่งการให้เจ้าหน้าที่ผู้มีอำนาจในด้านการสืบสวนและสอบสวนดำเนินการต่อไป

ข้อ ๓๑ ความรับผิดชอบของผู้บังคับบัญชา

๓๑.๑ แจ้งให้ส่วนราชการเจ้าของเรื่องเดิม หรือเจ้าของข้อมูลที่มีข่ายงานร่วมกันทราบทันที

๓๑.๒ สั่งการสอบสวนหาตัวผู้กระทำผิด และผู้รับผิดชอบโดยเร็วที่สุด

๓๑.๓ พิจารณาแก้ไขข้อบกพร่อง และป้องกันมิให้เหตุการณ์เช่นนี้อุบัติซ้ำอีก

๓๑.๔ พิจารณาสั่งการลงทัณฑ์ หรือดำเนินคดีตามกฎหมายต่อผู้ละเมิด ผู้เกี่ยวข้องกับการละเมิด และผู้รับผิดชอบเมื่อมีการละเมิด หรือไม่ปฏิบัติตามระเบียบนี้ จะโดยเจตนาหรือไม่เจตนาและการละเมิดนั้นจะเกิดความเสียหาย หรือยังไม่เกิดความเสียหายต่อทางราชการก็ตาม

/ข้อ ๓๒...

ข้อ ๓๒ ความรับผิดชอบของเจ้าของเรื่องเดิม

เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัย ให้ส่วนราชการเจ้าของเรื่องเดิมดำเนินการดังนี้

๓๒.๑ พิจารณาว่าเอกสารกรรมวิธีข้อมูล ประมวลลับ หรือรหัสที่จำเป็นในการใช้วงจรสื่อสารทางสายมีผลกระทบกระเทือนเสียหายอย่างใดหรือไม่

๓๒.๒ ขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันทีในการนี้อาจจะต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติ พร้อมทั้งปัจจัยต่าง ๆ ที่เกี่ยวข้องตามที่เห็นควร

ข้อ ๓๓ ในกรณีที่การละเมิดการรักษาความปลอดภัยเกิดผลกระทบกระเทือนเสียหายอย่างร้ายแรงให้อยู่ในดุลพินิจของของผู้บังคับบัญชาแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติ หากจำเป็นให้รายงานหน่วยเหนือตามความเหมาะสม

ข้อ ๓๔ ให้ส่วนราชการที่มีหน่วยกรรมวิธีข้อมูลอัตโนมัติอยู่ในสังกัด ออกระเบียบปลีกย่อยได้ โดยไม่ขัดต่อระเบียบนี้

ประกาศ ณ วันที่ ๒๓ กุมภาพันธ์ ๒๕๔๗

(ลงชื่อ) พลเอก สมทัต อัตตะนันทน์

(สมทัต อัตตะนันทน์)

ผู้บัญชาการทหารสูงสุด

กรมการสนเทศทหาร

<u>รายการผนวก</u>

ผนวก ก คำศัพท์คอมพิวเตอร์

ผนวก ข ตัวอย่างมาตรการรักษาความปลอดภัยด้านต่าง ๆ