นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดแนวทางและวิธีปฏิบัติในการป้องกันรักษาความมั่นคงปลอดภัยข้อมูลและระบบเทคโนโลยีสารสนเทศของกรมสอบสวนคดีพิเศษ

๑.๒ เพื่อให้มีระบบสารสนเทศใช้งานได้อย่างต่อเนื่อง และพร้อมใช้งานอยู่เสมอ โดยการจัดให้มีการสำรองข้อมูลสารสนเทศ อย่างสม่ำเสมอ

๑.๓ เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ โดยนำผลการประเมินความเสี่ยงไปดำเนินการปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๔ เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ ความเข้าใจและการอบรมทางด้านการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศของกรมสอบสวนคดีพิเศษ

๒. แนวทางปฏิบัติว่าด้วยการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ แบ่งออกเป็น ๔ หมวด คือ

หมวด ๑ นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย

๑) การกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒) การจัดการด้านบุคลากร

๓) การจัดการทรัพย์สิน หรือ สินทรัพย์เทคโนโลยีสารสนเทศ

๔) การจัดการพื้นที่ และการรักษาความปลอดภัยของระบบสารสนเทศกับหน่วยงานภายนอกหรือบุคคลภายนอก

๕) การจัดการและการควบคุมการเข้าถึงระบบเครือข่าย ระบบสารสนเทศและอุปกรณ์สารสนเทศของกรมสอบสวนคดีพิเศษ

๖) การจัดการและการควบคุมการเข้าถึงระบบปฏิบัติการ และโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ ของกรมสอบสวนคดีพิเศษ

๗) การจัดการระบบสารสนเทศกรณีพบเหตุละเมิดความมั่นคงปลอดภัย หรือสงสัยว่าจะเกิดเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ รวมถึงการป้องกันการละเมิดจากผู้ไม่พึงประสงค์ทั้งภายในและภายนอกองค์กร

๘) มาตรการสำหรับการพัฒนาซอฟต์แวร์

๙) การใช้งานระบบฐานข้อมูล/สารสนเทศของกรมสอบสวนคดีพิเศษ

หมวด ๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศระดับเจ้าหน้าที่ทั่วไป (เจ้าหน้าที่ของกรมสอบสวนคดีพิเศษ/ผู้ใช้งาน)

๑) การปฏิบัติหน้าที่ทั่วไป

๒) แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย

๓) แนวปฏิบัติการควบคุมเข้าถึงระบบปฏิบัติการ

๔) แนวปฏิบัติในการใช้งานบัญชีผู้ใช้บริการ (Account) / (Username)

๕) แนวปฏิบัติการกำหนดรหัสผ่าน (Password) การเปลี่ยนรหัสผ่าน และการใช้งานรหัสผ่าน

๖) แนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย (Malware)

๗) แนวปฏิบัติการใช้งานระบบอินเทอร์เน็ต (Internet)

๘) แนวปฏิบัติการใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

๙) แนวทางปฏิบัติการจัดการเหตุละเมิดการรักษาความมั่นคงปลอดภัย

๑๐) แนวทางปฏิบัติในการเคลื่อนย้ายและการทำสำเนาสารสนเทศ

๑๑) แนวทางปฏิบัติในการทำลายสื่อบันทึกข้อมูลหรือการทำลายไฟล์ข้อมูลที่มีระดับลับขึ้นไป

หมวด ๓ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศระดับเจ้าหน้าที่ผู้ดูแลระบบ

๑) แนวการปฏิบัติหน้าที่โดยทั่วไป ของผู้ดูแลระบบ (System Administrator)

๒) การกำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

๓) แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ

๔) แนวทางปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๕) แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๖) แนวทางการปฏิบัติเมื่อเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย (กรณีการเข้าถึงระบบโดยไม่ได้รับอนุญาต)

๗) แนวทางการปฏิบัติภายหลังการเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย

๘) แนวทางการปฏิบัติการสำรองข้อมูล

๙) การสำรองและกู้คืนข้อมูล

๑๐) แผนรักษาความปลอดภัยกรณีการเข้าถึงระบบโดยไม่มีสิทธิ

๑๑) แผนรักษาความปลอดภัยกรณีเกิดเพลิงไหม้

๑๒) แผนรักษาความปลอดภัยกรณีไฟฟ้าดับ

หมวด ๔ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบุคคลภายนอก

<u>คำนิยาม</u>

๑) **หน่วยงาน** หมายความว่า กรมสอบสวนคดีพิเศษ

๒) **ระบบคอมพิวเตอร์** หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางการปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๓) **ระบบเครือข่าย** หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานได้ เช่น ระบบเครือข่ายภายใน(LAN) ระบบอินทราเน็ต(Intranet) ระบบอินเทอร์เน็ต(Internet) เป็นต้น

๔) **ความมั่นคงปลอดภัย** หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๕) **ระบบเครือข่ายภายใน (Local Area Network-LAN) และ ระบบอินทราเน็ต (Intranet)** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลสื่อสารสนเทศภายในหน่วยงาน

๖) **ระบบอินเทอร์เน็ต (Internet)** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

๗) **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบเช่น ระบบคอมพิวเตอร์ ระบบเครือข่ายโปรแกรม ข้อมูลสารสนเทศ เป็นต้น

๘) **เครื่องคอมพิวเตอร์** หมายความว่า เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา

๙) **ข้อมูลคอมพิวเตอร์** หมายความว่าข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจจะประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๐) **สารสนเทศ (Information)** หมายความว่า ข้อเท็จจริงที่ได้จากการนำเข้าข้อมูลผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

๑๑) **ผู้บริหารระดับสูง** หมายความถึง อธิบดีกรมสอบสวนคดีพิเศษ, รองอธิบดีกรมสอบสวนคดีพิเศษ

๑๒) **ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)** หมายความถึง ผู้บริหารระดับสูงที่ได้รับการแต่งตั้งให้เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ CIO ของกรมสอบสวนคดีพิเศษ

๑๓) **ผู้บังคับบัญชา** หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมสอบสวนคดีพิเศษ

๑๔) **ผู้ใช้บริการ หรือ ผู้ใช้งาน** หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างตามสัญญาจ้างในสังกัดหน่วยงาน และให้ความหมายรวมถึงบุคคลในหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

๑๕) **ผู้ดูแลระบบ (System Administrator)** หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

๑๖) **หน่วยงานภายนอก** หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๑๗) **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร** หมายความว่า พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

(๑) พื้นที่ทำงาน หมายความว่า พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน รวมถึงพื้นที่ทำงานของผู้ดูแลระบบ (System Administrator)

(๒) พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย หมายความว่า พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย และให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์

(๓) พื้นที่ใช้งานระบบเครือข่ายไร้สาย หมายความว่า พื้นที่ในการให้บริการระบบเครือข่ายไร้สาย

๑๘) **สิทธิของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๑๙) **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๒๐) **ความมั่นคงปลอดภัยด้านสารสนเทศ (Information security)** หมายความว่า การธำรงไว้ซึ่งความลับ(confidentiality) ความถูกต้องครบถ้วน(integrity) และสภาพพร้อมใช้งาน(availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง(authenticity) ความรับผิด(accountability) การห้ามปฏิเสธความรับผิด(non-repudiation) และความน่าเชื่อถือ(reliability)

๒๑) **เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event)** หมายความว่ากรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าเกี่ยวข้องกับความมั่นคงปลอดภัย

๒๒) **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security incident)** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยคุกคาม

๒๓) **ทรัพย์สิน หรือ สินทรัพย์(Asset)** หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร ได้แก่ ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารหน่วยงาน เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

๒๔) **จดหมายอิเล็กทรอนิกส์ (Electronic mail : e-mail)** หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะ

เป็นได้ทั้งตัวอักษร ภาพถ่าย กราฟฟิก ภาพเคลื่อนไหว และเสียง ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น

๒๕) **รหัสผ่าน (Password)** หมายความว่า ตัวอักษรหรืออักขระตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๒๖) **บัญชีผู้ใช้บริการ (Account)** หมายความว่า รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของหน่วยงาน

๒๗) **โปรแกรมประสงค์ร้าย (Malware)** หมายความว่า โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาเพื่อวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่ายเช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spy ware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือ ฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

๒๘) **ชื่อเครื่องคอมพิวเตอร์ (Computer Name)** หมายความว่า ชื่อที่กำหนดให้เฉพาะกับเครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

๒๙) **สื่อบันทึกพกพา** หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้งานการบันทึกหรือจัดเก็บข้อมูลได้แก่ Flash Drive หรือ Handy Drive หรือ Thump Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น

๓๐) **ปุ่มกดง่าย (Shortcut)** หมายความว่า เครื่องมือที่ช่วยในการเรียกใช้โปรแกรมได้อย่างรวดเร็วและสามารถเข้าถึงโปรแกรมหรือแฟ้มข้อมูลที่ต้องการได้ทันที ซึ่งผู้ใช้สามารถลบ หรือสร้างใหม่ได้

๓๑) **ไบออส (BIOS)** หมายความว่า ซอฟแวร์ขนาดเล็กซึ่งเก็บข้อมูลอยู่ในหน่วยความจำแบบเมนบอร์ดของเครื่องคอมพิวเตอร์ ทำหน้าที่ควบคุมขั้นตอนการบูตและการทำงานของอุปกรณ์พื้นฐานต่างๆ ที่ติดตั้งอยู่บนเมนบอร์ด

๓๒) **การตั้งค่าระบบ (Configuration)** หมายความว่า ค่าที่ใช่กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์หรือซอฟต์แวร์

๓๓) **เลขที่อยู่ไอพี (IP Address)** หมายถึงตัวเลขประจำเครื่องที่ต่ออยู่ในระบบเครือข่ายซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วน(IPv๔) หรือ ๖ ส่วน(IPv๖) แต่ละกลุ่มตัวเลขคั่นด้วยเครื่องหมายจุด (.) หรือเครื่องหมายทวิภาค(: หรือ semi-colon)

๓๔) **เลขที่อยู่ไอพีสาธารณะ (Public IP Address)** หมายความว่าเลขที่อยู่ไอพีมีไว้สำหรับให้แต่ละหน่วยงาน หรือบุคคลสามารถเชื่อมต่อเข้าหากัน หรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

๓๕) **แบนด์วิดท์ (Bandwidth)** หมายความว่า ปริมาณที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถโอนถ่ายได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

๓๖) **ชื่อผู้ใช้ (Username)** หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

๓๗) **ลงบันทึกเข้า (Login)** หมายความว่า กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้น ตามเงื่อนไขที่ตั้งไว้เพื่อการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

๓๘) **ลงบันทึกออก (Logout)** หมายความว่า กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

๓๙) **อัพเดท (Update)** หมายความว่า ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

๔๐) **ช่องโหว่ (Vulnerability)** หมายความว่า ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔๑) **ไฟล์ที่สามารถประมวลผลได้ (Executable file)** หมายความว่า โปรแกรมที่สามารถเรียกใช้งานได้ทันที เช่น .inf .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe ในขณะที่ไฟล์ข้อมูลอื่นๆจะเป็นไฟล์ข้อมูลประกอบ

๔๒) **การเข้ารหัส (Encryption)** หมายความว่า การนำข้อมูลเข้ารหัสเพื่อป้องกันการลักลอบ เข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๔๓) **อุปกรณ์กระจายสัญญาณ (Access Point)** หมายความว่า อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

๔๔) **SSID (Service Set Identifier)** หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID เดียวกัน

๔๕) **โดยปริยาย (Default)** หมายความว่า ค่าที่เครื่องคอมพิวเตอร์หรือโปรแกรมได้กำหนดไว้ล่วงหน้า และนำไปใช้ได้โดยปริยายหากไม่มีการเปลี่ยนแปลงจากผู้ใช้บริการ

๔๖) **WEP (Wire Equivalent Privacy)** หมายความว่า ระบบการเข้ารหัสเพื่อความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้ด้วย

๔๗) **WPA (Wi-Fi Protected Access)** หมายความว่า ระบบการเข้ารหัสเพื่อความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wire Equivalent Privacy) ส่วน WPA๒ เป็นการพัฒนาการเข้ารหัสแบบ WPA ที่ถูกพัฒนาเพิ่มเติมด้านการเข้ารหัสในระบบสื่อสารไร้สายโดยผู้ใช้เลือกอัลกอริธึม(Algorithm) ในการเข้ารหัส คือ TKIP(Temporal Key Integrity Protocol) หรือ CCMP(Counter mode with Cipher Block Chaining-Message Authentication Code)

๔๘) **Wireless LAN Client** หมายความว่า เครื่องคอมพิวเตอร์ลูกข่ายที่ต่ออยู่ในระบบแลน โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ โดยเครื่องคอมพิวเตอร์แต่ล่ะเครื่องจะต้องมีทั้งตัวรับและส่งสัญญาณ ซึ่งมีมาตรฐานที่นิยมใช้เรียกว่า IEEE ๘๐๒.๑๑

๔๙) **MAC Address (Media Access Control Address)** หมายความว่า หมายเลขเฉพาะเครื่องที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับเครือข่าย และกำหนดมาพร้อมกับอีเธอร์เน็ตการ์ด(Ethernet Card หรือ LAN Card) ซึ่งแต่ล่ะการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

๕๐) **ไฟร์วอลล์ (Firewall)** หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ได้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

๕๑) **VPN (Virtual Private Network)** หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปถึงปลายทาง

๕๒) **Web Server** หมายความว่า เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บ และมีหน้าที่ให้บริการเว็บเพจต่างๆ

๕๓) **ชื่อโดเมนย่อย (Sub Domain Name)** หมายความว่า ส่วนย่อยที่จะทำหน้าที่ช่วยขยายให้ทราบถึงกลุ่มต่างๆภายในโดเมนนั้น ซึ่งเป็นชื่อที่ระบุให้กับผู้ใช้เพื่อเข้ามายังเว็บไซต์ของตน หรืออาจจะใช้ที่อยู่เว็บไซต์แทนก็ได้

๕๔) **อุปกรณ์จัดหาเส้นทาง (Router)** หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดหาเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลไปยังระบบเครือข่ายอื่น

๕๕) **การพิสูจน์ยืนยันตัวตน (Authentication)** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการในระบบ ทั่วไปแล้วเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

๕๖) **แผนผังระบบเครือข่าย (Network Diagram)** หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

๕๗) **Command Line** หมายความว่า บรรทัดที่ให้ผู้ใช้งานป้อนคำสั่งแบบข้อความ เพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานตามต้องการ

๕๘) **Firewall Log** หมายความว่า การบันทึกสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่าไฟร์วอลล์ (Firewall) จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ซึ่งสามารถนำมาใช้ในการวิเคราะห์ เพื่อตรวจสอบประเภทของการสื่อสาร ปริมาณการสื่อสาร นอกจากนั้นแล้วยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในหน่วยงาน

๕๙) **DOD ๕๒๒๐.๒๒-M** หมายความว่า การลบข้อมูลอย่างสมบูรณ์ซึ่งได้รับการยอมรับและใช้งานกับกระทรวงกลาโหม ประเทศสหรัฐอเมริกา โดยทำให้ไม่สามารถกู้ไฟล์กลับคืนมาได้ ซึ่งการลบข้อมูล ๓ รอบรอบแรกด้วยข้อมูลแบบสุ่ม รอบที่สองด้วยบิตที่ตรงกันข้าม รอบสุดท้ายด้วยข้อมูลแบบไบต์สุ่ม

๖๐) **ผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor)** หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่ตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ (Log) และรับผิดชอบให้สามารถเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ (Log)

๖๑) **เวลาอ้างอิงสากล (Stratum o)** หมายความว่า การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากล ในประเทศไทยนั้นเราอ้างอิงกับหน่วยงานมาตรฐาน (เช่น กรมอุทกศาสตร์ กองทัพเรือ, ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ เป็นต้น) เพื่อให้สอดคล้องกับพระราชบัญญัติว่าการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

๖๒) **ข้อมูลจราจรทางคอมพิวเตอร์ (Log)** หมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการอื่นๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

หมวดที่ ๑
นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมสอบสวนคดีพิเศษ ปี พ.ศ. ๒๕๕๕

๑. การกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๑ อธิบดีกรมสอบสวนคดีพิเศษ เป็นผู้พิจารณา อนุมัติและลงนาม นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เป็นผู้เสนอร่างนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ควบคุม กำกับ ดูแลการปฏิบัติ ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยเสนอให้อธิบดีกรมสอบสวนคดีพิเศษเป็นผู้พิจารณานโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ก่อนลงนามอนุมัติ

๑.๓ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง(CIO) มีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กร อันเกิดขึ้นจากผู้หนึ่งผู้ใดที่กระทำการบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ จะต้องตรวจสอบ วิเคราะห์ แก้ไข และเสนอแนะแนวทางปรับแก้ไขแนวนโยบายและวิธีปฏิบัติให้เหมาะสม (ความรับผิดชอบของผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ตามภาคผนวก ๑)

๑.๔ ศูนย์สารสนเทศ มีหน้าที่

๑.๔.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสารเทศอย่างน้อยปีละ ๑ ครั้ง ร่วมกับกลุ่มงานตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของกรมสอบสวนคดีพิเศษ

๑.๔.๒ จัดทำร่างแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเสนอผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เห็นชอบ/ลงนาม เสนอต่ออธิบดีกรมสอบสวนคดีพิเศษเพื่อลงนามและประกาศนโยบายและแนวปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบเพื่อให้สามารถเข้าถึงเข้าใจ และปฏิบัติงานตามนโยบายและแนวปฏิบัติฯ

๑.๔.๓ ทบทวนปรับปรุงนโยบายและแนวปฏิบัติฯ ทุก ๑ ปี ให้เป็นปัจจุบันอยู่เสมอ กรณีมีการเปลี่ยนแปลงหรือปรับปรุงนโยบายและข้อปฏิบัติฯ ต้องเสนอนโยบายฯ ที่มีการเปลี่ยนแปลงให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ลงนามหรือให้ความเห็นชอบ และเสนอต่ออธิบดีกรมสอบสวนคดีพิเศษเพื่อลงนาม และดำเนินการประกาศหรือแจ้งการเปลี่ยนแปลงนโยบายฯ ให้ผู้เกี่ยวข้องทั้งหมดทราบ

๑.๔.๔ ติดตามประเมินผล การปฏิบัติตามแนวทางในการรักษาความมั่งคงปลอดภัยด้านสารสนเทศ ของกรมสอบสวนคดีพิเศษ

๑.๔.๕ ทบทวนและจัดทำแผนการรักษาความมั่งคงปลอดภัยด้านสารสนเทศ และจัดหาระบบสารสนเทศสำรอง รวมทั้งอุปกรณ์ที่เกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศ ของกรมสอบสวนคดีพิเศษ ดังนี้

๑) พิจารณาคัดเลือกและจัดทำระบบสารสนเทศระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน

๒) จัดหาอุปกรณ์ที่เกี่ยวกับการรักษาความปลอดภัยของระบบสารสนเทศ

๓) กำหนดหน้าที่ความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง

๔) จัดทำแผนต่างๆ ทดสอบสภาพพร้อมใช้งานระบบสารสนเทศ ระบบสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปรกติต่อเนื่องและเหมาะสม สอดคล้องกับการใช้งานตามภารกิจ เช่น แผนรักษาความปลอดภัยกรณีการเข้าถึงระบบโดยไม่มีสิทธิ, แผนการรักษาความปลอดภัยกรณีเกิดเพลิงไหม้, แผนทดสอบความมั่นคงปลอดภัยกรณีเพลิงไหม้ เป็นต้น

๕) ฝึกซ้อมตามแผนต่าง ๆ ที่ได้กำหนดและทดสอบสภาพพร้อมใช้งานระบบสารสนเทศระบบสำรอง ไว้อย่างน้อยปีละ ๑ ครั้ง

๑.๔.๖ ให้ความรู้แก่ผู้ใช้งานสารสนเทศของกรมสอบสวนคดีพิเศษ ในการรักษาความปลอดภัยด้านสารสนเทศ การใช้ระบบสารสนเทศของหน่วยราชการ

๒. การจัดการด้านบุคลากร

๒.๑ กลุ่มบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม ปฏิบัติดังนี้

๒.๑.๑ ชี้แจงนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงทัณฑ์ทางวินัยและโทษตามกฎหมายในการเปิดเผยความลับของทางราชการแก่บุคคลผู้ไม่มีหน้าที่เกี่ยวข้อง และการไม่ปฏิบัติตามนโยบายและแนวทางในการรักษาความมั่นคงปลอดภัยสารสนเทศ ให้แก่ ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ และลูกจ้าง ทราบ

๒.๑.๒ เมื่อบุคคลใดตามข้อ ๒.๑.๑ จะเข้าปฏิบัติหน้าที่หรือพ้นหน้าที่เกี่ยวกับระบบสารสนเทศ ให้ลงชื่อในใบบันทึกรับรองการรักษาความลับเมื่อเข้ารับตำแหน่ง หรือใบรับรองการรักษาความลับเมื่อพ้นตำแหน่งแล้วแต่กรณี ตามที่กำหนดไว้ในระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗

๒.๑.๓ กรณีที่มีการเปลี่ยนแปลงสถานะของบุคลากร เช่น การรับพนักงานเข้าใหม่ การย้ายแผนก การเลื่อนตำแหน่ง เมื่อมีการอนุมัติให้แจ้งศูนย์สารสนเทศซึ่งเป็นผู้ดูแลและควบคุมการใช้งานระบบทราบ เพื่อให้ศูนย์สารสนเทศแจ้งให้เจ้าหน้าที่ดูแลระบบฯ สร้าง ระงับหรือเปลี่ยนแปลงบัญชีผู้ใช้ และสิทธิ์การใช้งานระบบสารสนเทศตามความเหมาะสม

๒.๑.๔ กรณีเกิดสถานการณ์การจัดการด้านบุคคลที่ต้องดำเนินการอย่างทันที ได้แก่ การไล่ออก การปลดออก หรือการพ้นจากตำแหน่ง ให้แจ้งศูนย์สารสนเทศทราบ เพื่อศูนย์สารสนเทศจะได้แจ้งให้เจ้าหน้าที่ผู้ดูแลระบบดำเนินการเปลี่ยนแปลงสิทธิ์การใช้งานระบบสารสนเทศโดยทันที จากนั้นให้เพิกถอนบัตรเข้า-ออกพื้นที่ทำการกรมสอบสวนคดีพิเศษ และแจ้งหน่วยงานที่เกี่ยวข้อง เช่น เจ้าหน้าที่ของฝ่ายอาคารสถานที่ทราบเพื่อห้ามมิให้บุคคลดังกล่าวเข้าพื้นที่ ที่ทำการกรมสอบสวนคดีพิเศษโดยไม่มีความจำเป็น เป็นต้น

๒.๑.๕ นับการเข้าร่วมและประเมินผลการฝึกอบรม การฝึกซ้อมแผนรับมือที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศตามระยะเวลาที่กำหนด เป็นส่วนหนึ่งของการประเมินบุคลากร

๒.๒ กองพัฒนาและสนับสนุนคดีพิเศษ ปฏิบัติดังนี้

๒.๒.๑ กำหนดหลักสูตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และ หลักสูตรการใช้ระบบสารสนเทศสำหรับการปฏิบัติราชการ ให้แก่ บุคลากรของกรมสอบสวนคดีพิเศษเป็นหลักสูตรภาคบังคับ

๒.๒.๒ กรณีที่มีการเปลี่ยนแปลงสถานะของพนักงาน เช่น การรับพนักงานเข้าใหม่ การย้ายแผนก การเลื่อนตำแหน่ง ให้สำนักพัฒนาและสนับสนุนคดีพิเศษพิจารณาประวัติการฝึกอบรมของบุคลากร ในเรื่องความต้องการการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อจัดฝึกอบรมเพิ่มเติมตามความเหมาะสม

๒.๒.๓ ประเมินผลการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและการใช้งานระบบสารสนเทศของกรมสอบสวนคดีพิเศษ

๒.๓ กองปฏิบัติการพิเศษ ปฏิบัติดังนี้

๒.๓.๑ กำหนดหลักสูตรภาคปฏิบัติการในรักษาความมั่นคงปลอดภัย โดยให้รวมถึง การดูแลรักษาความมั่นคงปลอดภัยรักษากับศูนย์สารสนเทศ และขั้นตอนการปฏิบัติในสถานะฉุกเฉินหรือภาวะวิกฤต ให้แก่บุคลากรของกรมสอบสวนคดีพิเศษเป็นหลักสูตรภาคบังคับ

๒.๓.๒ กรณีที่มีการเปลี่ยนแปลงสถานะของพนักงาน เช่น การรับพนักงานเข้าใหม่ การย้ายแผนก การเลื่อนตำแหน่ง ให้สำนักปฏิบัติการพิเศษพิจารณาประวัติการฝึกอบรมของบุคลากร ในเรื่องความต้องการการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อจัดฝึกอบรมเพิ่มเติม ตามความเหมาะสม

๒.๓.๓ ประเมินผลการฝึกภาคปฏิบัติการในรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกรมสอบสวนคดีพิเศษ

๓. การจัดการทรัพย์สิน หรือ สินทรัพย์เทคโนโลยีสารสนเทศ ให้ศูนย์สารสนเทศดำเนินการ ดังนี้

๓.๑ ดูแลทรัพย์สินสารสนเทศ จัดทำรายการบัญชีทรัพย์สินทั้งฮาร์ดแวร์และซอฟต์แวร์ และกำหนดผู้ที่รับผิดชอบทรัพย์สินเทคโนโลยีสารสนเทศ ตลอดจนวิธีการใช้งานทรัพย์สินเทคโนโลยีสารสนเทศต่างๆ รวมทั้งการจัดการกับสื่อบันทึกข้อมูลและวัสดุสิ้นเปลือง

๓.๒ บันทึกและปรับปรุงการกำหนดค่าระบบ (Configuration parameters) ของทรัพย์สินสารสนเทศทุกรายการ และเมื่อมีการติดตั้งอุปกรณ์หรือซอฟต์แวร์ใหม่ทุกครั้ง ให้พิจารณาความสอดคล้องในการแก้ไขการตั้งค่าด้วยทุกครั้ง เมื่อต้องการเปลี่ยนแปลงแก้ไขต้องทำการบันทึกและแจ้งผู้ใช้งานให้ปรับปรุงตามทุกครั้ง

๓.๓ รับผิดชอบ การจัดหมวดหมู่ การตรวจสอบ และเก็บสถิติการใช้วัสดุที่เกี่ยวข้องกับงานสารสนเทศ รวมทั้งเนื้อที่บันทึกข้อมูลในหน่วยความจำสำรองของระบบสารสนเทศ และทำรายงานแผนการใช้วัสดุสารสนเทศ และแจ้งเตือนหน่วยงานที่เกี่ยวข้องให้จัดหาทรัพยากรเพิ่มเติมเมื่อจำนวนทรัพยากรใกล้ถึงจุดวิกฤติ

๔. การจัดการพื้นที่ และการรักษาความปลอดภัยของระบบสารสนเทศกับหน่วยงานภายนอกหรือบุคคลภายนอก

๔.๑ กำหนดให้ศูนย์สารสนเทศ เป็นบริเวณที่ต้องรักษาความปลอดภัย

๔.๒ ให้หน่วยงานที่รับผิดชอบในการติดต่อนำบุคคลภายนอกเข้ามา รวมถึง ฝ่ายอาคารสถานที่ สำนักงานเลขานุการกรม จะต้องจัดทำบัญชีการเข้า-ออก สถานที่ทำการกรมสอบสวนคดีพิเศษ กรณีมีบุคคลภายนอกเข้า-ออก พื้นที่ทำการกรมสอบสวนคดีพิเศษไม่ว่าจะเป็นประจำหรือชั่วคราว เช่น พนักงานรักษาความสะอาด พนักงานส่งเอกสาร พนักงานซ่อมบำรุง โดยต้องระบุ วัน เวลา ที่เข้า-ออก, ชื่อ-นามสกุล, เลขบัตรประจำตัวประชาชน, เบอร์โทรที่สามารถติดต่อได้, สถานที่หรือหน่วยงานที่ติดต่อ, ผู้ที่ต้องการติดต่อ และวัตถุประสงค์ของการเข้าพื้นที่ทำการกรมสอบสวนคดีพิเศษ เป็นอย่างน้อย

๔.๓ ให้ศูนย์สารสนเทศ จัดทำบัญชีการเข้า-ออก สถานที่ทำการกรมสอบสวนคดีพิเศษ กรณีมีบุคคลภายในหรือภายนอกเข้า-ออก พื้นที่ศูนย์สารสนเทศรวมถึงห้องแม่ข่าย (Server Room) โดยต้องระบุ วัน เวลา ที่เข้า-ออก, ชื่อ-นามสกุล, เลขบัตรประจำตัวประชาชน, เบอร์โทรที่สามารถติดต่อได้, สถานที่หรือหน่วยงานที่ติดต่อ, ผู้ที่ต้องการติดต่อ และวัตถุประสงค์ของการเข้าพื้นที่ทำการกรมสอบสวนคดีพิเศษ รวมถึงติดตั้งกล้องวงจรปิดในพื้นที่รักษาความปลอดภัยของศูนย์สารสนเทศ โดยสามารถให้ผู้บังคับบัญชาสามารถควบคุมได้จากภายนอกพื้นที่ทำการ

๔.๔ กรณีเกิดเหตุละเมิดความมั่นคงปลอดภัยโดยบุคคลภายนอก หน่วยงานที่รับผิดชอบในการติดต่อนำบุคคลภายนอกเข้ามาต้องทำรายงานเหตุดังกล่าวและสอบสวนว่า ได้ดำเนินการตามข้อ ๔.๒ หรือ ๔.๓ หรือไม่ กรณีที่ไม่ได้ดำเนินการจะต้องถูกสอบสวนทางวินัยฐานละเมิดวินัยและระเบียบราชการ หย่อนยานหรือเพิกเฉย แล้วแต่กรณี

๕. การจัดการและการควบคุมการเข้าถึงระบบเครือข่าย ระบบสารสนเทศและอุปกรณ์สารสนเทศของกรมสอบสวนคดีพิเศษ ศูนย์สารสนเทศต้องดำเนินการ ดังนี้

๕.๑ กำหนดสิทธิ์และควบคุมการเข้าถึงระบบเครือข่าย ระบบสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูลให้แก่ผู้ใช้งาน ตลอดจนการเข้ารหัสและการจัดการกุญแจรหัส ให้มีความถูกต้องและเป็นความลับ โดยต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อการเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

๕.๒ กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงระบบเครือข่าย ระบบสารสนเทศและอุปกรณ์สารสนเทศ ตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย โดยกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ

๕.๓ กำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๕.๔ จากข้อ ๕.๑ และ ๕.๒ ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว เช่น ลาออก, เกษียณ หรือพ้นจากตำแหน่ง โดยต้องจัดให้มีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศ เป็นประจำทุกๆ ๓ เดือน

๕.๕ ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๕.๖ ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

๕.๗ ต้องระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๕.๘ ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและเครือข่าย

๕.๙ ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๕.๑๐ ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

๕.๑๑ ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์ และการส่งผ่าน หรือไหลเวียนของข้อมูลหรือสารสนเทศ สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง หรือการประยุกต์ใช้งานตามภารกิจ

๕.๑๒ ไม่อนุญาตให้เชื่อมต่อระบบเครือข่ายกรมสอบสวนคดีพิเศษแบบไร้สาย อาทิเช่น Wireless LAN, Wi-Fi และการเชื่อมต่อระบบเครือข่ายไร้สายรูปแบบอื่น ๆ ที่เป็นการเชื่อมต่อระบบสารสนเทศของกรมสอบสวนคดีพิเศษ

๕.๑๓ ให้บันทึก เฝ้าสังเกต ตรวจสอบการรายงานการเข้าถึงระบบเครือข่าย และกิจกรรมอื่นใด เพื่อความมั่นคงปลอดภัยระบบสารสนเทศ ทั้งระบบเครือข่ายคอมพิวเตอร์และระบบสื่อสารข้อมูลอื่นๆ เป็นประจำทุกห้วงเวลา เช่น ทุก ๆ ๑ เดือน, ๓ เดือน เป็นต้น

๖. การจัดการและการควบคุมการเข้าถึงระบบปฏิบัติการ และโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ ของกรมสอบสวนคดีพิเศษ ศูนย์สารสนเทศต้องดำเนินการ ดังนี้

๖.๑ การควบคุมการเข้าถึงระบบปฏิบัติการ

๑) ควบคุมการเข้าถึงโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๒) กำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๓) จัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๔) จำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๕) ยุติการใช้งานระบบสารสนเทศ กรณีมีการว่างเว้นจากการใช้งานเกินกว่า ๓๐ นาที

๖.๒ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๑) จำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานในการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๒) ระบบสารสนเทศที่มีความไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร

๓) กำหนดข้อปฏิบัติและมาตราการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๔) กำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

๕) กรมสอบสวนคดีพิเศษ กำหนดให้ใช้โปรแกรมที่มีลิขสิทธิ์โดยกรมสอบสวนคดีพิเศษจัดซื้อจัดหาตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการพัสดุฯ เท่านั้น

๖) อนุญาตให้ใช้โปรแกรม Browser สำหรับใช้งานในระบบสารสนเทศได้เฉพาะ Internet Explorer Version ล่าสุด และ Mozilla Firefox Version ล่าสุด

๗. การจัดการระบบสารสนเทศกรณีพบเหตุละเมิดความมั่นคงปลอดภัยหรือสงสัยว่าจะเกิดเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ รวมถึงการป้องกันการละเมิดจากผู้ไม่พึงประสงค์ทั้งภายในและภายนอกองค์กร โดยให้ศูนย์สารสนเทศ ดำเนินการดังนี้

๗.๑ กรณีพบเหตุละเมิดความมั่นคงปลอดภัยหรือสงสัยว่าจะเกิดเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ

๗.๑.๑ กรณีพบการเกิดเหตุหรือสงสัยว่าจะเกิดเหตุละเมิดความมั่นคงปลอดภัยเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา เจ้าหน้าที่ผู้ดูแลระบบต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษรและรวบรวมหลักฐาน เพื่ออ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง ให้เจ้าหน้าที่ที่มอบหมายโดย ศูนย์สารสนเทศทำหน้าที่ สำรวจ ตรวจสอบ ความเสียหายเบื้องต้น และรายงานเหตุละเมิดความมั่นคงปลอดภัยระบบสารสนเทศ

๗.๑.๒ ดำเนินการตามแผนรักษาความมั่นคงปลอดภัยฯ และดำเนินการจัดหา พัฒนาและบำรุงรักษาระบบสารสนเทศ ให้สามารถใช้งานได้เมื่อถูกละเมิดฯ

๗.๑.๓ วางแผนจัดหาระบบสารสนเทศใหม่จะต้องประเมินความเสี่ยงและกำหนดมาตรการการรักษาความมั่นคงปลอดภัยตามความเหมาะสม

๗.๒ การป้องกันการละเมิดจากผู้ไม่พึงประสงค์ทั้งภายในและภายนอกองค์กร

๗.๒.๑ กำหนดหน้าที่ความรับผิดชอบรวมถึงโทษของผู้ใช้งาน ในการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีการกำหนดดังนี้

๑) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๒) ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๓) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ยังไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน โดยการบันทึกประวัติการซ่อมบำรุงทรัพย์สินเทคโนโลยีสารสนเทศ โดยเก็บข้อมูล วันและเวลาที่ซ่อม ชื่อผู้ซ่อม ชื่อผู้ร่วมงาน รายละเอียดการซ่อม และรายการอุปกรณ์ที่เปลี่ยนหรือเอาออกเป็นอย่างน้อย

๔) กำหนดบทลงโทษผู้ใช้งาน กรณีที่ผู้ใช้งานการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต เปิดเผย ล่วงรู้ ลักลอบทำสำเนาข้อมูลสารสนเทศ และลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ให้เป็นไปตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

๗.๒.๒ การพัฒนาหรือปรับปรุงซอฟต์แวร์ระบบสารสนเทศใหม่ ทั้งที่ว่าจ้างให้หน่วยงานภายนอกเป็นผู้จัดทำหรือให้หน่วยงานของกรมสอบสวนคดีพิเศษจัดทำขึ้นเอง ให้นำมาตรการสำหรับการพัฒนาซอฟต์แวร์เป็นส่วนหนึ่งของข้อกำหนดของระบบ ในทุกขั้นตอนตั้งแต่การออกแบบจนถึงการส่งมอบสำหรับการพัฒนาระบบสารสนเทศโดยหน่วยงานภายใน จะต้องจัดให้มีระบบสำหรับการพัฒนา และการทดสอบโดยเฉพาะ ห้ามใช้หรือเชื่อมต่อกับระบบที่ใช้งานจริง

๗.๒.๓ กำหนดวิธีการทดสอบประสิทธิภาพและทดสอบภาระสูงสุดของระบบ และให้วิธีดังกล่าวเป็นส่วนหนึ่งของเกณฑ์การตรวจรับระบบสารสนเทศใหม่รวมทั้งการปรับปรุงระบบสารสนเทศบำรุงรักษาหรือซ่อมแซมเครื่องมือหรืออุปกรณ์สารสนเทศต้องทำโดยบุคลากร ที่ได้รับอนุญาตจากกรมสอบสวนคดีพิเศษเท่านั้น

๗.๒.๔ กรณีที่การซ่อมแซมหรือบำรุงรักษาระบบสารสนเทศทำโดยหน่วยงานภายนอก บุคลากรของหน่วยงานภายนอกจะต้องได้รับการกลั่นกรองในเรื่องการเข้าถึงความลับตามความเหมาะสมจากเจ้าหน้าที่ศูนย์สารสนเทศที่รับผิดชอบ

๗.๒.๕ กำหนดวิธีการและความถี่การสำรองข้อมูล การเข้ารหัส และดำเนินการสำรองข้อมูลให้ถูกต้องและสมบูรณ์ รวมทั้งระบุวิธีการนำข้อมูลกลับคืน

๗.๒.๖ ทดสอบแผนการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อหาช่องโหว่ของระบบเป็นระยะทั้งด้วยระบบอัตโนมัติและด้วยบุคคล

๘. มาตรการสำหรับการพัฒนาซอฟต์แวร์ มีดังนี้

๘.๑ การคัดเลือกผู้พัฒนาซอฟต์แวร์จากภายนอกจะต้องมีการตรวจสอบความไว้ใจได้ของบุคลากรในทีมงานในการเข้าถึงเอกสารราชการในระดับลับ การทำสัญญาจะต้องระบุความรับผิดชอบของผู้พัฒนาและทีมงานในการปกปิด และรักษาความลับ ทั้งระหว่างการพัฒนาและหลังการส่งมอบซอฟต์แวร์

๘.๒ ผู้พัฒนาซอฟต์แวร์ต้องพัฒนาซอฟต์แวร์ตามหลักวิชาการที่ยอมรับโดยทั่วไป และยินยอมให้ทำการตรวจสอบได้ตลอดเวลา รวมทั้งแสดงรายละเอียดที่จำเป็นไว้ในซอร์สโค้ด เช่น ชื่อผู้เขียน วัน เดือน ปีที่เขียน หรือ ปรับปรุง วัตถุประสงค์ ระดับการป้องกัน สำหรับข้อมูลที่จำเป็นต้องใช้ในการพัฒนา เช่น ความสัมพันธ์ที่

สามารถเชื่อมโยงไปถึงโปรแกรมหรือข้อมูลลับอื่นๆ หรือ ผู้ที่ได้รับอนุญาตให้นำซอฟต์แวร์ไปใช้งานได้ให้เพิ่มเติมไว้ในเอกสารคู่มือ

๘.๓ ผู้พัฒนาซอฟต์แวร์ทั้งที่เป็นบุคลากรทางคอมพิวเตอร์ของกรมสอบสวนคดีพิเศษ และบุคคลภายนอกที่รับจัดทำซอฟต์แวร์ให้กรมสอบสวนคดีพิเศษ ต้องคำนึงถึงความมั่นคงปลอดภัยระบบสารสนเทศในทุกขั้นตอนของการพัฒนาซอฟต์แวร์ รวมทั้งปฏิบัติต่อเอกสารหรือคู่มือระหว่างการพัฒนาซอฟต์แวร์โดยถือเป็นเอกสารระดับลับ

๘.๔ ผู้พัฒนาซอฟต์แวร์ต้องแสดงหรือพิมพ์ ตัวอักษรตามชั้นความลับกึ่งกลางหน้าทั้งด้านบน และด้านล่างของทุกหน้าเอกสารที่มีชั้นความลับนั้นสารสนเทศที่จัดทำในรูปแบบเอกสารหรือรายงาน โดยใช้ตัวอักษรที่มีขนาดใหญ่กว่าที่ใช้ในข้อความปกติ และใช้สีหรือความเข้มของตัวอักษรที่มีขนาดใหญ่

๘.๕ ผู้พัฒนาซอฟต์แวร์ต้องจัดทำสารสนเทศที่ในรูปแบบ ภาพเขียน เรขา ภาพถ่าย แผนที่ แผนภูมิ แผนผัง ให้แสดงหรือพิมพ์ตัวอักษรตามชั้นความลับ โดยให้แสดงชั้นความลับให้ปรากฏเห็นได้ชัดเจน หรือแสดงไว้ใกล้ชื่อภาพ

๘.๖ การเข้าถึงระบบสารสนเทศของกรมสอบสวนคดีพิเศษจากภายในและภายนอกสถานที่ทำการกรมสอบสวนคดีพิเศษ ผู้พัฒนาซอฟต์แวร์ต้องเข้าถึงโดยจำกัดและจะต้องแจ้งให้เจ้าหน้าที่ผู้ดูแลระบบทราบทุกครั้ง

๙. การใช้งานระบบฐานข้อมูล/สารสนเทศของกรมสอบสวนคดีพิเศษ

๙.๑ ผู้ใช้งานต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ และไม่ใช้งานคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ในเชิงพาณิชย์ และในทางที่ผิดกฎหมาย หรือก่อให้เกิดความเสียหายแก่บุคคลอื่น

๙.๒ ผู้ใช้งานต้องกรอกแบบฟอร์มการขอสิทธิ์การเข้าใช้งานระบบสารสนเทศ (แบบฟอร์มตามภาคผนวก ๓) โดยให้ผู้บังคับบัญชาเป็นผู้อนุมัติ และจัดส่งแบบฟอร์มดังกล่าวให้ศูนย์สารสนเทศเป็นผู้กำหนดสิทธิ์การใช้งานหรือบัญชีผู้ใช้บริการ (Account) ได้แก่ Username และ Password

๙.๓ เมื่อเกิดปัญหาในการใช้งาน ผู้ใช้งานต้องแจ้งศูนย์สารสนเทศเป็นผู้ดำเนินการแก้ไขหรือปฏิบัติตามคำแนะนำของศูนย์สารสนเทศ

๙.๔ ผู้ใช้งานต้องรับผิดชอบในการเก็บรักษารหัสผ่านของตนไว้เป็นความลับ และไม่สามารถปฏิเสธความรับผิดชอบได้ หากมีผู้อื่นล่วงรู้และนำไปใช้ในทางที่ผิด

๙.๕ ผู้ใช้งานต้องไม่นำข้อมูลสารสนเทศที่ตนเองเข้าถึงไปเผยแพร่หรือส่งให้กับผู้ใด โดยไม่ได้รับอนุญาต

๙.๖ ผู้ใช้งานต้องรับผิดชอบ หมั่นตรวจตราเครื่องคอมพิวเตอร์ของตนเอง เพื่อให้มั่นใจว่าปลอดภัยจากซอฟต์แวร์ประสงค์ร้ายต่างๆ

๙.๗ เมื่อตรวจพบหรือสงสัยว่ามีการละเมิดการรักษาความปลอดภัยระบบฐานข้อมูล และสารสนเทศหรือมีสิ่งผิดปกติเกิดขึ้น ให้รีบแจ้งศูนย์สารสนเทศทราบโดยเร็วที่สุด

๙.๘ คืนคอมพิวเตอร์และอุปกรณ์ของกรมสอบสวนคดีพิเศษ ในการเข้าใช้งาน ระบบฐานข้อมูลและสารสนเทศ ให้แก่กรมสอบสวนคดีพิเศษ เมื่อพ้นสภาพการเป็นข้าราชการ พนักงานราชการ หรือลูกจ้าง

๙.๙ ข้าราชการและลูกจ้างของกรมสอบสวนคดีพิเศษ มีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมสอบสวนคดีพิเศษ

๙.๑๐ ผู้ละเมิดนโยบายการรักษาความปลอดภัยระบบฐานข้อมูลและสารสนเทศ ต้องรับผิดชอบต่อความเสียหายต่างๆ ที่เกิดขึ้น รวมทั้งอาจถูกลงโทษทางวินัยและถูกดำเนินคดีในทางอาญาด้วย

หมวด ๒

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศระดับเจ้าหน้าที่ทั่วไป

(เจ้าหน้าที่ของกรมสอบสวนคดีพิเศษ/ผู้ใช้งาน)

๑. การปฏิบัติหน้าที่ทั่วไป

๑.๑ เข้าร่วมการฝึกอบรมในลักษณะของการติดตามการเปลี่ยนแปลงของเทคโนโลยีด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อให้เกิดความตระหนักและมีความรู้เท่าทันเหตุการณ์ที่จะทำให้เกิดภัยคุกคามต่อระบบสารสนเทศ โดยต้องผ่านการฝึกอบรมหลักสูตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่กรมสอบสวนคดีพิเศษได้จัดขึ้นอย่างน้อย ๑ หลักสูตร

๑.๒ ลงนามรับทราบในข้อนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศที่กรมสอบสวนคดีพิเศษประกาศ

๑.๓ ให้ความร่วมมือ ในการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หรือข้อกำหนดอื่นใดที่เกี่ยวข้องตามที่กรมสอบสวนคดีพิเศษได้จัดทำขึ้น ตลอดจนให้ข้อเสนอแนะในการปรับปรุงให้มีประสิทธิภาพดีขึ้น

๑.๓ รักษาความลับและความมั่นคงปลอดภัยระบบสารสนเทศของกรมสอบสวนคดีพิเศษ จากผู้ไม่ได้รับอนุญาตหรือไม่มีหน้าที่รับผิดชอบโดยตรงตามกฎหมาย ไม่ว่าจะเป็นผู้บังคับบัญชาหรือผู้มีตำแหน่งสูงกว่าก็ตาม รวมถึงหน่วยงานภายนอกหรือบุคคลภายนอกที่ไม่มีส่วนเกี่ยวข้อง โดยอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

๑.๔ ดูแลรักษาป้องกันและใช้งานทรัพย์สินเทคโนโลยีสารสนเทศของกรมสอบสวนคดีพิเศษอย่างถูกวิธี ทั้งทรัพย์สินในครอบครองและทรัพย์สินส่วนกลางตามมาตรการต่างๆ ที่กำหนดไว้ ตามแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย

๒. แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย

๒.๑ ผู้ใช้บริการจะต้องไม่ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายโดยมีวัตถุประสงค์ดังต่อไปนี้

๒.๑.๑ ทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๒.๑.๒ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อผู้อื่น

๒.๑.๓ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

๒.๑.๔ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

๒.๑.๕ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

๒.๑.๖ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชังหรือได้รับความอับอาย

๒.๑.๗ เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม ๒.๑.๑ - ๒.๑.๖

๒.๒ ผู้ใช้บริการจะต้องไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตาม ๒.๑ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

๒.๓ ผู้ใช้บริการต้องไม่กระทำการดังต่อไปนี้

๒.๓.๑ เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน

๒.๓.๒ นำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นเฉพาะไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

๒.๓.๓ เข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

๒.๓.๔ กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สารธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

๒.๓.๕ ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

๒.๓.๖ กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

๒.๓.๗ ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (e-mail) แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

๒.๓.๘ กระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

๒.๓.๙ ติดตั้งระบบเครือข่ายสารสนเทศ(Network) ทุกประเภท คือ แบบมีสายและแบบไร้สาย (Wire/Wireless) ในหน่วยงานหรือในพื้นที่ของกรมสอบสวนคดีพิเศษโดยไม่ได้รับอนุญาต

๒.๓.๑๐ จำหน่ายหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม ๒.๓.๑-๒.๓.๘

๒.๔ แนวปฏิบัติการทำงานกับทรัพย์สินสารสนเทศ (การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายและอุปกรณ์ต่อพ่วง) ผู้ใช้บริการควรปฏิบัติดังต่อไปนี้

๒.๔.๑ ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บัญชาการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบหรือผู้ที่ผู้บัญชาการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบมอบหมายและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

๒.๔.๒ ห้ามมิให้ทำการแก้ไข ซ่อมแซม ทรัพย์สินสารสนเทศที่ชำรุดเสียหายด้วยตนเองโดยพลการหรือให้ผู้อื่นที่ไม่มีอำนาจหน้าที่ดำเนินการให้ กรณีที่มีความจำเป็นให้แจ้งศูนย์สารสนเทศเป็นผู้ดำเนินการ

๒.๔.๓ ห้ามมิให้นำอุปกรณ์สารสนเทศหรืออุปกรณ์สื่อสารทั้งแบบใช้สายและไม่ใช้สายนอกเหนือจากที่ผู้ดูแลระบบติดตั้งไว้เดิม มาเชื่อมต่อกับระบบสารสนเทศของกรมสอบสวนคดีพิเศษโดยมิได้รับอนุญาต กรณีที่มีความจำเป็นต้องใช้หรือต่อเชื่อมกับระบบให้แจ้งศูนย์สารสนเทศเป็นผู้ดำเนินการ

๒.๔.๔ กรณีที่ต้องการนำทรัพย์สินสารสนเทศที่มิใช่สมบัติของกรมสอบสวนคดีพิเศษมาใช้งานในพันธกิจของกรมสอบสวนคดีพิเศษ ทรัพย์สินนั้นจะต้องได้รับอนุญาตให้ใช้จากศูนย์สารสนเทศ ตลอดจนขึ้นบัญชีเป็นส่วนหนึ่งของทรัพย์สินสารสนเทศที่นำมาใช้ในระบบสารสนเทศ

๒.๔.๕ การปฏิบัติงานกับอุปกรณ์เทคโนโลยีสารสนเทศให้ปฏิบัติตามแนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย (Malware)

๒.๔.๖ การปฏิบัติงานกับอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ มีดังนี้

๒.๔.๖.๑ ให้ระวังและมีการป้องกันจากการถูกโจรกรรม เช่น การใช้สายคล้องหรือการเข้ารหัสข้อมูล

๒.๔.๖.๒ ให้ระวังและมีการป้องกันจากการถูกดักฟังข้อมูล หรือการแอบดูจอภาพหรือการป้อนรหัสผ่าน

๒.๔.๖.๓ ให้ระวังการเข้าถึงสารสนเทศโดยมิได้รับอนุญาตโดยใช้ความสัมพันธ์ส่วนตัว เช่น ครอบครัว หรือเพื่อน เป็นต้น

๒.๔.๖.๔ ติดตั้งโปรแกรมสำหรับการเชื่อมต่อกับเครือข่ายของกรมสอบสวนคดีพิเศษเป็นการเฉพาะ โดยเป็นโปรแกรมที่ Deploy จากอุปกรณ์ที่ศูนย์สารสนเทศเป็นผู้กำหนด โดยอธิบดีกรมสอบสวนคดีพิเศษอนุมัติ

๒.๔.๖.๕ อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ จะไม่ติดตั้งโปรแกรมที่ไม่มีลิขสิทธิ์ หรือผ่านการ Jail Break หรือ การ Root System

๒.๔.๖.๖ ให้นำเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารมาตรวจสอบที่ศูนย์สารสนเทศทุก ๓ เดือน เพื่อป้องกันการปรับแก้ไขค่าของอุปกรณ์

๒.๔.๗ ใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่ายของหน่วยงานอย่างมีประสิทธิภาพ และเกิดประโยชน์สูงสุดแก่ทางราชการ

๒.๔.๘ ไม่คัดลอกโปรแกรมต่างๆ ที่หน่วยงานได้ซื้อสิขสิทธิ์มาอย่างถูกต้องตามกฎหมายไปติดตั้งบนคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒.๔.๙ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ของหน่วยงานจะต้องกำหนดโดยเจ้าหน้าที่ศูนย์สารสนเทศเท่านั้น

๒.๔.๑๐ ไม่ทำการปรับแต่งไบออส (Bios) หรือการตั้งค่าระบบ (Configuration) อื่นใดที่อาจส่งผลกระทบต่อระบบการทำงานของคอมพิวเตอร์ อันเป็นเหตุให้ไม่สามารถเปิดเครื่องใช้งานได้เป็นปกติ

๒.๔.๑๑ ไม่ทำการเปลี่ยนแปลงเลขที่อยู่ไอพี (IP Address) ของเครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพาภายในหน่วยงาน

๒.๔.๑๒ หากผู้ใช้บริการที่มีความประสงค์จะขอใช้เลขที่อยู่ไอพีสาธารณะ (Public IP Address) จะต้องทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บัญชาการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบเพื่อเสนอความเห็นต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

๒.๔.๑๓ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย เว้นแต่จะได้รับอนุญาตจากผู้บัญชาการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ หรือผู้ที่ผู้บัญชาการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบมอบหมาย

๒.๔.๑๔ ไม่ทำการ Format เครื่องคอมพิวเตอร์ ติดตั้งโปรแกรมคอมพิวเตอร์ หรือโปรแกรมอรรถประโยชน์รวมทั้งโปรแกรมละเมิดลิขสิทธิ์ และอุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงาน เพื่อให้สามารถใช้งานเครื่องคอมพิวเตอร์และระบบ

เครือข่ายของหน่วยงานได้ หากมีความจำเป็นให้แจ้งศูนย์สารสทเทศเป็นผู้ดำเนินการ โดยกรอกแบบฟร์อมการขอรับบริการที่ศูนย์สารสนเทศได้จัดทำไว้ (แบบฟอร์มตามภาคผนวก ๒)

๒.๔.๑๕ ไม่ใช้บริการระบบอินเทอร์เน็ต (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) จำนวนมากหรือเป็นเวลานานในระหว่างเวลาทำงาน

๒.๔.๑๖ ห้ามผู้ใดกระทำเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยที่ไม่รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๓. แนวปฏิบัติการควบคุมเข้าถึงระบบปฏิบัติการ

๓.๑ ผู้ใช้บริการต้องกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ในการใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

๓.๒ ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๓.๓ ผู้ใช้บริการควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๓.๔ ผู้ใช้บริการควรทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๔. แนวปฏิบัติในการใช้งานบัญชีผู้ใช้บริการ(Account/Username)

๔.๑ ผู้ใช้บริการที่เป็นเจ้าของบัญชีผู้ใช้บริการ ต้องเป็นผู้รับผิดชอบในผลต่างๆอันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการของตนเอง จากเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่พิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๔.๒ ผู้ใช้บริการจะต้องเก็บรักษาบัญชีผู้ใช้บริการไว้เป็นความลับและห้ามเปิดเผยต่อผู้บุคคลอื่น ห้ามโอนจำหน่ายจ่ายแจก ให้กับผู้อื่น

๔.๓ ผู้ใช้บริการจะต้องลงบันทึกการเข้าใช้ (Login) โดยบัญชีผู้ใช้บริการของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดงานชั่วคราว

๕. แนวปฏิบัติการกำหนดรหัสผ่าน(Password) การเปลี่ยนรหัสผ่าน และการใช้งานรหัสผ่าน

๕.๑ รหัสผ่านควรมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยอาจจะผสมกันระหว่างตัวเลขและตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษ (เช่น @ # $ %) และสัญลักษณ์ต่างๆ ด้วย

๕.๒ ไม่ควรกำหนดรหัสผ่านจากชื่อ หรือนามสกุลของผู้ใช้บริการ ชื่อบุคคลในครอบครัวบุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์

๕.๓ เมื่อผู้ใช้งานได้รับรหัสผ่านจากระบบสารสนเทศ หรือได้รับจากผู้ดูแลระบบ ให้ทำการเปลี่ยนรหัสผ่านทันทีเมื่อเข้าใช้งานระบบฯครั้งแรก และควรทำการเปลี่ยนรหัสผ่าน ทุก ๒ เดือน หรือเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

๕.๔ ผู้ใช้บริการจะต้องเก็บรักษารหัสผ่านสำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศ ที่ได้มาโดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำใดให้ผู้อื่นทราบโดยมิได้รับอนุญาตจากผู้บังคับบัญชา

๕.๕ ไม่ทำการบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์/เครื่องคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๖. แนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย(Malware)

๖.๑ เครื่องคอมพิวเตอร์ที่ใช้งานภายในหน่วยงานต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๖.๒ ผู้ใช้บริการควรทำการอัพเดท (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานต่างๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอร์ฟแวร์ เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ ตามคำแนะนำที่ผู้ดูแลระบบจะแจ้งให้ทราบเป็นระยะๆ

๖.๓ ห้ามมิให้ผู้ใช้บริการทำการปิดหรือยกเลิกหรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้าย (Malware) ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator) หรือศูนย์สารสนเทศ

๖.๔ หากผู้ใช้บริการพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย (Malware) ห้ามมิให้ผู้ใช้บริการเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้าย (Malware) ไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ และให้แจ้งศูนย์สารสนเทศเพื่อทำการแก้ไข

๖.๕ ก่อนการใช้งานสื่อบันทึกพกพา ควรมีการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware)

๖.๖ ในการรับส่งข้อมูลคอมพิวเตอร์ หรือสารสนเทศ (Information) ผ่านระบบเครือข่าย ผู้ใบริการต้องทำการตรวจสอบ เพื่อป้องกันแล้วกำจัดโปรแกรมประสงค์ร้าย (Malware) ก่อนการรับส่งทุกครั้ง

๖.๗ ผู้ใช้บริการควรทำการตรวจสอบไฟล์ก่อนทำการเปิด โดยโปรแกมป้องกันโปรแกรมประสงค์ร้าย (Malware) เป็นการป้องกันในการเปิดไฟล์ที่สามารถประมวลผลได้ (Executable file) เช่น .inf .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe เป็นต้น

๗. แนวปฏิบัติการใช้งานระบบสารสนเทศของกรมสอบสวนคดีพิเศษ และระบบอินเทอร์เน็ต (Internet)

๗.๑ ในการเข้าใช้งานระบบสารสนเทศต่าง ๆ ของ กรมสอบสวนคดีพิเศษ รวมถึงการขอรหัสการเข้าใช้งานระบบสารนเทศของกรมสอบสวนคดีพิเศษจากภายนอกองค์กรเพื่อยืนยันตัวบุคคล (VPN) ต้องกรอกแบบฟอร์มการขอสิทธิ์การเข้าใช้งานระบบสารสนเทศ (แบบฟอร์มตามภาคผนวก ๓) โดยให้ผู้บังคับบัญชาเป็นผู้อนุมัติ และจัดส่งแบบฟอร์มดังกล่าวให้ศูนย์สารสนเทศเป็นผู้กำหนดสิทธิ์การใช้งานหรือบัญชีผู้ใช้บริการ (Account) ได้แก่ Username และ Password

๗.๒ ในการรับรหัสการเข้าใช้งานระบบสารสนเทศต้องได้รับการแจ้งจากศูนย์สารสนเทศ เมื่อศูนย์สารสนเทศดำเนินการกำหนดสิทธิ์ผู้ใช้งานเรียบร้อยแล้ว และทำการลงลายมือชื่อในบัญชีการขอรับสิทธิ์การใช้งานเพื่อรับรหัสผ่าน

๗.๓ ผู้ใช้บริการต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น โดยใส่ชื่อผู้ใช้บริการและรหัสผ่านที่ได้รับตามข้อ ๗.๒ และห้ามผู้ใช้บริการทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุความจำเป็นและทำการขออนุญาตจากผู้บัญชาการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบเป็นลายลักษณ์ อักษรแล้ว

๗.๔ ผู้ใช้บริการต้องไม่เชื่อมต่อระบบเครือข่ายกรมสอบสวนคดีพิเศษแบบไร้สาย อาทิเช่น Wireless LAN, Wi-Fi และการเชื่อมโยงเครือข่ายไร้สายรูปแบบอื่นๆ ที่เป็นการเชื่อมต่อระบบสารสนเทศของกรมสอบสวนคดีพิเศษ

๗.๕ ผู้ใช้บริการต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของหน่วยงาน และต้องไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาผลประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็ปไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา

พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดลิขสิทธิ์ผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน เป็นต้น เว้นแต่กรณีการปฏิบัติตามหน้าที่ โดยได้รับมอบหมายจากผู้บังคับบัญชา

๗.๖ ห้ามผู้ใช้บริการเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการบนอินเทอร์เน็ต (Internet)

๗.๗ ผู้ใช้บริการต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) ซึ่งรวมถึงการดาวน์โหลดอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือ ทรัพย์สินทางปัญญา

๗.๘ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้บริการต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

๗.๙ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้บริการต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานทั้งภายในและภายนอก รวมถึงหน่วยงานอื่นๆ

๗.๑๐ หลังจากการใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ผู้ใช้บริการทำการปิดเว็บบราวเซอร์เพื่อป้องกันการใช้งานโดยบุคคลอื่นๆ

๗.๑๑ การขอใช้บริการอินเทอร์เน็ตจากโครงข่ายหรือผู้ให้บริการอื่นนอกเหนือจากที่ศูนย์สารสนเทศ กรมสอบสวนคดีพิเศษ เป็นผู้ให้บริการภายในกรมสอบสวนคดีพิเศษ จะต้องได้รับอนุมัติการผู้บริหารเทคโนโลยีสารสนเทศระดับสูง(CIO) ก่อน

๘. แนวปฏิบัติการใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

๘.๑แนวปฏิบัติการใช้งานสำหรับผู้ใช้บริการ

๘.๑.๑ ผู้ใช้บริการต้องกรอกแบบคำขอใช้ระบบระบบสารสนเทศ/จดหมายอิเล็กทรอนิกส์ (e-mail) ตามข้อ ๗.๑

๘.๑.๒ ผู้ใช้บริการที่ได้รับรหัสผ่าน (Password) ครั้งแรกในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และเมื่อมีการเข้าสู่ระบบครั้งแรกนั้นจะต้องเปลี่ยนรหัสผ่าน (Password) โดยทันที

๘.๑.๓ ผู้ใช้บริการไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๘.๑.๔ ผู้ใช้บริการควรมีการเปลี่ยนรหัสผ่าน (Password) ทุก ๒ เดือน

๘.๑.๕ ผู้ใช้บริการไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านรับส่งข้อความ ยกเว้นแต่จะได้การยินยอมจากเจ้าขอผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานต่างๆในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

๘.๑.๖ ห้ามไม่ให้ผู้ใช้บริการ ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของกรมสอบสวนคดีพิเศษ(xxxxx@dsi.go.th) สำหรับงานส่วนบุคคลหรือลงทะเบียนในเครือข่ายอินเทอร์เน็ต หรือใช้อ้างอิงกับธุรกรรมการเงินส่วนบุคคล หรือเว็บไซต์เชิงพาณิชย์ หรือเครือข่ายสังคมออนไลน์

๘.๑.๗ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นผู้ใช้บริการควรทำการลงบันทึกออก (Logout) ทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

๘.๑.๘ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้บริการไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

๘.๑.๙ ผู้ใช้บริการมีหน้าที่จะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๙. แนวทางปฏิบัติการจัดการเหตุละเมิดการรักษาความมั่นคงปลอดภัย

๙.๑ ให้เจ้าหน้าที่ทุกคนหรือผู้ใช้บริการตรวจตราและสังเกตพฤติกรรมของระบบหรือบุคคลที่น่าสงสัย และแจ้งเจ้าหน้าที่ผู้ดูแลระบบที่รับผิดชอบ เมื่อสังเกตเห็นสิ่งผิดปกติหรืออาจเป็นเหตุละเมิดความมั่นคงปลอดภัย อันได้แก่ การใช้สิทธิ์ของผู้ดูแลระบบจากระยะไกลเพื่อเข้าถึงระบบสารสนเทศ การแก้ไขข้อมูลบนเว็บไซต์ การพยายามสอบถามหรือหลอกถามรหัสผ่าน การเข้ามาใช้อุปกรณ์สารสนเทศโดยไม่ได้รับอนุญาต เป็นต้น

๙.๒ เมื่อเกิดหรือสงสัยว่าจะเกิดเหตุละเมิดความมั่นคงปลอดภัย เช่น ทรัพย์สินสารสนเทศสูญหาย ความพยายามเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต เป็นต้น ให้เจ้าหน้าที่หรือผู้ใช้บริการที่พบเหตุปฏิบัติตามแนวทางปฏิบัติการจัดการเหตุละเมิดการรักษาความมั่นคงปลอดภัย และห้ามมิให้เจ้าหน้าที่ไม่ได้รับมอบหมายปฏิบัติการอื่นใดที่ไม่ได้กำหนดไว้ในขั้นตอนรับมือเหตุละเมิดโดยพลการ และดำเนินการแจ้งเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยระบบสารสนเทศตามแบบฟอร์มแจ้งเหตุ (ภาคผนวก ๔)

๙.๓ ห้ามมิให้เจ้าหน้าที่หรือผู้ใช้บริการที่ไม่ได้รับอนุญาต ทำการทดสอบระบบรักษาความมั่นคงปลอดภัยโดยเด็ดขาด ถ้าพบว่ามีการกระทำเกิดขึ้นจะถือว่าเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๙.๔ ห้ามมิให้เจ้าหน้าที่หรือผู้ใช้บริการที่ไม่ได้อนุญาต ทำการตรวจจับ เฝ้าฟัง ติดตาม ถอดรหัส บันทึกการสื่อสารข้อมูลทั้งในเครือข่ายคอมพิวเตอร์และระบบสื่อสารโดยเด็ดขาด และให้ถือว่าการกระทำดังกล่าวเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๙.๕ เจ้าหน้าที่หรือผู้ใช้บริการที่ละเมิดความมั่นคงปลอดภัยระบบสารสนเทศ และบุกรุกทรัพย์สินทางราชการหรืออื่นๆ แล้วแต่กรณี จะถูกดำเนินการทางวินัยฐาน**ฝ่าฝืนระเบียบวินัยทางราชการ**

๙.๖ เจ้าหน้าที่หรือผู้ใช้บริการที่ไม่แจ้งเหตุละเมิดโดยทันทีหรือไม่ปฏิบัติตามขั้นตอนรับมือเหตุละเมิดโดยทันที จะถูกดำเนินการทางวินัยฐานหย่อนยานหรือเพิกเฉยในการปฏิบัติหน้าที่หรือแล้วแต่กรณี

๙.๗ เมื่อศูนย์สารสนเทศขอความร่วมมือในการปรับปรุงเวอร์ชั่นหรือระงับการใช้ทรัพย์สินสารสนเทศเพื่อป้องกันการเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย ให้เจ้าหน้าที่หรือผู้ใช้บริการปฏิบัติในทันที

๙.๘ ภายหลังการเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย เจ้าหน้าที่หรือผู้ใช้บริการที่ตรวจพบเหตุละเมิดการรักษาความมั่นคงปลอดภัย จะต้องทำรายงานเหตุการณ์ที่เกิดขึ้นเสนอต่อผู้บัญชาการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ การละเลยไม่ทำรายงานในเวลาที่กำหนดถือเป็นความบกพร่องในหน้าที่ อาจ/ต้องถูกดำเนินการทางวินัยฐานหย่อนยานหรือเพิกเฉยในการปฏิบัติหน้าที่หรือแล้วแต่กรณี

๑๐.แนวทางปฏิบัติในการเคลื่อนย้ายและการทำสำเนาสารสนเทศ

๑๐.๑ ห้ามมิให้คัดลอกหรือทำสำเนา เอกสาร/ข้อมูลคอมพิวเตอร์/ข้อมูลสารสนเทศ ที่มีระดับลับขึ้นไปในระบบสารสนเทศของกรมสอบสวนคดีพิเศษ โดยไม่ได้รับอนุญาต ถ้าพบว่ามีการกระทำเกิดขึ้นจะถือว่าเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑๐.๒ ห้ามมิให้ส่งข้อมูลสารสนเทศของระบบสารสนเทศ ของกรมสอบสวนคดีพิเศษ ออกไปนอกเครือข่ายของกรมสอบสวนคดีพิเศษ หรือนำสำเนาสารสนเทศระดับลับขึ้นไปในระบบสารสนเทศของกรมสอบสวนคดีพิเศษออกนอกพื้นที่รักษาการณ์โดยไม่ได้รับอนุญาต ถ้าพบว่ามีการกระทำเกิดขึ้นจะถือว่าเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑๐.๓ การทำสำเนาข้อมูลและการส่งข้อมูลของระบบสารสนเทศ ที่มีระดับความลับตามข้อ ๑๐.๑ ของกรมสอบสวนคดีพิเศษ ออกไปนอกเครือข่าย/ระบบสารสนเทศของกรมสอบสวนคดีพิเศษ ผู้ร้องขอ/ผู้ที่ต้องการใช้สำเนาหรือส่งข้อมูลดังกล่าว เพื่อใช้ในราชการ จะต้องขออนุญาตจากผู้บริหารระดับสูง และให้ผู้ที่ได้รับอนุญาตจากหัวหน้าส่วนราชการ ในการเข้าถึงเอกสารลับเป็นผู้ทำสำเนาออกจากระบบสารสนเทศของ

กรมสอบสวนคดีพิเศษ โดยส่งสำเนาดังกล่าวให้กับผู้ร้องขอ ด้วยแผ่น CD/DVD หรือ e-mail ของกรมสอบสวนคดีพิเศษเท่านั้นและห้ามมิให้คัดลอกหรือทำสำเนาส่งต่อให้ผู้ที่มิได้รับอนุญาต

๑๐.๔ การใช้งานการสื่อสารข้อมูลในระบบอีเมล์หรือจดหมายอิเล็กทรอนิกส์ ให้ปฏิบัติตามแนวปฏิบัติการใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

๑๑. แนวทางปฏิบัติในการทำลายสื่อบันทึกข้อมูลหรือการทำลายไฟล์ข้อมูลที่มีระดับลับขึ้นไป

๑๑.๑ กรณีผู้ร้องขอสำเนาข้อมูล และได้รับสำเนาข้อมูลตามข้อ ๑๐.๓ ด้วยแผ่น CD/DVD เมื่อใช้งานตามภารกิจแล้ว ให้นำสื่อบันทึกนั้น ๆ ส่งคืนหัวหน้าส่วนราชการผู้อนุญาตเพื่อทำลาย

๑๑.๒ กรณีผู้ร้องขอสำเนาข้อมูล และได้รับสำเนาข้อมูลตามข้อ ๑๐.๓ ทาง e-mail ของกรมสอบสวนคดีพิเศษ เมื่อใช้งานตามภารกิจแล้ว ให้ทำการลบ e-mail นั้น ใน Inbox และ Trash ออก

๑๑.๓ หากผู้ที่ได้รับสำเนาข้อมูล ตามข้อ ๑๑.๑ และ ๑๑.๒ ที่ร้องขอทำการบันทึกข้อมูลหรือสำเนาข้อมูลที่ได้ตามข้อ ๑๐.๓ ลงสื่อบันทึกข้อมูลอื่น ๆ อาทิเช่น Flash Drive, Harddisk ฯลฯ เพื่อใช้ในราชการตามภารกิจแล้ว ให้ทำการลบ/ล้าง ไฟล์ข้อมูล นั้น ๆ ด้วยโปรแกรมเขียนทับ (Wiping) ด้วย บิท ๐ หรือ ๑ ในไฟล์ข้อมูลดังกล่าว ทั้งนี้จะต้องแจ้งให้หัวหน้าส่วนราชการผู้อนุญาตตามข้อ ๑๐.๓ ทราบว่าได้ทำลายข้อมูลแล้วเป็นลายลักษณ์อักษร

หมวด ๓

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศระดับเจ้าหน้าที่ผู้ดูแลระบบ หรือศูนย์สารสนเทศ

๑. แนวการปฏิบัติหน้าที่โดยทั่วไป ของผู้ดูแลระบบ (System Administrator)

๑.๑ เจ้าหน้าที่ผู้ดูแลระบบมีหน้าที่ปฏิบัติต่อระบบสารสนเทศตามระเบียบเช่นเดียวกับเจ้าหน้าที่ทั่วไป และมีอำนาจการบริหารและจัดการสารสนเทศหรือระบบสารสนเทศต่อไปนี้ ซึ่งต้องปฏิบัติหรือควบคุมโดยเจ้าหน้าที่ผู้ดูแลระบบที่ได้รับการแต่งตั้งโดยหัวหน้าศูนย์สารสนเทศ ทั้งนี้ต้องเป็นไปตามแผนที่ได้รับการอนุมัติและในช่วงเวลาที่ได้รับการอนุมัติเท่านั้น

๑.๑.๑ ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่ายของหน่วยงานให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้บริการที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ใช้บริการผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่เกิดขึ้นแก่หน่วยงานให้ ผู้ดูแลระบบ(System Administrator) พิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้บริการดังกล่าวได้ทันที

๑.๑.๒ ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และระบบบนเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

๑.๑.๓ ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย

๑.๑.๔ ลบข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์แม่ข่าย (Server) อย่างถาวร หรือทำลายข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานของหน่วยงานบนเครื่องคอมพิวเตอร์และระบบเครือข่ายเมื่อหมดความจำเป็นในการใช้งาน ด้วยวิธีการตามมาตรฐาน DOD ๕๒๒๐.๒๒-M

๑.๑.๕ ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

๑.๑.๖ ดูแลรักษาและปรับปรุงบัญชีจดหมายอิเล็กทรอนิกส์ (e-mail) ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิ์การใช้งานของผู้ใช้บริการที่พ้นสภาพการเป็นผู้ใช้บริการ

๑.๑.๗ ตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้บริการให้มีการกำหนดรหัสผ่าน (Password) รวมทั้งการเก็บรักษารหัสผ่าน (Password)

๑.๑.๘ ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

๑.๑.๙ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์ หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

๑.๑.๑๐ ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๑.๑.๑๑ เมื่อผู้ดูแลระบบ(System Administrator) พ้นจากหน้าที่จะต้องคืนทรัพย์สินของหน่วยงานที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้หัวหน้าศูนย์สารสนเทศ หรือผู้ที่ได้รับมอบหมายตรวจสอบการคืนทรัพย์สิน

๑.๒ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ดูแลระบบ(System Administrator) จะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์(Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้งานบริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์(Log) ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

๑.๒.๑ เก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้

๑.๒.๒ มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบ (System Administrator) สามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน(IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

๑.๒.๓ ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้

๑.๒.๔ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum ๐) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

๒. การกำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

๒.๑ กำหนดประเภทข้อมูลหลัก ๆ ดังนี้

๒.๑.๑. ข้อมูลทั่วไป เช่น ข้อมูลงานสารบรรณ

๒.๑.๒ ข้อมูลที่เป็นความลับ เช่น ข้อมูลด้านคดีและข่าว

๒.๒ ลำดับความสำคัญของข้อมูล หรือชั้นความลับของข้อมูลแบ่งตามความสำคัญของข้อมูล เช่นข้อมูลด้านคดีหรือข่าว ผู้ที่มีสิทธิ์เข้าถึงต้องเป็นผู้ที่ได้รับมอบหมายให้รับผิดชอบงานข่าวหรือคดีนั้นๆ

๒.๓ ระดับชั้นการเข้าถึง แบ่งตามตำแหน่งและหน้าที่ความรับผิดชอบของผู้ใช้งาน

๓. แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนทศ

๓.๑ ให้ศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ กำหนดมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของกรมสอบสวนคดีพิเศษ จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่ออธิบดีกรมสอบสวนคดีพิเศษ โดยผู้บัญชาการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบเป็นผู้เสนอความเห็น

๓.๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงตามคำร้องขอ เพิ่มเติม/เปลี่ยนแปลง/ยกเลิก สิทธิ์ของผู้ใช้งาน ภายใน ๓ วัน หลังจากได้รับอนุมัติจากหัวหน้าหน่วยงานของผู้ใช้งาน หรือตามคำสั่งเปลี่ยนแปลงหน้าที่ความรับผิดชอบของบุคลากรกรมสอบสวนคดีพิเศษ

๓.๓ ผู้ดูแลระบบ (System Administrator) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

๓.๔ ผู้ดูแลระบบ (System Administrator) ต้องจัดบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๓.๕ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการรหัสผ่านและสิทธิ์การใช้งานระบบสารสนเทศของบุคลากร ดังต่อไปนี้

๓.๕.๑ กำหนดรหัสผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานเริ่มต้นเป็นรหัสชั่วคราว โดยชื่อผู้ใช้งานหรือรหัสผ่านต้องไม่ซ้ำกัน และกำหนดให้ระบบจัดการรหัสผ่านตรวจสอบรหัสผ่านว่าต้องประกอบด้วย อักขระ, ตัวเลข และอักขระพิเศษ ความยาวรวมกันไม่น้อยกว่า ๘ ตัวอักษร กรณีที่ผู้ใช้งานทำการเปลี่ยนรหัสเอง (สามารถตั้งค่าการจัดการรหัสผ่าน ผ่านระบบรักษาความมั่นคงปลอดภัยเพิ่มเติมได้ ตัวอย่างตามภาคผนวก ๗)

๓.๕.๒ ส่งมอบรหัสผ่านชั่วคราว (Temporary Password) ให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๓.๕.๓ เมื่อมีการส่งมอบรหัสผ่านตามข้อ ๓.๕.๒ ให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน และกำหนดและแจ้งผู้ใช้บริการให้ทำการเปลี่ยนรหัสผ่านใหม่

๓.๕.๔ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๓.๕.๕ แจ้งผู้ใช้งาน ไม่ให้ทำการบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๓.๕.๖ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓.๕.๗ กำหนดให้ระบบแจ้งเตือนให้ผู้ใช้งานทำการเปลี่ยนรหัสผ่านทุกๆ ๒ เดือน

๓.๕.๘ กำหนดระยะเวลาการใช้งานระบบสารสนเทศภายในของกรมสอบสวนคดีพิเศษ โดยผู้ใช้งานต้องใช้งานระบบสารสนเทศอย่างต่อเนื่อง หากว่างเว้นจากการใช้งานระบบสารสนเทศมากกว่า ๓๐ นาที ต้องกำหนดให้โปรแกรม Browser ปิดการทำงาน และกำหนดให้ผู้ใช้งานกรอกรหัสผู้ใช้งานและรหัสผ่านเพื่อเข้าสู่ระบบสารสนเทศใหม่

๓.๖ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๓.๖.๑ ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๓.๖.๒ กำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๓.๖.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๓.๖.๔ กำหนดรหัสยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร เพื่อให้สามารถเข้าถึงเครือข่ายและระบบสารสนเทศของกรมสอบสวนคดีพิเศษ โดยการให้ผู้ใช้งานยื่นแบบคำขอรหัสการเข้าใช้งาน VPN ตามแบบคำขอใช้งาน VPN (ภาคผนวก ๓) โดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

๓.๖.๕ กำหนดค่าการเปลี่ยนรหัส (Password) ตามระยะเวลาที่กำหนดของความสำคัญของข้อมูล

๓.๖.๖ ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๔. แนวทางปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๔.๑ ผู้ดูแลระบบ(System Administrator) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้ระบบเครือข่ายไร้สายน้อยที่สุด

๔.๒ ผู้ดูแลระบบ(System Administrator) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำ อุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

๔.๓ ผู้ดูแลระบบ(System Administrator) ต้องกำหนดค่า WPA-๒ (Wi-Fi Protected Access) เป็นระดับเบื้องต้นในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๔.๔ ผู้ดูแลระบบ(System Administrator) ควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๔.๕ ผู้ดูแลระบบ(System Administrator) ควรมีการติดตั้งไฟร์วอลล์(Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

๔.๖ ผู้ดูแลระบบ(System Administrator) ควรกำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

๔.๗ ผู้ดูแลระบบ(System Administrator) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นจากในระบบเครือข่ายไร้สายและจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบ(System Administrator) รายงานต่อผู้บัญชาการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบทราบทันที

๔.๘ ผู้ดูแลระบบ(System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

๕. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๕.๑ ให้กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบกำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๕.๒ การอนุญาตใช้พื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่ออธิบดีกรมสอบสวนคดีพิเศษผ่านผู้บัญชาการเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบและจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่นๆ

๕.๓ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๕.๓.๑ จำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕.๓.๒ จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๕.๓.๓ จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆได้

๕.๓.๔ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๕.๓.๕ ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปรกติ

๕.๓.๖ ผู้ดูแลระบบต้องดูแลการเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวบุคคล (Authentication) เพื่อการตรวจสอบความถูกต้องของผู้ใช้บริการ

๕.๓.๗ เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

๕.๓.๘ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ โดยกำหนดชื่อและหมายเลขของอุปกรณ์บนเครือข่าย (IP Address) ชื่อระบุถึงตำแหน่งและที่ตั้งของอุปกรณ์ประกอบด้วย AA-XX-YY-ZZ เพื่อใช้ในการตรวจสอบและยืนยันอุปกรณ์บนเครือข่าย

AA = ประเภทของอุปกรณ์
XX = ชื่ออาคารที่ติดตั้ง
YY = ชั้นของอาคาร
ZZ = ลำดับที่ของเครื่องในชั้น

๕.๓.๙ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะที่จำเป็น

๕.๔ ผู้ดูแลระบบ (System Administrator) ต้องบริการควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟแวร์ระบบ (System Software)

๕.๕ ให้ศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทางดังต่อไปนี้

๕.๕.๑ ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

๕.๕.๒ ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

๕.๕.๓ ควรตรวจสอบบันทึกการปฏิบัติงานหรือรายงานการเข้าถึงของผู้ใช้งานระบบสารสนเทศของกรมสอบสวนคดีพิเศษอย่างสม่ำเสมอ

๕.๕.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๕.๖ ให้ศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบภายนอกตามแนวทาง ดังต่อไปนี้

๕.๖.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากอธิบดีกรมสอบสวนคดีพิเศษผ่านผู้บัญชาการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ

๕.๖.๒ มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ดังนี้

๕.๖.๒.๑ กำหนดให้มีการเข้ารหัสในลักษณะของ SSL สำหรับการเข้าถึงพอร์ตที่ใช้ปรับแต่งระบบ

๕.๖.๒.๒ กำหนดรหัสผู้ใช้และรหัสผ่านสำหรับผู้ที่มีสิทธิ์

๕.๖.๒.๓ ติดตั้งอุปกรณ์สำหรับการป้องกันตรวจสอบระบบเครือข่ายจากภายนอก

๕.๖.๓ ทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ รวมถึงระบบสารสนเทศที่ไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อองค์กรต้องได้รับการแยกออกจากระบบอื่นๆ ดังนี้

๕.๖.๓.๑ แบ่งแยกเครือข่ายด้วยอุปกรณ์ป้องกันการบุกรุก (Firewall) โดยเฉพาะในส่วนของระบบฐานข้อมูล และระบบโปรแกรมประยุกต์ (Application) ด้วยพอร์ตการใช้งานเฉพาะ

๕.๖.๓.๒ กำหนดกลุ่มของเครือข่ายเสมือน (VLAN) เพื่อแบ่งแยก

- ผู้ใช้งานระหว่างกลุ่มหรือหน่วยงานหรือพื้นที่การใช้งาน
- กลุ่มผู้ใช้งานกับระบบสารสนเทศหลัก
- ระบบสารสนเทศหลักกับเครือข่ายภายนอก

๕.๖.๔ การควบคุมการเชื่อมต่อทางเครือข่ายที่มีการใช้งานร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ดังนี้

๕.๖.๔.๑ กำหนดให้แต่ละกลุ่มหรือหน่วยงานภายในมีเครือข่ายเสมือนของตนเอง

๕.๖.๔.๒ การเชื่อมต่อระหว่างเครือข่ายกำหนดโดยอุปกรณ์สลับเส้นทางหลัก(Core Switch)

๕.๖.๔.๓ เครือข่ายเสมือนที่ต่างกันไม่สามารถติดต่อกันได้ ยกเว้นการเชื่อมต่อมายังระบบสารสนเทศกลาง

๕.๖.๕ การควบคุมการจัดเส้นทางบนเครือข่าย มีดังนี้

๕.๖.๕.๑ กำหนดการควบคุมการจัดการเส้นทางบนเครือข่ายผ่านอุปกรณ์สลับเส้นทางหลัก(Core Switch)

๕.๖.๒.๒ เครือข่ายเสมือนที่ต่างกันไม่สามารถติดต่อกันได้ ยกเว้นการเชื่อมต่อมายังระบบสารสนเทศกลาง

๕.๖.๖ วิธีการใดๆที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะทางไกลต้องได้รับการอนุญาตจากอธิบดีกรมสอบสวนคดีพิเศษผ่านผู้บัญชาการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ

๕.๖.๗ การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

๕.๖.๘ การใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

๖. แนวทางการปฏิบัติเมื่อเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย (กรณีการเข้าถึงระบบโดยไม่ได้รับอนุญาต)

๖.๑ เมื่อเจ้าหน้าที่ผู้ดูแลระบบได้รับแจ้งเหตุให้วิเคราะห์ว่าเป็นเหตุละเมิดประเภทใด เกิดผลกระทบอย่างไร มีวิธีการรับมืออย่างไรบ้าง

๖.๒ เจ้าหน้าที่ผู้ดูแลระบบรายงานให้บุคคลและหน่วยงานที่เกี่ยวข้องรับทราบทันที

๖.๓ เจ้าหน้าที่ผู้ดูแลระบบปฏิบัติการตามวิธีรับมือกับเหตุละเมิดตามความเหมาะสม ในกรณีนี้อาจได้แก่ การเปลี่ยนแปลงรหัสผ่าน การแยกระบบที่มีปัญหาออก การปิดบริการที่สงสัย การปิดเส้นทางการเข้าสู่ระบบสารสนเทศ การยกเลิกบัญชีผู้ใช้งานที่ถูกใช้ในการเข้าถึงระบบโดยมิได้รับอนุญาต ในบางกรณีเจ้าหน้าที่ที่เกี่ยวข้องจะต้องค้นหาและจับกุมผู้ก่อเหตุละเมิด

๖.๔ เจ้าหน้าที่ผู้ดูแลระบบและเจ้าหน้าที่ที่เกี่ยวข้องรวบรวมข้อมูลและหลักฐานของเหตุการณ์

๖.๕ เจ้าหน้าที่ผู้ดูแลระบบตรวจสอบว่าวิธีการรับมือที่ใช้ได้ผลหรือมีประสิทธิภาพหรือไม่ แล้วเพิ่มเติมมาตรการเพื่อลดช่องโหว่หรือถอดแยกส่วนของระบบสารสนเทศที่มีปัญหาออก

๖.๖ เจ้าหน้าที่ผู้ดูแลระบบกู้คืนระบบสารสนเทศสู่สภาพเดิม และทำรายงานแจ้งผู้ที่เกี่ยวข้อง

๗. แนวทางการปฏิบัติภายหลังการเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย

๗.๑ หลังจากเกิดเหตุละเมิดความมั่นคงปลอดภัย ศูนย์สารสนเทศ สำนักเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ ต้องสำรวจความเสียหายที่เกิดจากเหตุละเมิดการรักษาความมั่นคงปลอดภัย ตรวจสอบสาเหตุและจุดอ่อนหรือข้อบกพร่องที่ก่อให้เกิดการละเมิด ทำรายงานและทบทวนมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้อง เสนอผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เพื่อพิจารณา

๗.๒ เสนอลงโทษทางวินัยแก่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) รวมทั้งดำเนินคดีทั้งทางแพ่งและอาญาตามความเหมาะสม ในกรณีผู้ละเมิดเป็นกรมสอบสวนคดีพิเศษให้แจ้งหน่วยงานที่เกี่ยวข้องดำเนินการตามกฎหมายต่อไป

๘. แนวทางการปฏิบัติการสำรองข้อมูล

๘.๑ การพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม เจ้าหน้าที่ผู้ดูแลระบบจะต้องปฏิบัติดังต่อไปนี้

๘.๑.๑ พิจารณาและจัดหมวดหมู่ของข้อมูล โดยกำหนดระดับความสำคัญของข้อมูลที่จำเป็นต้องทำสำรอง

๘.๑.๒ สำหรับข้อมูลที่มีความลับสูงให้ทำการเข้ารหัสก่อนทำการสำรอง

๘.๑.๓ พิจารณากำหนดวิธีการสำรองในประเด็นดังนี้

๑) ขนาด (สำรองทั้งหมดหรือสำรองเฉพาะส่วนที่แตกต่าง)

๒) ความถี่ของการสำรอง ควรกำหนดโดยคำนึงถึงความต้องการใช้หากข้อมูลสูญหายหรือเรียกใช้งานไม่ได้ และความจำเป็นของข้อมูลเพื่อให้ธุรกิจขององค์กรดำเนินต่อไปได้อย่างไม่ติดขัด หรือเพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้

๓) วางขั้นตอนการเรียกกลับมาใช้อย่างเป็นลายลักษณ์อักษร

๘.๒ ระหว่างทำการสำรอง เจ้าหน้าที่จะต้องปฏิบัติดังต่อไปนี้

๘.๒.๑ ตรวจสอบผลการสำรองข้อมูล ว่าได้ข้อมูลที่ถูกต้องและครบถ้วนสมบูรณ์หรือไม่

๘.๒.๒ จัดทำป้ายบอกสารสนเทศที่ทำการสำรองให้ชัดเจน

๘.๓ หลังทำการสำรอง เจ้าหน้าที่จะต้องปฏิบัติดังต่อไปนี้

๘.๓.๑ เก็บข้อมูลที่สำรองเอาไว้ในพื้นที่ที่ห่างออกไป ไกลพอที่จะไม่ได้รับความเสียหายอันเกิดจากภัยพิบัติในพื้นที่หลัก

๘.๓.๒ ข้อมูลที่สำรองจะต้องได้รับการป้องกันทั้งทางกายภาพและสภาพแวดล้อมที่เหมาะสมตามมาตรฐานเดียวกับที่ใช้ในข้อมูลหลัก มาตรการที่ใช้ป้องกันสื่อบันทึกข้อมูลในพื้นที่หลักก็ควรนำมาใช้กับพื้นที่สำรองด้วย

๘.๓.๓ ทำการทดสอบสื่อบันทึกข้อมูลสำรองเป็นประจำทุกเดือน เพื่อให้มั่นใจว่า สามารถนำกลับมาใช้อีกได้เมื่อเกิดเหตุการณ์ฉุกเฉินจริง

๘.๓.๔ ขั้นตอนในการนำข้อมูลสำรองกลับมาใช้ ควรได้รับการตรวจสอบและทดสอบทุกๆ ๓ เดือน เพื่อให้มั่นใจว่ามีประสิทธิภาพเพียงพอ และสามารถทำได้เสร็จสิ้นภายในระยะเวลาที่ถูกจัดสรรไว้ตามกระบวนการกู้คืน

๘.๓.๕ จัดหาตู้เก็บหรือที่จัดเก็บสื่อบันทึกข้อมูลสำรอง เพื่อให้เป็นหมวดหมู่ และเป็นระเบียบเรียบร้อย **ง่ายต่อการค้นหา หรือนำกลับมาใช้ และจัดให้มีการควบคุมการนำสื่อบันทึกไปใช้ที่สามารถตรวจสอบได้**

๙. การสำรองและกู้คืนข้อมูล

๙.๑ ผู้รับผิดชอบในการสำรองและกู้คืนข้อมูล

๑) ผู้อำนวยการศูนย์สารสนเทศ เป็น ผู้กำกับดูแลการปฏิบัติงานในการสำรองและกู้คืนข้อมูล

๒) ข้าราชการที่ได้รับมอบหมายระดับชำนาญการของศูนย์สารสนเทศ เป็นเจ้าหน้าที่ผู้ปฏิบัติงานในการสำรองและกู้คืนข้อมูล

๙.๒ การสำรองและกู้คืนข้อมูลระบบฐานข้อมูล (Database Server)

๑) การสำรองข้อมูล

ลำดับ	ขั้นตอน	หมายเหตุ
๑.	จัดเก็บแผ่นติดตั้งระบบปฏิบัติการ	
๒.	จัดเก็บแผ่นติดตั้งโปรแกรมจัดการฐานข้อมูล	
๓.	บันทึกข้อมูลการปรับตั้งค่าของระบบฐานข้อมูล	
๔.	จัดเตรียมพื้นที่จัดเก็บข้อมูลสำรอง	Backup Server
๕.	จัดเตรียมสื่อบันทึกข้อมูลสำรอง	USB External Harddisk
๖.	ตั้งค่าให้ระบบทำการสำรองข้อมูลอัตโนมัติ ช่วงเวลา ๒๒.๐๐ น. ของทุกวันจนกว่าจะทำการสำรองเสร็จ	ทุกวัน
๗.	บันทึกข้อมูลแบบ Full Backup ใน Backup Server	ทุกวันเสาร์
๘.	บันทึกข้อมูลแบบ Full Backup ใน USB External Harddisk	ทุกวันเสาร์
๙.	จัดเก็บ USB External Harddisk ที่สำรองข้อมูลแล้ว	ในตู้เก็บ

๒) การกู้คืนข้อมูล

ลำดับ	ขั้นตอน	หมายเหตุ
๑.	ติดตั้งระบบปฏิบัติการ	
๒.	ลงโปรแกรมฐานข้อมูลใหม่ หรือลบฐานข้อมูลเก่าทิ้ง	
๓.	ปรับตั้งค่าการทำงานของระบบฐานข้อมูล	
๔.	Import ข้อมูล จาก Backup Server	
๕.	กรณี Import ข้อมูล จาก Backup Server ไม่ได้ จึงทำการ Import จาก USB External Harddisk	

๙.๓ การสำรองและกู้คืนข้อมูลโปรแกรมประยุกต์ (Application Server)

๑) การสำรองข้อมูล

ลำดับ	ขั้นตอน	หมายเหตุ
๑.	จัดเก็บแผ่นติดตั้งระบบปฏิบัติการ	
๒.	จัดเก็บแผ่นติดตั้งโปรแกรมประยุกต์	
๓.	บันทึกข้อมูลการปรับตั้งค่าของโปรแกรมประยุกต์	

๒) การกู้คืนข้อมูล

ลำดับ	ขั้นตอน	หมายเหตุ
๑.	ติดตั้งระบบปฏิบัติการ	
๒.	ลงโปรแกรมประยุกต์	
๓.	ปรับตั้งค่าการทำงานของโปรแกรมประยุกต์	

๑๐.แผนรักษาความปลอดภัยกรณีการเข้าถึงระบบโดยไม่มีสิทธิ์

๑๐.๑ แผนป้องกันและแก้ไขปัญหาอุบัติภัยกรณีมีผู้เข้าถึงระบบโดยไม่มีสิทธิ์

๑) การบังคับบัญชา

๑.๑) รองอธิบดีกรมสอบสวนคดีพิเศษ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เป็นผู้อำนวยการเหตุการณ์ มีหน้าที่ควบคุม สั่งการ ดูแลการปฏิบัติการในการควบคุมเหตุการณ์

๑.๒) ผู้อำนวยการศูนย์สารสนเทศ เป็น รองผู้อำนวยการเหตุการณ์ มีหน้าที่ช่วยเหลือผู้อำนวยการเหตุการณ์ และปฏิบัติหน้าที่แทน กรณีผู้อำนวยการเหตุการณ์ไม่สามารถปฏิบัติหน้าที่ได้

๑.๓) ข้าราชการระดับชำนาญการพิเศษหรือระดับชำนาญการ เป็นผู้ช่วยผู้อำนวยการเหตุการณ์ มีหน้าที่ช่วยเหลือรองผู้อำนวยการเหตุการณ์ และปฏิบัติหน้าที่แทน กรณีรองผู้อำนวยการเหตุการณ์ ไม่สามารถปฏิบัติหน้าที่ได้

๑.๔) ข้าราชการศูนย์สารสนเทศระดับชำนาญการ เป็นเจ้าหน้าที่ดูแลระบบ มีหน้าที่ควบคุมการเข้าใช้งานของผู้ใช้งาน และควบคุมดูแลระบบรักษาความปลอดภัยระบบฐานข้อมูลและสารสนเทศ

๒) การติดต่อสื่อสาร

๒.๑) ผู้รับผิดชอบการปฏิบัติตามแผน

ชื่อ-นามสกุล
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)
ผู้อำนวยการศูนย์สารสนเทศ
รองผู้อำนวยการศูนย์สารสนเทศ

๒.๒) หน่วยงานสนับสนุน

หน่วยงาน
ส่วนตรวจ ๓

๒.๓) การปฏิบัติ

ขั้นตอนการปฏิบัติ	ผู้รับผิดชอบ
๑. ตรวจสอบผู้ใช้งานที่เข้าใช้งานระบบฐานข้อมูลและสารสนเทศโดยไม่มีสิทธิ์	เจ้าหน้าที่ดูแลระบบ
๒. ระงับบัญชีผู้ใช้งานซึ่งไม่มีสิทธิ์	เจ้าหน้าที่ดูแลระบบ

ขั้นตอนการปฏิบัติ	ผู้รับผิดชอบ
๓. แจ้งส่วนตรวจ ๓ ดำเนินการรวบรวมพยานหลักฐานและตรวจพิสูจน์การกระทำความผิด	เจ้าหน้าที่ดูแลระบบ
๔. ตรวจสอบความเสียหายและกู้คืนข้อมูลที่ได้รับความเสียหาย	เจ้าหน้าที่ดูแลระบบ
๕. จัดทำรายงานความเสียหายตามภาคผนวก ๕ และเสนอแนวทางป้องกันแก้ไขรายงานผู้บังคับบัญชา	เจ้าหน้าที่ดูแลระบบ

๑๐.๒ แผนทดสอบความมั่นคงปลดภัยกรณีมีผู้เข้าถึงระบบโดยไม่มีสิทธิ์

๑) เหตุการณ์จำลอง

๑.๑) มีผู้ลักลอบใช้บัญชีผู้ใช้งานและรหัสผ่านของผู้ดูแลระบบ ในการเข้าถึงระบบเทคโนโลยีสารสนเทศเพื่อการบริหาร (MIS)

๑.๒) ผู้ลักลอบใช้งานเข้าถึงระบบเฉพาะในหน้าจอ Login

๑.๓) การเข้าถึงระบบไม่ก่อให้เกิดความเสียหายใดๆ

๒) เครื่องมือที่ใช้

๒.๑) เครื่องคอมพิวเตอร์สำหรับผู้ลักลอบใช้งาน

๒.๒) บัญชีผู้ใช้งานและรหัสผ่านของผู้ดูแลระบบ

๓) การประเมินผล

๓.๑) หัวหน้าศูนย์สารสนเทศเป็นผู้ประเมินผล

๓.๒) มีการประเมินเกี่ยวกับการปฏิบัติตามขั้นตอนของเจ้าหน้าที่ดูแลระบบ

๑๑. แผนรักษาความปลอดภัยกรณีเกิดเพลิงไหม้

๑๑.๑ แผนป้องกันและแก้ไขปัญหาอุบัติภัยกรณีเพลิงไหม้

๑) การบังคับบัญชา

๑.๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เป็น ผู้อำนวยการดับเพลิง มีหน้าที่ควบคุม สั่งการ ดูแลการปฏิบัติการดับเพลิง

๑.๒) ผู้อำนวยการศูนย์สารสนเทศ เป็น รองผู้อำนวยการดับเพลิง มีหน้าที่ช่วยเหลือผู้อำนวยการดับเพลิง และปฏิบัติหน้าที่แทน กรณีผู้อำนวยการดับเพลิงไม่สามารถปฏิบัติหน้าที่ได้

๑.๓) รองผู้อำนวยการศูนย์สารสนเทศ เป็น ผู้ช่วยผู้อำนวยการดับเพลิง มีหน้าที่ช่วยเหลือรองผู้อำนวยการดับเพลิง และปฏิบัติหน้าที่แทน กรณีรองผู้อำนวยการดับเพลิง ไม่สามารถปฏิบัติหน้าที่ได้

๑.๔) เจ้าหน้าที่ฝ่ายอำนวยการ เป็นเจ้าหน้าที่อำนวยการดับเพลิง มีหน้าที่รับผิดชอบสนับสนุน การปฏิบัติงานผู้อำนวยการดับเพลิง และการติดต่อประสานงานกับเจ้าหน้าที่หรือหน่วยงานที่เกี่ยวข้องต่างๆ

๑.๕) เจ้าหน้าที่ดูแลระบบ เป็นเจ้าหน้าที่ระงับเหตุเพลิงไหม้ มีหน้าที่รับผิดชอบในตรวจสอบ ควบคุม ระงับเหตุ เพลิงไหม้เบื้องต้น รวมทั้งการฟื้นฟูระบบฐานข้อมูลและสารสนเทศ

๑.๖) เจ้าหน้าที่คอมพิวเตอร์ เป็นเจ้าหน้าที่อพยพสิ่งของ มีหน้าที่รับผิดชอบเกี่ยวกับการอพยพขนย้าย ข้อมูล Backup รวมทั้ง เอกสารและอุปกรณ์ที่สำคัญ

๑.๗) เจ้าหน้าที่ธุรการ เป็นผู้รับผิดชอบ เป็นเจ้าหน้าที่อพยพคน มีหน้าที่รับผิดชอบเกี่ยวกับการอพยพคนออกจากที่เกิดเหตุเพลิงไหม้

๒) การติดต่อสื่อสาร

๒.๑) ผู้รับผิดชอบการปฏิบัติตามแผน

ชื่อ-นามสกุล
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)
ผู้อำนวยการศูนย์สารสนเทศ
รองผู้อำนวยการศูนย์สารสนเทศ
นางณิชาดา ชื่นชมสิรกุล
นายปัญญา ว่องไว
นายพงศ์บัณฑิต ชัยชาญ
นายอเนก สมดี
นายสัมฤทธิ์ ดวงแก้ว

๒.๒) หน่วยงานสนับสนุน

หน่วยงาน
ศูนย์สื่อสาร กรมสอบสวนคดีพิเศษ
เจ้าหน้าที่รักษาความปลอดภัย กรมสอบสวนคดีพิเศษ(ชั้น G)
ผู้รับเหมาดูแลห้องศูนย์คอมพิวเตอร์ (SITEM)
ศูนย์ดับเพลิงศรีอยุธยา
หน่วยแพทย์กู้ชีพ กทม.

๓) เส้นทางหนีไฟและจุดรวมพล

๓.๑) เส้นทางหนีไฟ ใช้เส้นทางบันไดหนีไฟข้างอาคารด้านทิศตะวันตก

๓.๒) จุดรวมพล ที่บริเวณลานจอดรถหน้าอาคารสถานที่ทำการกรมสอบสวนคดีพิเศษ ถนนแจ้งวัฒนะ

๔) การปฏิบัติ

ขั้นตอนการปฏิบัติ	ผู้รับผิดชอบ
๑. แจ้งเหตุเพลิงใหม้ กับเจ้าหน้าที่ระงับเหตุเพลิงไหม้ หรือเจ้าหน้าที่อำนวยการดับเพลิง	ผู้พบเหตุเพลงไหม้
๒. ตรวจสอบและระงับเหตุเพลิงไหม้เบื้องต้น โดยกรณี ไม่สามารถระงับเหตุเพลิงไหม้ได้ด้วยตนเอง ให้แจ้งเจ้าหน้าที่อำนวยการดับเพลิง	เจ้าหน้าที่ระงับเหตุเพลิงไหม้
๓. แจ้งผู้บังคับบัญชาเกี่ยวกับเหตุเพลิงไหม้	เจ้าหน้าที่อำนวยการดับเพลิง
๔. ตัดสินในอพยพหนีไฟ	ผู้อำนวยการดับเพลิง
๕. แจ้งเจ้าหน้าที่และหน่วยงานที่เกี่ยวข้องในการดับเพลิง	เจ้าหน้าที่อำนวยการดับเพลิง
๖. กดสัญญาณแจ้งเหตุเพลิงไหม้ และตัดระบบไฟฟ้า	เจ้าหน้าระงับเหตุเพลิงไหม้
๗. อพยพคนไปตามเส้นทางหนีไฟ ไปที่จุดรวมพล ปฐมพยาบาลผู้บาดเจ็บ ตรวจสอบผู้ติดค้างเพื่อค้นหา รวมทั้งจัดส่งผู้บาดเจ็บไปโรงพยาบาล	เจ้าหน้าที่อพยพคน
๘. อพยพสิ่งของไปตามส้นทางหนีไฟ ไปที่จุดรวมพล และควบคุมดูแลสิ่งของนั้น	เจ้าหน้าที่อพยพสิ่งของ
๙. ตัดสินในให้เข้าสู่ภาวะปกติ	ผู้อำนวยการดับเพลิง
๑๐. ตรวจสอบความเสียหายเบื้องต้น	เจ้าหน้าที่อำนวยการดับเพลิง
๑๑. ฟื้นฟูระบบฐานข้อมูลและสารสนเทศ	เจ้าหน้าระงับเหตุเพลิงไหม้

๑๒. จัดทำรายงานความเสียหาย และเสนอแนวทางป้องกันแก้ไข รายงานผู้บังคับบัญชา	เจ้าหน้าที่อำนวยการดับเพลิง

๑๑.๒ แผนทดสอบความมั่นคงปลอดภัยกรณีเพลิงไหม้

๑) เหตุการณ์จำลอง

๑.๑) เกิดเหตุเพลิงไหม้ที่ รางปล๊ักไฟ ภายในห้องศูนย์คอมพิวเตอร์ ชั้น ๕ อาคารกรมสอบสวนคดีพิเศษ โดยต้นเหตุของเพลิงเกิดจาก ไฟฟ้าลัดวงจร

๑.๒) เจ้าหน้าที่ระงับเหตุเพลิงไหม้ เข้าระงับเพลิงแล้ว ประเมินว่าไม่สามารถดับเพลิงขั้นต้นได้ เนื่องจากไฟลุกลามมากขึ้น

๑.๓) ในเหตุการณ์สมมุตว่าไม่มีผู้ติดค้าง และผู้ได้รับบาดเจ็บหรือเสียชีวิต

๑.๔) ภายหลังจากเพลิงสงบ พบว่าฮาร์ดิสก์ของเครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูลได้รับความเสียหายเนื่องจากไฟฟ้าลัดวงจร

๒) อุปกรณ์และระยะเวลาฝึกซ้อม

๒.๑) ใช้อุปกรณ์จำลองในฝึกซ้อม เช่น อุปกรณ์ดับเพลิง อุปกรณ์สำรองข้อมูล ฯลฯ

๒.๒) ใช้ระยะเวลาในการฝึกซ้อม ประมาณ ๑ ชั่วโมง

๓) การประเมินผล

๓.๑) หัวหน้าศูนย์สารสนเทศเป็นผู้ประเมินผล

๓.๒) มีการประเมินเกี่ยวกับการปฏิบัติตามขั้นตอนของผู้ที่เกี่ยวข้องต่างๆ

๑๒. แผนรักษาความปลอดภัยกรณีไฟฟ้าดับ

๑๒.๑) แผนป้องกันและแก้ไขปัญหาอุบัติภัยกรณีไฟฟ้าดับ

๑) การบังคับบัญชา

๑.๑) ผู้อำนวยการศูนย์สารสนเทศ เป็น ผู้อำนวยการเหตุการณ์ มีหน้าที่ควบคุม สั่งการ ดูแลการปฏิบัติการในการควบคุมเหตุการณ์

๑.๒) รองผู้อำนวยการศูนย์สารสนเทศ มีหน้าที่ช่วยเหลือผู้อำนวยเหตุการณ์ และปฏิบัติหน้าที่แทน กรณีรองผู้อำนวยการเหตุการณ์ไม่สามารถปฏิบัติหน้าที่ได้

๑.๓) เจ้าหน้าที่ดูแลระบบ มีหน้าที่ควบคุมดูแลระบบรักษา ความปลอดภัยระบบฐานข้อมูลและสารสนเทศ

๑๒.๒) แผนทดสอบความมั่นคงปลอดภัยกรณีไฟฟ้าดับ

๑) เหตุการณ์จำลอง

๑.๑) เกิดเหตุไฟฟ้าดับ โดยมิได้รับแจ้งล่วงหน้าจากการไฟฟ้า เนื่องจากหม้อแปลงไฟฟ้าที่หน้ากรมสอบนสวนคดีพิเศษระเบิด

๑.๒) การไฟฟ้าแจ้งว่าใช้เวลาในการแก้ไขปัญหาเป็นเวลา ๒ ชั่วโมง

๑.๓) ทำการปิดเครื่องคอมพิวเตอร์เพียงเฉพาะบางส่วน

๒) อุปกรณ์ที่ใช้

๒.๑) เครื่องคอมพิวเตอร์แม่ข่าย

๒.๒) อุปกรณ์สำรองกระแสไฟฟ้า

๓) การประเมินผล

๓.๑) หัวหน้าศูนย์สารสนเทศเป็นผู้ประเมินผล

๓.๒) มีการประเมินเกี่ยวกับการปฏิบัติตามขั้นตอนของเจ้าหน้าที่ดูแลระบบ

หมวด ๔

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบุคคลภายนอก

๑. ผู้ติดต่อจากหน่วยงานภายนอก ต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือ ใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อแล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสารบันทึกการเข้าออกพื้นที่

๒. ผู้ติดต่อจากหน่วยงานภายนอก ที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

๓. ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในกรมสอบสวนคดีพิเศษ

๔. ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าออกศูนย์สารสนเทศได้ด้วยบัตรผู้ติดต่อ โดยสิทธิ์จะขึ้นอยู่กับเหตุผลความจำเป็นในการขอเข้าปฏิบัติงานภายในศูนย์สารสนเทศ

๖. พื้นที่ที่ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าได้ตามที่ระบุไว้ในแบบฟอร์มการขออนุญาตเข้าออก และต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา

๗. ผู้ติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัย ซึ่งเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบการคืนบัตรและตรวจสอบแบบฟอร์มการขออนุญาตเข้าออกว่ามีเจ้าหน้าที่ลงนามอนุญาตแล้วทุกครั้ง