บันทึกข้อความ

ส่วนราชการ ศทส.บช.ศ. **โทร.** 0-2513-3054

ที่ 0036.02/ 260 **วันที่** 28 กันยายน 2550

เรื่อง ระเบียบว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ บช.ศ. พ.ศ.2550

เรียน ผบก.อมศ., ผบก.สบพ., ผบก.กส.
ผกก.ศฝก.

ตามรายงานผลการปฏิบัติราชการตามคำรับรองการปฏิบัติราชการ ประจำปีงบประมาณ พ.ศ.2550 มิติที่ 4 ตัวชี้วัดที่ 14 ระดับคุณภาพของการบริหารจัดการระบบฐานข้อมูลสารสนเทศของส่วนราชการ ซึ่ง ศทส. ได้จัดทำแผนปฏิบัติการบริหารจัดการระบบสารสนเทศของ บช.ศ. ประกอบด้วย 3 ประเด็นหลัก และ 10 ประเด็นย่อย โดยมีแผนงาน/กิจกรรม/โครงการที่ได้ดำเนินการไปส่วนหนึ่งแล้วนั้น

บัดนี้ ศทส. ได้จัดทำระเบียบว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ บช.ศ. พ.ศ.2550 ตามแผนการจัดการหรือแก้ไขปัญหาภัยพิบัติของระบบฐานข้อมูลสารสนเทศ เพื่อให้หน่วยงานในสังกัด บช.ศ. ใช้เป็นแนวทางในการปฏิบัติเพื่อการรักษาความปลอดภัยระบบสารสนเทศของหน่วยต่อไป

จึงเรียนมาเพื่อโปรดพิจารณา

พ.ต.ท.
(รัชชัย สุขเกษม)
รอง ผกก.ศทส.บช.ศ.

ได้รับเรื่องไว้แล้ว

อมศ.

สบพ. ขอ 2 ชุดครับ

กส. 29 ก.ย. 50

ศฝก. พ.ต.ท.หญิง

ระเบียบกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ
ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ
พ.ศ. ๒๕๕๐

เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติเป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ จึงวางระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า "ระเบียบกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ พ.ศ. ๒๕๕๐"

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ การดำเนินการรักษาความปลอดภัยตามระเบียบนี้ ให้ยึดถือและปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗ ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติเกี่ยวกับการสื่อสาร พ.ศ. ๒๕๒๕ และคำสั่งกองบัญชาการศึกษา ที่ ๒๕๗/๒๕๔๘ ลง ๑๗ พฤศจิกายน พ.ศ. ๒๕๔๘ เรื่อง มาตรการและระเบียบวิธีปฏิบัติเกี่ยวกับการรักษาความปลอดภัย กองบัญชาการศึกษา (พุทธศักราช ๒๕๔๘) เป็นมูลฐาน

บรรดาระเบียบ และคำสั่งอื่นใดในส่วนที่กำหนดไว้แล้วในระเบียบนี้ หรือซึ่งขัด หรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน

ข้อ ๔ ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ และลูกจ้างของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ

ข้อ ๕ ในระเบียบนี้

๕.๑. "ระบบสารสนเทศ (Information System)" หมายความว่า ระบบข่าวสารของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ ที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และเทคโนโลยีของระบบสื่อสารมาช่วยในการสร้างสารสนเทศที่กองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติสามารถนำมาใช้ในการวางแผน การบริหาร การพัฒนาและควบคุม ซึ่งมีองค์ประกอบดังนี้

๕.๑.๑ ระบบคอมพิวเตอร์ (Computer System)

๕.๑.๒ ระบบสื่อสาร (Communication System)

๕.๑.๓ สารสนเทศ (Information) ที่ดำเนินการในระบบคอมพิวเตอร์ และระบบสื่อสาร

๕.๒ “ภัย (Threat)” หมายความว่า อันตรายที่อาจเกิดขึ้นกับระบบสารสนเทศ โดย คน (Person) สิ่งต่าง ๆ (Thing) หรือ เหตุการณ์ (Event) ทั้งเจตนาและไม่เจตนา อันเป็นเหตุทำให้ข้อมูล ข่าวสารของระบบสารสนเทศถูกเปิดเผย เปลี่ยนแปลง บิดเบือน ทำลาย ปฏิเสธการทำงาน หรือ การกระทำ อื่น ๆ ตามความต้องการของภัยนั้น

๕.๓ “ความอ่อนแอ (Vulnerability)” หมายความว่า จุดอ่อน หรือข้อบกพร่องใด ๆ ก็ตามของระบบสารสนเทศที่ภัยในรูปแบบที่เหมาะกัน สามารถนำไปใช้ประโยชน์เพื่อก่อให้เกิดอันตราย ต่อระบบสารสนเทศนั้น ๆ ได้

๕.๔ “ความเสี่ยง (Risk)” หมายความว่า โอกาสของการเกิดภัยในรูปแบบที่เหมาะกับ ความอ่อนแอที่มีอยู่ของระบบสารสนเทศ และความรุนแรงที่เกิดจากภัยนั้น ซึ่งภัยประเภทเดียวกันอาจมี ระดับความเสี่ยงไม่เท่ากันในแต่ละพื้นที่ใช้งานระบบสารสนเทศ ฯ ความเสี่ยงเป็นสิ่งที่ใช้ตัดสินว่า ณ พื้นที่ใช้งานระบบสารสนเทศ ฯ แต่ละแห่งควรจัดเตรียมระบบการรักษาความปลอดภัยให้หนาแน่น เพียงใด

๕.๕ “ประเมินความเสี่ยง (Risk Assessment)” หมายความว่า กระบวนการวิเคราะห์ ภัยและความอ่อนแอของระบบสารสนเทศ รวมทั้งผลกระทบจากการสูญเสียสารสนเทศ หรือการสูญเสีย ความสามารถในการรักษาความปลอดภัยของระบบสารสนเทศ การประเมินความเสี่ยง ใช้เป็นพื้นฐานใน การกำหนดมาตรการรักษาความปลอดภัยที่เหมาะสมให้ระบบสารสนเทศต่อไป

๕.๖ “ระบบสื่อสาร (Communication System)” หมายความว่า ระบบที่ประกอบด้วย ผู้รับ ผู้ส่ง และสื่อกลางในระบบสื่อสารที่ใช้ในการส่งผ่านข้อมูล (ตัวอักษร ตัวเลข ภาพ เสียง เป็นต้น) ทั้งระบบวงจรทางสาย เช่น สายเคเบิล (Cable) โคแอกเชียล (Coaxial Cable) วิทยาการเส้นใยนำแสง (Fiber Optic) และระบบไร้สาย เช่น ไมโครเวฟ (Microwave) ดาวเทียม (Satellite) รวมทั้งอุปกรณ์อื่น ๆ เช่น ฮับ (Hub) การสลับ (Switching) อุปกรณ์จัดเส้นทาง (Router)

๕.๗ “ระบบคอมพิวเตอร์ (Computer System)” หมายความว่า ระบบที่ ประกอบด้วย ส่วนเครื่อง (Hardware) ส่วนชุดคำสั่ง (Software) และบุคลากรทางคอมพิวเตอร์ (Peopleware) ที่ใช้ ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ

๕.๘ “สารสนเทศ (Information)” หมายความว่า ข้อเท็จจริงที่ได้จากการสกัด ข้อมูล ให้มีความหมาย โดยผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของ ตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย เช่น รายงาน ตาราง แผนภูมิ เป็นต้น และ สามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๕.๙ “พื้นที่ใช้งานระบบสารสนเทศ (Information System Workspaces)” หมายความว่า พื้นที่ที่ใช้ติดตั้งระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ หรือ เตรียมข้อมูล เก็บ อุปกรณ์คอมพิวเตอร์ พื้นที่ที่เป็นห้องทำงานของบุคลากรทางคอมพิวเตอร์ รวมทั้ง เครื่องคอมพิวเตอร์ ส่วนบุคคลที่ติดตั้งประจำโต๊ะทำงาน

๕.๑๐ “เครือข่ายระบบสารสนเทศ” หมายความว่า การติดต่อสื่อสารหรือการส่ง ข้อมูลระหว่างระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ เช่น ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

๕.๑๑ “สารสนเทศที่กำหนดชั้นความลับ” หมายความว่า สารสนเทศในรูปข้อมูลหรือข่าวสารที่บันทึกไว้ในแบบใด ๆ ที่กำหนดชั้นความลับตามความสำคัญของเนื้อหาจำกัดการเข้าถึงและหรือจำกัดให้ทราบเท่าที่จำเป็น และให้รวมถึงจานบันทึก ประมวลลับ รหัส และรหัสผ่านที่กำลังใช้อยู่หรือเตรียมจะใช้ ตลอดจนวัสดุ หรือเอกสารทุกอย่างที่บันทึกเรื่องดังกล่าว

ข้อ ๖ ให้ รองผู้บัญชาการ กองบัญชาการศึกษา ที่กำกับดูแลศูนย์เทคโนโลยีสารสนเทศ กองบัญชาการศึกษา รักษาการให้เป็นไป ตามระเบียบนี้

ส่วนที่ ๑
กล่าวทั่วไป

ข้อ ๗ ความมุ่งหมายของระเบียบนี้เพื่อ

๗.๑ กำหนดหลักการและมาตรการป้องกันภัยของระบบสารสนเทศ ของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ

๗.๒ พิทักษ์รักษาและป้องกันสารสนเทศที่กำหนดชั้นความลับ มิให้รั่วไหล หรือรู้ไปถึงหรือตกไปอยู่กับบุคคลผู้ไม่มีอำนาจหน้าที่ที่จะต้องทราบ

๗.๓ พิทักษ์รักษาและป้องกันการก่อวินาศกรรมแก่ระบบสารสนเทศของ กองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ ในส่วนที่เป็นระบบคอมพิวเตอร์และระบบสื่อสาร

๗.๔ พิทักษ์รักษาและป้องกันระบบเทคโนโลยีสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ จากการโจมตีของแฮกเกอร์ไวรัส สปายแวร์ มัลแวร์ ฯลฯ

ข้อ ๘ หน่วยงานในสังกัดสามารถกำหนดมาตรการรักษาความปลอดภัย ให้ระบบสารสนเทศของส่วนราชการหรือแต่งตั้งเจ้าหน้าที่เกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการเพิ่มเติมได้ โดยให้สอดคล้องและไม่ขัด หรือแย้งกับระเบียบนี้ โดยให้ ผู้กำกับดูแลศูนย์เทคโนโลยีสารสนเทศ ของหน่วยงานหรือผู้ที่หัวหน้าหน่วยงานมอบหมาย เป็นเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของหน่วยงาน

ข้อ ๙ ให้ รองผู้บัญชาการ กองบัญชาการศึกษา ที่กำกับดูแลศูนย์เทคโนโลยีสารสนเทศของกองบัญชาการศึกษา เป็นผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ

ข้อ ๑๐ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตามกฎหมาย หรือระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ หรือระเบียบอื่นใดซึ่งกำหนดไว้เป็นอย่างอื่น

ส่วนที่ ๒

การรักษาความปลอดภัยสภาพแวดล้อมของระบบสารสนเทศ และการจัดการด้านการรักษาความปลอดภัยระบบสารสนเทศ (Physical Security and Administrative Security)

ข้อ ๑๑ ความหมาย เป็นมาตรการรักษาความปลอดภัยทางด้านกายภาพบุคคล และการจัดการของระบบสารสนเทศ ที่ช่วยสนับสนุนให้เกิดความปลอดภัยในสภาพแวดล้อมของระบบสารสนเทศที่กำลังดำเนินการป้องกันอยู่ในขณะนั้น

หมวด ๑
การรักษาความปลอดภัยเกี่ยวกับบุคคล (Personal Security)

ข้อ ๑๒ ความมุ่งหมาย เพื่อตรวจสอบบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ และเพื่อกำหนดระดับความไว้วางใจที่ให้ปฏิบัติหน้าที่เกี่ยวกับข้อมูล ซึ่งเป็นความลับของทางราชการ ตลอดจนควบคุมบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับระบบสารสนเทศ

ข้อ ๑๓ ก่อนที่จะมอบหมายให้บุคคลใดปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศให้ส่วนราชการต้นสังกัด ดำเนินการขอตรวจสอบความไว้วางใจโดยละเอียด และให้หัวหน้าส่วนราชการนั้น ๆ รับรองความไว้วางใจบุคคล โดยยึดถือผลการตรวจสอบประวัติและพฤติการณ์ของบุคคลนั้น เป็นแนวทางการพิจารณาตามที่เห็นสมควร ในกรณีจำเป็นเร่งด่วนหัวหน้าส่วนราชการอาจ รับรองความไว้วางใจบุคคลได้โดยไม่ต้องรอผลการตรวจสอบ แต่มีเงื่อนไขว่าหากผลการตรวจสอบปรากฏว่าผู้นั้นมีประวัติหรือพฤติการณ์ไม่เหมาะสม ให้ผู้ที่ได้รับการมอบหมายพ้นจากการปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศทันที บุคคลที่ไม่เกี่ยวข้องกับระบบสารสนเทศโดยตรง เข้ามาทำงานเป็นประจำ ภายในพื้นที่ใช้งานระบบสารสนเทศ เช่น เจ้าหน้าที่รับ-ส่งหนังสือราชการ พนักงานทำความสะอาด หรือบุคคลอื่นๆ ต้องทำการตรวจสอบประวัติ ตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗ ข้อ ๒๐ ด้วย และให้กำหนดช่วงเวลาทำงานที่แน่นอนของบุคคลดังกล่าวในระหว่างนั้น ต้องมีเจ้าหน้าที่ประจำพื้นที่ใช้งานระบบสารสนเทศควบคุมดูแลอยู่ด้วยอย่างน้อย ๑ คน

ข้อ ๑๔ บุคคลที่จะปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ ต้องผ่านการอบรมในเรื่องการรักษาความปลอดภัยตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ และเรื่องการรักษาความปลอดภัยเกี่ยวกับระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ ตามระเบียบนี้ เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของส่วนราชการ และผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการ ต้องมีความรู้เกี่ยวกับคอมพิวเตอร์ หรือระบบสารสนเทศโดยจะต้องผ่านการทดสอบความรู้เกี่ยวกับการรักษาความปลอดภัยระบบ สารสนเทศมาก่อน และจะต้องไม่ได้รับมอบหมายให้รับผิดชอบต่อภารกิจอื่นที่เป็นอุปสรรค หรือเป็นภัยต่อการรักษาความปลอดภัยระบบสารสนเทศ เมื่อได้รับมอบหมายให้ปฏิบัติหน้าที่การรักษาความปลอดภัยระบบสารสนเทศแล้ว ต้องปฏิบัติหน้าที่ด้วยความซื่อสัตย์ อดทน เสียสละ

ข้อ ๑๕ ให้ส่วนราชการที่ปฏิบัติงานเกี่ยวกับระบบสารสนเทศจัดทำทะเบียนความไว้วางใจของบุคคลที่ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศตามระดับความไว้วางใจที่แต่ละบุคคลได้รับอนุมัติ และสำเนาส่งให้ศูนย์เทคโนโลยีสารสนเทศ กองบัญชาการศึกษา ทราบด้วย

ข้อ ๑๖ เมื่อบุคคลใดพ้นจากหน้าที่เกี่ยวกับระบบสารสนเทศ ให้ส่วนราชการนั้นตัดชื่อออกจากทะเบียนความไว้วางใจของบุคคลที่ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ และสำเนาส่งให้ ศูนย์เทคโนโลยีสารสนเทศ กองบัญชาการศึกษา ทราบด้วย

ข้อ ๑๗ ให้หัวหน้าส่วนราชการหรือผู้ที่ได้รับมอบหมาย หรือเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของส่วนราชการ หรือผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศของ ส่วนราชการ ชี้แจงให้บุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศได้ทราบถึง ความเสียหายต่อความมั่นคงของชาติ ทัณฑ์ทางวินัยในการเปิดเผยความลับของทางราชการ รวมทั้ง โทษตามกฎหมายในการเปิดเผยความลับของทางราชการแก่บุคคลผู้ไม่มีหน้าที่เกี่ยวข้องทราบ

ข้อ ๑๘ เมื่อบุคคลใดจะเข้าปฏิบัติหน้าที่ หรือพ้นหน้าที่เกี่ยวกับระบบสารสนเทศ ให้ลงชื่อในใบบันทึกรับรองการรักษาความลับเมื่อเข้ารับตำแหน่งหน้าที่ (รปภ.๑๗) หรือใบรับรองการรักษาความลับเมื่อพ้นตำแหน่งหรือหน้าที่ (รปภ.๑๘) แล้วแต่กรณี ตามที่กำหนดไว้ในระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗

ข้อ ๑๙ บุคคลไม่สามารถอ้างยศ ตำแหน่ง หรืออำนาจ เพื่อขอทราบ หรือให้ได้มาซึ่งข้อมูลที่ตนไม่ได้รับอนุญาต

ข้อ ๒๐ เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของหน่วยงาน ควบคุม ดูแล และตรวจสอบสิทธิ์การเข้าถึงระบบสารสนเทศต่าง ๆ บุคคลที่จะเข้าใช้ระบบสารสนเทศจะต้องได้รับอนุญาตก่อน และการเข้าถึงระบบสารสนเทศต้องคำนึงถึงความปลอดภัยของระบบสารสนเทศเป็นหลัก บุคคลที่ไม่มีอำนาจหน้าที่ จะอนุญาตให้บุคคลอื่นเข้าถึงระบบสารสนเทศไม่ได้

ข้อ ๒๑ หากเจ้าหน้าที่หรือบุคคลผู้ใดมีพฤติการณ์ไม่น่าไว้วางใจ และอาจเป็นภัยต่อระบบสารสนเทศ ให้รีบรายงานตามลำดับชั้นถึง ผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศ ทราบ เพื่อดำเนินการตามมาตรการรักษาความปลอดภัยต่อไป

หมวด ๒
การรักษาความปลอดภัยอาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ
(Building and Workspace Security)

ข้อ ๒๒ ความมุ่งหมาย เพื่อกำหนดมาตรการควบคุมและป้องกันภัยเกี่ยวกับสถานที่ ซึ่งเป็นที่ตั้งของระบบสารสนเทศ เพิ่มเติมจากระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ และและคำสั่งกองบัญชาการศึกษา ที่ ๒๕๗/๒๕๔๘ ลง ๑๗ พฤศจิกายน พ.ศ. ๒๕๔๘ เรื่อง มาตรการ และระเบียบวิธีปฏิบัติเกี่ยวกับการรักษาความปลอดภัย กองบัญชาการศึกษา (พุทธศักราช ๒๕๔๘)

ข้อ ๒๓ ให้ส่วนราชการกำหนดให้ อาคาร สถานที่ซึ่งเป็นที่ตั้งของระบบสารสนเทศ และพื้นที่ใช้งานระบบสารสนเทศอื่นใดเป็นพื้นที่หวงห้าม โดยพิจารณาตามความสำคัญว่าจะต้องพิทักษ์รักษาสิ่งที่เป็นความลับของระบบสารสนเทศในระดับใด โดยกำหนดเป็น "เขตหวงห้ามเด็ดขาด" หรือ "เขตหวงห้ามเฉพาะ" แล้วแต่กรณี พื้นที่ใช้งานระบบสารสนเทศในส่วนที่เป็นหน่วยแสดงผล ต้องปลอดภัยจากการได้ยิน และการแลเห็นของผู้ไม่มีอำนาจหน้าที่ที่จะเข้าถึง จึงให้กำหนดมาตรการควบคุมบุคคลก่อนจะเข้าพื้นที่หวงห้ามอีกชั้นหนึ่งด้วย

ข้อ ๒๔ การปฏิบัติในเวลาฉุกเฉิน

๒๔.๑ อาคาร สถานที่ ซึ่งเป็นที่ตั้งของระบบสารสนเทศใด ที่จัดให้มีเวร - ยามรักษาการณ์เพื่อพิทักษ์รักษาระบบสารสนเทศโดยเฉพาะแล้ว ให้ถือว่าเป็นการปฏิบัติตามและคำสั่งกองบัญชาการศึกษา ที่ ๒๕๗/๒๕๔๙ ลง ๑๗ พฤศจิกายน พ.ศ. ๒๕๔๙ เรื่อง มาตรการ และระเบียบวิธีปฏิบัติเกี่ยวกับการรักษาความปลอดภัย กองบัญชาการศึกษา (พุทธศักราช ๒๕๔๙)

๒๔.๒ ให้ส่วนราชการเจ้าของอาคารสถานที่ จัดทำแผนเตรียมรับสถานการณ์ฉุกเฉินต่าง ๆ เช่น แผนการพิทักษ์รักษาระบบสารสนเทศ แผนการเคลื่อนย้ายและแผนการทำลายระบบสารสนเทศในเวลาฉุกเฉิน โดยเตรียมอุปกรณ์สนับสนุนในการเคลื่อนย้ายและทำลายไว้ให้พร้อมที่จะปฏิบัติได้ทันท่วงที และชี้แจงให้เจ้าหน้าที่ผู้เกี่ยวข้องเข้าใจวิธีและขั้นตอนปฏิบัติ และยึดแนวทางปฏิบัติตามและคำสั่งกองบัญชาการศึกษา ที่ ๒๕๗/๒๕๔๙ ลง ๑๗ พฤศจิกายน พ.ศ. ๒๕๔๙ เรื่อง มาตรการและระเบียบวิธีปฏิบัติเกี่ยวกับการรักษาความปลอดภัย กองบัญชาการศึกษา (พุทธศักราช ๒๕๔๙)

๒๔.๓ เพื่อมิให้ส่วนใดส่วนหนึ่งของระบบสารสนเทศที่กำหนดชั้นความลับตกไปอยู่ในมือของฝ่ายตรงข้ามหรือผู้ไม่มีอำนาจหน้าที่อย่างเด็ดขาด ให้ทำลายตามลำดับความสำคัญชั้นลับที่สุดก่อน

๒๔.๔ ให้ส่วนราชการเจ้าของอาคารสถานที่ กำหนดมาตรการการป้องกันอัคคีภัย พร้อมจัดเตรียมอุปกรณ์ในการดับเพลิงสำหรับระบบคอมพิวเตอร์ มาตรการป้องกันภัยธรรมชาติ พร้อมจัดเตรียมอุปกรณ์ป้องกันภัยธรรมชาติสำหรับระบบคอมพิวเตอร์ จัดเตรียมสถานที่ วัสดุ อุปกรณ์ที่จำเป็นสำหรับการฟื้นฟูระบบ รวมทั้งสถานที่เก็บรักษาสำรองข้อมูลที่ปลอดภัย

หมวด ๓
การจัดการการรักษาความปลอดภัยระบบสารสนเทศ
(Information System Security Management)

ข้อ ๒๕ ความมุ่งหมาย เพื่อกำหนดแนวทางการจัดการสำหรับผู้เกี่ยวข้องในระดับต่าง ๆ ของ กองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ ใช้ในการพิจารณามาตรการควบคุมและป้องกันภัยระบบสารสนเทศ ที่เหมาะสมกับสภาพแวดล้อมของแต่ละระบบ

ข้อ ๒๖ การกำหนดมาตรการหรือระบบการรักษาความปลอดภัย ต้องผ่านการประเมินความเสี่ยงภัย (Risk Assessment) ระบบสารสนเทศ เพื่อให้ได้มาตรการป้องกันที่เหมาะสมกับสภาพแวดล้อมของแต่ละระบบ

ข้อ ๒๗ การรักษาความปลอดภัยระบบสารสนเทศ ต้องดำเนินการป้องกันให้ถึงระดับที่สมดุลกับความเสี่ยงภัยระบบสารสนเทศที่ประเมินได้

ข้อ ๒๘ ผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ มีอำนาจและหน้าที่

๒๘.๑ กำหนดและรักษานโยบายการรักษาความปลอดภัยระบบสารสนเทศ ของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ

๒๘.๒ แต่งตั้งเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ ของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ

๒๘.๓ กำหนดหน้าที่รับผิดชอบเกี่ยวกับรักษาความปลอดภัยระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ

๒๘.๔ ประเมินความเสี่ยงภัยระบบสารสนเทศเพื่อระบุภัยที่จะเกิดกับระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ

๒๘.๕ พัฒนาหลักการและกระบวนการด้านการรักษาความปลอดภัยระบบสารสนเทศ และประสานงานด้านการรักษาความปลอดภัยระบบสารสนเทศกับสำนักงานตำรวจแห่งชาติและหน่วยงานที่เกี่ยวข้อง

๒๘.๖ ตรวจสอบให้มีการปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัย ที่เกี่ยวข้อง กับระบบสารสนเทศ

๒๘.๗ รายงานอันตรายที่อาจเกิดขึ้น หรือที่เกิดขึ้นแล้วกับระบบสารสนเทศ ของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ ให้แก่ผู้บัญชาการ กองบัญชาการศึกษา และหรือผู้ที่ได้รับมอบหมายจากผู้บัญชาการ กองบัญชาการศึกษา

ข้อ ๒๙ เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของส่วนราชการ มีอำนาจหน้าที่

๒๙.๑ กำหนดมาตรการป้องกันสำหรับพื้นที่ที่จะให้มีการรักษาความปลอดภัย ตามข้อ ๒๓ ตามผลการประเมินความเสี่ยงภัยระบบสารสนเทศและแจ้งให้ผู้เกี่ยวข้องทราบ

๒๙.๒ ควบคุม ดูแลการใช้งานอุปกรณ์คอมพิวเตอร์ทั้งหมดของหน่วยงาน

๒๙.๓ ควบคุมและตรวจสอบการติดตั้งโปรแกรมเข้าสู่ระบบสารสนเทศ ให้เป็นไปตามความมุ่งหมายของทางราชการ

๒๙.๔ ควบคุม กำกับ ดูแลการเข้าใช้เครือข่ายระบบสารสนเทศให้เป็นไป ตามที่ส่วนราชการเจ้าของระบบสารสนเทศนั้น ๆ กำหนด

๒๙.๕ รับผิดชอบการตรวจสอบไวรัสคอมพิวเตอร์ รวมทั้งมาตรการป้องกัน และการปรับแก้ไข

๒๙.๖ ศึกษา ค้นคว้า และติดตามข้อมูลข่าวสารเกี่ยวกับการค้นพบจุดอ่อนของระบบต่าง ๆ หรือภัยรูปแบบใหม่ ๆ ของระบบสารสนเทศ เพื่อปรับปรุงมาตรการป้องกันให้ทันสมัยเสมอ

๒๙.๗ พัฒนากระบวนการรักษาความปลอดภัยร่วมกับศูนย์เทคโนโลยีสารสนเทศกองบัญชาการศึกษา

๒๙.๘ ตรวจสอบให้มีการปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัย ที่เกี่ยวข้องภายในส่วนราชการ

๒๙.๙ ให้คำแนะนำและส่งเสริมผู้ใต้บังคับบัญชาให้มีความรู้และปฏิบัติตามกระบวนการรักษาความปลอดภัย

ข้อ ๓๐ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการ

๓๐.๑ ผู้บริหารระบบ (System Administrator) มีหน้าที่ดำเนินการให้ผู้ใช้ ที่ได้รับอนุญาตเข้าถึงระบบคอมพิวเตอร์ได้ วางระบบป้องกันการเข้าถึงแฟ้มรหัสผ่าน ของผู้ใช้ (Password File) ในระบบสารสนเทศให้พ้นจากผู้ไม่เกี่ยวข้อง รักษาความลับ คงสภาพและสร้างสภาพพร้อมใช้งานให้ระบบ ตามมาตรการป้องกันข้อ ๒๙.๑

๓๐.๒ ผู้จัดการฐานข้อมูล (Database Manager) มีหน้าที่ดำเนินการให้ผู้ใช้ ที่ได้รับอนุญาตเข้าถึงฐานข้อมูลได้ วางระบบป้องกันการเข้าถึงฐานข้อมูลให้พ้นจากผู้ไม่เกี่ยวข้อง รักษาความลับ คงสภาพและสร้างสภาพพร้อมใช้งานให้ฐานข้อมูล ตามมาตรการป้องกันข้อ ๒๙.๑

๓๐.๓ ผู้จัดการเครือข่าย (Network Manager) มีหน้าที่ดำเนินการเพื่อให้ผู้ได้รับอนุญาตสามารถเข้าถึงระบบเครือข่ายได้ วางระบบป้องกันการเข้าถึงเครือข่ายให้พ้นจากผู้ไม่เกี่ยวข้อง รักษาความลับ คงสภาพและสร้างสภาพพร้อมใช้งานให้ระบบเครือข่าย รวมถึงดูแลการเชื่อมต่ออุปกรณ์คอมพิวเตอร์กันทางกายภาพให้ตรงตามการใช้งานที่ได้กำหนดไว้ ตามมาตรการป้องกันข้อ ๒๙.๑

๓๐.๔ ผู้เขียนโปรแกรม (Programmer) มีหน้าที่ดำเนินการให้ผู้ใช้ที่ได้รับอนุญาตสามารถเข้าถึงโปรแกรมได้ ตรวจหาข้อบกพร่อง หรือสิ่งอื่นใดที่เป็นภัยต่อโปรแกรม เพื่อกำจัดก่อนนำเข้าสู่ระบบสารสนเทศ ตามมาตรการป้องกันข้อ ๒๙.๑

ข้อ ๓๑ ผู้ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศ ต้องปฏิบัติและดำเนินการดังนี้

๓๑.๑ ปฏิบัติตามมาตรการข้อ ๒๙.๑

๓๑.๒ ดำเนินการใด ๆ กับข้อมูลเฉพาะที่ได้รับอนุญาตแล้วเท่านั้น และต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศอย่างเคร่งครัด

๓๑.๓ ใช้ระบบสารสนเทศอย่างระมัดระวังถูกต้องตามกระบวนการรักษาความปลอดภัย และใช้ในกิจการงานที่ได้รับอนุญาต หรือได้รับมอบหมายเท่านั้น

๓๑.๔ ตรวจสอบโปรแกรมประสงค์ร้ายก่อนนำมาใช้งานในระบบ

๓๑.๕ ไม่นำโปรแกรมที่ไม่ได้รับอนุญาต หรือไม่เกี่ยวข้องกับภารกิจหน้าที่ที่ได้รับมอบหมายเข้าสู่ระบบสารสนเทศ

๓๑.๖ เก็บรักษาและใช้งานบัญชีผู้ใช้ (Account) รหัสผ่าน (Password) ให้เป็นไปด้วยความปลอดภัย ไม่รั่วไหลถึงบุคคลอื่น

ข้อ ๓๒ ผู้รับผิดชอบพื้นที่ใช้งานระบบสารสนเทศของหน่วยงาน ต้องปฏิบัติและดำเนินการดังนี้

๓๒.๑ ดำเนินการตามมาตรการป้องกัน ข้อ ๒๙.๑

๓๒.๒ ดูแลการใช้งานอุปกรณ์คอมพิวเตอร์ในพื้นที่ที่รับผิดชอบ

๓๒.๓ จัดทำแผนผัง สถานที่ที่ติดตั้งอุปกรณ์คอมพิวเตอร์และเครือข่ายคอมพิวเตอร์

๓๒.๔ จัดทำรายการอุปกรณ์ สถานภาพการใช้งาน และกำหนดการใช้งานอุปกรณ์

ข้อ ๓๓ ผู้รับผิดชอบอุปกรณ์คอมพิวเตอร์แต่ละหน่วยมีหน้าที่ ดูแล บำรุงรักษา ป้องกันภัย ตรวจสอบความพร้อมใช้งานตลอดจนควบคุมการใช้งานอุปกรณ์ให้เป็นไปตามที่กำหนดไว้

ข้อ ๓๔ การควบคุมดูแลพื้นที่ใช้งานระบบสารสนเทศต้องมีการจัดทำแผนป้องกันภัยของระบบสารสนเทศ

๓๔.๑ แผนการสำรองข้อมูลของระบบสารสนเทศ

๓๔.๒ แผนฟื้นฟูระบบสารสนเทศ

๓๔.๓ แผนป้องกันภัยธรรมชาติของระบบสารสนเทศ

๓๔.๔ แผนป้องกันอัคคีภัยของระบบสารสนเทศ

๓๔.๕ แผนป้องกันภัยที่ส่วนราชการนั้นพิจารณาว่าควรจัดทำตาม สภาพแวดล้อม

ส่วนที่ ๓

การรักษาความปลอดภัยระบบคอมพิวเตอร์

(Computer System Security)

ข้อ ๓๕ ความหมาย เป็นมาตรการควบคุมและป้องกัน เพื่อยืนยันถึงความถูกต้อง สิทธิ์การเข้าใช้ ความลับ และความพร้อมใช้งานของสารสนเทศที่ดำเนินการ หรือที่เก็บรักษาในระบบคอมพิวเตอร์

หมวด ๔

การรักษาความปลอดภัยอุปกรณ์คอมพิวเตอร์

(Computer Equipment Security)

ข้อ ๓๖ ความมุ่งหมาย เพื่อกำหนดมาตรการป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์ การรั่วไหล และความเสียหายของข้อมูลที่เกิดจากจุดอ่อน หรือข้อบกพร่องของอุปกรณ์คอมพิวเตอร์ หรือซอฟต์แวร์ที่เกี่ยวข้อง รวมทั้งสร้างสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์

ข้อ ๓๗ อุปกรณ์คอมพิวเตอร์ในระบบสารสนเทศของทุกหน่วย หรือทุกชุด ต้องมีการกำหนดผู้รับผิดชอบ และจัดทำรายละเอียดที่จำเป็น เช่น ผู้ที่ได้รับอนุญาตให้เข้าใช้ การใช้งานตลอดจนระดับของการป้องกัน เป็นต้น

ข้อ ๓๘ จัดเก็บสิ่งบันทึกที่สามารถแสดงผลหรือสื่อความเป็นสารสนเทศที่มีชั้นความลับได้ เช่น จานบันทึก ซีดีรอม และอื่น ๆ ที่นำมาแสดงผลโดยระบบคอมพิวเตอร์ได้ หากแสดงชั้นความลับไว้ในที่ดังกล่าวไม่ได้ ให้พิทักษ์รักษาตามชั้นความลับนั้น และให้เก็บในกล่อง หรือหีบห่อ ซึ่งมีเครื่องหมายแสดงชั้นความลับนั้น ๆ

ข้อ ๓๙ ให้ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการตรวจสอบอุปกรณ์ที่นำมาติดตั้งใหม่ทุกครั้ง สำหรับอุปกรณ์คอมพิวเตอร์ที่ใช้งานอยู่แล้ว ให้ตรวจสอบทุกรอบ ๓ เดือน หรือเมื่อมีเหตุอันควรแก่การตรวจสอบ และรายงานให้หัวหน้าส่วนราชการทราบเมื่อสิ้นสุดระยะเวลาการตรวจสอบ

ข้อ ๔๐ การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เข้า – ออกนอกพื้นที่ใช้งานระบบสารสนเทศของส่วนราชการ หรือการเคลื่อนย้ายที่มีผลทำให้สภาวะการทำงานของอุปกรณ์ เปลี่ยนแปลงไป จะต้องแจ้งและขออนุญาตตามลำดับชั้นถึงเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของส่วนราชการ และให้ผู้รับผิดชอบพื้นที่ใช้งานระบบสารสนเทศของส่วนราชการตรวจสอบความปลอดภัยก่อนการเคลื่อนย้ายทุกครั้ง

ข้อ ๔๑ ก่อนนำอุปกรณ์คอมพิวเตอร์ไปซ่อมบำรุง หรือจำหน่ายขายซากให้บุคคลภายนอกกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ หรือนำอุปกรณ์คอมพิวเตอร์กลับไปใช้ในงานของภารกิจใหม่ภายหลังจากใช้ในงานของภารกิจอื่น ๆ มาแล้ว หรือต้องการทำลายข้อมูลเมื่อหมดความจำเป็นในการใช้งานแล้ว หรือเป็น การโอนสิทธิ์การถือครองอุปกรณ์คอมพิวเตอร์ในลักษณะอื่น ๆ ต้องทำลายข้อมูลทั้งหมดที่มีชั้นความลับตั้งแต่ “ลับ” ขึ้นไปที่อยู่ในอุปกรณ์ดังกล่าวไม่ให้สามารถกู้คืนมาใช้งานได้อีก ในกรณีที่นำอุปกรณ์คอมพิวเตอร์ไปซ่อมภายนอกกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ และมีการเปลี่ยน ชิ้นส่วนเพื่อทดแทนชิ้นส่วนที่ชำรุดเสียหาย ให้เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของ ส่วนราชการที่ดำเนินการซ่อมบำรุงติดตามนำชิ้นส่วนดังกล่าวกลับมาดำเนินการให้ถูกต้องต่อไป

หมวด ๕

การรักษาความปลอดภัยการโปรแกรม

(Program Security)

ข้อ ๔๒ ความมุ่งหมาย เพื่อขจัดการใช้ประโยชน์จากจุดอ่อนหรือข้อบกพร่องของโปรแกรมในการทำอันตรายระบบสารสนเทศ

ข้อ ๔๓ ผู้พัฒนาโปรแกรมเพื่อนำไปใช้ในระบบสารสนเทศ ต้องพัฒนาโปรแกรมตามหลักวิชาการที่ยอมรับโดยทั่วไปและยินยอมให้ทำการตรวจสอบได้ตลอดเวลา รวมทั้งแสดงรายละเอียดที่จำเป็นต่อการรักษาความปลอดภัยไว้ที่รหัสต้นทาง (Source Code) เช่น ชื่อผู้เขียน วัน เดือน ปีที่เขียน หรือปรับปรุงวัตถุประสงค์ ระดับการป้องกัน สำหรับข้อมูลที่จำเป็นต้องใช้ในการพัฒนา เช่น ความสัมพันธ์ที่สามารถเชื่อมโยงไปถึงโปรแกรมหรือข้อมูลลับอื่น ๆ หรือผู้ที่ได้รับอนุญาตให้นำโปรแกรมไปใช้งานได้ให้เพิ่มเติมไว้ในเอกสารคู่มือผู้พัฒนาโปรแกรม ทั้งที่เป็นบุคลากรทางคอมพิวเตอร์ของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ และบุคคลภายนอกที่รับจัดทำโปรแกรมให้กองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ ต้องคำนึงถึงความปลอดภัยในทุกขั้นตอนของการพัฒนาโปรแกรม รวมทั้งรับผิดชอบต่อการรักษาความลับของข้อมูลและความถูกต้องของโปรแกรม จัดทำเอกสารหรือคู่มือประกอบการใช้งานสำหรับผู้พัฒนาโปรแกรมและผู้ใช้ และพัฒนาโปรแกรมให้ตรงตาม วัตถุประสงค์ของทางราชการเท่านั้น ให้ใช้เฉพาะซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นเพื่อป้องกันโปรแกรมประสงค์ร้าย

ข้อ ๔๔ การพัฒนาโปรแกรมประยุกต์ให้ส่วนราชการ ผู้มีสิทธิ์และอำนาจในสารสนเทศนั้นเป็นผู้พิจารณาคุณสมบัติของผู้ที่สามารถใช้งานโปรแกรมดังกล่าวได้ตามสิทธิ์

ส่วน ๔

การรักษาความปลอดภัยระบบสื่อสาร

(Communication Security)

ข้อ ๔๕ ความหมาย เป็นมาตรการควบคุมและป้องกันเพื่อยืนยันถึงความถูกต้อง ของการโอน การแลกเปลี่ยนสารสนเทศ หรือการติดต่อกันในลักษณะใดลักษณะหนึ่งผ่านทางระบบสื่อสารว่าได้กระทำโดยผู้มีอำนาจหน้าที่และป้องกันผู้ไม่เกี่ยวข้องเข้าถึงระบบสื่อสาร

หมวด ๖

การรักษาความปลอดภัยเกี่ยวกับระบบเครือข่ายคอมพิวเตอร์

(Computer Network Security)

ข้อ ๔๖ ความมุ่งหมาย เพื่อกำหนดมาตรการควบคุมและป้องกันการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต ความลับรั่วไหล การบิดเบือนและการทำลายสารสนเทศในระหว่างส่งผ่านทางระบบเครือข่ายคอมพิวเตอร์

ข้อ ๔๗ ส่วนราชการเจ้าของเรื่องสารสนเทศในเครือข่ายระบบสารสนเทศ ผู้มีสิทธิ์ และอำนาจในสายงาน ที่มีการติดต่อแลกเปลี่ยนสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ เป็นผู้พิจารณาคุณสมบัติของผู้ใช้ที่ได้รับอนุญาตให้เข้าถึงและดำเนินการกับสารสนเทศดังกล่าว รวมทั้งพิจารณาระดับของการป้องกันที่ต้องการ

ข้อ ๔๘ การส่งสารสนเทศที่มีชั้นความลับผ่านระบบเครือข่ายคอมพิวเตอร์ จะต้องได้รับอนุมัติจากเจ้าของเรื่องสารสนเทศผู้มีสิทธิ์และอำนาจในสายงานที่กำหนดชั้นความลับนั้นก่อน เมื่อได้รับอนุมัติแล้ว สารสนเทศกำหนดชั้นลับจะต้องส่งเข้ารหัส (Encryption) โดยมาตรฐานที่ได้รับการรับรองแล้วส่วนราชการเจ้าของเรื่องสารสนเทศในเครือข่ายระบบสารสนเทศ ผู้มีสิทธิ์ และอำนาจในสายงานสามารถกำหนดระเบียบปฏิบัติของการเข้าใช้ที่สอดคล้องกับระเบียบนี้

ส่วนที่ ๕

การรักษาความปลอดภัยสารสนเทศ

(Information Security)

ข้อ ๔๙ ความหมาย เป็นมาตรการป้องกันสารสนเทศที่อยู่ในระบบจากการเข้าถึง ด้วยการรักษาความลับไม่ให้รั่วไหล การคงสภาพข้อมูล และการสร้างสภาพพร้อมใช้งานให้แก่ผู้มีสิทธิ์ รวมถึงมาตรการป้องกันอื่น ๆ ที่จำเป็น

หมวด ๗

การรักษาความปลอดภัยฐานข้อมูล

(Database Security)

ข้อ ๕๐ ความมุ่งหมาย เพื่อกำหนดมาตรการป้องกันฐานข้อมูลจากการเข้าถึง การเปลี่ยนแปลง การโอนถ่ายข้อมูลหรือการกระทำใด ๆ โดยผู้ไม่เกี่ยวข้อง ตลอดจนการเตรียมระบบสำรองและการฟื้นฟูระบบ

ข้อ ๕๑ ข้อมูล ข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ ๕๒ ส่วนราชการเจ้าของฐานข้อมูล ผู้มีสิทธิและอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้และโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิ์ และจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ใน การตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ ๕๓ ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างราชการให้จัดทำข้อตกลงการใช้

หมวด ๘

การจัดการสารสนเทศ

(Information Mangament)

ข้อ ๕๔ ความมุ่งหมาย เพื่อกำหนดมาตรการป้องกันและควบคุมการใช้สารสนเทศ ที่มีชั้นความลับในรูปแบบต่าง ๆ

ข้อ ๕๕ ให้ผู้มีส่วนเกี่ยวข้องกับการแสดงชั้นความลับของสารสนเทศ ปฏิบัติดังนี้

๕๕.๑ สารสนเทศที่จัดทำในรูปแบบเอกสารหรือรายงาน ให้แสดงหรือพิมพ์ตัวอักษรตามชั้นความลับกึ่งกลางหน้าทั้งด้านบนและด้านล่างของทุกหน้าเอกสารที่มีชั้นความลับนั้น โดยใช้ตัวอักษรที่มีขนาดใหญ่กว่าที่ใช้ในข้อความปกติ และใช้สีหรือความเข้มของตัวอักษรที่มีขนาดใหญ่

๕๕.๒ สารสนเทศที่จัดทำในรูปแบบ ภาพเขียน เรขา ภาพถ่าย แผนที่ แผนภูมิ แผนผัง ให้แสดงหรือพิมพ์ตัวอักษรตามชั้นความลับ เช่นเดียวกับข้อ ๕๕.๑ โดยให้แสดงชั้นความลับให้ปรากฏเห็นได้ชัดเจน หรือแสดงไว้ใกล้ชื่อภาพ หรือมาตรส่วน

๕๕.๓ ในการแสดง นำเสนอ หรือพูดถึงสารสนเทศที่มีชั้นความลับ ให้ผู้แสดงหรือผู้พูดแจ้งให้ผู้ดูหรือผู้ฟังทราบชั้นความลับที่กำหนดของสารสนเทศนั้น ๆ หากแสดงภาพฉายบนจอภาพให้แสดงชั้นความลับด้วยอักษร ทั้งก่อนและเมื่อเสร็จสิ้นการแสดง การนำเสนอหรือพูดแล้ว

๕๕.๔ สารสนเทศที่กำหนดชั้นความลับ จะต้องวางระบบป้องกันมิให้ผู้ไม่มี หน้าที่เกี่ยวข้องเข้าถึงและแก้ไข ลบล้าง หรือทำลายโดยพลการ และหากมีข้อมูลที่เป็นชั้นความลับหลายชั้นความลับอยู่ในแฟ้มข้อมูลเดียวกัน ให้กำหนดชั้นความลับสูงสุดของสารสนเทศนั้นไว้ที่แฟ้มข้อมูลดังกล่าว

ข้อ ๕๖ การจัดทำซ้ำ หรือจัดทำสำเนาข้อมูลสารสนเทศที่กำหนดชั้นความลับ ต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากเจ้าของเรื่องสารสนเทศ ที่กำหนดชั้นความลับนั้น และให้รวมหมายถึงการสั่งงานระบบคอมพิวเตอร์ให้จัดการพิมพ์ออกเป็นเอกสารลับนั้นด้วย

ข้อ ๕๗ การปรับและยกเลิกชั้นความลับของสารสนเทศ ให้เจ้าของสารสนเทศตรวจสอบอยู่เสมอว่าชั้นความลับของสารสนเทศที่กำหนดไว้แต่เดิมยังจำเป็นต้องใช้อยู่หรือไม่ เพราะสารสนเทศอาจลดชั้น เพิ่มชั้นหรือยกเลิกชั้นความลับได้ตามความจำเป็น และควรลดชั้นลงทุกโอกาสเท่าที่กระทำได้เพื่อลดภาระในการรักษาความปลอดภัย

ข้อ ๕๘ สารสนเทศที่ได้รับจากรัฐบาลต่างประเทศหรือองค์การระหว่างประเทศ หากรัฐบาลหรือองค์การนั้น ๆ ได้กำหนดชั้นความลับไว้ จะต้องปฏิบัติต่อสารสนเทศนั้นเท่าเทียมกับสารสนเทศที่กำหนดชั้นความลับ

ข้อ ๕๙ การเผยแพร่ข้อมูล ข่าวสาร หรือสารสนเทศใด ๆ ของทางราชการ ผ่านสื่อทางระบบสารสนเทศให้เป็นไปตามระเบียบคำสั่งของกองบัญชาการศึกษา หรือสำนักงานตำรวจแห่งชาติ ที่เกี่ยวข้อง

ข้อ ๖๐ สารสนเทศที่กำหนดชั้นความลับ “ลับที่สุด” และ “ลับมาก” ที่ใช้ร่วมกันระหว่างส่วนราชการต้องแบ่งระดับการเข้าถึงสารสนเทศตามหน้าที่ของผู้ใช้

ข้อ ๖๑ สารสนเทศที่อยู่ในระบบคอมพิวเตอร์ หากสารสนเทศเป็นร่างหรือสำเนาของเอกสารที่มีชั้นความลับ จะต้องแสดงชั้นความลับเช่นเดียวกับเอกสารต้นฉบับ ในกรณีที่เอกสารต้นฉบับได้ดำเนินการทำลายแล้วให้ลบทิ้งสารสนเทศที่อยู่ในระบบคอมพิวเตอร์นั้นด้วย โดยการทำลายแบบไม่ให้สามารถกู้ข้อมูลกลับคืนได้ภายหลัง

ข้อ ๖๒ กุญแจเพื่อการถอดรหัสลับ (Decryption Key) ทุกชนิดที่ใช้ในการเข้ารหัสระบบสารสนเทศให้จัดเป็นสารสนเทศที่มีชั้นความลับ “ลับ” ขึ้นไป ต้องจำกัดการเข้าถึงเท่าที่จำเป็นและ ควรเปลี่ยนตามวาระดังนี้

๖๒.๑ ตามห้วงระยะเวลาอย่างน้อย ๓ เดือนต่อหนึ่งครั้ง แต่ต้องไม่กำหนดระยะเวลาที่แน่นอนได้

๖๒.๒ เมื่อมีการเปลี่ยนเจ้าหน้าที่ที่เกี่ยวข้องกับการเข้ารหัส พร้อมทั้งสั่งยกเลิกกุญแจเพื่อการถอดรหัสลับ (Decryption Key) เดิม

๖๒.๓ เมื่อความลับรั่วไหลหรือสงสัยว่า ความลับรั่วไหล

ข้อ ๖๓ รหัสผ่าน (Password) และแฟ้มรหัสผ่าน (Password File) ของผู้ใช้ ที่ใช้ในระบบสารสนเทศให้จัดเป็นสารสนเทศที่มีชั้นความลับ “ลับ” ขึ้นไป และให้ผู้ใช้ทุกคนปฏิบัติตามวิธีการ รักษาความปลอดภัยเกี่ยวกับรหัสผ่านประจำตัว

ส่วนที่ ๖

การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย

ข้อ ๖๔ ความมุ่งหมาย เพื่อให้เป็นแนวทางปฏิบัติเมื่อเกิดการละเมิดการรักษาความ ปลอดภัยต่อระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ และลดความเสียหายที่เกิดขึ้นจากการกระทำที่ฝ่าฝืน หรือละเลยให้เหลือน้อยที่สุด พร้อมทั้งตรวจสอบค้นหาสาเหตุผลเสียหายเพื่อปรับปรุงมาตรการป้องกันการละเมิดที่จะเกิดขึ้นซ้ำอีกกับกำหนดวิธีดำเนินการต่อผู้ละเมิดการรักษาความปลอดภัย

ข้อ ๖๕ การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย

๖๕.๑ เมื่อตรวจพบหรือสงสัยว่ามีการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ หรือมีสิ่งผิดปกติเกิดขึ้นในระบบสารสนเทศ ให้รีบรายงานผู้บังคับบัญชา หรือเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของส่วนราชการทราบโดยเร็วที่สุด

๖๕.๒ เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของส่วนราชการดำเนินการดังนี้ต่อไปนี้

๖๕.๒.๑ รายงานขั้นต้นต่อผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ หากพบว่าเป็นการละเมิดต่อสารสนเทศที่มีชั้นความลับ

๖๕.๒.๒ ลดความเสียหายเบื้องต้น โดยการระงับใช้ แก้ไข หรือยกเลิกระบบสารสนเทศที่สงสัยว่าถูกละเมิดนั้น หากเป็นสารสนเทศที่มีชั้นความลับจะต้องยกเลิกชั้นความลับโดยทันที และแจ้งให้เจ้าของเรื่องสารสารเทศที่มีชั้นความลับนั้นทราบด้วย

๖๕.๒.๓ สำรวจความเสียหายที่เกิดจากการละเมิด ตรวจสอบสาเหตุ และจุดอ่อนหรือข้อบกพร่องที่ก่อให้เกิดการละเมิด ให้มีผู้แทนจากศูนย์เทคโนโลยีสารสนเทศ กองบัญชาการศึกษาร่วมในการตรวจสอบสาเหตุด้วย

๖๕.๒.๔ รายงานเหตุการณ์ที่เกิดขึ้น ให้ผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ ทราบ พร้อมทั้งแนวทางป้องกันมิให้เกิดการละเมิดซ้ำ

๖๕.๒.๕ ในกรณีที่ระบบรหัส ประมวลลับที่ใช้ในระบบสารสนเทศสูญหาย หรือสงสัยว่ามีผู้ไม่มีอำนาจหน้าที่ทราบระบบรหัส ประมวลลับ ให้ระงับใช้ ยกเลิกหรือเปลี่ยนแปลงรหัสประมวลลับนั้นโดยทันที แล้วรายงานให้ผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ ทราบโดยเร็วที่สุด

ข้อ ๖๖ ความรับผิดชอบของผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ

๖๖.๑ แจ้งให้ส่วนราชการเจ้าของสารสนเทศร่วม ทราบโดยเร็วที่สุด

๖๖.๒ ตั้งคณะกรรมการร่วมกับส่วนราชการที่มีการละเมิดต่อสารสนเทศ สืบสวนสอบหาตัวผู้รับผิดชอบและผู้กระทำผิดโดยเร็วที่สุด

๖๖.๓ แจ้งให้ส่วนราชการต้นสังกัดลงโทษผู้รับผิดชอบและผู้กระทำผิดต่อการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ ตามกรณีที่ก่อให้เกิดความเสียหายต่อระบบหรือส่งตัวผู้กระทำผิดไปดำเนินการตามกฎหมายต่อไป

๖๖.๔ สั่งให้แก้ไขข้อบกพร่อง และป้องกันมิให้เกิดเหตุการณ์ซ้ำขึ้นอีก

ข้อ ๖๗ ความรับผิดชอบของส่วนราชการที่มีผู้ละเมิดการรักษาความปลอดภัย

๖๗.๑ ลงโทษทางวินัยผู้ละเมิดและผู้รับผิดชอบต่อการละเมิด ตามความเหมาะสมเพื่อมิให้เกิดการละเมิดซ้ำขึ้นอีก ในกรณีผู้ละเมิดเป็นบุคคลภายนอกกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติให้หน่วยเกี่ยวข้องดำเนินการตามกฎหมายต่อไป

๖๗.๒ หากก่อให้เกิดความเสียหายต่อทางราชการอย่างร้ายแรง หรือเข้าข่ายความผิดตามกฎหมาย ให้ส่งตัวไปดำเนินการตามกฎหมายต่อไป

๖๗.๓ พิจารณาข้อมูลสารสนเทศที่มีชั้นความลับ รหัส ประมวลลับ ที่อยู่ในความรับผิดชอบ หากได้รับความเสียหายหรือได้รับความกระทบกระเทือน ต้องดำเนินการแก้ไขโดยเร็วที่สุด

๖๗.๔ กำหนดมาตรการป้องกันเพิ่มเติม เพื่อขจัดความเสียหายที่เกิดการละเมิดซ้ำหรือเปลี่ยนแปลงวิธีการปฏิบัติ ยกเลิกโปรแกรมและอื่น ๆ

๖๗.๕ หากก่อให้เกิดความเสียหายต่อระบบสารสนเทศ และต้องเสียค่าใช้จ่ายในการกู้คืนมา ให้ส่วนราชการเรียกร้องค่าเสียหายส่วนนี้ เพื่อเป็นค่าใช้จ่ายในการกู้ระบบ

ข้อ ๖๘ ในกรณีที่มีการละเมิดการรักษาความปลอดภัยหรือก่อให้เกิดความเสียหายต่อระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ อย่างร้ายแรง ให้ผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศ ของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ สั่งการแก้ไข เปลี่ยนแปลงระบบ แผนงาน และวิธีปฏิบัติได้ตามความจำเป็นและความเหมาะสม

ข้อ ๖๙ เพื่อให้การดำเนินมาตรการรักษาความปลอดภัยเกี่ยวกับระบบสารสนเทศตามระเบียบนี้เป็นไปด้วยความเรียบร้อยและรวดเร็ว จึงอธิบายศัพท์เฉพาะบางคำที่ปรากฏอยู่ในระเบียบนี้เพิ่มเติม รวมทั้งคำศัพท์คอมพิวเตอร์ซึ่งมีความหมายใกล้เคียงกัน ดังนี้

๖๙.๑ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการ (ผนวก ๑)

๖๙.๒ ศัพท์คอมพิวเตอร์ที่เกี่ยวข้อง (ผนวก ๒)

ประกาศ ณ วันที่ ๒๘ กันยายน พ.ศ.๒๕๕๐

พลตำรวจโท

(สถาพร ดวงแก้ว)

ผู้บัญชาการ กองบัญชาการศึกษา

ผนวก ๑

ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการ

๑. ผู้บริหารระบบ (System Administrator) มีความรู้ด้านฮาร์ดแวร์ ซอฟต์แวร์ระบบเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๑.๑ บริหารและดูแลอุปกรณ์คอมพิวเตอร์ซึ่งเป็นแม่ข่ายบริการแก่หน่วยงานต่าง ๆ ของส่วนราชการ

๑.๒ ควบคุมและตรวจสอบการใช้งานระบบ

๑.๓ ตรวจสอบ ควบคุม ดูแล การบำรุงรักษาระบบ

๑.๔ รักษาความปลอดภัยระบบ เช่น รักษาความลับ ความคงสภาพและความพร้อมใช้งาน

๒. ผู้จัดการฐานข้อมูล (Database Manager) มีความรู้ด้านการจัดการฐานข้อมูล ระบบคอมพิวเตอร์เป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๒.๑ ควบคุมดูแลฐานข้อมูล เช่น การรวบรวม การเพิ่ม การเปลี่ยนแปลง การลบ การจัดโครงสร้าง การใช้งาน การเก็บ และการเรียกดู

๒.๒ เลือก ตัดตอน และกำหนดรูปแบบข้อมูลที่เก็บในแฟ้มข้อมูล

๒.๓ รักษาความปลอดภัยฐานข้อมูล เช่น รักษาความลับ ความคงสภาพ และความพร้อมใช้งานให้ฐานข้อมูล

๒.๔ ตรวจสอบฐานข้อมูล และวิเคราะห์ข้อมูล

๒.๕ ควบคุม และบริการการใช้งานฐานข้อมูล

๓. ผู้จัดการเครือข่าย (Network Manager) มีความรู้ด้านฮาร์ดแวร์ การสื่อสารข้อมูล และอุปกรณ์ในระบบเครือข่ายเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๓.๑ กำหนดเลขที่อยู่ไอพี (IP Adress) ให้คอมพิวเตอร์ในเครือข่ายของส่วนราชการโดยประสานกับส่วนราชการ หรือผู้บริหารระบบเครือข่ายคอมพิวเตอร์ของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ

๓.๒ กำหนดบัญชีผู้ใช้ (Account) และรหัสผ่าน (Password) ของผู้ใช้ภายในเครือข่ายที่รับผิดชอบ

๓.๓ ดูแลการใช้เครือข่ายคอมพิวเตอร์ภายในส่วนราชการ

๓.๔ ดูแลโครงสร้างพื้นฐานและอุปกรณ์ที่เกี่ยวกับระบบเครือข่าย เช่น โทรศัพท์ โมเด็ม ฮับ เป็นต้น

๓.๕ รักษาความปลอดภัยระบบเครือข่าย เช่น รักษาความลับ ความคงสภาพ และความพร้อมใช้งานให้ระบบเครือข่าย

๔. ผู้เขียนโปรแกรม (Programmer) มีความรู้เรื่องระบบคอมพิวเตอร์ การเขียนโปรแกรมคอมพิวเตอร์และฐานข้อมูลเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๔.๑ เขียนและพัฒนาโปรแกรมที่ได้รับมอบหมาย

๔.๒ จัดหาข้อมูลเพื่อทดสอบโปรแกรม

๔.๓ ดูแลบำรุงรักษาโปรแกรมที่พัฒนา

๔.๔ รักษาความปลอดภัยโปรแกรม เช่น รักษาความลับ ความคงสภาพ และความพร้อมใช้งานให้โปรแกรม

ผนวก ๒

คำศัพท์คอมพิวเตอร์ที่เกี่ยวข้อง

๑. Account ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: บัญชีผู้ใช้

อธิบายความหมาย

: เป็นสัญลักษณ์หรือชุดของตัวอักษรเรียงติดต่อกัน มีลักษณะเป็นหนึ่งเดียว (Unique) ไม่ซ้ำกันเพื่อเป็นการระบุตัว (Identification) เจ้าของบัญชี หรือกลุ่มคนที่สามารถเข้าถึงระบบได้ บัญชีผู้ใช้เป็นเครื่องมือรักษาความปลอดภัยที่ใช้ควบคู่กับรหัสผ่าน (Password)

๒. Application ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: การประยุกต์

อธิบายความหมาย

: งานที่ทำด้วยโปรแกรมคอมพิวเตอร์หรือระบบคอมพิวเตอร์ เพื่อให้ได้ผลลัพธ์ตามที่ต้องการ เช่น งานออกแบบโครงสร้างทางวิศวกรรม งานพยากรณ์ทางธุรกิจ งานด้านการจัดการสถานพยาบาล เป็นต้น การประยุกต์ มีความหมายรวมถึงโปรแกรมประยุกต์ หรือโปรแกรมใช้งาน (Application Program) และซอฟต์แวร์ประยุกต์ (Application Software)

๓. Computer Network ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: เครือข่ายคอมพิวเตอร์, ข่ายงานคอมพิวเตอร์

อธิบายความหมาย

: เป็นคำกล่าวโดยทั่ว ๆ ไปของการเชื่อมต่อสื่อสารกันระหว่างระบบคอมพิวเตอร์ ตั้งแต่ ๒ ระบบขึ้นไป หรือระหว่างเครื่องคอมพิวเตอร์กับเครื่องปลายทาง (Terminals) ทั้งหลาย เพื่อให้สามารถนำข้อมูล โปรแกรม รวมทั้งอุปกรณ์รอบข้างมาใช้งานร่วมกันได้ โดยมีอุปกรณ์ ในระบบสื่อสารเป็นตัวเชื่อมโยง

๔. Decryption/Encryption ยังไม่มีการกำหนดไว้ในศัพท์คอมพิวเตอร์ฉบับราชบัณฑิตยสถาน

: การถอดรหัสลับ / เพื่อการเข้ารหัสลับ

อธิบายความหมาย

: การถอดรหัสลับ (Decryption)

(๑) กระบวนการนำข้อความ (Message) ที่ผ่านการเข้ารหัสลับ (Encrypted) แล้วมาแปลงกลับให้เป็นข้อความดั้งเดิม (Original meaningful Message) หรือข้อความธรรมดา (plaintext) เป็นความที่ตรงกันข้ามกับคำว่า <u>การเข้ารหัสลับ</u>

(๒) กระบวนการที่ตรงข้าม คือ การแปลงข้อความที่เข้ารหัสลับแล้ว ให้กลับไปอยู่ในรูปแบบปกติ คำที่มีความหมายเหมือนกัน คือ เข้ารหัส (encode) และถอดรหัส (decode) หรือ เข้ารหัส (encipher) และถอดรหัส (decipher) ซึ่งใช้แทนคำว่า เข้ารหัส (encrypt) และถอดรหัส (decrypt) และเรียกระบบที่มีการเข้ารหัสลับและถอดรหัสลับว่า ระบบการเข้ารหัสลับ (cryptosystem)

: การเข้ารหัสลับ

(๑) เป็นขบวนการเข้ารหัสให้ข้อความเพื่อทำให้ไม่ทราบความหมาย ที่แท้จริงของข้อความดังกล่าว

(๒) กระบวนการเข้ารหัส (encode) หรือการเข้ารหัสลับ (encryption) ให้แก่ข้อมูล (data) ใด ๆ ก็ตาม ซึ่งต้องการรหัสเฉพาะเจาะจง (spceific code) หรือ กุญแจ (key) สำหรับการแปลงให้กลับมาเป็นข้อมูลดั้งเดิม (Original data)

(๓) เป็นการเข้ารหัสข้อมูลสื่อสาร (communication data)

๕. Decryption Key/Encryption Key ยังไม่มีการกำหนดไว้ในศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: กุญแจเพื่อการถอดรหัสลับ / กุญแจเพื่อการเข้ารหัสลับ

อธิบายความหมาย

: เป็นคำศัพท์สำหรับการเข้ารหัสแบบกุญแจสาธารณะ (Public Key System) ประกอบด้วยไฟล์คอมพิวเตอร์คู่หนึ่ง คือ กุญแจสาธารณะ (Public Key) ใช้ในการเข้ารหัสลับ ซึ่งไฟล์สำหรับการเข้ารหัสคือ Encryption Key และ กุญแจลับ (Secret Key) ใช้เมื่อถอดรหัสลับ ซึ่งไฟล์สำหรับการถอดรหัสคือ Decryption Key

๖. Hardware ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: ๑. ส่วนเครื่อง, ฮาร์ดแวร์

: ๒. ส่วนอุปกรณ์, ฮาร์ดแวร์

อธิบายความหมาย

: ระบบคอมพิวเตอร์ส่วนที่เป็นอุปกรณ์ทางกายภาพ เช่น อิเล็กทรอนิกส์ แม่เหล็กและเครื่องจักรกล แสดงให้เห็นถึงความแตกต่างของฮาร์ดแวร์และซอฟต์แวร์ ซึ่งเป็นองค์ประกอบของระบบคอมพิวเตอร์เช่นเดียวกัน

๗. Log File ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: แฟ้มลงบันทึกเข้าออก

อธิบายความหมาย

: เป็นการบันทึกการปฏิบัติทั้งหมดของอุปกรณ์ที่เกี่ยวข้องกับการประมวลผลข้อมูล (Data Processing Equipment) จะบันทึกงานทุกงานหรือการดำเนินการ (Run) ตามลำดับที่เกิดขึ้นเวลาเริ่มต้นและสิ้นสุดของแต่ละงาน รวมทั้งกิจกรรมที่ทำ ทั้งนี้เพื่อนำมาตรวจสอบ ความถูกต้องของการใช้งานได้ในภายหลัง

๘. Malicious Code ยังไม่กำหนดความหมายไว้ในศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: โปรแกรมประสงค์ร้าย

อธิบายความหมาย

: โปรแกรมหรือส่วนของโปรแกรมที่สร้างขึ้นและเผยแพร่ โดยผู้มีเจตนาร้าย มุ่งทำลายอย่างใดอย่างหนึ่งต่อสิ่งที่เป็นเป้าหมาย โดยทั่วไปโปรแกรมประสงค์ร้ายจะแบ่งตามลักษณะการแพร่กระจายและการกระทำได้ ๕ ประเภท คือ

๘.๑ ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นโปรแกรมหรือส่วนของโปรแกรม ที่ผู้เขียนมีวัตถุประสงค์ในการทำลายอย่างใดอย่างหนึ่ง หนทางเข้าสู่ระบบคอมพิวเตอร์โดยการเกาะติดกับโปรแกรมที่ใช้งานทั่ว ๆ ไป ภายในระบบคอมพิวเตอร์และทำให้โปรแกรมเป้าหมายที่อาศัยอยู่นั้นกลายเป็นโปรแกรมประสงค์ร้ายด้วย ไวรัสคอมพิวเตอร์แพร่กระจายโดยสำเนาตัวเอง (Copy) ไปเกาะติดกับโปรแกรมต่าง ๆ เพื่อให้โปรแกรมเหล่านั้นนำพาไปยังส่วนต่าง ๆ ของระบบ เพื่อจะได้แพร่กระจายไปสู่โปรแกรมอื่น ๆ ที่ยังไม่มีโปรแกรมไวรัสเกาะอยู่ ซึ่งการแพร่กระจายจะเป็นลักษณะทวีคูณ ทำลายเป้าหมายได้ทุกรูปแบบตามเจตนาของผู้เขียนโปรแกรม ไวรัสคอมพิวเตอร์มักจะแบ่งประเภทตามแหล่งที่อาศัยภายในระบบ หรือโปรแกรมที่จะกระทำการโดยเฉพาะ เช่น ไวรัสในส่วนการปลุกเครื่อง (Boot Sector Virus) แมโครไวรัส (Macro Virus) เป็นต้น ไวรัสคอมพิวเตอร์จะกระทำการ (Active) ได้ก็ต่อเมื่อโปรแกรมเป้าหมาย ที่โปรแกรมไวรัสอาศัยอยู่มีการดำเนินการ (Run/Process)

๘.๒ หนอน (Worm) เป็นโปรแกรมที่สามารถสำเนาตัวเอง (Copy) ให้แพร่กระจายในระบบเครือข่าย และสามารถกระทำการ (Active) ต่าง ๆ ได้โดยลำพัง ไม่ต้องอาศัยโปรแกรมอื่น ๆ ในการนำพาไปยังส่วนต่าง ๆ ของระบบ ทำลายระบบโดยการสำเนาตัวเองเพิ่มขึ้นเรื่อย ๆ จนระบบไม่สามารถทำงานต่อไปได้

๘.๓ ตัวลวง หรือ ม้าโทรจัน (Trojan Horse) เป็นโปรแกรม หรือส่วนของโปรแกรม ที่ถูกนำมาซ่อนไว้ในโปรแกรมใช้งานโปรแกรมใดโปรแกรมหนึ่งภายในระบบโดยผู้ใช้ไม่ทราบและคิดว่าเป็นโปรแกรมที่ใช้งานตามปกติ มักกระทำโดยผู้พัฒนาโปรแกรมหรือบุคคลอื่นที่เกี่ยวข้องกับการบำรุงรักษาโปรแกรม เช่น โปรแกรมม้าโทรจันที่แทรกมากับบท (คำสั่ง) ลงบันทึกเข้า (Login Script) ที่รอให้บริการแก่ผู้ใช้ที่ต้องการเข้าสู่ระบบใดระบบหนึ่ง โดยการใส่บัญชีผู้ใช้และรหัสผ่าน ซึ่งนอกจากทำหน้าที่ตรวจสอบความถูกต้องแท้จริงในการเข้าระบบของผู้ใช้แล้วยังแอบสำเนาบัญชีผู้ใช้และรหัสผ่านดังกล่าวเก็บไว้ใช้ประโยชน์ส่วนตัวในภายหลัง

ม้าโทรจัน ไม่สามารถเคลื่อนย้ายหรือสำเนาตัวเองได้ บางครั้งใช้เป็นที่พรางตัวของโปรแกรมประสงค์ร้ายอื่น ๆ มักเป็นไปในลักษณะของการเชิญชวนให้เกิดความสนใจและนำโปรแกรมดังกล่าวบรรจุเข้าในระบบ ซึ่งผู้ใช้เองที่นำม้าโทรจันเข้าสู่ระบบโดยไม่เจตนา เช่น เกมส์คอมพิวเตอร์ (Computer Game) โปรแกรมอรรถประโยชน์ (Utility Program) ภาพอนาจาร (Nude) เป็นต้น ซึ่งโปรแกรมเหล่านี้เมื่อบรรจุเข้าระบบได้แล้วก็อาจแพร่ไวรัสหรือโปรแกรมประสงค์ร้ายอื่น ๆ ได้

๘.๔ กับดัก (Trap Door) เป็นโปรแกรมที่สร้างให้มีหนทางลับหรืออภิสิทธิ์ ในการเข้าสู่ระบบ โปรแกรมหรือข้อมูลเป้าหมายได้เฉพาะบุคคลและตลอดเวลาที่ต้องการ โดยปกติมีวัตถุประสงค์ให้ผู้ควบคุมระบบใช้เป็นทางเข้าเพื่อดูแล บำรุงรักษา หรือตรวจสอบระบบ เช่น โปรแกรมของเครื่องรับจ่ายเงินอัตโนมัติ (Automatic Teller Machine) กำหนดให้รหัสผ่าน ๙๙๙๙ เป็นรหัสผ่านที่สามารถเข้าถึงการบันทึกเข้าออก (Log) ของรายการเปลี่ยนแปลง (Transaction) ยอดเงินฝากเข้าลูกค้า

กับดัก กระทำได้โดยผู้พัฒนาโปรแกรมหรือบุคคลอื่นที่เกี่ยวข้องในช่วงที่กำลังพัฒนาโปรแกรมซึ่งอาจสร้างทางลับเพื่อหาประโยชน์อย่างใดอย่างหนึ่งจากระบบในภายหลังจากตัวอย่างข้างต้นเมื่อสามารถเข้าสู่แฟ้มบันทึกเข้าออก (Log File) ของรายการเปลี่ยนแปลงได้แล้วอาจสร้างโปรแกรมให้มีการโอนเงินหลังจุดทศนิยมจากรายการเปลี่ยนแปลงมาสะสมไว้ในบัญชีลับบัญชีใดบัญชีหนึ่งได้

๘.๕ ระเบิด (Bomb) เป็นโปรแกรมที่มีเจตนาร้ายอย่างใดอย่างหนึ่ง จะดำเนินการเมื่อมีเหตุการณ์ตรงตามเงื่อนไขเกิดขึ้น ได้แก่ เงื่อนไขเวลา วันที่ หรือเงื่อนไขอื่น ๆ เช่น โปรแกรมกำหนดให้จัดรูปแบบจานบันทึกแบบแข็ง (Format HardDisk) เมื่อมีผู้เข้าใช้ระบบที่มีบัญชีผู้ใช้ขึ้นต้นด้วยอักษร “ S” ครบ ๕๐ ครั้ง เป็นต้น อย่างไรก็ตามปัจจุบันโปรแกรมประสงค์ร้ายได้มีการพัฒนาความสามารถ ในการทำลายและการหลบหลีกการตรวจจับของโปรแกรมป้องกันต่าง ๆ อยู่เสมอ ดังนั้น ในอนาคตจะปรากฏโปรแกรมประสงค์ร้ายในรูปแบบที่มีการผสมผสานกันหลายๆ ประเภทมากยิ่งขึ้น

๙. Password ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: รหัสผ่าน

๙. Password ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: รหัสผ่าน

อธิบายความหมาย

: เป็นชุดของตัวอักษรหรือคำพิเศษ (Spacial Word) หรือวลี (Phase) ซึ่งให้สิทธิ์ในการเข้าถึงระบบแก่ผู้ใช้แต่ละคน นอกจากนี้ รหัสผ่านยังเป็นเครื่องมือรักษาความปลอดภัย ที่ใช้แสดงต่อระบบคอมพิวเตอร์เพื่อให้การรับรองความถูกต้องแท้จริง (Authentication) ของผู้ใช้ และ ตรวจสอบสิทธิ์ในการใช้งานระบบ (Access to its Resources) ดังนั้น จึงต้องมีการกำหนดระเบียบปฏิบัติให้ผู้ใช้สามารถจัดการรหัสผ่านของตนเองได้อย่างปลอดภัยและถูกต้อง

๑๐. Program ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: ๑. โปรแกรม, ชุดคำสั่ง

: ๒. สร้างโปรแกรม

อธิบายความหมาย

: เป็นชุดคำสั่งที่ต่อเนื่องกันเป็นลำดับเพื่อให้คอมพิวเตอร์ประมวลผล ในลักษณะที่ต้องการ อาจอยู่ในรูปของการเขียนโปรแกรมด้วยภาษาระดับสูง (High-Leve) ซึ่งต้องผ่านการแปลความหมายให้เป็นรหัสจุดหมาย (Object Code) ก่อนคอมพิวเตอร์จึงประมวลผลได้ หรืออาจอยู่ในรูปของรหัสจุดหมาย(Object Code) ซึ่งสามารถสั่งให้คอมพิวเตอร์ประมวลผลได้โดยตรง โปรแกรมคอมพิวเตอร์โดยทั่วไปแบ่งเป็น ๒ ประเภท คือ

- โปรแกรมระบบ (System Program) ได้แก่ โปรแกรมระบบปฏิบัติการ (Operating System Program) โปรแกรมบรรจุ (Loader, Loading Program) ตัวแปลโปรแกรม หรือโปรแกรมแปลโปรแกรมหรือคอมไพเลอร์ (Compiler) เป็นต้น โปรแกรมเหล่านี้ช่วยอำนวยความสะดวก ในการใช้งานคอมพิวเตอร์ โปรแกรมประยุกต์ หรือโปรแกรมใช้งาน (Application Program) เป็นโปรแกรมที่สร้างขึ้นโดยมีวัตถุประสงค์เพื่อการใช้งานในลักษณะใดลักษณะหนึ่งโดยเฉพาะ เช่น โปรแกรมประมวลผลคำ (Word Processing) - สารบรรณ - ธุรการ โปรแกรมทางธุรกิจ – การเงิน - การธนาคาร โปรแกรมเกี่ยวกับงานวิจัย - การศึกษา – การพยากรณ์ โปรแกรมควบคุมการทำงานของอุปกรณ์ – เครื่องมือเฉพาะอย่าง เป็นต้น

โปรแกรมเหล่านี้มักจะเขียนด้วยภาษาระดับสูงและใช้ประโยชน์เพียงกลุ่มผู้ใช้บางกลุ่มเท่านั้น รวมทั้งต้องมีการปรับปรุงเปลี่ยนแปลงโปรแกรมเพื่อให้ใช้งานได้ทันสมัยอยู่เสมอ

๑๑. Software ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: ส่วนชุดคำสั่ง ซอฟต์แวร์

อธิบายความหมาย

: เป็นคำที่ใช้เรียกโปรแกรมหรือโปรแกรมคอมพิวเตอร์โดยทั่วไป ต้องการแสดงให้เห็นถึงความแตกต่างระหว่าง ฮาร์ดแวร์ และซอฟต์แวร์ ซึ่งเป็นองค์ประกอบของระบบคอมพิวเตอร์

: เป็นคำสั่งที่อยู่ในรูปภาษาเครื่อง (Machine Language) ซึ่งเป็นภาษาระดับต่ำ (Low-Level) ที่หน่วยประมวลผลกลางของคอมพิวเตอร์สามารถเข้าใจและประมวลผลตามคำสั่งนั้นได้ทันที โดยทั่วไปมี ๒ ประเภท คือ ซอฟต์แวร์ระบบปฏิบัติการ (Operating System Software) และซอฟต์แวร์ประยุกต์ (Application Software)