แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กองบังคับการปราบปราม
พ.ศ. .....

คำนำ

กองบังคับการปราบปรามได้ออกประกาศเรื่องนโยบายในการรักษาความปลอดภัย พ.ศ. ..... และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ..... เพื่อให้การดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศเป็นไปอย่างมีประสิทธิภาพ และมีความน่าเชื่อถือ สอดคล้องตามมาตราฐานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (ISO ๒๗๐๐๑)

กองบังคับการปราบปรามจึงได้ทำการวางแนวปฏิบัติที่กำหนดต่อไปนี้ เป็นสิ่งสำคัญที่ผู้ปฏิบัติงานต้องถือปฏิบัติเพื่อให้การให้บริการต่างๆ ตามภารกิจของกองบังคับการปราบปรามที่ดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ และเพื่อให้ง่ายต่อการนำไปปฏิบัติหรืออ้างอิง จึงแบ่งแนวปฏิบัติออกเป็น ๑๓ หมวด ดังนี้

หมวด ๑ แนวปฏิบัติในการรักษาความปลอดภัยทางกายภาพ
หมวด ๒ แนวปฏิบัติในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย
หมวด ๓ แนวปฏิบัติในการควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์
หมวด ๔ แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการของผู้ใช้งาน
หมวด ๕ แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน
หมวด ๖ แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
หมวด ๗ แนวปฏิบัติในการจัดซื้อจัดจ้างระบบสารสนเทศ
หมวด ๘ แนวปฏิบัติในการควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น
หมวด ๙ แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ
หมวด ๑๐ แนวปฏิบัติในการแบ่งแยกอำนาจหน้าที่
หมวด ๑๑ แนวปฏิบัติในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์
หมวด ๑๒ แนวปฏิบัติในการเผยแพร่ข้อมูลต่อสาธารณะ
หมวด ๑๓ แนวปฏิบัติในการพัฒนาและบำรุงรักษาระบบ

สารบัญ

หมวด ๑

แนวปฏิบัติในการรักษาความปลอดภัยทางกายภาพ

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องมีหน้าที่บริหารจัดการรักษาความปลอดภัยทางกายภาพ (Physical Security Management) ดังนี้

๑.๑ กำหนดระดับความสำคัญของพื้นที่ หรือจำแนกพื้นที่การใช้งานกับพื้นที่การควบคุม

๑.๒ ทดสอบระบบควบคุมการเข้าถึงพื้นที่ทางกายภาพเพื่อให้ทราบว่าระบบยังใช้งานได้ตามปกติหรือไม่

๑.๓ ผู้ปฏิบัติงานควรปิดประตูและหน้าต่าง รวมถึงช่องทางต่างๆที่อาจเป็นเส้นทางเข้าถึงพื้นที่ซึ่งไม่ผ่านการตรวจสอบและการอนุมัติการเข้าถึงพื้นที่อยู่ตลอดเวลา

ข้อ ๒ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องมีหน้าที่บริหารจัดการควบคุมพื้นที่การเข้า - ออกพื้นที่การควบคุม ได้แก่ ห้องปฏิบัติการคอมพิวเตอร์ ดังนี้

๒.๑ มีการบันทึกวันและเวลาการเข้า - ออกพื้นที่การควบคุมของผู้มาเยือน (Visitor)

๒.๒ ดูแลผู้มาเยือนในพื้นที่หรือบริเวณที่มีการควบคุมจนกระทั่งเสร็จสิ้นภารกิจ และกลับไปเพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๒.๓ จัดให้มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของกองบังคับการปราบปราม โดยบุคคลภายนอกและควรมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๒.๔ จัดสื่อประชาสัมพันธ์เพื่อสร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๒.๕ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๒.๖ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ เว้นแต่ได้รับอนุญาต

๒.๗ มีการพิสูจน์ตัวตน ได้แก่ การแสดงบัตรผ่าน การใช้บัตรแถบแม่เหล็ก การสแกนลายนิ้วมือ เป็นต้น โดยเฉพาะห้องปฏิบัติการคอมพิวเตอร์ เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ

๒.๘ จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ โดยเฉพาะห้องปฏิบัติการคอมพิวเตอร์ เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๒.๙ บุคคลภายนอก ได้แก่ เจ้าหน้าที่บริษัท นักศึกษาฝึกงานหรือผู้ได้รับการว่าจ้างอื่น ๆ ต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

๒.๑๐ ผู้มาเยือนต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในกองบังคับการปราบปราม

๒.๑๑ ควรจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๒.๑๒ จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

ข้อ ๓ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องกำหนดการจัดวางและการป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (Hardware) ดังนี้

๓.๑ จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงของบุคคลภายนอก

๓.๒ ระบบงานที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่มีความมั่นคงปลอดภัยเพียงพอ

๓.๓ ไม่ให้มีการนำอาหาร เครื่องดื่ม หรือสูบบุหรี่ภายในบริเวณห้องปฏิบัติการคอมพิวเตอร์

๓.๔ ตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว ได้แก่ การตรวจสอบระดับอุณหภูมิ ความชื้น ให้อยู่ในระดับปกติอยู่เสมอ

ข้อ ๔ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องกำหนดให้มีระบบป้องกันและสนับสนุนการทำงาน ดังนี้

๔.๑ มีระบบสนับสนุนการทำงานของระบบสารสนเทศ ที่เพียงพอต่อความต้องการใช้งาน โดยให้มีอย่างน้อย ดังนี้

(๑) ระบบสำรองกระแสไฟฟ้า (UPS)

(๒) ระบบระบายอากาศ

(๓) ระบบปรับอากาศ

๔.๒ ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนอย่างสม่ำเสมอเพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๔.๓ ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องปฏิบัติการคอมพิวเตอร์ทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๕ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องกำหนดและควบคุมการเดินสายไฟ สายสัญญาณการสื่อสาร และสายเคเบิ้ลอื่นๆ ดังนี้

๕.๑ เครือข่ายภายในกองบังคับการปราบปราม ในลักษณะที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ต้องให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณและป้องกันสัตว์ต่างๆ กัดสาย ได้แก่ หนู แมลงสาบ เป็นต้น ซึ่งจะทำให้เกิดความเสียหายต่อสายสัญญาณ

๕.๒ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๕.๓ จัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

๕.๔ ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

ข้อ ๖ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องกำหนดการบำรุงรักษาอุปกรณ์ ดังนี้

๖.๑ กำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

๖.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๖.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๖.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๖.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในกองบังคับการปราบปราม

๖.๖ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่เข้าทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๗ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องบริหารจัดการควบคุมอุปกรณ์ที่ใช้งานอยู่ภายนอกกองบังคับการปราบปราม ดังนี้

๗.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นๆ ของกองบังคับการปราบปราม ออกไปใช้งานนอกสถานที่

๗.๒ กำหนดมาตรการควบคุมและบันทึกการนำอุปกรณ์ไปใช้นอกสถานที่ รายละเอียดผู้รับผิดชอบและผู้ประสานงานที่ชัดเจน

หมวด ๒

แนวปฏิบัติในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องบริหารจัดการข้อมูล ดังนี้

๑.๑ กำหนดมาตรการต่างๆ เพื่อการธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๑.๒ การกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทชั้นความลับ และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน (Data Classification and Access Control) รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ (Data Sanitization)

๑.๓ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ มีการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล

๑.๔ มีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (storage) นำเข้า (input) ประมวลผล (operate) และแสดงผล (output) นอกจากนี้ ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (distributed database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน

๑.๕ มาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

ข้อ ๒ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) ของผู้ใช้งาน ดังนี้

๒.๑ กำหนดบัญชีชื่อผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน

๒.๒ ไม่อนุญาตให้ผู้ร้องขอใช้ระบบงานเข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้น

๒.๓ จัดเก็บข้อมูลการลงทะเบียนขอเข้าใช้งานระบบ เพื่อใช้อ้างอิงหรือตรวจสอบข้อมูลในภายหลัง

๒.๔ ทบทวนบัญชีผู้ใช้งานทั้งหมดอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

(๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงานภายในของกองบังคับการปราบปราม

(๒) จัดส่งรายชื่อนั้นให้ผู้บังคับบัญชาของหน่วยงานภายในกองบังคับการปราบปราม เพื่อให้ทบทวนว่ายังมีรายชื่อของผู้ที่โอน/ลาออกไปแล้ว หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้มีการแก้ไขสิทธิการเข้าถึงให้ถูกต้อง

(๓) ผู้บังคับบัญชาของหน่วยงานภายในกองบังคับการปราบปราม แจ้งกลับว่ามีรายชื่อใดที่ต้องปรับปรุงแก้ไขให้ถูกต้อง

(๔) แก้ไขข้อมูลสิทธิให้ถูกต้องตามที่ได้รับแจ้ง (ถ้ามี)

ข้อ ๓ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องกำหนดให้มีการพิสูจน์ตัวตนผู้ใช้งาน (Authentication) และกำหนดสิทธิ์ที่เหมาะสมแก่ผู้ใช้งาน (Authorization) และมีการบันทึกการใช้งานที่เหมาะสม (Accounting) โดยผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานต้องผ่านการพิสูจน์ตัวตนจากระบบ โดยมีแนวทางปฏิบัติ ดังนี้

๓.๑ การแสดงตัวตนด้วยชื่อบัญชีผู้ใช้งาน (User Account)

๓.๒ การพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน (Password) หรือ การยืนยันตัวตนด้วยรูปแบบอื่นตามสมควร เช่น Pin Code, Biometric, Card

๓.๓ การเข้าใช้ระบบงานสำคัญของกองบังคับการปราบปรามผ่านเครือข่ายอินเทอร์เน็ต จะมีการตรวจสอบผู้ใช้งานด้วย

๓.๔ การเข้าใช้ระบบงานสำคัญของกองบังคับการปราบปรามจากระยะไกล (Remote Access) จะมีการตรวจสอบเพื่อเพิ่มความปลอดภัยและเพื่อพิสูจน์ตัวตนของผู้ใช้งาน ได้แก่ รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

๓.๕ ในการใช้งานระบบสารสนเทศ เมื่อมีการว่างเว้นจากการใช้งานเกินเวลา ๓๐ นาที ระบบจะทำการยกเลิกการใช้งานและการเชื่อมต่อเข้าระบบโดยอัตโนมัติ และผู้ใช้ต้องล็อกหน้าจอโดยทันทีขณะไม่มีผู้ดูแลเพื่อป้องกันผู้ไม่มีสิทธิ์เข้าถึงอุปกรณ์

ข้อ ๔ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปรามต้องกำหนดวิธีการใช้รหัสผ่านให้มีความมั่นคงปลอดภัย ดังนี้

๔.๑ การบริหารจัดการรหัสผ่าน มีมาตรการและการควบคุม ดังนี้

(๑) กำหนดให้ต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน

(๒) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๖ ตัวอักษร โดยมีการผสมกัน ระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๓) กรณีผู้ใช้งานเปลี่ยนหน้าที่ความรับผิดชอบหรือลาออกจะต้องเปลี่ยน หรือถอดถอนสิทธินั้นทันทีเมื่อได้รับแจ้ง

(๔) กำหนดให้การเข้าใช้งานระบบครั้งแรกมีการโต้ตอบด้วยการยืนยันตัวตนและเปลี่ยนรหัสผ่านเพื่อเพิ่มความปลอดภัย

(๕) การกำหนดรหัสผ่านควรใช้อักขระพิเศษประกอบ เช่น : ; < > @ !

(๖) การกำหนดรหัสผ่าน ควรกำหนดตัวอักษร อักขระพิเศษ หรือเลข หลีกเลี่ยงการกำหนดรหัสผ่านแบบแผน เช่น “abcdef” “aaaaaa” “๑๒๓๔๕๖”

(๗) การกำหนดรหัสผ่านควรกำหนดตัวอักษร อักขระพิเศษ หรือเลข หลีกเลี่ยงการกำหนดรัหสเป็น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่

(๘) การกำหนดรหัสผ่าน หลีกเลี่ยงการกำหนดเป็นคำศัพท์ที่อยู่ในพจนานุกรม

(๙) การกำหนดรหัสผ่าน ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน ๕ ครั้ง

(๑๐) การจัดส่งรหัสผ่านให้กับผู้ใช้งาน ให้มีการจัดส่งให้กับผู้ใช้งานอย่างปลอดภัย เช่น การใส่ซองปิดผนึก

(๑๑) ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งเรก (default password) หรือได้รับรหัสผ่านใหม่ ให้เปลี่ยนรหัสผ่านนั้นโดยทันที

(๑๒) ผู้ใช้งานควรเก็บรักษารหัสผ่านไว้เป็นความลับ

(๑๓) กำหนดความรับผิดชอบต่อ User Account ของตนเองและผลแห่งการกระทำของ User Account ของตนเอง

๔.๒ การใช้รหัสผ่าน มีมาตรการให้ผู้ใช้งานต้องใช้ด้วยความระมัดระวัง ดังนี้

(๑) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๒) ไม่ใช้โปรแกรมสำนักงานคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

(๓) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๔) กำหนดรหัสผ่านให้ยากต่อการคาดเดา

(๕) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่น เนื่องจากความจำเป็นในการปฏิบัติงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๖) กรณีผู้ใช้งานลาออกหรือเปลี่ยนหน้าที่ความรับผิดชอบ ต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศ ทราบทันที

ข้อ ๕ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย มีแนวทางการปฏิบัติดังนี้

๕.๑ มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

๕.๒ เปิดใช้บริการ (service) เท่าที่จำเป็น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติม

๕.๓ ดำเนินการติดตั้ง patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (system software) เช่น ระบบปฏิบัติการ DBMS และ web server เป็นต้น อย่างสม่ำเสมอ

๕.๔ ทดสอบ system software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา

๕.๕ มีแนวทางปฏิบัติในการใช้งาน software utility เช่น personal firewall password cracker เป็นต้น และตรวจสอบการใช้งาน software utility อย่างสม่ำเสมอ

๕.๖ กำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่างๆ ของโปรแกรมระบบอย่างชัดเจน

ข้อ ๖ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องจัดการและการตรวจสอบระบบเครือข่าย มีแนวทางการปฏิบัติดังนี้

๖.๑ แบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่ายภายใน ส่วนเครือข่ายภายนอก ส่วน DMZ เป็นต้น

๖.๒ มีระบบป้องกันการบุกรุก เช่น firewall เป็นต้น ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก

๖.๓ มีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ

๖.๔ จัดทำแผนผังระบบเครือข่าย (network diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๖.๕ ตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส ตรวจสอบการกำหนดค่า parameter ต่างๆ เกี่ยวกับการรักษาความปลอดภัย เป็นต้น และต้องตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (physical disconnect) และจุดเชื่อมต่อ (disable port) ที่ไม่มีความจำเป็นต้องเชื่อมต่อกับระบบเครือข่าย ออกจากระบบเครือข่ายโดยสิ้นเชิง

๖.๖ ในกรณีที่มีการเข้าถึงระบบเครือข่ายในลักษณะ remote access ต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่และมีการควบคุมอย่างเข้มงวด เช่น การตรวจสอบตัวตนจริงและสิทธิของผู้ใช้งาน การบันทึกรายละเอียดการใช้งาน และควรตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ที่ใช้เชื่อมต่อออกจากระบบเครือข่ายภายใน เป็นต้น รวมทั้งต้องตัดการเชื่อมต่อการเข้าถึงดังกล่าวเมื่อไม่ใช้งานแล้ว หรือเมื่อขาดการใช้งาน (Idle) เป็นระยะเวลาหนึ่ง

๖.๗ กำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่างๆ ของระบบเครือข่าย และอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ก็ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๖.๘ การใช้เครื่องมือต่างๆ (tools) เพื่อตรวจเช็คระบบเครือข่าย ควรได้รับการอนุมัติจากผู้มีอำนาจหน้าที่ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ข้อ ๗ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องมีบริหารการเปลี่ยนแปลงระบบคอมพิวเตอร์ มีแนวทางการปฏิบัติดังนี้

๗.๑ ก่อนการเปลี่ยนแปลงระบบและอุปกรณ์คอมพิวเตอร์ ควรมีการประเมินผลกระทบที่เกี่ยวข้อง และบันทึกการเปลี่ยนแปลงให้เป็นปัจจุบันอยู่เสมอ รวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ

๗.๒ ควรติดตั้งซอฟต์แวร์เท่าที่จำเป็นแก่การใช้งาน และถูกต้องตามลิขสิทธิ์

ข้อ ๘ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องมีการวางแผนการรองรับประสิทธิภาพของระบบคอมพิวเตอร์ มีแนวทางการปฏิบัติดังนี้

๘.๑ ประเมินการใช้งานระบบคอมพิวเตอร์สำคัญไว้ล่วงหน้า เพื่อรองรับการใช้งานในอนาคต

ข้อ ๙ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องมีการป้องกันไวรัส และ malicious code มีแนวทางการปฏิบัติดังนี้

๙.๑ มีมาตรการป้องกันไวรัสที่มีประสิทธิภาพและปรับปรุงให้เป็นปัจจุบันอยู่เสมอสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น ติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น

๙.๒ ฝ่ายคอมพิวเตอร์ควรจัดทำคู่มือในการป้องกันไวรัสให้แก่ผู้ใช้งานเพื่อใช้เป็นแนวทางปฏิบัติ รวมทั้งแจ้งและให้ความรู้แก่ผู้ใช้งานเกี่ยวกับไวรัสชนิดใหม่ๆ อย่างสม่ำเสมอ

๙.๓ ควบคุมมิให้ผู้ใช้งานระงับการใช้งาน (disable) ระบบป้องกันไวรัสที่ได้ติดตั้งไว้ และควรแจ้งบุคคลที่เกี่ยวข้องทันทีในกรณีที่พบว่ามีไวรัส

ข้อ ๑๐ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องมีการบันทึกเพื่อการตรวจสอบ มีแนวทางการปฏิบัติดังนี้

๑๐.๑ กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ (login-logout logs) บันทึกการพยายามเข้าสู่ระบบ (login attempts) บันทึกการใช้ command line และ firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึก ดังกล่าวไว้อย่างน้อย ๓ เดือน

๑๐.๒ ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๑๐.๓ วิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกต่างๆ ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวด ๓

แนวปฏิบัติในการควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องทำตามขั้นตอนของการร้องขอ มีแนวทางการปฏิบัติดังนี้

๑.๑ การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร (อาจเป็น electronic transaction เช่น email เป็นต้น) และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ หัวหน้าฝ่ายคอมพิวเตอร์ เป็นต้น

๑.๒ ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (operation) ระบบรักษาความปลอดภัย (security) และการทำงาน (functionality) ของระบบงานที่เกี่ยวข้อง

๑.๓ ควรสอบทานกฎเกณฑ์ของทางการที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของทางการ

๑.๔ มีการบันทึกการเปลี่ยนแปลงและลงนามเป็นลายลักษณ์อักษรหรือการยืนยันผ่านระบบสารสนเทศจากผู้มีอำนาจสั่งการ (Authorized Person)

ข้อ ๒ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องทำตามขั้นตอนของการปฏิบัติงานพัฒนาระบบงาน มีแนวทางการปฏิบัติดังนี้

๒.๑ ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) ออกจากส่วนที่ใช้งานจริง (production environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนตามที่กล่าว อาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้

๒.๒ ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้องควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ

๒.๓ ควรตระหนักถึงระบบรักษาความปลอดภัย (security) และเสถียรภาพการทำงาน (availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง

ข้อ ๓ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องทำตามขั้นตอนของการทดสอบ มีแนวทางการปฏิบัติดังนี้

๓.๑ ผู้ที่ร้องขอและฝ่ายคอมพิวเตอร์ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

๓.๒ ในระบบงานสำคัญควรมีหน่วยงานหรือทีมงานอิสระ เข้าตรวจสอบว่ามีการปฏิบัติตามขั้นตอนการพัฒนาและการทดสอบระบบ ก่อนที่จะโอนย้ายไปใช้งานจริง

ข้อ ๔ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องทำตามขั้นตอนของการโอนย้ายระบบงานเพื่อใช้งานจริง มีแนวทางการปฏิบัติดังนี้

๔.๑ ตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ

ข้อ ๕ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องทำตามขั้นตอนของการจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน และจัดเก็บ version ของระบบงานที่ได้รับการพัฒนา มีแนวทางการปฏิบัติดังนี้

๕.๑ จัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา

๕.๒ ปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และ program specification เป็นต้น และต้องจัดเก็บเอกสารตามที่กล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

๕.๓ จัดเก็บโปรแกรม version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

ข้อ ๖ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องทำตามขั้นตอนของการทดสอบหลังการใช้งาน มีแนวทางการปฏิบัติดังนี้

๖.๑ กำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

ข้อ ๗ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องทำตามขั้นตอนของการสื่อสารการเปลี่ยนแปลง มีแนวทางการปฏิบัติดังนี้

๗.๑ ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

หมวด ๔
แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการของผู้ใช้งาน

ข้อ ๑. ผู้ใช้งานจะต้องยืนยันตัวตนด้วย User account และพิสูจน์ตนด้วย รหัสผ่าน ของตนเองก่อนเข้าใช้งานระบบปฏิบัติการเครื่องคอมพิวเตอร์ทุกครั้ง

ข้อ ๒. ผู้ใช้งานต้องไม่อนุญาตให้บุคคลอื่นใช้ User account ของตนเองในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

ข้อ ๓. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมเพื่อล็อคหน้าจอโดยอัตโนมัติ หลังจากที่ไม่ได้ใช้งานเกินกว่า ๑๕ นาที ทั้งนี้ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อระบบ (Limitation of Connection Time) เมื่อผู้ใช้ว่างเว้นการใช้งานเกินกว่า ๓๐ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องยืนยันตัวตนใหม่อีกครั้ง

ข้อ ๔. ผู้ใช้งานควรทำการลงบันทึกออก (Log off) ทุกครั้งที่มิได้ปฏิบัติงานอยู่หน้าเครื่องคอมพิวเตอร์ รวมทั้งปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเลิกใช้งาน

ข้อ ๕. ผู้ใช้งานต้องไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) รวมถึงโปรแกรมอรรถประโยชน์ใดๆ ที่อาจละเมิดหรือทำให้หลีกเลี่ยงมาตรการความมั่นคงปลอดภัยได้ ทั้งนี้ผู้ดูแลระบบต้องมีการจำกัดสิทธิ์และควบคุมการเข้าถึงโปรแกรมอรรถประโยชน์ของระบบ (Use of System Utilities) และตรวจสอบโดยสม่ำเสมอ

ข้อ ๖. ผู้ใช้งานต้องใช้งานรหัสผ่านไม่น้อยกว่า ๖ ตัวอักษร โดยไม่นำชื่อหรือนามสกุลของตนเองหรือคำที่ง่ายต่อการคาดเดามาตั้ง และต้องเปลี่ยนรหัสผ่านทุก ๖ เดือน โดยระบบปฏิบัติการจะตรวจสอบรหัสผ่านให้มีคุณภาพ รวมถึงเตือนหากใช้รหัสผ่านซ้ำนาน ซึ่งควบคุมผ่านระบบบริหารจัดการรหัสผ่านส่วนกลาง (Active Directory) และนโยบายกลุ่ม (Group Policy)

หมวด ๕
แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม เป็นผู้พิจารณาคัดเลือกระบบสารสนเทศเพื่อจัดทำระบบสำรอง นำส่งแผนสำรองข้อมูล อีกทั้งต้องใช้แนวทางปฏิบัติในการสำรอง

และกู้คืนข้อมูล เมื่อมีระบบงานใหม่ เกิดข้อมูลใหม่ หรือข้อมูลที่มีการเปลี่ยนแปลงใหม่ ควรกำหนดให้ใช้แนวทางการสำรองและกู้คืนข้อมูล ที่เหมาะสม ดังนี้

๑.๑ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนพร้อมกรณีฉุกเฉิน

๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลสูงขึ้น

๑.๓ กำหนดประเภทของข้อมูลที่ต้องสำรองเก็บไว้ และความถี่ในการสำรอง

๑.๔ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะสำรอง คือ การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๑.๕ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง และผลความสำเร็จ

๑.๖ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ทั้งข้อมูลฐานข้อมูล ซอฟต์แวร์ และข้อมูลการตั้งค่า

๑.๗ ดำเนินการป้องกันทางกายภาพและการเข้ารหัสลับอย่างเพียงพอในการเก็บข้อมูลสำรองดังกล่าว

๑.๘ ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ และสภาพพร้อมใช้งานของ ระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้หรือไม่

๑.๙ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยแผนฯ ควรมีรายละเอียดอย่างน้อยดังต่อไปนี้

(๑) การมอบหมายหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด ให้ชัดเจนที่สามารถเชื่อมโยงถึงตัวของบุคลากร ในเรื่องต่อไปนี้ ระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

(๒) การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และวางมาตรการเพื่อลดความเสี่ยงเหล่านั้น ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) การระบุขั้นตอนปฏิบัติในการกู้คืนระบบงาน

(๔) การระบุขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) การระบุช่องทางในการติดต่อสื่อสารกับผู้ให้บริการภายนอก ได้แก่ ผู้ให้บริการเครื่องคอมพิวเตอร์ โปรแกรมและระบบเครือข่าย เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อในกรณีเกิดเหตุฉุกเฉินต่างๆ ไม่ว่า เกิดอัคคีภัย การก่อวินาศกรรม เป็นต้น

๑.๑๐ ให้ทำการปรับปรุงแผนฯ ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๑.๑๑ ให้จัดประชุมและแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนฯ รวมทั้งเมื่อมีการปรับปรุงแผนใหม่จะต้องจัดประชุมใหม่และแจ้งให้ผู้ที่เกี่ยวข้องทราบเช่นเดียวกัน

หมวด ๖
แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

ข้อ ๑ การแจ้งเหตุการณ์ทางด้านความมั่นคงปลอดภัย แนวปฏิบัติดังนี้

๑.๑ ให้เจ้าหน้าที่หรือผู้ปฏิบัติงานแจ้งไปยังฝ่ายอาคารหรือศูนย์รับเจ้งความ ทันทีที่พบเห็นเหตุการณ์ที่อาจเป็นปัญหาต่อความมั่นคงปลอดภัยในการใช้ระบบสารสนเทศของกองบังคับการปราบปราม ได้แก่

(๑) มีโปรแกรมสำนักงานไม่ประสงค์ดีเข้ามาในระบบคอมพิวเตอร์

(๒) มีการบุกรุกเข้ามาในระบบเครือข่าย

(๓) ข้อมูลสำคัญเปลี่ยนแปลง หรือสูญหาย

(๔) มีการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๕) มีการนำข้อมูลสำคัญไปใช้ผิดวัตถุประสงค์

(๖) มีการใช้ระบบสารสนเทศ ผิดวัตถุประสงค์

(๗) พบจุดอ่อนในเครื่องคอมพิวเตอร์ โปรแกรมและระบบเครือข่ายที่ใช้งาน

(๘) มีการโจมตีเข้ามาในระบบจนไม่สามารถให้บริการได้

(๙) ระบบสารสนเทศ ชำรุดหรือสูญหาย

(๑๐) บุคคลภายนอกเข้าใช้ระบบงานของกองบังคับการปราบปราม โดยไม่ได้รับอนุญาต

(๑๑) มีการติดตั้งโปรแกรมเพื่อขโมยข้อมูลหรือเข้าถึงข้อมูลในระบบเครือข่าย

(๑๒) เหตุการณ์อื่นๆ ที่เป็นการละเมิดความมั่นคงปลอดภัยของกองบังคับการปราบปราม

๑.๒ ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชาหรือศูนย์เทคโนโลยีสารสนเทศในการตรวจสอบเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้นรวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชาหรือศูนย์เทคโนโลยีสารสนเทศ ด้วย

ข้อ ๒ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม เมื่อได้รับแจ้งจากผู้ใช้งานเกี่ยวกับเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้นหรือที่พบ ให้ปฏิบัติตามขั้นตอนดังต่อไปนี้

๒.๑ ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้นว่ามีผลกระทบในระดับใด (สูง กลาง หรือต่ำ)

๒.๒ แจ้งให้ผู้บังคับบัญชาตามลำดับชั้นได้รับทราบตามระดับของผลกระทบ กล่าวคือ รายงานไปสู่ระดับชั้นของผู้บังคับบัญชาที่สูงขึ้นตามลำดับสำหรับเหตุการณ์ที่มีผลกระทบสูงกว่า

๒.๓ วิเคราะห์และแก้ไขสถานการณ์ตามความจำเป็นกรณีการบุกรุก การโจมตีระบบ หรือระบบได้รับความเสียหาย อาจประสานงานขอความช่วยเหลือจากผู้รู้ ได้แก่ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT)

๒.๔ กรณีมีความจำเป็นต้องเก็บหลักฐานทางคอมพิวเตอร์ ให้ผู้ที่ผ่านการอบรมหรือฝึกฝนเป็นผู้ดำเนินการเพื่อป้องกันไม่ให้หลักฐานเกิดความเสียหาย จัดเก็บหลักฐานไว้ในสถานที่ที่ปลอดภัย และจำกัดการเข้าถึงหลักฐานนั้น

๒.๕ จัดทำรายงานสรุปเหตุการณ์นับตั้งแต่ได้รับแจ้งเฉพาะเหตุการณ์ที่มีผลกระทบตั้งแต่ระดับปานกลาง ขึ้นไปและแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ โดยมีข้อมูลอย่างน้อยในรายงานดังนี้

(๑) รายละเอียดเหตุการณ์

(๒) วันเวลาที่เกิดขึ้น

(๓) ชื่อผู้แจ้ง/หน่วยงานผู้แจ้ง

(๔) สถานะของเหตุการณ์ในแต่ละช่วงเวลา

(๕) ความคืบหน้าในการดำเนินการในแต่ละช่วงเวลา

(๖) สาเหตุและวิธีการแก้ไข

(๗) ข้อเสนอแนะเพื่อป้องกันการเกิดซ้ำ

ข้อ ๓ ความรับผิดชอบของผู้บังคับบัญชากรณีที่มีการละเมิดการปฏิบัตินี้

๓.๑ ให้แจ้งรายงานตามสายการบังคับบัญชาให้หน่วยที่เกี่ยวข้องทราบ

๓.๒ สั่งการสอบสวนหาตัวผู้กระทำผิดและผู้รับผิดชอบโดยเร็วที่สุด

๓.๓ พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เช่นนี้อุบัติซ้ำอีก

๓.๔ ให้พิจารณาการลงโทษทางวินัยตามกฎหมายต่อผู้ละเมิด ผู้เกี่ยวข้องกับการละเมิด และผู้รับผิดชอบเมื่อมีการละเมิด หรือไม่ปฏิบัติตามระเบียบนี้โดยเจตนาหรือไม่เจตนา และการละเมิดนั้นก่อให้เกิดความเสียหายหรือยังไม่เกิดความเสียหายต่อทางราชการก็ตาม

ข้อ ๔ ความรับผิดชอบของหน่วยงานที่รับผิดชอบระบบสารสนเทศ เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัย ให้ส่วนราชการเจ้าของระบบสารสนเทศ ดำเนินการ ดังนี้

๔.๑ พิจารณาว่าข้อมูลสารสนเทศ เอกสารกรรมวิธีข้อมูลต่างๆ ประมวลลับ หรือรหัสผ่านที่จำเป็นในการใช้เครือข่ายสื่อสารข้อมูลสารสนเทศมีผลกระทบกระเทือนเสียหายอย่างใดหรือไม่

๔.๒ ขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันทีในการนี้อาจจะต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติพร้อมทั้งปัจจัยต่างๆ ที่เกี่ยวข้องตามที่เห็นสมควร

ข้อ ๕ ความรับผิดชอบของผู้ใช้งานต่อประกาศฉบับนี้มี ดังนี้

๕.๑ ปฏิบัติตามประกาศนี้อย่างเคร่งครัดและต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง

๕.๒ ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ได้รับอนุญาต หรือทำให้เสียหายต่อระบบคอมพิวเตอร์และเครือข่ายของกองบังคับการปราบปราม

๕.๓ ไม่รบกวนหรือแทรกแซงการสื่อสารข้อมูลในเครือข่ายของกองบังคับการปราบปราม

๕.๔ รายงานเหตุการณ์ความเสี่ยง จุดอ่อน หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบไปยังกองบังคับการปราบปรามโดยเร็วที่สุด

ข้อ ๖ มีการควบคุมสินทรัพย์ด้านสารสนเทศต่อการเข้าถึงต้องได้รับการอนุญาตโดยปฏิบัติ ดังนี้

๖.๑ กำหนดมาตรการป้องกันทรัพย์สินขององค์กร โดยรวบรวมสินทรัพย์ทั้งหมดไว้อย่างเป็นระบบ

๖.๒ เมื่อใช้งานระบบเสร็จ ต้องออกจากระบบทันที

๖.๓ ป้องกันไม่ให้ผู้ที่ไม่เกี่ยวข้องใช้อุปกรณ์ด้านสารสนเทศโดยไม่ได้รับอนุญาต

๖.๔ นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

หมวด ๗
แนวปฏิบัติในการจัดซื้อจัดจ้างระบบสารสนเทศ

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องควบคุมการพัฒนาหรือจัดหาระบบงานเพื่อให้ระบบงานที่ได้รับมีความมั่นคงปลอดภัยเพียงพอ ดังนี้

๑.๑ ให้ประเมินความเสี่ยงและระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Requirements) ของระบบงานที่จะจัดหาหรือพัฒนาอย่างเป็นลายลักษณ์อักษร ข้อกำหนดดังกล่าวอย่างน้อยควรมีคุณสมบัติของการเข้าสู่ระบบงาน (Login) ที่มีความมั่นคงปลอดภัย ดังนี้

(๑) ไม่มีหรือไม่แสดงรูปแบบการใช้งาน (Function) ให้การช่วยเหลือในระหว่างที่ Login

(๒) บันทึกความพยายามในการล็อกอินทั้งที่สำเร็จและไม่สำเร็จ และแสดงประวัติการ Login ๓ ครั้งล่าสุด

(๓) ตัดการเชื่อมต่อหลังจากที่ทำการ Login ไม่สำเร็จเกินกว่า ๕ ครั้ง เป็นระยะเวลาที่เหมาะสมแล้วแต่ระบบงาน

(๔) เมื่อใส่ข้อมูลบัญชีชื่อผู้ใช้งานและรหัสผ่านที่ไม่ถูกต้อง ให้แสดงข้อความปรากฏ ว่า “ข้อมูลการ Login ไม่ถูกต้อง” หรือทำนองนี้

(๕) ให้แสดงข้อความเตือนที่หน้าจอภายหลังจากการ Login เสร็จสิ้น ข้อความเตือนดังกล่าว ได้แก่ “ระบบนี้เป็นระบบที่เป็นทรัพย์สินของกองบังคับการปราบปราม การใช้งานจะต้องได้รับการอนุมัติก่อนเท่านั้นจึงจะสามารถใช้งานได้ ผู้ที่ไม่ได้รับสิทธิและเข้ามาใช้ระบบงานหากมีการตรวจพบและเป็นความผิดจะดำเนินการลงโทษทางวินัยหรือดำเนินการทางกฎหมายตามความเหมาะสม สิทธิในการตรวจสอบพฤติกรรมการใช้งานในระหว่างที่ผู้ใช้งานใช้ระบบงานนี้โดยไม่ถือว่าเป็นการละเมิดความเป็นส่วนตัว”

(๖) ไม่แสดงรายละเอียดของระบบใดๆ จนกว่าจะ Login สำเร็จ

(๗) การกำหนดหรือตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับเข้าถึงระบบงาน

(๘) การเข้ารหัสข้อมูลสำคัญที่มีการรับส่งระหว่างเครื่องคอมพิวเตอร์ลูกข่ายกับเครื่องคอมพิวเตอร์ที่ให้บริการ

(๙) การเข้ารหัสข้อมูลสำคัญ ได้แก่ ข้อมูลลับ ที่จัดเก็บไว้ในฐานข้อมูล

(๑๐) การตัดและหมดเวลาการใช้งานหลังจากที่ไม่ได้ใช้ระบบงานเกินกว่าระยะเวลาตามที่กำหนดไว้ ในช่วง ๑๕ - ๓๐ นาที สำหรับระบบทั่วไป และในช่วง ๕ - ๑๕ นาที สำหรับระบบที่มีความเสี่ยงหรือมีความสำคัญสูง

(๑๑) การบันทึกบัญชีชื่อผู้ใช้งานที่ Login เข้าระบบ หมายเลข IP Address วันเวลาที่เข้าใช้ระบบ ความสำเร็จหรือไม่สำเร็จในการ Login ของผู้ใช้งาน

๑.๒ พัฒนาหรือจัดหาระบบงานให้ได้ตามข้อกำหนดทางด้านความมั่นคงปลอดภัยที่ระบุไว้

๑.๓ พัฒนาหรือจัดหาระบบงานเพื่อให้มีหน้าจอสำหรับผู้ดูแลระบบเพื่อทำการบันทึกและปรับปรุงสิทธิของผู้ใช้งานได้ รวมทั้งต้องสามารถบันทึกสิทธิดังกล่าวลงเก็บไว้ในฐานข้อมูลได้ด้วย

๑.๔ กำหนดให้มีการจัดทำแผนการทดสอบโดยผู้พัฒนาระบบ นำเสนอแผนฯ ดังกล่าวเพื่อพิจารณาอนุมัติโดยผู้มีอำนาจ ดำเนินการทดสอบตามแผนฯ บันทึกผลการทดสอบ และรายงานผลการทดสอบ ให้ผู้มีอำนาจได้รับทราบเพื่อให้คำแนะนำในการปรับปรุงต่างๆ ที่จำเป็นแผนการทดสอบที่จัดทำอย่างน้อยประกอบด้วย

(๑) แผนการทดสอบ UAT (User Acceptance Test)

(๒) แผนการทดสอบ System Integration Test

๑.๕ ไม่อนุญาตการนำข้อมูลสำคัญของกองบังคับการปราบปราม ไปใช้ในการทดสอบกับระบบงานเพื่อป้องกันการรั่วไหลของข้อมูล เว้นเสียแต่มีความจำเป็นและได้รับการอนุมัติเท่านั้น

ข้อ ๒ ภายหลังจากที่ได้มีการตรวจรับระบบที่พัฒนาขึ้นใหม่แล้ว ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องกำหนดการควบคุมการติดตั้งโปรแกรมลงไปยังระบบเครื่องคอมพิวเตอร์ที่ให้บริการ ดังนี้

๒.๑ ให้มีการควบคุมการเปลี่ยนแปลงระบบงานภายในกองบังคับการปราบปราม เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น

๒.๒ ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงระบบงานภายในกองบังคับการปราบปราม

๒.๓ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

๒.๔ กำหนดให้มีการจัดเก็บรหัสโปรแกรม (Source Code) และบรรณานุกรมคำศัพท์ (Library) สำหรับโปรแกรมของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๒.๕ กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน ได้แก่ โปรแกรมระบบปฏิบัติการ โปรแกรมระบบงาน เป็นต้น

๒.๖ ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

๒.๘ ในกรณีที่เป็นการติดตั้งระบบเพื่อทดแทนระบบงานเดิมให้ทำการสำรองข้อมูลที่จำเป็น ได้แก่ ฐานข้อมูล โปรแกรม ค่าปรับแต่งและติดตั้งระบบ หรืออื่นๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งทำไม่สำเร็จจะได้สามารถถอยหลังกลับไปใช้ระบบงานเดิมได้

๒.๙ ในกรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบงานเดิมไปสู่ข้อมูลในระบบงานที่ทำการติดตั้ง ให้กำหนดแผนการถ่ายโอนหรือแปลงข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ ให้ถ่ายโอนข้อมูลตามแผนฯ และร่วมกับผู้ใช้งานเพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้องและครบถ้วนหรือไม่

๒.๑๐ ให้กำหนดแผนการติดตั้งสำหรับระบบงานซึ่งรวมถึงระยะเวลาที่จะดำเนินการ รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า ได้แก่ แผนการติดตั้งเครื่องคอมพิวเตอร์ โปรแกรม ระบบเครือข่าย และอื่น ๆ

๒.๑๑ สำหรับโปรแกรมที่จะทำการติดตั้ง ให้ตรวจสอบก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตโปรแกรมนั้น

๒.๑๒ ให้อ่านและปฏิบัติตามเงื่อนไขหรือข้อตกลงการใช้งานโปรแกรมที่จะทำการติดตั้งอย่างเคร่งครัด

๒.๑๓ สำหรับการติดตั้งโปรแกรมอเนกประสงค์ (Utility Software) ต้องตรวจสอบก่อนว่าเป็นโปรแกรมที่มีการทำงานที่ถูกต้องและเชื่อถือได้

๒.๑๔ ติดตั้งโปรแกรมสำนักงานแก้ไขช่องโหว่ (Patch) ที่เกี่ยวข้องกับระบบงาน ตามความจำเป็น ได้แก่ โปรแกรมสำนักงานแก้ไขช่องโหว่สำหรับระบบปฏิบัติการ โปรแกรมสำนักงานแก้ไขช่องโหว่สำหรับระบบบริหารจัดการฐานข้อมูล เป็นต้น

๒.๑๕ ตรวจสอบและปิดพอร์ต (Port) บนระบบงานที่ไม่มีความจำเป็นในการใช้งานก่อนเปิดระบบให้บริการ

ข้อ ๓ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องกำหนดให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating System Changes) ดังนี้

๓.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๓.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่กองบังคับการปราบปราม ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

ข้อ ๔ การดำเนินงานของบประมาณที่เกี่ยวข้องกับระบบสารสนเทศ หรือวัสดุอุปกรณ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ ต้องผ่านการพิจารณากลั่นกรองความเหมาะสมเบื้องต้นจากศูนย์เทคโนโลยีสารสนเทศ และนำเสนอคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์กองบังคับการปราบปราม ให้ความเห็นชอบ โดยผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำกองบังคับการปราบปราม เป็นผู้พิจารณารับรองก่อนจะพิจารณาในขั้นตอนต่อไป

หมวด ๘

แนวปฏิบัติในการควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องมีการคัดเลือกผู้ให้บริการ ดังนี้

๑.๑ มีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ

๑.๒ มีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (data confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (service level agreement) อย่างชัดเจน

ข้อ ๒ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องมีควบคุมผู้ให้บริการ ดังนี้

๒.๑ ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (production environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ เช่น ให้เจ้าหน้าที่ควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่หน่วยงาน (onsite service) และให้เจ้าหน้าที่ตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ remote access และปิด Access ทันทีที่การให้บริการเสร็จสิ้น

๒.๒ ในกรณีที่ใช้บริการด้านการทำงานที่เป็นความเสี่ยงสูง เช่น การพิสูจน์หลักฐานดิจิทัล (Digital Forensics) ให้ดำเนินการอย่างรัดกุม กำหนดสิทธิให้เพียงพอแค่สำหรับการปฏิบัติงานที่ได้รับมอบหมาย และมีการเฝ้าติดตามการทำงานของผู้ให้บริการอย่างสม่ำเสมอ รวมถึง ระงับการเข้าถึงของผู้ให้บริการทันทีเมื่อสิ้นสุดการให้บริการ

๒.๓ กำหนดมาตรการควบคุมข้อมูลทั้ง Physical และ Logical ไม่ให้ถูกนำออกนอกสถานที่โดยไม่ได้รับอนุญาต

๒.๔ ดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

๒.๕ มีการกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไข

๒.๖ มีขั้นตอนในการตรวจรับงานของผู้ให้บริการ ซึ่งรวมถึงขั้นตอนการตรวจสอบด้านความปลอดภัย

หมวด ๙
แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

ข้อ ๑ ผู้บังคับบัญชากองบังคับการปราบปราม ต้องจัดให้มีวิธีการกำหนดประเภทข้อมูลและจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ ซึ่งเบื้องต้นใช้แนวทางตาม พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และระเบียบที่เกี่ยวข้องในการกำหนดชั้นความลับของข้อมูล จึงกำหนดให้มีแนวทางปฏิบัติ ดังนี้

๑.๑ ผู้ใช้งานต้องแบ่งประเภทของข้อมูลและชั้นความลับของข้อมูลตามที่ศูนย์เทคโนโลยีสารสนเทศ ได้กำหนดชั้นความลับของข้อมูลอย่างน้อยเป็น ๔ ระดับ ดังนี้

- ชั้นความลับ (Top secret/Secret/Confidential)
- ใช้ภายในเท่านั้น (Internal use)
- ส่วนบุคคล (Personal)
- เปิดเผยได้ (Public)

๑.๒ ผู้ใช้งานต้องพิจารณาองค์ประกอบต่อไปนี้เพื่อเป็นแนวทางกำหนดชั้นความลับของข้อมูล

(๑) ความสำคัญของเนื้อหา คือ เนื้อหาของข้อมูลนั้นมีความสำคัญต่อความสำเร็จของงานตามภารกิจของกองบังคับการปราบปราม มากน้อยเพียงใด หากมีความสำคัญสูง ข้อมูลนั้นจะสามารถจัดอยู่ในชั้นความลับประเภทใช้ภายในเท่านั้น หรือลับ เป็นต้น

(๒) แหล่งที่มาของข้อมูล คือ หากข้อมูลนั้นมาจากภายนอกและเป็นข้อมูลลับ ชั้นความลับจะต้องคงไว้เช่นเดิม หรือหากข้อมูลนั้นมาจากอินเทอร์เน็ต ชั้นความลับจะเป็นประเภทเปิดเผยได้ เป็นต้น

(๓) วิธีการนำไปใช้ประโยชน์ คือ หากข้อมูลนั้นสามารถนำไปใช้ประโยชน์ในเชิงพาณิชย์ได้ หากถูกเปิดเผยจะส่งผลกระทบด้านการดำเนินคดีของกองบังคับการปราบปราม ดังนั้น ข้อมูลนี้จะอยู่ในประเภทชั้นความลับ เป็นต้น

(๔) จำนวนบุคคลที่ควรรับทราบ ได้แก่ หากข้อมูลนั้นสามารถเปิดเผยต่อผู้ใช้งานข้อมูลเป็นจำนวนมาก ชั้นความลับจะเป็นข้อมูลเปิดเผยได้ เป็นต้น

(๕) ผลกระทบหากมีการเปิดเผย คือ หากข้อมูลนั้นถูกเปิดเผย จะมีผลกระทบด้านชื่อเสียงและภาพลักษณ์ ด้านการดำเนินคดี ด้านการปฏิบัติตามกฎระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม หรือด้านการมีส่วนได้ส่วนเสียของผู้ที่เกี่ยวข้อง ดังนั้น ข้อมูลสามารถจัดอยู่ในชั้นความลับประเภทใช้ภายใน หรือลับ เป็นต้น

(๖) หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่อง คือ ข้อมูลสำคัญหรือข้อมูลลับที่มาจากเจ้าของเรื่องใดจะต้องคงชั้นความลับไว้เช่นเดิม การนำไปใช้งานควรขออนุญาตจากผู้ที่เป็นเจ้าของเรื่องก่อน เป็นต้น

(๗) สำหรับข้อมูลในชั้นความลับ “ลับ” ได้แก่ ลับ ลับมาก หรือลับที่สุด โดยเจ้าของข้อมูลต้องพิจารณาเกณฑ์ต่อไปนี้เพิ่มเติมเพื่อกำหนดชั้นความลับที่ถูกต้อง

- ลับที่สุด หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อประโยชน์แห่งรัฐหรือหน่วยงานอย่างร้ายแรงที่สุด
- ลับมาก หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อประโยชน์แห่งรัฐหรือหน่วยงานอย่างร้ายแรง
- ลับ หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อประโยชน์แห่งรัฐหรือหน่วยงาน

(๘) การดำเนินการกับข้อมูลลับ (ถ้ามี) เจ้าของข้อมูลลับต้องจัดทำทะเบียนข้อมูลลับที่ตนเองดูแลหรือรับผิดชอบ ซึ่งมีรายการดังนี้

- ชื่อของข้อมูล
- ระดับชั้นความลับและระดับชั้นการเข้าถึง
- ชื่อเจ้าของข้อมูลลับ
- หน่วยงานภายในที่สามารถเข้าถึงได้
- หน่วยงานภายนอกที่อนุญาตให้เข้าถึงได้
- สถานที่จัดเก็บข้อมูล
- ช่องทางการเข้าถึง คือ ติดต่อด้วยตนเอง หรือ ศูนย์ข้อมูลข่าวสาร โทรศัพท์หรือโทรสาร หรือ หนังสือหรือบันทึกข้อความ หรือ ระบบอินทราเน็ต หรือ ระบบอินเทอร์เน็ต หรือ ระบบจดหมายอิเล็กทรอนิกส์ หรือ เว็บไซต์
- ระยะเวลาการเก็บรักษาข้อมูล
- ระยะเวลาที่ได้เข้าถึง คือ เฉพาะในเวลาราชการ (๐๘.๓๐ – ๑๖.๐๐ น.) หรือ ตลอดเวลา

(๙) พิจารณาปรับชั้นความลับ (ปรับลด เพิ่ม หรือยกเลิกชั้นความลับ) ตามความจำเป็นปรับปรุงทะเบียนข้อมูลลับให้ถูกต้องและทันสมัย และต้องแจ้งให้หน่วยงานที่สามารถเข้าถึงข้อมูลหรือที่ได้รับการแจกจ่ายทราบด้วยทุกครั้ง เพื่อแก้ไขชั้นความลับให้ถูกต้อง

(๑๐) ในการจัดทำหรือจัดเตรียมข้อมูลลับให้ผู้ใช้งานปฏิบัติ ดังนี้

- จัดทำหรือจัดเตรียมข้อมูลในสถานที่ปลอดภัย ได้แก่ จัดทำภายในกองบังคับการปราบปราม ไม่จัดทำในสถานที่สาธารณะซึ่งบุคคลภายนอกสามารถเห็นข้อมูลที่จัดทำได้ และจำกัดบุคคลเฉพาะผู้ที่เกี่ยวข้องในการเข้าถึงข้อมูล
- ในการจัดทำข้อมูลลับซึ่งใช้กระดาษหรือวัสดุชั่วคราว ได้แก่ กระดาษร่าง กระดาษคาร์บอน ต้องทำลายกระดาษหรือวัสดุนั้นทันทีที่จัดทำเสร็จเรียบร้อย ถ้าเป็นการจัดทำโดยใช้เครื่องคอมพิวเตอร์ จะต้องลบหรือทำลายสื่อบันทึกข้อมูลจนไม่สามารถนำไปใช้ประโยชน์ได้ (ดูวิธีการทำลายในตารางแสดงแนวทางปฏิบัติในการทำลายข้อมูลบนสื่อบันทึกข้อมูลในข้อ (๑๖) ที่จะกล่าวต่อไป) หากไม่ทำลายต้องเก็บรักษาไว้ในสถานที่ที่ปลอดภัย
- จัดทำข้อมูลโดยแสดงเลขที่หน้าของจำนวนหน้าทั้งหมดไว้ในทุกหน้าของข้อมูลลับ และแสดงไว้ในส่วนที่สามารถเห็นได้ชัดเจน ได้แก่ มุมขวาด้านบนของเอกสาร (การบันทึกเลขหน้ามีจุดประสงค์ เพื่อให้ทราบว่าข้อมูลลับนั้นเป็นหน้าใดของจำนวนทั้งหมด หากมีการสูญหายไปหน้าใดหน้าหนึ่งจะได้ทราบและสามารถติดตามหาผู้ละเมิดและหาทางลดหรือแก้ไขความเสียหายที่เกิดขึ้นได้)

(๑๑) ในการแสดงชั้นความลับบนข้อมูลลับ ให้ปฏิบัติดังนี้

- แสดงชั้นความลับของข้อมูล ซึ่งประกอบด้วย “ลับ” “ลับมาก” หรือ “ลับที่สุด” ให้ปรากฏเห็นอย่างเด่นชัดทั้งข้อมูลที่มีสภาพเป็นกระดาษ ไฟล์อิเล็กทรอนิกส์ เทป External Hard Disk, Flash Drive แผ่น CD/DVD หรือข้อมูลลับที่อยู่ในรูปแบบอื่นๆ

- แสดงชั้นความลับบนเอกสารลับในทุกหน้าของเอกสารให้ปรากฏเห็นอย่างเด่นชัด

(๑๒) ในการทำสำเนาหรือแจกจ่ายข้อมูลลับให้ปฏิบัติ ดังนี้

- ทำสำเนาหรือแจกจ่ายข้อมูลลับให้แก่ผู้รับปลายทางซึ่งเป็นผู้ที่มีสิทธิในการเข้าถึงข้อมูลตามที่ระบุไว้ในทะเบียนข้อมูลลับ หรือสามารถแจกจ่ายให้ได้ตามความจำเป็นในการเข้าถึงข้อมูลนั้น
- แจ้งให้หน่วยงานภายนอกที่อนุญาตให้เข้าถึงข้อมูลลับนั้นได้ ว่าไม่อนุญาตให้ทำสำเนาเพิ่มเติม เว้นเสียแต่ได้รับอนุญาตจากผู้มีอำนาจลงนามอนุญาตก่อน

(๑๓) ในการเก็บรักษาเอกสารลับให้ปฏิบัติ ดังนี้

- จัดเก็บเอกสารลับไว้ในแฟ้มข้อมูลลับ และนำไปเก็บไว้ในตู้เก็บเอกสารลับโดยแยกเก็บเป็นแต่ละเรื่องหรือแต่ละหัวข้อ
- ไม่จัดเก็บเอกสารลับร่วมกับเอกสารที่อยู่ในชั้นความลับอื่นๆ ได้แก่ ข้อมูลใช้ภายในเท่านั้น ข้อมูลส่วนบุคคล หรือข้อมูลที่เปิดเผยได้
- จัดเก็บแฟ้มข้อมูลลับไว้ในตู้และปิดล็อคด้วยกุญแจที่แข็งแรงและมั่นคง

(๑๔) ในการยืมหรือขอเข้าถึงข้อมูลลับให้ปฏิบัติ ดังนี้

- เมื่อมีการขอยืมหรือขอเข้าถึงข้อมูลลับโดยผู้อื่นที่ไม่ได้เป็นผู้มีสิทธิในการเข้าถึงข้อมูลตามทะเบียนข้อมูลลับ ให้หัวหน้าของส่วนงานที่รับผิดชอบเป็นผู้พิจารณาตรวจสอบคุณสมบัติของผู้ยืมหรือขอเข้าถึงก่อนว่าเป็นผู้มีอำนาจหน้าที่ที่เกี่ยวข้องหรือไม่ หรือมีความจำเป็นในการเข้าถึงข้อมูลนั้นหรือไม่พร้อมทั้งต้องทำบันทึกหลักฐานการยืมหรือการขอเข้าถึงข้อมูลนั้นด้วย และแจ้งให้ผู้ยืมหรือขอเข้าถึงทราบว่าห้ามทำสำเนาเพิ่มเติม
- เมื่อหมดความจำเป็นในการใช้งานแล้ว หัวหน้าของส่วนงานที่รับผิดชอบกำหนดให้ผู้ขอยืมจัดส่งข้อมูลนั้นกลับคืน

มาโดยทันที สำหรับกรณีการเข้าถึงระบบสารสนเทศ ให้ยกเลิกบัญชีผู้ใช้งานที่ขอเข้าถึงข้อมูลลับโดยทันที

(๑๕) ในการส่งเอกสารลับทางจดหมายอิเล็กทรอนิกส์ (E-Mail) ให้ปฏิบัติตามระเบียบการส่งเอกสารลับของกองบังคับการปราบปราม เพื่อตรวจสอบที่อยู่ E-Mail ของผู้รับปลายทางให้ถูกต้อง ก่อนจัดส่งไฟล์ข้อมูลนั้นไปยังผู้รับเพื่อป้องกันการส่งผิดตัวบุคคล

(๑๖) ในการทำลายข้อมูลลับ ให้ปฏิบัติตามมาตรฐาน NIST๘๐๐-๘๘ เพื่อทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ

(๑๗) ในการจัดการกับไฟล์ข้อมูลลับให้ปฏิบัติ ดังนี้

- จัดหมวดหมู่ข้อมูลอิเล็กทรอนิกส์ (E-File) ที่เป็นความลับหรือที่มีระดับความสำคัญสูงไว้ต่างหาก และป้องกันให้มีความปลอดภัยอย่างพอเพียงต่อการเข้าถึงและควรแสดงชั้นความลับบนไฟล์ข้อมูลลับ โดยการทำสัญลักษณ์ลายน้ำและแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว
- การสำเนา E-File ที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูงต้องได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูล
- ระมัดระวังการเผยแพร่ หรือแจกจ่าย E-File ที่เป็นความลับของกองบังคับการปราบปรามไปยังกลุ่มผู้รับต้องเฉพาะกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น
- ผู้เป็นเจ้าของ E-File ต้องตรวจสอบความถูกต้องของ E-File ก่อนนำไปใช้งาน
- ห้ามผู้เป็นเจ้าของ E-File ที่เป็นความลับ หรือที่มีระดับความสำคัญสูง ส่งข้อมูลดังกล่าวไปทางไปรษณีย์ เว้นแต่จะได้ใช้วิธีเข้ารหัสที่กองบังคับการปราบปราม กำหนดไว้
- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยการใช้รหัสผ่านที่มีความมั่นคงปลอดภัย และไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์
- ห้ามแบ่งปัน (Share) ไฟล์ข้อมูลลับบนเครือข่ายสาธารณะ (Internet)

ของกองบังคับการปราบปรามเพื่ออนุญาตให้ผู้อื่นเข้าถึง

ได้ (ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการ Share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)

- ตรวจสอบการทำงานของระบบป้องกันไวรัสในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลลับอย่างสม่ำเสมอว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่
- ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมสำนักงานเพื่อแก้ไขช่องโหว่ของโปรแกรมในเครื่องตามปกติหรือไม่
- สำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น
- ต้องทำลาย E-File บนหน่วยความจำหลัก (Hard disk) ของเครื่องคอมพิวเตอร์ที่ถูกยกเลิกการใช้งาน

หมวด ๑๐
แนวปฏิบัติในการแบ่งแยกอำนาจหน้าที่

ข้อ ๑ กำหนดให้มีการแบ่งแยกหน้าที่ของเจ้าหน้าที่หรือภารกิจที่ต้องมีการตรวจสอบหรือสอบทานความถูกต้องแยกออกจากกัน ไม่มีผลประโยชน์ซ้อนทับกัน

ข้อ ๒ การแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (system administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง (production environment)

ข้อ ๓ การแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการตรวจพิสูจน์หลักฐาน (Digital Forensics) และบุคลากรที่ปฏิบัติหน้าที่ในส่วนการสอบทาน (Review) รายงานการตรวจพิสูจน์หลักฐานออกจากกัน

หมวด ๑๑
แนวปฏิบัติในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องมีการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ ดังนี้

๑.๑ มีขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่างๆ ที่สำคัญเป็นลายลักษณ์อักษรเพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (computer operator) เช่น ขั้นตอนในการเปิด-ปิดระบบ ขั้นตอนการประมวลผล ขั้นตอนการตรวจสอบประสิทธิภาพการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน เป็นต้น และปรับปรุงขั้นตอนหรือวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ

๑.๒ กำหนดให้เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ปฏิบัติงานโดยผ่านเมนู และควรจำกัดการปฏิบัติงานโดยใช้ command line เท่าที่จำเป็น

๑.๓ ควรกำหนดให้มีการบันทึก (log book) รายละเอียดเกี่ยวกับการปฏิบัติงานประจำในด้านต่างๆ โดยบันทึกดังกล่าวควรมีรายละเอียดในเรื่องต่อไปนี้

(๑) ผู้ปฏิบัติงาน

(๒) เวลาปฏิบัติงาน

(๓) รายละเอียดการปฏิบัติงาน

(๔) ปัญหาที่เกิดขึ้นและการแก้ไข

(๕) สถานะของระบบ

(๖) ผู้ตรวจทานการปฏิบัติงาน

ข้อ ๒ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องมีการติดตามการทำงานของระบบคอมพิวเตอร์ ดังนี้

๒.๑ มีการติดตามประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เช่น การใช้งานฮาร์ดดิสก์ การใช้งานหน่วยประมวลผล (CPU) เป็นต้น เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพ (capacity) ของระบบ

๒.๒ บำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์ต่างๆ ให้อยู่ในสภาพที่ดีและพร้อมใช้งานอยู่เสมอ

๒.๓ มีกระบวนการรับเรื่องขัดข้อง ปัญหาการใช้งาน อย่างเป็นระบบและมีกระบวนการติดตามการแก้ไขปัญหา รวมถึงสรุปผลการดำเนินการ

ข้อ ๓ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องมีการจัดการปัญหาต่างๆ ดังนี้

๓.๑ กำหนดรายชื่อ หน้าที่และความรับผิดชอบในการแก้ไขปัญหาอย่างชัดเจน เช่น กำหนดผู้รับผิดชอบในการแก้ไขปัญหาระบบ กำหนดผู้รับผิดชอบในการตอบสนองต่อเหตุการณ์ต่างๆ เป็นต้น รวมถึงเบอร์โทรศัพท์ของผู้ที่เกี่ยวข้องเพื่อใช้ติดต่อในกรณีที่มีปัญหา

๓.๒ มีระบบจัดเก็บบันทึกปัญหาและเหตุการณ์ผิดปกติที่เกิดขึ้น และรายงานให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ เพื่อประโยชน์ในการรวบรวมปัญหาและตรวจสอบถึงสาเหตุที่เกิดขึ้น รวมทั้งเพื่อศึกษาแนวทางแก้ไขและป้องกันปัญหาต่อไป

ข้อ ๔ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องมีการควบคุมการจัดทำรายงานดังนี้

๔.๑ การขอให้จัดพิมพ์รายงานต่างๆ ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่

๔.๒ มีทะเบียนคุมการพิมพ์และการจัดส่งรายงาน จัดเก็บรายงานต่าง ๆ ที่ได้จัดพิมพ์แล้วอย่างรัดกุม และกำหนดให้มีการลงลายมือชื่อเมื่อมีการรับรายงาน นอกจากนี้ควรทำลายรายงานที่ไม่ได้ใช้งานแล้ว

หมวด ๑๒
แนวปฏิบัติในการเผยแพร่ข้อมูลต่อสาธารณะ

ข้อ ๑ การเผยแพร่ข้อมูลในความรับผิดชอบของกองบังคับการปราบปราม ต่อสาธารณะโดยผ่านระบบสารสนเทศของกองบังคับการปราบปราม หน่วยงานเจ้าของข้อมูลจะต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำออกเผยแพร่ และหากข้อมูลที่นำออกเผยแพร่เกี่ยวข้องกับเรื่องนโยบายจะต้องได้รับความเห็นชอบจากคณะกรรมการของกองบังคับการปราบปราม ซึ่ง คณะกรรมการฯ มอบหมายก่อนนำออกเผยแพร่ ในกรณีที่ข้อมูลที่นำออกเผยแพร่มีความผิดพลาด และมีความเสียหายเกิดขึ้น โดยความเสียหายนั้นเกิดจากความจงใจหรือประมาทเลินเล่ออย่างร้ายแรง ให้เป็นความรับผิดชอบของเจ้าหน้าที่ผู้นำข้อมูลดังกล่าวออกเผยแพร่

ข้อ ๒ การเผยแพร่ข้อมูลต่อสาธารณะโดยผ่านระบบสารสนเทศของกองบังคับการปราบปราม ให้ดำเนินการโดยหน่วยงานเจ้าของข้อมูล เว้นแต่กรณีที่คณะกรรมการของกองบังคับการปราบปรามหรือผู้ซึ่ง คณะกรรมการฯ มอบหมาย ได้สั่งการ หรือเห็นชอบไว้เป็นอย่างอื่น

หมวด ๑๓
แนวปฏิบัติในการพัฒนาและบำรุงรักษาระบบ

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องมีการพัฒนาและบำรุงรักษาฮาร์ดแวร์ ดังนี้

๑.๑ มีหน่วยงานที่ดูแลเรื่องการซ่อมบำรุงภายในและสามารถดูแลประสานงานให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

๑.๒ ใช้บริการจากภายนอกโดยกำหนดค่าดูแลฮาร์ดแวร์จากผู้จำหน่าย ให้ได้มาตรฐานตามกำหนดขององค์กร

๑.๓ มีการใช้บริการแบบผสมผสานระหว่างการบริการภายในองค์กรและการบริการภายนอกองค์กร โดยใช้มาตรฐานการบำรุงรักษาเดียวกัน

๑.๔ เอกสารในการตรวจสอบสภาพการใช้งานของอุปกรณ์

๑.๕ การตรวจเช็คอุปกรณ์อย่างน้อย ๓ เดือน เพื่อตรวจสอบประสิทธิภาพการทำงานของอุปกรณ์

๑.๖ การดูแลรักษาในเรื่องของที่ตั้งอุปกรณ์ การจัดเก็บ มีการจัดพื้นที่ในการจัดเก็บอุปกรณ์อย่างมีระบบเพื่อป้องกันการสูญหายของอุปกรณ์

ข้อ ๒ ผู้รับผิดชอบระบบสารสนเทศของกองบังคับการปราบปราม ต้องมีการพัฒนาและบำรุงรักษาซอฟต์แวร์ ดังนี้

๑.๑ การกำหนดหน้าที่ความรับผิดชอบของบุคลากรให้มีหน้าที่ดูแลการ บำรุงรักษา

๑.๒ การดูแลการจัดทำสัญญาเรื่องการบำรุงรักษาระบบและประสานงาน

๑.๓ การกำหนดค่าใช้จ่าย การให้บริการบำรุงรักษาต่อหน่วยงาน ในสังกัดอื่นอย่างชัดเจน เพื่อผลของการประเมิน

๑.๔ มีเอกสารในการตรวจสอบสภาพการใช้งานของซอฟต์แวร์ทั้งหมด

๑.๕ การตรวจเช็คซอฟต์แวร์ในเรื่องของการใช้งาน อย่างน้อย ๓ เดือน เพื่อตรวจสอบประสิทธิภาพการทำงานของซอฟต์แวร์