นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สถาบันมาตรวิทยาแห่งชาติ
ประจำปี พ.ศ. ๒๕๖๙

ข้อ ๑ วัตถุประสงค์และขอบเขต

เพื่อให้ระบบสารสนเทศของสถาบันมาตรวิทยาแห่งชาติ หรือต่อไปนี้เรียกว่า “สถาบัน” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ สถาบันจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐานและแนวปฏิบัติให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ดังต่อไปนี้

๑.๑ การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ของสถาบัน ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๑.๒ กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ และมีการปรับปรุงอย่างต่อเนื่อง

๑.๓ นโยบายนี้จะต้องทำการเผยแพร่ให้พนักงานทุกระดับของสถาบัน ได้รับทราบและพนักงานทุกคนจะต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๑.๔ เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหาร พนักงาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับสถาบัน ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศของสถาบันในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๑.๕ นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย ๑ ครั้งต่อปี

ข้อ ๒ องค์ประกอบของนโยบาย

๒.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

- ๒.๑.๑ การเข้าถึงระบบสารสนเทศ
- ๒.๑.๒ การเข้าถึงระบบเครือข่าย
- ๒.๑.๓ การเข้าถึงระบบปฏิบัติการ
- ๒.๑.๔ การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชั่น
- ๒.๑.๕ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
- ๒.๑.๖ หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)
- ๒.๑.๗ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๒.๑.๘ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๒.๑.๙ การควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

๒.๑.๑๐ การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)

๒.๑.๑๑ การเข้าถึงและการควบคุมการใช้งานด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Access Control)

๒.๑.๑๒ การควบคุมระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ได้ทำการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ

๒.๑.๑๓ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒.๒ การใช้งานอินเทอร์เน็ต ระบบเครือข่ายไร้สาย และไปรษณีย์อิเล็กทรอนิกส์

๒.๓ การจัดทำระบบสำรองข้อมูล

๒.๔ การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศ

๒.๕ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๖ ความรับผิดชอบของผู้บริหารและผู้ดูแลระบบ

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันแต่ละส่วนที่กล่าวข้างต้น ประกอบด้วยแนวทางปฏิบัติ เพื่อที่จะทำให้สถาบันมีมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากรของสถาบัน ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย สอดคล้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบสารสนเทศของสถาบัน ซึ่งพนักงานของสถาบันจะต้องปฏิบัติตามอย่างเคร่งครัด และหน่วยงานภายนอกต้องได้รับอนุญาตก่อนดำเนินการ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สถาบันมาตรวิทยาแห่งชาติ
ประจำปี พ.ศ. ๒๕๖๙

ด้วยระบบสารสนเทศและเครือข่ายของสถาบันมาตรวิทยาแห่งชาติ มีความสำคัญต่อการปฏิบัติงานของผู้บริหารและพนักงาน รวมทั้งการให้บริการแก่หน่วยงานทั้งภาครัฐ ภาคเอกชน และประชาชน ทั้งอุตสาหกรรมและบริการต่างๆ สถาบันจึงได้จัดทำแนวทางปฏิบัติที่สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน และข้อกำหนดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อให้ระบบสารสนเทศและเครือข่ายสามารถใช้งานได้อย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยน่าเชื่อถือ สามารถใช้งานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่างๆ ทั้งภายในและภายนอกสถาบันที่อาจก่อให้เกิดความเสียหายต่อสถาบัน จึงได้กำหนดแนวทางปฏิบัติไว้ ดังนี้

หมวดที่ ๑
การเข้าถึงและควบคุมการ ใช้งานสารสนเทศ (Access Control)

ข้อ ๑ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๑.๑ การลงทะเบียนผู้ใช้งาน (User Registration)

๑.๑.๑ กำหนดให้มีขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน โดยใช้แบบฟอร์มลงทะเบียนตามที่กำหนด เพื่อขออนุมัติสิทธิในการเข้าใช้งานระบบสารสนเทศจากแบบฟอร์ม FM-IT-๐๐๔ แบบฟอร์มการสร้างสิทธิ/ กำหนดสิทธิ/ ยกเลิกสิทธิในระบบเครือข่ายคอมพิวเตอร์ ตามระบบบริหารนายภาพ ISO ๙๐๐๑:๒๐๑๕ และเมื่อได้รับการอนุมัติแล้ว ให้ผู้ดูแลระบบสร้างชื่อผู้ใช้ในการใช้งาน พร้อมทั้งมีการจัดเก็บไว้เป็นหลักฐาน

๑.๑.๒ ผู้ดูแลระบบต้องมีการทบทวน ตรวจสอบอำนาจหน้าที่ของผู้ใช้งานอยู่เสมอ

๑.๑.๓ กำหนดให้มีขั้นตอนปฏิบัติในการตัดออกจากทะเบียนของผู้ใช้งาน โดยเมื่อผู้ใช้งานมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ ให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิการใช้งานของผู้ใช้ให้เหมาะสม หรือหากผู้ใช้ถูกเพิกถอนการอนุญาต ย้าย หรือลาออก ผู้ดูแลระบบต้องถอดถอนสิทธิของผู้ใช้งานนั้นออกจากระบบทันทีที่ได้รับแจ้งจากเจ้าของข้อมูล หรือกลุ่มงานบริหารและพัฒนาทรัพยากรบุคคล ฝ่ายบริหารกลาง (กบค.ฝบ.) ผ่านระบบแจ้งปัญหาคอมพิวเตอร์ออนไลน์ ตามระบบบริหารคุณภาพ ISO ๙๐๐๑:๒๐๑๕ พร้อมทั้งให้มีการบันทึก จัดเก็บไว้เป็นหลักฐาน

๑.๑.๔ การลงทะเบียนผู้ใช้ที่เป็นบุคคลภายนอกที่ไม่ใช่พนักงานจะต้องเขียนคำร้องเพื่อขอใช้บริการเครือข่าย

๑.๑.๕ กลุ่มงานเทคโนโลยีสารสนเทศ ฝ่ายนโยบายและยุทธศาสตร์ (กทส.ฝน.) มีหน้าที่จัดสรรและส่งมอบเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ตามแผนอัตรากำลังประจำปี ของ กบค.ฝบ. เฉพาะพนักงานและลูกจ้างรายปี หรือได้รับการอนุมัติจาก ผู้อำนวยการ สถาบันมาตรวิทยาแห่งชาติ (ผมว.)

๑.๑.๖ หน่วยงานภายในสถาบัน ที่จะดำเนินการจัดหาระบบคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้จัดทำข้อเสนอโครงการเฉพาะรายการคอมพิวเตอร์และซอฟท์แวร์ ที่ไม่ใช่เครื่องมือทางวิทยาศาสตร์ เพื่อให้ กทส.ฝน.ให้ความเห็นชอบ โดยขอให้ระบุรายละเอียดความจำเป็นให้ครบถ้วนเพื่อประโยชน์ในการพิจารณาของ กทส.ฝน.

๑.๑.๗ การจัดหาครุภัณฑ์คอมพิวเตอร์ของหน่วยงานภายในสถาบันต้องอ้างอิงเกณฑ์ราคากลางพื้นฐานครุภัณฑ์คอมพิวเตอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นอย่างน้อย โดย กทส.ฝน.จะพิจารณาตามเกณฑ์ที่กำหนด กรณีจัดหาครุภัณฑ์คอมพิวเตอร์สำหรับรายการที่ไม่ใช่ราคาตามเกณฑ์ราคากลางของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ให้ดำเนินการขออนุมัติ ผมว.ก่อน ต้องแนบใบเสนอราคาอย่างน้อย 3 ราย พร้อมระบุเหตุผลเพิ่มเติมสาเหตุที่ไม่ใช้ราคากลางจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และระบุความประสงค์ของการใช้งานที่จำเป็นต้องใช้

๑.๒ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

๑.๒.๑ การขอสิทธิเข้าใช้ระบบสารสนเทศของสถาบัน ผู้ใช้ต้องขออนุญาตจากผู้บังคับบัญชาระดับหัวหน้ากลุ่มงานขึ้นไปเป็นลายลักษณ์อักษร พร้อมทั้งมีการจัดเก็บไว้เป็นหลักฐาน

๑.๒.๒ ผู้ดูแลระบบมีหน้าที่ควบคุมและกำหนดสิทธิการใช้งานให้ผู้ใช้งานตามหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งานเท่านั้น

๑.๒.๓ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

๑.๒.๔ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ควรให้มีการใช้เฉพาะกรณีที่จำเป็นเท่านั้น โดยต้องมีการพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาระดับหัวหน้ากลุ่มงานขึ้นไป ซึ่งควรกำหนดระยะเวลาในการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๑.๒.๕ กรณีผู้ใช้งานที่เป็นบุคคลภายนอก ต้องดำเนินการกำหนดระยะเวลาการสิ้นสุดการใช้งานที่ชัดเจน และดำเนินการลบผู้ใช้งานดังกล่าวทันทีเมื่อสิ้นสุดระยะเวลาการใช้งานที่กำหนดไว้

๑.๒.๖ ผู้ดูแลระบบ มีหน้าที่ กำหนดสิทธิ์การใช้งานตามหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน โดยต้องได้รับรหัสพนักงาน จาก กบค.ฝบ. หรือตามที่ได้รับอนุมัติจาก ผมว.

๑.๓ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password)

๑.๓.๑ กำหนดรหัสผ่าน (Password) ต้องมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยกำหนดให้มีการผสมกันระหว่างตัวเลข ตัวอักษร ตัวอักขระพิเศษ และสัญลักษณ์ต่างๆ และกำหนดให้มีการเปลี่ยนรหัสผ่านทุก ๖ เดือน

๑.๓.๒ จัดให้มีการบริหารจัดการ การจัดส่งรหัสผ่านให้กับผู้ใช้งาน และกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านทันทีที่ใช้งานครั้งแรก

๑.๔ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบ ทบทวนสิทธิในการใช้งานของผู้ใช้งาน ให้ถูกต้องเป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง รวมถึงการยกเลิกสิทธิการใช้งานเมื่อผู้ใช้งานลาออก โอนย้ายงาน หรือพ้นสภาพการเป็นพนักงาน

๑.๕ การบริหารจัดการการเข้าถึงข้อมูลระดับชั้นความลับ (Secret Level Access Management)

๑.๕.๑ กำหนดให้มีการจัดประเภทของข้อมูล ได้แก่ ข้อมูลทั่วไป ข้อมูลส่วนบุคคล ข้อมูลภายในและข้อมูลลับ เป็นต้น โดยมีการกำหนดชั้นความลับของข้อมูลตามระดับความสำคัญ โดยยึดหลักการปฏิบัติงานตามระเบียบว่าด้วยการรักษาความลับของราชการ พ.ศ.๒๕๔๔ ตามระเบียบว่าด้วยการรักษาความลับของราชการ (ฉบับที่ ๒) พ.ศ. ๒๕๖๑ และตามประกาศสำนักนายกรัฐมนตรี เรื่องกำหนดแบบเอกสารตามระเบียบ ตามระเบียบว่าด้วยการรักษาความลับของราชการ ฉบับที่ ๒ พ.ศ. ๒๕๖๑ และระเบียบสถาบันฯ ว่าด้วยงานสารบรรณ พ.ศ. ๒๕๖๐ ตามระดับความสำคัญ และควรได้รับการเข้ารหัสลับ (Encryption) ตามมาตรฐานสากล ดังนี้

๑.๕.๑.๑ ข้อมูลทั่วไป เช่น Microsoft office Word, Excel ทั้งหมด เป็นต้น เป็นข้อมูลที่ทุกคนสามารถเข้าถึงขั้นข้อมูลได้กำหนดสิทธิตามอำนาจหน้าที่ตามที่รับผิดชอบ

๑.๕.๑.๒ ข้อมูลส่วนบุคคล เช่น Database ทั้งงาน Forma, ระบบเงินเดือน (HRM) เป็นต้น เป็นข้อมูลประเภทเกี่ยวกับหมายเลขบัญชี บัตรประชาชน และการเบิกค่ารักษาพยาบาล กำหนดสิทธิเฉพาะบุคคลเจ้าของข้อมูลและตามอำนาจหน้าที่ของผู้ดูแล

๑.๕.๑.๓ ข้อมูลภายใน เช่น Transaction ระบบงานบัญชี, ระบบงานบุคคล (HRM), ข้อมูลการสอบเทียบของลูกค้า, ข้อมูลการอบรมของลูกค้า เป็นต้น เป็นข้อมูลที่อยู่ภายในสถาบัน ที่พนักงานสามารถเข้าถึงได้ กำหนดสิทธิเฉพาะบุคคลเจ้าของข้อมูลและตามอำนาจหน้าที่ของผู้ดูแล

๑.๕.๑.๔ ข้อมูลลับ เช่น ระบบงานบุคคล (HRM) ,ข้อมูลประวัติส่วนตัวของพนักงาน, ข้อมูลประวัติของลูกค้า เป็นต้น เป็นข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล อาทิ การเงิน สุขภาพ ประวัติส่วนตัว เป็นตามพรบ.ข้อมูลข่าวสารส่วนบุคคล กำหนดสิทธิในการเข้าถึงจะต้องได้รับอนุมัติจากผู้บริหารระดับสูงสุดของสถาบันเท่านั้น ระยะเวลาในการเข้าถึงข้อมูลตั้งแต่เวลา ๘.๐๐ –๑๗.๐๐น. ในเวลาราชการ

๑.๕.๒ เจ้าของข้อมูลเป็นผู้กำหนดชั้นความลับของข้อมูลตามระดับความสำคัญ รวมทั้งการให้สิทธิในการเข้าถึงข้อมูลกับผู้ใช้ตามความจำเป็นและความเหมาะสม โดยต้องมีการทบทวน ปรับปรุงสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๒ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๑.๕.๓ การจัดเก็บข้อมูล ให้มีการจัดทำและกำหนดผู้ควบคุมทะเบียนข้อมูลลับ จัดเก็บข้อมูลเอกสาร และสื่อบันทึกข้อมูล ไว้ในสถานที่ที่ปลอดภัย ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน โดยผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) รหัสผ่าน (Password) สิทธิที่ได้รับ และระยะเวลาในการเข้าถึงข้อมูลของผู้ใช้งานให้เหมาะสมตามระดับชั้นความลับ เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ที่เป็นมาตรฐานสากล

๑.๕.๔ การนำเข้า และนำข้อมูลออกไปใช้งานต้องมีการตรวจสอบความครบถ้วน ถูกต้องของข้อมูลก่อนนำไปใช้

๑.๕.๕ การรับส่งข้อมูลลับผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล เช่น TLS / VPN หรือ XML Encryption เป็นต้น)

๑.๕.๖ ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๑.๕.๗ ในกรณีนำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๑.๕.๘ การทำลายข้อมูลประเภทข้อมูลลับ และข้อมูลส่วนบุคคลจะต้องมีการลบข้อมูลหรือทำลายข้อมูลแบบไม่สามารถนำกลับมาใช้งานได้

๑.๕.๙ การนำวิธีการเข้ารหัสลับข้อมูลเพื่อนำมาใช้กับข้อมูลที่มีการจัดเก็บตามข้อมูลประเภทข้อมูลลับและข้อมูลส่วนบุคคล

ข้อ ๒. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

ผู้ใช้งานจะต้องมีหน้าที่ความรับผิดชอบคลอบคลุมถึงการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย ล่วงรู้ การลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

๒.๑ การใช้งานรหัสผ่าน (Password Use)

๒.๑.๑ ให้ผู้ใช้เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับแจ้งจากผู้ดูแลระบบทันทีที่เข้าใช้งานเป็นครั้งแรก

๒.๑.๒ ควรตั้งรหัสผ่านให้มีความยาวไม่น้อยกว่า ๘ ตัวอักษร ที่ยากต่อการเดา มีการผสมกันระหว่างตัวเลข ตัวอักษร และสัญลักษณ์เข้าด้วยกัน และควรเปลี่ยนรหัสผ่าน ทุก ๖ เดือน

๒.๑.๓ ไม่ควรจดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือบันทึกไว้ในโปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำ

๒.๑.๔ หากมีความจำเป็น อนุญาตให้บอกรหัสผ่านให้บุคคลอื่นปฏิบัติงานแทนได้ เพื่อให้สามารถปฏิบัติงานแทนตนเองได้หลังจากดำเนินการเรียบร้อยแล้วให้ทำการเปลี่ยนรหัสผ่านทันที และทำบันทึกเป็นลายลักษณ์อักษรเป็นการเก็บข้อมูล ในรูปแบบอิเล็กทรอนิกส์ เช่น อีเมล แอปพลิเคชัน Line, ระบบสารบรรณ เป็นต้น

๒.๑.๕ ผู้ใช้ที่มีสิทธิตามบัญชีผู้ใช้ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีผู้ใช้ของตนเพื่อเข้าใช้ระบบคอมพิวเตอร์และเครือข่ายของสถาบัน และต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากบัญชีผู้ใช้งานของตน

๒.๑.๖ กลุ่มผู้ใช้งานที่มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านเดียวกันจะต้องร่วมกันรับผิดชอบหากมีความเสียหาย หรือมีปัญหาเกิดขึ้นกับระบบที่เข้าถึง

๒.๒ ให้ปิดเครื่องคอมพิวเตอร์ที่ใช้งานอยู่เมื่อใช้งานเสร็จสิ้น หรือเมื่อยุติการใช้งานนานเกินกว่า ๓ ชั่วโมง

๒.๓ เมื่อไม่มีการใช้งานระบบเป็นระยะเวลา ๓๐ นาที ให้ระบบทำการ Logout ผู้ใช้ออกจากระบบโดยอัตโนมัติ

๒.๔ ให้ทำการตั้งค่า Screen Server ของเครื่องคอมพิวเตอร์ที่รับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานนานเกินกว่า ๑๕ นาที และมีการป้องกันด้วยรหัสผ่านด้วย

๒.๕ ให้ Logout ออกจากระบบทันทีที่ใช้งานเสร็จ

๒.๖ เครื่องโทรสาร เครื่องถ่ายเอกสาร ควรได้รับการปกป้องจากการใช้งานที่ไม่ได้รับอนุญาตด้วยการล็อกกุญแจ หรือรหัสผ่าน

๒.๗ ให้แต่ละฝ่ายมีผู้รับผิดชอบจัดทำทะเบียนสินทรัพย์ และปรับปรุงให้ถูกต้องเป็นปัจจุบันอยู่เสมอ

๒.๘ ให้จัดเก็บสื่อบันทึกข้อมูล ข้อมูล เอกสารสำคัญไว้ในตู้นิรภัยและล็อกกุญแจ ไม่วางทิ้งไว้ในที่เปิดเผย

๒.๙ เอกสารข้อมูลที่มีความสำคัญควรนำออกจากเครื่องพิมพ์ทันที

๒.๑๐ ในกรณีที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ไปใช้งานนอกสถาบัน จะต้องขออนุญาตจากสถาบันอย่างเป็นลายลักษณ์อักษรก่อน และให้ระมัดระวังรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ ที่นำไปใช้งานนอกสถานที่มิให้เกิดความเสียหาย หรือสูญหาย รวมทั้งให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลป้องกันไม่ให้บุคคลอื่นเข้าถึงข้อมูลภายในเครื่องได้ เพื่อป้องกันมิให้ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวรั่วไหล

๒.๑๑ การเข้าปฏิบัติงานในห้องเครื่องคอมพิวเตอร์ (Data Center) ของสถาบัน ให้มีการบันทึกรายละเอียดเกี่ยวกับบุคคล และเวลาเข้าและออกทุกครั้ง ตามบันทึกการเข้าและออกศูนย์คอมพิวเตอร์

๒.๑๒ ในกรณีที่มีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องหรือบุคคลภายนอกที่จำเป็นต้องเข้าปฏิบัติงานในห้องเครื่องคอมพิวเตอร์ (Data Center) ของสถาบัน ให้ผู้ดูแลระบบคอยควบคุมดูแลการปฏิบัติงานของบุคคลดังกล่าวด้วย

ข้อ ๓ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๓.๑ ผู้ดูแลระบบจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๓.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายในสถาบัน (User Authentication for External Conductions) การเข้าใช้งานระบบเครือข่ายและระบบสารสนเทศของสถาบันจากภายนอก ต้องมีการระบุ

ตัวตนของผู้ใช้งาน และการยืนยันตัวตน ด้วยชื่อผู้ใช้ และรหัสผ่าน เพื่อยืนยันและตรวจสอบความถูกต้องก่อนเข้าใช้งาน

๓.๓ การระบุอุปกรณ์บนเครือข่าย (Devices identification in Networks)

๓.๓.๑ ให้ใช้หมายเลข IP เป็นการระบุตัวตนของอุปกรณ์ที่เชื่อมต่อเข้ากับเครือข่าย

๓.๓.๒ กำหนดให้เครื่องคอมพิวเตอร์ของผู้ดูแลระบบเท่านั้นที่สามารถเชื่อมต่อไปยังเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายของสถาบัน โดยมีการยืนยันตัวบุคคลด้วยชื่อผู้ใช้และการใช้รหัสผ่าน

๓.๓.๓ จัดทำตารางการใช้งาน IP address ภายในระบบเครือข่ายคอมพิวเตอร์ของสถาบัน โดยต้องมีการทบทวนและปรับปรุงตารางดังกล่าว อย่างน้อยปีละ ๑ ครั้ง

๓.๓.๔ ป้องกัน IP address ภายในของระบบเครือข่ายภายในสถาบัน มิให้หน่วยงานภายนอกรับรู้

๓.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote usage protection)

๓.๔.๑ การเข้าสู่ระบบระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ของสถาบันจะต้องมีการตรวจสอบเพื่อการยืนยันตัวตนของผู้ใช้งาน เช่น รหัสผ่านหรือวิธีการเข้ารหัสลับ (Encryption) เป็นต้น

๓.๔.๒ การเปิด Port สำหรับ Remote เข้าเครื่องแม่ข่าย หรืออุปกรณ์เครือข่าย เพื่อการตรวจวินิจฉัยและการปรับแต่งระบบจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น และอยู่ภายใต้การควบคุมดูแลของผู้ดูแลระบบ โดยให้ผู้ดูแลระบบปิดพอร์ต นั้นทันทีที่ใช้งานเสร็จ

๓.๔.๓ ผู้ดูแลระบบต้องมีการกำหนดสิทธิ ควบคุมการเปิดพอร์ต ที่ใช้ในการเข้าสู่ระบบของสถาบันอย่างรัดกุม ไม่เปิด Port ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว

๓.๔.๔ ผู้ดูแลระบบต้องติดตั้ง Fire wall พร้อมทั้งสร้างกฎเกณฑ์โดยการทำงานของ Server แต่ละตัว โดยใช้ IP Table สำหรับการติดตั้งให้ทำงานเป็น Personal Firewall และกำหนดค่าตั้งต้นใหม่ ให้ละทิ้งทุก package ที่ส่งเข้ามา แล้วสร้างกฎเกณฑ์ขึ้นมาใหม่ เพื่อยอมรับ Package ที่จำเป็นเท่านั้น จะต้องคำนึงถึงการทำงานของแต่ละ Server

๓.๕ การแบ่งแยกเครือข่าย (Segregation in Networks)

๓.๕.๑ มีการออกแบบระบบเครือข่ายตามกลุ่ม VLAN ที่แยกออกเป็นฝ่ายต่าง ๆ เครื่องแม่ข่ายตามระบบ ๆ ระบบสื่อสารไร้สายที่ยังแยกออกเป็นกลุ่มพนักงาน ลูกค้าฝึกอบรม และผู้มาเยือน เป็นต้น ทั้งนี้เพื่อเป็นการป้องกันการบุกรุก

๓.๕.๒ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๓.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

๓.๖.๑ ผู้ดูแลระบบต้องมีการทบทวน ปรับปรุงสิทธิในการเข้าถึงและการใช้งานของผู้ใช้ให้เหมาะสมลักษณะงาน

๓.๖.๒ กำหนดรูปแบบการเชื่อมต่อและเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกันอย่างปลอดภัย

๓.๖.๓ ผู้ดูแลระบบต้องจำกัดการเข้าถึงการใช้งานระบบเครือข่ายโดยการ Configuring Switch ให้ตรวจสอบหมายเลขรหัส MAC Address ก่อนการเชื่อมต่อเข้าใช้ระบบเครือข่ายของสถาบัน

๓.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

๓.๗.๑ ระบบเครือข่ายทั้งหมดของสถาบันที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกสถาบัน ต้องจัดให้มีอุปกรณ์ป้องกันการบุกรุกติดตั้งประจำทุกเส้นทางที่มีการเชื่อมต่อ

๓.๗.๒ ผู้ดูแลระบบควบคุมจำกัดสิทธิการเข้าถึง Firewall และ IPS (Intrusion prevention system) ของสถาบัน ทั้งทางกายภาพ และการกำหนดบัญชีผู้ใช้งานบน Firewall ให้มีน้อยที่สุดเท่าที่จำเป็น

๓.๗.๓ ผู้ดูแลระบบจำกัดการเข้าถึงระบบสารสนเทศของสถาบันโดยกำหนดกฎของ Firewall ให้เหมาะสมและสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งทบทวนกฎ Firewall อย่างสม่ำเสมอ เพื่อป้องกันกฎใน Firewall ที่ขัดแย้งกันและทำให้ Firewall ทำงานไม่ถูกต้อง

๓.๗.๔ ให้มีการตรวจสอบการแจ้งเตือน ปรับปรุงฐานข้อมูลการโจมตีใหม่ๆของ IPS สม่ำเสมอเพื่อป้องกันกรณีเกิดเหตุบุกรุกขึ้นจริง

๓.๗.๕ กำหนดการไหลเวียนของข้อมูลขาเข้าทำได้เพียง http, https, ssh, ntp และขาออกไม่อนุญาตสำหรับ smtp ยกเว้นตามพอร์ตที่ ส.พ.ร. กำหนดสำหรับ mail.go.th โดยสามารถปรับเปลี่ยนให้เหมาะสมตามกิจกรรมของสถาบันที่ได้รับการอนุมัติจากผู้บังคับบัญชา

๓.๗.๖ การออกระบบเครือข่ายภายนอกให้ผ่าน Proxy สำหรับรูปแบบการเชื่อมต่ออื่น ๆ จะต้องขออนุม้ติจากผู้บังคับบัญชา

ข้อ ๔ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๔.๑ ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์

๔.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน(User Identification and Authentication) ผู้ดูแลระบบจัดให้ผู้ใช้งานมีชื่อผู้ใช้(Username) และรหัสผ่าน(Password) ที่ไม่ซ้ำซ้อนกันในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์และต้องให้มีการยืนยันตัวตนก่อนเข้าใช้งาน

๔.๓ การบริหารจัดการรหัสผ่าน (Password Management System)

๔.๓.๑ มีระบบบริหารจัดการรหัสผ่านแบบอัตโนมัติ โดยบังคับให้มีการเปลี่ยนรหัสผ่านในการใช้งานครั้งแรกและการเปลี่ยนรหัสผ่านจะไม่แสดงรหัสผ่านให้เห็นบนหน้าจอทั้งนี้การกำหนดรหัสผ่านเป็นไปตามข้อ ๑.๓

๔.๓.๒ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์

๔.๓.๓ ตั้งรหัสผ่านในการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน

๔.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use Of System Utilities)

๔.๔.๑ ให้ใช้โปรแกรมอรรถประโยชน์ที่ทำงานบนระบบปฏิบัติการเพื่อบำรุงรักษาและเพิ่มประสิทธิภาพการทำงานของเครื่องคอมพิวเตอร์ เช่น Disk Clean Up, Disk Scanner, Disk Defragmenter, Screen Saver

๔.๔.๒ ห้ามไม่ให้ผู้ใช้ติดตั้ง หรือใช้โปรแกรมตรวจจับ เฝ้าดู Scan ข้อมูลภายในเครือข่ายคอมพิวเตอร์ เพื่อดูข้อมูลที่รับ ส่งผ่านในเครือข่ายคอมพิวเตอร์ ยกเว้นผู้ดูแลระบบที่มีหน้าที่รับผิดชอบด้านความปลอดภัยของเครือข่ายคอมพิวเตอร์

๔.๔.๓ การติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกเหนือจากที่สถาบัน ได้จัดหาและติดตั้งไว้แล้ว ให้แจ้งต่อเจ้าหน้าที่ผู้ดูแลเครื่องคอมพิวเตอร์เพื่อดำเนินการติดตั้ง โดยโปรแกรมที่ติดตั้งห้ามเป็นโปรแกรมที่มีลักษณะเป็นการละเมิดลิขสิทธิในทางทรัพย์สินปัญญาของบุคคลอื่น

๔.๔.๔ ให้ตรวจสอบว่าเครื่องคอมพิวเตอร์ส่วนบุคคลและโน้ตบุ๊คที่ใช้งานอยู่มีการติดตั้งโปรแกรมป้องกันไวรัสของสถาบันหรือไม่ หากไม่มีให้แจ้งเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการติดตั้ง

๔.๔.๕ ตรวจสอบว่าโปรแกรมป้องกันไวรัสยังทำงานตามปกติ มีการปรับปรุงข้อมูลไวรัสอย่างสม่ำเสมอ หากพบว่าทำงานผิดปกติให้รีบแจ้งเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการแก้ไข

๔.๔.๖ ห้ามถอดถอนโปรแกรมป้องกันไวรัสที่สถาบัน ติดตั้งไว้บนเครื่องคอมพิวเตอร์

๔.๕ เมื่อไม่มีการใช้งานระบบเป็นระยะเวลาหนึ่ง (Session Timeout) ได้แก่ ๓๐ นาที ให้ระบบทำการ Logout ผู้ใช้ออกจากระบบสารบรรณอิเล็กทรอนิกส์

๔.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Restrict Information system connection period)

๔.๖.๑ กำหนดให้มีการจำกัดช่วงระยะเวลาการเชื่อมต่อระบบสารสนเทศ เพื่อให้มีการใช้งานภายในระยะเวลาที่กำหนด โดยกำหนดให้ใช้งานได้ตั้งแต่เวลา ๖.๐๐ น. ถึง ๑๙.๐๐ น. ในวันทำการเท่านั้น

๔.๖.๒ กำหนดให้มีการจำกัดระยะเวลาในการเชื่อมต่อที่สั้นลงสำหรับระบบสารสนเทศที่มีความสำคัญเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต และเป็นไปตามข้อ ๒.๒ ข้อ ๒.๓ และข้อ ๒.๔

๔.๖.๓ ยกเว้นบางระบบเชื่อมที่ต้องใช้การเชื่อมต่อตลอดเวลาที่จำเป็นในการ Script เพื่อทำการ Backup ข้อมูล และในบางระบบที่จำเป็นต้องเชื่อมตลอดเวลาเช่น ระบบสอบเทียบ เพื่อสนองความต้องการของลูกค้าตลอด ๒๔ ชั่วโมง

๔.๖.๓.๑ ระบบภายใน สามารถเชื่อมต่อในเวลาราชการ

๔.๖.๓.๒ ระบบภายนอก เปิดตลอดเวลา (ระบบทำงาน ๒๔ ชั่วโมง) เช่น ระบบสำรองข้อมูล ระบบสอบเทียบบริการลูกค้า การ Monitor ระบบวันละ ๑ ครั้ง

ข้อ ๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application And Information Access Control)

๕.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

๕.๑.๑ ผู้ดูแลระบบต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชั่นต่างๆ ของแอปพลิเคชั่นตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกประเภทของผู้ใช้งาน

๕.๑.๒ ต้องจำกัดหรือควบคุมการเข้าถึงสารสนเทศของผู้ใช้งาน ให้เป็นไปตามข้อปฏิบัติในการเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ

๕.๑.๓ ให้ผู้ดูแลระบบตรวจสอบ ควบคุมการเข้าใช้งานของผู้ใช้ที่ได้รับสิทธิในการเข้าถึงข้อมูลแต่ละประเภท โดยให้มีการใช้สิทธิตามที่ได้รับ โดยเฉพาะการเข้าถึงข้อมูลลับตามระดับชั้นความลับ รวมถึงระบบที่สำคัญสูง ได้แก่ ระบบบริการสอบเทียบ ระบบบัญชีการเงินและระบบบุคคล ซึ่งถูกควบคุมสิ่งแวดล้อมภายในศูนย์คอมพิวเตอร์ (Data Center)

๕.๒ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๕.๒.๑ เครื่องคอมพิวเตอร์ที่จะนำมาใช้งานภายในสถาบันจะต้องมีการติดตั้งโปรแกรมป้องกันไวรัส

๕.๒.๒ การนำเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่เชื่อมต่อเข้ากับระบบเครือข่ายของสถาบัน จะต้องมีการลงทะเบียนการใช้งานอย่างเป็นลายลักษณ์อักษร และให้ผู้ดูแลระบบแบ่งกลุ่มผู้ใช้งาน กำหนดระยะเวลา และสิทธิในการใช้งานตามกลุ่มผู้ใช้งาน รวมทั้งให้ยกเลิกสิทธิเมื่อสิ้นสุดการใช้งาน

๕.๒.๓ ผู้ดูแลระบบทบทวน ปรับปรุงบัญชีรายชื่อผู้ใช้งานอย่างสม่ำเสมอ รวมทั้งจัดเก็บ Log

๕.๓ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

๕.๓.๑ การควบคุมการเข้าใช้งานระบบจากภายนอกต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ ผู้ดูแลระบบได้ติดตั้งไว้ภายในสถาบัน เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกดังนี้

๕.๓.๑.๑ การเข้าสู่ระบบระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ของสถาบันจะต้องมีการตรวจสอบ เพื่อยืนยันตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัสลับ (Encryption) เป็นต้น

๕.๓.๑.๒ ต้องไม่เปิด Port ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๕.๓.๑.๓ การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องได้รับอนุมัติจากหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศอย่างเป็นทางการ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของสถาบันในการเข้าสู่ระบบจากระยะไกลโดยเคร่งครัด

๕.๓.๒ ในกรณีนำเครื่องคอมพิวเตอร์หรืออุปกรณ์ไปใช้งานนอกสถาบัน ให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันมิให้ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวรั่วไหล

ข้อ ๖ การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)

๖.๑ ผู้ดูแลระบบที่ดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) มีหน้าที่กำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) รวมทั้งการกำกับ ดูแล บำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย (Server) ให้มีการตรวจสอบทรัพยากรบนเครื่องคอมพิวเตอร์แม่ข่ายของระบบที่สำคัญอย่างน้อยเดือนละ ๑ ครั้ง

๖.๒ การกำหนดสิทธิการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย ต้องกำหนดระดับสิทธิการใช้งานตามความจำเป็น เท่านั้น

๖.๓ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่าย ในกรณีที่พบว่า มีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขและให้รายงานแก่หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศทราบโดยทันที

๖.๔ เปิดใช้บริการ (Service) ของคอมพิวเตอร์แม่ข่ายเท่าที่จำเป็นเท่านั้น

๖.๕ ควรมีการทดสอบโปรแกรม (System Software) เกี่ยวกับความมั่นคงปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการเปลี่ยนแปลง

๖.๖ จำกัดการเชื่อมต่อไปยังเครื่องคอมพิวเตอร์แม่ข่าย โดยเครื่องคอมพิวเตอร์ของผู้ดูแลระบบเท่านั้นที่สามารถเชื่อมต่อไปยังเครื่องคอมพิวเตอร์แม่ข่ายได้

ข้อ ๗ การเข้าถึงและการควบคุมการใช้งานด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Access Control)

๗.๑ กลุ่มงานเทคโนโลยีสารสนเทศ จัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

๗.๒ การเข้าปฏิบัติงานในศูนย์คอมพิวเตอร์ (Data Center) ของสถาบัน ให้มีการบันทึกรายละเอียดเกี่ยวกับบุคคล เวลาเข้าและออกทุกครั้ง ตามบันทึกการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์

๗.๓ ในกรณีที่มีบุคคลที่ไม่หน้าที่เกี่ยวข้อง หรือบุคคลภายนอกที่จำเป็นต้องเข้าปฏิบัติงานในศูนย์คอมพิวเตอร์ (Data Center) ของสถาบัน ให้พนักงานกลุ่มงานเทคโนโลยีสารสนเทศ เป็นผู้ควบคุมดูแลการปฏิบัติงานของบุคคลดังกล่าวด้วย

๗.๔ มีมาตรการควบคุมการเข้าออกศูนย์คอมพิวเตอร์ (Data Center) ของสถาบัน โดยห้ามมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าโดยเด็ดขาด โดยมีเครื่องสแกนลายนิ้วมือ (Finger Print) สำหรับผู้มีสิทธิเท่านั้น หากจำเป็นให้มีพนักงานของกลุ่มงานเทคโนโลยีสารสนเทศเป็นผู้ดูแลและรับผิดชอบ พร้อมทั้งบันทึกการเข้าและออกไว้เป็นหลักฐานทุกครั้ง

๗.๕ มีกล้องวงจรปิด (CCTV) ติดตั้งเพื่อบันทึกเหตุการณ์บริเวณด้านหน้าและภายในศูนย์คอมพิวเตอร์ (Data Center) ตลอด ๒๔ ชั่วโมง

๗.๖ เพื่อป้องกันการเข้าถึงพอร์ตทางกายภาพอุปกรณ์ที่มีพอร์ตจะต้องจัดเก็บในตู้จัดเก็บอุปกรณ์ (Rack) ที่มีกุญแจ หรือระบบป้องกันทางกายภาพ จากผู้ไม่มีหน้าที่รับผิดชอบ โดยทุกครั้งที่ผู้ดูแลระบบเสร็จสิ้นการใช้งานจะต้องทำการปิดตู้จัดเก็บอุปกรณ์ (Rack)

ข้อ ๘ การควบคุมระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ได้ทำการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ

๘.๑ ภายในศูนย์คอมพิวเตอร์ (Data Center) มีระบบปรับอากาศที่ควบคุมอุณหภูมิและความชื้นให้ได้ตามมาตรฐานห้อง Data Center

๘.๒ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับภายในศูนย์คอมพิวเตอร์ (Data Center) มีการติดตั้ง UPS และมีระบบจ่ายไฟฟ้าสำรองจากเครื่องกำเนิดกระแสไฟฟ้าของอาคาร (Generator)

๘.๓ มีระบบป้องกันอัคคีภัยแบบฉีดสารเคมีอัตโนมัติ เมื่อเกิดเพลิงไหม้ โดยมีระบบตรวจจับควันติดตั้งภายในศูนย์คอมพิวเตอร์ (Data Center) เพื่อป้องกันเพลิงไหม้อันเกิดความสูญเสียอุปกรณ์และข้อมูลกลางที่สำคัญของสถาบัน

หมวดที่ ๒
การใช้งานอินเทอร์เน็ต ระบบเครือข่ายไร้สาย และไปรษณีย์อิเล็กทรอนิกส์

ข้อ ๑ การป้องกันการใช้ทรัพยากรผิดวัตถุประสงค์

ผู้ใช้งานต้องไม่ใช้ระบบเครือข่ายสถาบัน เพื่อวัตถุประสงค์ ดังนี้

๑.๑ เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่ บุคคลอื่น กลุ่มบุคคล หน่วยงาน และสถาบัน

๑.๒ เพื่อการกระทำที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑.๓ เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๑.๔ เพื่อการค้าขาย หรือผลประโยชน์ส่วนตัว หรือผลประโยชน์ทางการเมือง

๑.๕ เพื่อการเข้าถึง แสดง จัดเก็บ แจกจ่าย แก้ไข จัดทำ หรือบันทึกข้อมูลที่มีเนื้อหาไม่เหมาะสม เช่น ข้อมูลอันเป็นเท็จ ข้อมูลที่มีผลต่อความมั่นคงของสถาบันชาติ ศาสนา และพระมหากษัตริย์ ภาพลามกอนาจาร ภาพตัดต่อของบุคคลอื่น หรือข้อมูลที่ก่อให้เกิดความเสื่อมเสียอับอายแก่สถาบันหรือบุคคลอื่น เป็นต้น

๑.๖ เพื่อทำการเผยแพร่ข้อมูล หรืออนุญาตให้ผู้อื่นเผยแพร่ข้อมูลเพื่อการกล่าวร้าย หมิ่นประมาทหรือพาดพิงบุคคลอื่น จนทำให้สถาบันถูกฟ้องร้องหรือก่อให้เกิดความเสียหายแก่สถาบัน

๑.๗ เพื่อการเปิดเผยข้อมูลลับซึ่งได้มาจากการปฏิบัติงานให้แก่สถาบันไม่ว่าจะเป็นข้อมูลของสถาบันหรือบุคคลภายนอกก็ตาม

๑.๘ เพื่อขัดขวางหรือโจมตีการใช้งานระบบเครือข่ายของสถาบัน หรือของหน่วยงานภายนอก

๑.๙ เพื่อแพร่กระจายไวรัส หนอน ม้าโทรจัน สปายแวร์ สแปมเมล์ หรือโปรแกรมไม่ประสงค์ดี อื่นๆ

ข้อ ๒ การใช้งานอินเทอร์เน็ต

๒.๑ ผู้ใช้งานอินเทอร์เน็ต ต้องปฏิบัติตามระเบียบที่สถาบันกำหนด และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อย่างเคร่งครัด และต้องรับผิดชอบต่อสิ่งที่อาจเกิดจากการเรียกใช้อินเทอร์เน็ต

๒.๒ ห้ามทำการดาวน์โหลด หรือส่งไฟล์ประเภทสื่อลามกอนาจาร

๒.๓ ห้ามเล่นเกมส์ ดูภาพยนตร์ ฟังเพลงผ่านทางอินเทอร์เน็ต หรือดาวน์โหลดไฟล์ที่ไม่เกี่ยวข้องกับการทำงานในเวลาทำงาน

๒.๔ ห้ามเข้าเว็บไซต์ประเภทการพนัน วิพากษ์วิจารณ์ที่เกี่ยวข้องกับชาติ ศาสนา พระมหากษัตริย์ และอื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือผิดศีลธรรม จริยธรรม

๒.๕ ห้ามใช้อินเทอร์เน็ตเพื่อส่งกระจาย หรือแจกจ่ายสื่อสิ่งพิมพ์อิเล็กทรอนิกส์ที่เป็นการละเมิดลิขสิทธิข้อมูลที่เป็นความลับของสถาบัน ข้อมูลส่วนบุคคลที่ไม่ได้รับอนุญาต

๒.๖ ห้ามใช้อินเทอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์และชื่อเสียงของสถาบัน

ข้อ ๓ การใช้งานระบบไปรษณีย์อิเล็กทรอนิกส์ของสถาบัน

๓.๑ การใช้บริการระบบไปรษณีย์อิเล็กทรอนิกส์ของสถาบัน ผู้ใช้งานต้องระมัดระวังการใช้งาน และต้องรับผิดชอบต่อสิ่งที่อาจจะเกิดจากการใช้งาน

๓.๒ ห้ามมิให้เข้าถึงข้อมูลอีเมล์ของบุคคลอื่นโดยไม่ได้รับอนุญาต

๓.๓ ให้ใช้อีเมล์ของสถาบัน เฉพาะเกี่ยวกับงานเท่านั้น ไม่ใช้ในเรื่องส่วนตัว หรือสิ่งอื่นใดที่ไม่เกี่ยวกับงานของสถาบัน

๓.๔ ห้ามใช้อีเมล์ของสถาบันลงทะเบียน หรือ Post ไว้ตามเว็บไซต์ต่างๆ ที่ไม่เกี่ยวข้องกับงานของสถาบัน

๓.๕ ห้ามส่งอีเมล์ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย สิทธิของผู้อื่น หรือมีลักษณะเป็นจดหมายขยะ จดหมายลูกโซ่

๓.๖ ห้ามส่งอีเมล์ที่มีไวรัสไปให้บุคคลอื่นโดยเจตนา

๓.๗ ห้ามปลอมแปลงอีเมล์ของบุคคลอื่น

๓.๘ ห้ามรับ หรือส่งอีเมล์แทนบุคคลอื่นโดยไม่ได้รับอนุญาต

๓.๙ ทำการสำรองอีเมล์ที่มีความสำคัญอย่างสม่ำเสมอ

๓.๑๐ ระมัดระวังในการระบุชื่อ ที่อยู่ อีเมล์ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งข้อมูลถึงผู้รับผิด

ข้อ ๔ การใช้งานเครือข่ายไร้สาย

๔.๑ ผู้ใช้งานต้องการเข้าถึงระบบเครือข่ายไร้สายของสถาบัน ให้ลงทะเบียนขอใช้งานตามแบบฟอร์มแจ้งในระบบออนไลน์ PM 2 และเมื่อได้รับอนุมัติ ให้ผู้ดูแลระบบสร้าง กำหนดสิทธิการใช้งาน และระยะเวลาในการใช้งาน ให้เหมาะสมกับหน้าที่ความรับผิดชอบของผู้ใช้ พร้อมจัดเก็บไว้เป็นหลักฐาน

๔.๒ ผู้ดูแลระบบดำเนินการจัดเก็บ Log สำหรับการเข้าถึงระบบเครือข่ายไร้สาย

๔.๓ ผู้ดูแลระบบดำเนินการทบทวน และปรับปรุงบัญชีรายชื่อผู้ใช้งานให้เป็นปัจจุบัน

ข้อ ๕ การใช้งาน Network Drive หรือ Drive X:

๕.๑ Network Drive เป็นการใช้ทรัพยากรส่วนรวมซึ่งใช้งานร่วมกัน ควรใช้เนื้อที่ดิสก์เท่าที่จำเป็น ไม่ควรลบ หรือแก้ไขไฟล์ที่ตนเองไม่ได้สร้าง นอกจากจะได้รับอนุญาตจากเจ้าของไฟล์หรือโฟลเดอร์นั้นๆ และควรสำรองไฟล์ที่สำคัญๆ ไว้อีกทางหนึ่งด้วย

๕.๒ ห้ามมิให้นำไฟล์ประเภทรูปภาพ เพลง หรือมัลติมีเดีย ที่มิได้ใช้เพื่อการปฏิบัติงานมาเก็บไว้บน Network Drive ทั้งนี้ ผู้ดูแลระบบมีสิทธิลบไฟล์ดังกล่าวได้ หากผู้ใช้มิได้ดำเนินการลบไฟล์ดังกล่าวหลังจากได้รับแจ้งจากผู้ดูแลระบบแล้ว

หมวดที่ ๓
การจัดทำระบบสำรองข้อมูล

ข้อ ๑ จัดทำรายชื่อระบบงาน และระดับสำคัญ เพื่อใช้พิจารณาคัดเลือกจัดทำระบบสำรองสำหรับระบบที่มีความสำคัญสูงในการปฏิบัติงาน และการให้บริการประชาชนเพื่อให้อยู่ในสภาพพร้อมใช้งาน

ข้อ ๒ จัดทำสำเนาข้อมูล และซอฟต์แวร์เก็บไว้ตามระยะเวลาที่เหมาะสม

ข้อ ๓ กำหนดให้ผู้ดูแลระบบเป็นผู้สำรองข้อมูลของระบบที่รับผิดชอบ

ข้อ ๔ มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลของระบบสารสนเทศ

ข้อ ๕ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการกำหนดชื่อบนสื่อบันทึกข้อมูลอย่างชัดเจน ได้แก่ ชื่อระบบ วันที่ เวลาที่สำรองข้อมูล ผู้รับผิดชอบในการสำรองข้อมูล ข้อมูลที่สำรองไว้นำไปจัดเก็บในตู้นิรภัยไว้นอกสถานที่

ข้อ ๖ ต้องมีการตรวจสอบข้อมูลที่สำรองไปนั้น สำเร็จครบถ้วนหรือไม่ และจดบันทึกผลการตรวจสอบทุกครั้งที่สำรองข้อมูล ในแบบฟอร์ม FM-IT-๐๐๒ ทะเบียนการสำรองข้อมูล ตามระบบบริหารคุณภาพ ISO ๙๐๐๑:๒๐๑๕

ข้อ ๗ ต้องมีการทำลายสื่อบันทึกข้อมูลเมื่อครบกำหนดอายุการใช้งานตามระยะเวลาอย่างถูกต้องและเหมาะสม ตามระบบบริหารคุณภาพ ๙๐๐๑:๒๐๑๕ และข้อกำหนดการจัดการ ทำลายข้อมูล และสื่อบันทึกข้อมูลด้านสารสนเทศ

ข้อ ๘ ให้กลุ่มงานเทคโนโลยีสารสนเทศ จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบภายในระยะเวลาที่เหมาะสม และจัดให้มีการทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙ ต้องนำผลที่ได้จากการทำสอบกู้คืนข้อมูล มาวิเคราะห์เพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๔
การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศ

ข้อ ๑ มีการดำเนินการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศโดยผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากหน่วยงานภายนอก อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ ดำเนินการลดความเสี่ยงด้านสารสนเทศที่ได้จากการตรวจสอบ และประเมินความเสี่ยงเพื่อให้ระบบมีความมั่นคงปลอดภัยสูงสุด

ข้อ ๓ กำหนดความรับผิดชอบของผู้ใช้งานหรือผู้บริหารให้ผู้ใช้งาน และผู้บริหารรับผิดชอบในกรณีเกิดความเสียหายหรืออันตรายอันเนื่องมาจากผู้ใช้งานหรือผู้บริหารบกพร่องหรือไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศแล้วแต่กรณี

ข้อ ๔ การรองรับเทคโนโลยีที่เปลี่ยนแปลงในอนาคต

หมวดที่ ๕
การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑ จัดฝึกอบรมข้อปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาข้อปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของสถาบัน

ข้อ ๒ เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากรอย่างเหมาะสม โดยจัดร่วมกับการสัมมนาอื่น หรือการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้และสร้างความตระหนักในการใช้ระบบคอมพิวเตอร์อย่างมั่นคงปลอดภัย อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๓ เผยแพร่ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้ใช้และผู้เกี่ยวข้องรับทราบผ่านทางอินเทอร์เน็ต และอินทราเน็ต

หมวดที่ ๖
ความรับผิดชอบของผู้บริหารและผู้ดูแลระบบ

ข้อ ๑ ผู้อำนวยการสถาบันมาตรวิทยาแห่งชาติรับผิดชอบตามประกาศฉบับนี้

ข้อ ๒ ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) รับผิดชอบในการกำกับดูแลให้เป็นไปตามประกาศฉบับนี้

ข้อ ๓ หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ รับผิดชอบควบคุมให้ปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศพร้อมติดตาม และรายงานให้ผู้บังคับบัญชาทราบตามลำดับชั้น

ข้อ ๔ ผู้ดูแลระบบรับผิดชอบเตรียมการจัดหา จัดทำ ปฏิบัติ สรุป และประเมินผลให้เพียงพอและเหมาะสมเพื่อให้เกิดประสิทธิภาพในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และรายงานต่อหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศอย่างเคร่งครัด

ข้อ ๕ หากระบบคอมพิวเตอร์และข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่สถาบันหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

แผนสำรองกรณีฉุกเฉิน

ข้อ ๑ วัตถุประสงค์

๑.๑ เพื่อใช้เป็นคู่มือในการปฏิบัติงานของผู้เกี่ยวข้องเมื่อเกิดเหตุการณ์ที่มีผลให้ระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของสถาบัน เสียหาย ไม่สามารถใช้งานได้ตามปกติ

๑.๒ เพื่อให้ระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของสถาบันมีความปลอดภัย ป้องกันและบรรเทาความเสียหายที่เกิดขึ้นน้อยที่สุด และสามารถกลับมาใช้งานได้โดยเร็วที่สุด

ข้อ ๒ ขอบเขต

ขอบเขตของแผนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ ครอบคลุมการดำเนินงานในทุกขั้นตอนเพื่อให้เครื่องคอมพิวเตอร์ ระบบงานและอุปกรณ์เครือข่ายของสถาบัน สามารถใช้งานได้ตามปกติ

ข้อ ๓ ความหมาย

สถานการณ์ความไม่แน่นอนและภัยพิบัติ หมายถึงเหตุการณ์ที่ก่อให้เกิดความเสียหายกับระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของสถาบัน ซึ่งส่งผลกระทบต่อการทำงานของระบบดังกล่าว ทำให้ไม่สามารถทำงานบางส่วนหรือทั้งหมดได้ อาทิ

๓.๑ ภัยธรรมชาติ ได้แก่ อัคคีภัย อุทกภัย แผ่นดินไหว ความชื้น อุณหภูมิ หรืออื่นๆ

๓.๒ ไวรัสคอมพิวเตอร์

๓.๓ ระบบคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย

๓.๔ การบุกรุกหรือโจมตีจากภายนอก

๓.๕ ระบบกระแสไฟฟ้าขัดข้อง หรือไฟฟ้าดับ

ข้อ ๔ ขั้นตอนการดำเนินการ

๔.๑ การเตรียมความพร้อม

๔.๑.๑ แจ้งให้พนักงานทราบถึงแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ

๔.๑.๒ แจ้งให้พนักงานสำรองข้อมูลคอมพิวเตอร์ที่ใช้ปฏิบัติงานอย่างสม่ำเสมอ

๔.๑.๓ ให้ผู้ดูแลระบบสำรองข้อมูล และฐานข้อมูลบนเครื่องคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นสูญหายหรือถูกทำลาย

๔.๑.๔ ให้ผู้ดูแลระบบตรวจสอบระดับอุณหภูมิ ความชื้น และความผิดปกติภายในศูนย์คอมพิวเตอร์อย่างสม่ำเสมอ หากพบว่ามีความผิดปกติให้รีบแจ้งผู้บังคับบัญชาและดำเนินการแก้ไขปัญหาโดยทันที

๔.๑.๕ ให้พนักงานสำรวจระบบและอุปกรณ์ที่มีอยู่ พร้อมปรับปรุงระเบียนครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ให้ถูกต้องเป็นปัจจุบันอยู่เสมอ

๔.๑.๖ ปรับปรุงแผนผังการเชื่อมโยงระบบเครือข่ายของสถาบันฯให้เป็นปัจจุบัน และติดไว้ภายในศูนย์คอมพิวเตอร์ (Data Center) เพื่อให้ทราบถึงข้อมูลการเชื่อมต่อและลักษณะโครงสร้างของระบบเครือข่าย

๔.๑.๗ สถาบัน ได้ว่าจ้างบริษัทจากภายนอกเพื่อทำการดูแลรักษา เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์คอมพิวเตอร์

๔.๑.๘ มีการติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์แบบอัตโนมัติ และมีการอัพเดทข้อมูลไวรัสแบบอัตโนมัติจากส่วนกลาง

๔.๑.๙ การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์และระบบเครือข่ายโดย

๔.๑.๙.๑ มีการติดตั้งระบบ Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบเครือข่ายภายในของสถาบัน

๔.๑.๙.๒ มีระบบการป้องกันการใช้งานคอมพิวเตอร์ และเครือข่ายภายในโดยไม่ได้รับอนุญาต ซึ่งอุปกรณ์คอมพิวเตอร์ทุกชนิดที่จะขอใช้ร่วมเครือข่ายสถาบัน ต้องรับการลงทะเบียน Mac Address และ IP Address โดยระบบเสียก่อน มิเช่นนั้นจะไม่สามารถใช้งานได้แม้จะเชื่อมต่อเข้าระบบแล้วก็ตาม

๔.๑.๙.๓ มีพนักงานดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์คอยตรวจสอบการใช้งานระบบคอมพิวเตอร์แม่ขายกลาง และระบบอินเตอร์เน็ตตลอดเวลา

๔.๑.๙.๔ การเรียกใช้ระบบสารสนเทศจากส่วนงานต่างๆ ผู้ใช้งานระบบจะได้รับการตรวจสอบ และยืนยันตัวตน (Authentication) ก่อนใช้งาน พร้อมกับมีการบันทึกการใช้งานตลอดเวลา

๔.๑.๑๐ มีระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๔.๑.๑๑ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับภายในศูนย์คอมพิวเตอร์ (Data Center) มีการติดตั้ง UPS และมีระบบจ่ายไฟฟ้าสำรองจากเครื่องกำเนิดกระแสไฟฟ้าของอาคาร (Generator)

๔.๑.๑๒ มีระบบแจ้งเตือนอุณหภูมิ ความชื้นภายในศูนย์คอมพิวเตอร์ (Data Center) ผ่านระบบ SMS ไปยังผู้ดูแลระบบ และผู้ที่เกี่ยวข้องให้รับทราบ เพื่อสามารถแก้ไขปัญหาได้ทัน เมื่อเกิดผิดปกติ

๔.๑.๑๓ มีมาตรการควบคุมการเข้าออกศูนย์คอมพิวเตอร์ (Data Center) (Access Control) โดยห้ามมิให้บุคคลที่ไม่มีหน้าที่เกี่ยวข้องเข้าโดยเด็ดขาด โดยมีเครื่องสแกนลายนิ้วมือ (Finger Print) สำหรับผู้มีสิทธิเท่านั้น หากจำเป็นให้มีพนักงานของกลุ่มงานเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบเป็นผู้ดูแลและรับผิดชอบ พร้อมทั้งบันทึกการเข้าและออกไว้เป็นหลักฐานทุกครั้ง

๔.๑.๑๔ มีกล้องวงจรปิด (CCTV) ติดตั้งเพื่อบันทึกเหตุการณ์บริเวณด้านหน้าและภายในศูนย์คอมพิวเตอร์ (Data Center) ตลอด ๒๔ ชั่วโมง

๔.๑.๑๕ มีระบบป้องกันอัคคีภัยแบบฉีดสารเคมีอัตโนมัติ เมื่อเกิดเพลิงไหม้ โดยมีระบบตรวจจับควัน ติดตั้งภายในศูนย์คอมพิวเตอร์ (Data Center) เพื่อป้องกันเพลิงไหม้อันเกิดความสูญเสียอุปกรณ์และข้อมูลกลางที่สำคัญของสถาบัน

๔.๒ แนวทางการปฏิบัติ

๔.๒.๑ ให้ติดต่อแจ้งเหตุกับผู้ดูแลระบบตลอด ๒๔ ชั่วโมงตามหมายเลขโทรศัพท์ที่แจ้งไว้หรือพนักงานกลุ่มงานเทคโนโลยีสารสนเทศภายในเวลาทำการ

๔.๒.๒ เมื่อรับทราบว่ามีเหตุการณ์เกิดขึ้น ให้ผู้ดูแลระบบสำรวจ ประเมินสถานการณ์ความรุนแรงที่เกิดขึ้นว่าอยู่ในระดับที่ผู้ดูแลระบบสามารถแก้ไขสถานการณ์ได้ด้วยตนเอง หรือต้องประสานงานขอความร่วมมือจากผู้เกี่ยวข้อง แล้วรายงานให้ผู้บังคับบัญชาทราบโดยเร็ว

๔.๒.๓ ในกรณีที่ผู้ดูแลระบบสามารถควบคุม แก้ไข สถานการณ์ได้ด้วยตนเอง เช่นการถูกบุกรุกโจมตีจากภายนอก การแพร่กระจายของไวรัสทางเครือข่าย ให้ดำเนินการดังนี้

๔.๒.๓.๑ แจ้งให้ผู้ใช้ทราบสาเหตุ แนวทาง และกำหนดการแก้ไขปัญหา

๔.๒.๓.๒ ดำเนินการตรวจสอบ ค้นหาสาเหตุ ประเมินสถานการณ์ เร่งแก้ไขปัญหา และทดสอบระบบให้ทำงานได้ตามปกติหากพบว่าเกิดความเสียหายต่อระบบหรือข้อมูลให้กู้จากข้อมูลที่ได้สำรองไว้

๔.๒.๓.๓ สรุปรายงานให้ผู้บังคับบัญชาทราบ

๔.๒.๔ ในกรณีที่ผู้ดูแลระบบไม่สามารถควบคุม แก้ไขสถานการณ์ได้ด้วยตนเอง ให้ดำเนินการดังนี้

๔.๒.๔.๑ หากอุปกรณ์คอมพิวเตอร์ หรือ Software เกิดชำรุดเสียหายไม่สามารถใช้การได้ ให้แจ้งบริษัทผู้รับจ้างฯ มาดำเนินการแก้ไขตามเงื่อนไขที่ระบุไว้ในสัญญา

๔.๒.๔.๒ หากกระแสไฟฟ้าขัดข้อง ให้ผู้ดูแลระบบประสานกับพนักงานอาคารสถานที่ ฝ่ายบริหารงานกลาง และถ้าไฟฟ้าดับเป็นเวลานานเกินกว่าที่เครื่องสำรองไฟฟ้าและเครื่องกำเนิดกระแสไฟฟ้าของอาคาร (Generator) จะจ่ายไฟฟ้าให้ได้ ให้ทำการ Shutdown ระบบคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย และทำการตรวจสอบ ทดสอบการทำงานของระบบและอุปกรณ์ต่างๆ ให้ทำงานได้ตามปกติ เมื่อระบบไฟฟ้าใช้การได้แล้ว

๔.๒.๔.๓ หากระดับอุณหภูมิความร้อนภายในศูนย์คอมพิวเตอร์ (Data Center) อยู่ในระดับที่ไม่หมาะสมให้ทำการตรวจสอบ และแจ้งให้พนักงานอาคารสถานที่ ฝ่ายบริหารงานกลางทราบเพื่อหาทางแก้ไข

๔.๒.๔.๔ หากเกิดอัคคีภัย ให้ผู้ดูแลระบบรายงานผู้บังคับบัญชา และประสานแจ้งไปยังหน่วยงานที่เกี่ยวข้อง ส่วนอาคารสถานที่ ฝ่ายบริหารงานกลางเพื่อร่วมกันแก้ไขปัญหา หากจำเป็นต้องมีการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ออกนอกอาคาร ให้จัดพนักงานควบคุมการดูแลขนย้าย และจัดทำรายการอุปกรณ์คอมพิวเตอร์ หลังจากนั้นให้ดำเนินการสำรวจความเสียหายที่เกิดขึ้น

๔.๒.๔.๕ หากอุปกรณ์ใดสามารถซ่อมแซมแก้ไขได้ ให้เริ่มดำเนินการขออนุมัติซ่อมแซมแก้ไขให้ใช้งานได้โดยเร็วที่สุด

๔.๒.๔.๖ จัดหาอุปกรณ์สำรองมาใช้งานโดยการเช่า หรือจัดซื้อ พร้อมทั้งติดตั้ง กู้คืนระบบ ให้สามารถใช้งานได้จากข้อมูลที่สำรองไว้ก่อนเกิดเหตุ

๔.๒.๕ กรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และระบบที่จำเป็นต้องดำเนินการให้ผู้ปฏิบัติดำเนินการด้วยเอกสารตามวิธีที่กำหนดไว้ตามระบบบริหารคุณภาพ ISO ๙๐๐๑: ๒๐๑๕ ของแต่ละส่วนงาน ทั้งนี้เมื่อระบบสามารถกลับมาใช้ได้ ให้ดำเนินการนำข้อมูลบันทึกเข้าสู่ระบบตามปกติ อย่างครบถ้วนสมบูรณ์พร้อมกับรายงานให้ผู้บังคับบัญชาทราบ

ข้อ ๕ การกำหนดผู้รับผิดชอบ

๕.๑ ผู้อำนวยการสถาบันมาตรวิทยาแห่งชาติ รับผิดชอบตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) สถาบันมาตรวิทยาแห่งชาติ

๕.๒ ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) รับผิดชอบในการกำกับดูแลให้เป็นไปตามแผนนี้

๕.๓ หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ รับผิดชอบควบคุมให้ปฏิบัติตามแผน และรายงานให้ผู้บังคับบัญชาทราบตามลำดับชั้น

๕.๔ ผู้ดูแลระบบรับผิดชอบ เตรียมการจัดหา จัดทำ ปฏิบัติสรุปและประเมินผลให้เพียงพอ และเหมาะสมเพื่อให้เกิดประสิทธิภาพตามแผนและรายงานต่อหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศอย่างเคร่งครัด

ข้อ ๖ รายชื่อเจ้าหน้าที่และเบอร์โทรศัพท์ที่ติดต่อ : สถาบันมาตรวิทยาแห่งชาติ

ผู้ติดต่อ	ตำแหน่ง	โทรศัพท์มือถือ	จดหมายอิเล็กทรอนิกส์	เบอร์โทรศัพท์
พลตำรวจโท พรชัย สุธีรคุณ	ผู้อำนวยการ	-	pornchais@nimt.or.th	๐ ๒๕๗๗ ๕๑๐๐
นายอนุสรณ์ ทนหมื่นไวย	CIO (รองผู้อำนวยการ)	๐๘ ๗๘๓๐ ๗๔๔๔	anusorn@nimt.or.th	๐ ๒๕๗๗ ๕๑๐๐
นางสาวพริมา เกิดอุดม	ผู้จัดการฝ่ายนโยบายและยุทธศาสตร์	๐๘ ๙๑๗๖ ๘๖๗๖	parima@nimt.ot.th	๐ ๒๕๗๗ ๕๑๐๐
นายวโรดม ขวัญเผือก	หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ	๐๘ ๗๘๓๐ ๗๔๔๔	varodome@nimt.or.th	๐ ๒๐๒๖ ๕๔๐๐
นายชูศักดิ์ กอนดี	ผู้ดูแลระบบ	๐๘ ๓๙๗๐ ๓๘๖๑	chusak@nimt.or.th	๐ ๒๐๒๖ ๕๔๐๐

การกำหนดหน้าที่การดำเนินงาน
ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
(IT Security and Policy)

ลำดับ	ประเด็นหัวข้อ	ผู้รับผิดชอบ
๑	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review access rights of the users) - ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบ ทบทวนสิทธิในการใช้งานของผู้ใช้งานให้ถูกต้องเป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง	* Network โดยนายวโรดม ขวัญเผือก * ระบบสอบเทียบ โดยนายธนัญชัย เทศวิรัช * ระบบสารบรรณ ตามประกาศฯ * ระบบลาออนไลน์ โดยนายชูศักดิ์ กอนดี * ระบบ Intranet โดยนายเจนศักดิ์ ยุติธรรม * ระบบ KM โดยนายธนัญชัย เทศวิรัช * ระบบงานฝึกอบรมและสัมมนา โดยนายเจนศักดิ์ ยุติธรรม * Windows โดยนายชัชชัย พงษ์วิเชียร
๒	การบริหารจัดการการเข้าถึงข้อมูลระดับชั้นความลับManagement of access to confidential information) - เจ้าของข้อมูลเป็นผู้กำหนดชั้นความลับของข้อมูลตามระดับความสำคัญ รวมทั้งการให้สิทธิในการเข้าถึงข้อมูลกับผู้ใช้ตามความจำเป็นและความเหมาะสม โดยต้องมีการทบทวนปรับปรุงสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๒ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม	
๓	การควบคุมการเข้าถึงเครือข่าย (Network Access Control) - จัดทำตารางการใช้งาน IP address ภายในระบบเครือข่ายคอมพิวเตอร์ของสถาบัน โดยต้องมีการทบทวนและปรับปรุงตารางดังกล่าวให้เป็นปัจจุบันอยู่เสมอ	นายวโรดม ขวัญเผือก นายยุทธนา ทิพาพงษ์ผกาพันธ์
	- ให้มีการตรวจสอบ Log file เพื่อตรวจสอบความผิดปกติ เช่น การโจมตีใหม่ๆ ในระบบ Firewall อย่างสม่ำเสมอ	นายยุทธนา ทิพาพงษ์ผกาพันธ์
๔	การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชัน และสารสนเทศ (Application And Information Access Control) - ให้ผู้ดูแลระบบตรวจสอบ ควบคุมการเข้าใช้งานของผู้ใช้ที่ได้รับสิทธิในการเข้าถึงข้อมูลแต่ละประเภท โดยให้มีการใช้สิทธิตามที่ได้รับโดย เฉพาะการเข้าถึงข้อมูลลับตามระดับชั้นความลับ รวมถึงระบบที่สำคัญสูงได้แก่ ระบบบริการสอบเทียบ ระบบบัญชีการเงินและระบบบุคคล ซึ่งถูกควบคุมสิ่งแวดล้อมภายในศูนย์คอมพิวเตอร์ (Data Center)	* ระบบ Intranet * ระบบ KM * ระบบงานฝึกอบรม และสัมมนา * ระบบสอบเทียบ * ระบบสารบรรณ ตามประกาศฯ * ระบบลาออนไลน์

ลำดับ	ประเด็นหัวข้อ	ผู้รับผิดชอบ
๕	การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control) - ผู้ดูแลระบบแม่ข่าย กำกับดูแล บำรุงรักษาเครื่องคอมพิวเตอร์ แม่ข่าย (Server) ให้มีการตรวจสอบทรัพยากรบนเครื่องคอมพิวเตอร์แม่ข่ายของระบบที่สำคัญอย่างสม่ำเสมอ	* Network โดยนายวโรดม ขวัญเผือก * Linux (web and app server) โดยนายชูศักดิ์ กอนดี * Windows โดยนายชัชชัย พงษ์วิเชียร
๖	การจัดทำระบบสำรองข้อมูล (The preparation of a backup system) - จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบภายในระยะเวลาที่เหมาะสมและจัดให้มีการทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ ๑ ครั้ง	นายชูศักดิ์ กอนดี นายวโรดม ขวัญเผือก นายชัชชัย พงษ์วิเชียร
	- ต้องนำผลที่ได้จากการทำสอบกู้คืนข้อมูลมาวิเคราะห์เพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง	* ซ้อม DR Site โดยนายชูศักดิ์ กอนดี
๗	การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศ (Monitoring and risk assessment, security information systems) - มีการดำเนินการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศโดยการประเมินตนเอง ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากหน่วยงานภายนอก อย่างน้อยปีละ ๑ ครั้ง	กทส./ ผตส.
๘	การสร้างความตระหนักในเรื่องการรักษาความมั่น คงปลอดภัยด้านสารสนเทศ (Raising awareness about information security) - จัดฝึกอบรมข้อปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาข้อปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของสถาบัน - เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากรอย่างเหมาะสมโดยจัดร่วมกับการสัมมนาอื่นหรือการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้ และสร้างความตระหนักในการใช้ระบบคอมพิวเตอร์อย่างมั่นคงปลอดภัยอย่างน้อยปีละ ๑ ครั้ง	ผมว. / CIO / หน.กทส. / กบค.

แผนฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๑. บทนำ

สถาบันมาตรวิทยาแห่งชาติได้ดำเนินการจัดทำแผนฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เป็นกรอบในการดำเนินงานให้สอดคล้องกับพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔- ๒๕๖๒ เพื่อให้สถาบันมีความพร้อมที่จะแก้ไขสถานการณ์วิกฤต ซึ่งเป็นสภาพที่ทำให้การดำเนินงาน หรือการให้บริการของสถาบันจะต้องหยุดชะงัก หรือไม่สามารถดำเนินงานได้ตามปกติ หรือไม่เป็นไปตามเป้าหมายที่กำหนดไว้

๒. วัตถุประสงค์

๒.๑ เพื่อใช้เป็นแนวทางในการบริหารความต่อเนื่อง

๒.๒ เพื่อให้สถาบันมีการเตรียมการรับมือกับสภาวะวิกฤต หรือเหตุการณ์ฉุกเฉินต่างๆ ที่อาจเกิดขึ้น

๒.๓ เพื่อลดผลกระทบจากการหยุดชะงักในการดำเนินงาน หรือการให้บริการ

๒.๔ เพื่อบรรเทาความเสียหายให้อยู่ระดับที่ยอมรับได้

๒.๕ เพื่อให้เจ้าหน้าที่ผู้มีส่วนได้ส่วนเสีย และประชาชนมีความเชื่อมั่นในศักยภาพของสถาบันแม้ต้องเผชิญกับเหตุการณ์สภาวะวิกฤต อันอาจส่งผลกระทบทำให้การดำเนินงานต้องหยุดชะงัก

๓. เกณฑ์การเรียกใช้แผนฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ข้อกำหนดในการเรียกใช้แผนกรณีระบบสำรองทำงานไม่ได้ ไม่มีไฟฟ้าเป็นเวลานานเกินกว่า ๑๕ วันต่อเนื่อง หรือเกิดภัยคุกคามอื่นที่ต้องหยุดใช้งานระบบคอมพิวเตอร์ หรือระบบเครือข่ายเทคโนโลยีสารสนเทศที่ทำให้การทำงานหยุดชะงักนานกว่า ๑๕ วันอย่างต่อเนื่อง

๔. แผนรองรับการทำงานในแต่ละด้าน

๔.๑ การให้บริการฝึกอบรม รับบริการด้วยการบันทึกชื่อและช่องทางการสื่อสารต่าง ๆ ลงสมุดไว้จนกว่าระบบจะกลับมาทำงานได้ตามปกติจึงติดต่อกลับไปภายหลัง

๔.๒ การให้บริการสอบเทียบเครื่องมือ รับบริการด้วยการบันทึกชื่อและช่องทางการสื่อสารต่าง ๆ ลงสมุดไว้จนกว่าระบบจะกลับมาทำงานได้ตามปกติจึงติดต่อกลับไปภายหลัง

๔.๓ การปฏิบัติงานด้านบริหารงานบุคคล บันทึกรายการต่างๆ ลงสมุดไว้จนกว่าระบบจะกลับมาทำงานได้ตามปกติ จึงบันทึกข้อมูลเหล่านั้นเข้าสู่ระบบ

๔.๔ การปฏิบัติงานด้านบัญชี บันทึกรายการต่างๆ ลงสมุดไว้จนกว่าระบบจะกลับมาทำงานได้ตามปกติ จึงบันทึกข้อมูลเหล่านั้นเข้าสู่ระบบ ในกรณีเป็นการติดต่อจากภายนอก ให้จดบันทึกชื่อและช่องทางการสื่อสารต่างๆ ลงสมุดไว้จนกว่าระบบจะกลับมาทำงานได้ตามปกติจึงติดต่อกลับไปภายหลัง

๔.๕ การปฏิบัติงานจัดซื้อ บันทึกรายการต่าง ๆ ลงสมุดไว้จนกว่าระบบจะกลับมาทำงานได้ตามปกติ จึงบันทึกข้อมูลเหล่านั้นเข้าสู่ระบบ ในกรณีเป็นการติดต่อจากภายนอก ให้จดบันทึกชื่อและช่องทางการสื่อสารต่าง ๆ ลงสมุดไว้จนกว่าระบบจะกลับมาทำงานได้ตามปกติจึงติดต่อกลับไปภายหลัง

๔.๖ การปฏิบัติงานระบบบริหารอาคารสถานที่ บันทึกรายการต่างๆ ลงสมุดไว้จนกว่าระบบจะกลับมาทำงานได้ตามปกติ จึงบันทึกข้อมูลเหล่านั้นเข้าสู่ระบบ

๔.๗ ระบบอื่นๆ เป็นไปตามประกาศ หรือแนวทางที่คณะทำงานบริหารจัดการในกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ จะเป็นผู้กำหนดวิธีการทำงาน

๕. การอนุมัติใช้งาน

ผู้อำนวยการสถาบันมาตรวิทยาแห่งชาติ เป็นผู้สั่งการเรียกใช้แผนฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๖. คณะทำงานบริหารจัดการในกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ในกรณีเกิดเหตุการณ์ตามเกณฑ์การเรียกใช้แผนฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์นานเกิน ๑ วันโดยไม่มีคำสั่งการใดๆ ให้มีคณะทำงานประกอบไปด้วย ผู้อำนวยการสถาบัน รองผู้อำนวยการ CIO ผู้ช่วยผู้อำนวยการ หัวหน้าฝ่าย และผู้จัดการฝ่าย หรือผู้บริหารในลำดับรอง ๆ ลงมารวมกัน ๓ ท่านขึ้นไป หารือเพื่อกำหนดแนวทางการทำงานที่นอกเหนือไปจากแนวทางที่กำหนดไว้

แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

สถาบันมาตรวิทยาแห่งชาติ (มว.) ตระหนักถึงความปลอดภัยของข้อมูลส่วนบุคคลและการรักษาข้อมูลส่วนบุคคลของผู้ใช้บริการที่ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ผ่านเว็บไซต์สถาบัน http://www.nimt.or.th หรือแบบฟอร์มต่างๆ ของทางสถาบันเพื่อคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการไว้อย่างมั่นคงปลอดภัย และปิดเป็นความลับ

๑. วัตถุประสงค์ของแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

๑.๑ เพื่อใช้บังคับกับพนักงานของสถาบันและลูกจ้าง ที่มีหน้าที่รับผิดชอบหรือได้รับอนุญาตในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยการรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลส่วนบุคคลของผู้ใช้บริการนั้น ต้องปฏิบัติให้เป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลในการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ของ มว.

๑.๒ ในกรณีที่สถาบันทำการเปลี่ยนแปลงวัตถุประสงค์การคุ้มครองข้อมูลส่วนบุคคลจะแจ้งล่วงหน้าไปยังเจ้าของข้อมูลผู้ใช้บริการให้ทราบก่อน ๓๐ วัน ผ่านทางเว็บไซต์ของ มว. หรือทางจดหมายอิเล็กทรอนิกส์ เว้นแต่มีกฎหมายกำหนดไว้เป็นอย่างอื่น

๒. การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคลของผู้ใช้บริการ

สถาบันมีการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ทั้งทางเว็บไซต์ http://www.nimt.or.th และกระดาษแบบฟอร์มต่างๆ ตามที่สถาบันกำหนด แล้วนำมาแปลงเป็นข้อมูลอิเล็กทรอนิกส์ หรือจัดเก็บโดยวิธีอื่น

๒.๑ การติดต่อผู้ใช้บริการสามารถแจ้งความประสงค์มายังสถาบันผ่านทางโทรศัพท์ โทรสาร หรือทางจดหมายอิเล็กทรอนิกส์ ได้

๒.๒ การใช้คุกกี้ (Cookies) หมายถึง ไฟล์ข้อมูลขนาดเล็กที่จะถูกส่งไปเก็บไว้ยังโปรแกรมค้นดูเว็บของผู้ใช้บริการ เพื่อเก็บข้อมูลที่ผู้ใช้บริการเข้าเยี่ยมชมไว้ เมื่อผู้ใช้บริการมีการเข้าไปเยี่ยมชมเว็บไซต์ต่าง ๆ อีกครั้งในภายหลัง โปรแกรมจะจดจำได้ว่า ผู้ใช้บริการเคยเข้าเยี่ยมชมแล้ว จนกว่าผู้ใช้บริการจะออกจากโปรแกรมหรือจนกว่าผู้ใช้บริการจะลบคุกกี้นั้น หรือไม่อนุญาตให้คุกกี้นั้นทำงานอีกต่อไป

๒.๓ การเก็บข้อมูลสถิติการให้บริการผ่านทางเว็บไซต์สถาบัน จะไม่มีการเก็บรวบรวมข้อมูลสถิติ ที่สามารถเชื่อมโยงกับข้อมูลที่เกี่ยวข้องกับฐานข้อมูลประชากรที่สามารถระบุตัวตนได้

๒.๔ บันทึกผู้เข้าชมเว็บไซต์ (Log Files) หมายถึง ไฟล์ข้อมูลจราจรคอมพิวเตอร์ เป็นข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ แสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ การใช้บริการของผ่านเว็บไซต์ http://www.nimt.or.th มีการเก็บบันทึกข้อมูลการเข้าออกและระหว่างในการเข้าใช้บริการของผู้ใช้บริการโดยอัตโนมัติที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลที่ระบุตัวบุคคลได้ เช่น หมายเลขไอพี (IP Address) ซึ่งใช้เป็นข้อมูลที่เชื่อมโยงกลับไปที่ข้อมูลการเชื่อมต่ออินเตอร์เน็ต ซึ่งอาจระบุถึงแหล่งที่มาในการ

โพสต์หรือบุคคลที่โพสต์ได้ รวมถึงเว็บไซต์ที่ เข้าและออกทั้งก่อนและหลัง และประเภทของโปรแกรมบราวเซอร์ (Browser)

๒.๕ การจัดเก็บผ่านทางเว็บไซต์ว่าเป็นข้อมูลที่ผู้ใช้บริการมีสิทธิเลือกว่าจะให้หรือไม่ให้ก็ได้ อย่างไรก็ตามในการให้ บริการผู้ใช้บริการต้องให้ข้อมูลที่จำเป็นต่อการประมวลผลและการดำเนินการตามคำขอ โดยจะระบุด้วยอักษรสีแดง หรือกำกับด้วยเครื่องหมายดอกจัน (*) และในส่วนของข้อมูลที่ผู้ใช้บริการมีสิทธิเลือกว่าจะให้ หรือไม่ให้ ก็ได้ ในกรณีที่ผู้ใช้บริการไม่ประสงค์จะให้ข้อมูลนั้นผ่านเว็บไซต์ ผู้ใช้บริการสามารถติดต่อกับพนักงานสถาบันโดยผ่านช่องทางอื่น ๆ ได้ เช่น จดหมายอิเล็กทรอนิกส์ โทรศัพท์ โทรสาร หรือเข้ามาติดต่อในสถานที่ทำการของสถาบัน เป็นต้น

๓. การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือสถาบันอื่น

เว็บไซต์ของสถาบัน จะไม่มีการเชื่อมโยงฐานข้อมูลส่วนบุคคลให้กับหน่วยงานหรือสถาบันอื่นใด

๔. การรวมข้อมูลจากที่มาหลาย ๆ แห่ง

จะไม่มีการนำข้อมูลส่วนบุคคลที่ได้รับมาจากผู้ใช้บริการผ่านทางเว็บไซต์ไปรวมกับข้อมูลที่ได้รับมาจากแหล่งที่มาอื่น ๆ

๕. การให้บุคคลอื่นใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล

จะไม่มีการอนุญาตให้บุคคลอื่นเข้าถึง หรือใช้ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมมาจากผู้ใช้บริการ เว้นแต่เป็นการอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายให้กระทำได้

๖. การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ ภายใต้วัตถุประสงค์ในการเก็บรวบรวม ดังนี้

๖.๑ ในการเก็บรวบรวมจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลผู้ใช้บริการ โดยผู้ขอใช้บริการมีสิทธิที่จะให้หรือไม่ให้ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น

๖.๒ ในการรวบรวม จัดเก็บข้อมูลส่วนบุคคลจะไม่จัดเก็บข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม เว้นแต่มีกฎหมายกำหนดให้กระทำได้ หรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

๖.๓ ในการใช้และการเปิดเผยข้อมูลของผู้ใช้บริการ จะขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน เว้นแต่เพื่อป้องกัน หรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล หรือเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลและเป็นกรณีที่ไม่สามารถขอความยินยอมในขณะนั้นได้ หรือเป็นการปฏิบัติตามสัญญาที่ทำระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล หรือเป็นการปฏิบัติตามกฎหมาย

๗. การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน

ผู้ใช้บริการมีสิทธิในการเข้าถึงและขอทำการแก้ไข หรือปรับปรุงข้อมูลส่วนบุคคลของต้นให้ถูกต้องเป็นปัจจุบัน และสมบูรณ์ได้ โดยกระทำผ่านทางเว็บไซด์ www.nimt.or.th

๘. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ได้กำหนดมาตรการ ดังต่อไปนี้

๘.๑ การกำหนดสิทธิและจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้บริการซึ่งเป็นบุคลากรของสถาบันในแต่ละระดับไว้อย่างชัดเจน และกำหนดให้มีการบันทึก รวมทั้งการสำรองข้อมูลในการเข้าถึงหรือการเข้าใช้งานข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด

๘.๒ กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์ หรือระบบสารสนเทศทั้งหมดของสถาบันที่มีการรวบรวม จัดเก็บ ใช้ ข้อมูลส่วนบุคคล

๘.๓ กำหนดมาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญ หรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชน หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลไว้อย่างชัดเจน เช่น หมายเลขบัตรเดบิตหรือบัตรเครดิต หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวบุคคล เชื้อชาติ ศาสนา เป็นต้น

๙. ผู้ใช้บริการสามารถติดต่อได้ผ่านทางเว็บไซด์ www.nimt.or.th หรือสถาบันมาตรวิทยาแห่งชาติ
ที่ตั้ง: เลขที่ ๓/๔-๕ ตำบลคลองห้า อำเภอคลองหลวง จังหวัดปทุมธานี ๑๒๑๒๐ โทรศัพท์: ๐ ๒๕๗๗ ๕๑๐๐

ข้อกำหนดการจัดการ ทำลายข้อมูล และสื่อบันทึกข้อมูลด้านสารสนเทศ

๑. วัตถุประสงค์

เพื่อให้การจัดการ ทำลายข้อมูลที่จัดเก็บอยู่บนสื่อบันทึกเป็นไปอย่างถูกต้อง ปกป้องไม่ให้ข้อมูลเกิดการรั่วไหล ที่ทำให้เกิดความเสียหาย

๒. คำนิยามศัพท์

๒.๑ ข้อมูล หมายถึง สิ่งที่สื่อความหมายให้รู้ถึงเรื่องราว ข้อเท็จจริง หรือสิ่งใดๆ ไม่ว่าการสื่อสารความหมายนั้น ไม่ว่าจะจัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน การบันทึกภาพหรือเสียง หรือวิธีการอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

๒.๒ Hard Disk หมายถึง อุปกรณ์ที่ใช้เก็บข้อมูลรูปแบบอิเล็กทรอนิกส์

๓. หน้าที่ความรับผิดชอบ

เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ ฝ่ายนโยบายและยุทธศาสตร์ (กทส.ฝน.) มีหน้าที่กำกับดูแล ป้องกัน และดำเนินการทำลายข้อมูลบนสื่อบันทึกข้อมูลด้านสารสนเทศ

๔. ขั้นตอนการทำงาน

๔.๑ การปกป้องข้อมูลขององค์กร

๔.๑.๑ กทส.ฝน. และผู้ใช้งานจะต้องปฏิบัติตามระเบียบนโยบาย

๔.๑.๒ ในกรณีต้องนำเครื่องคอมพิวเตอร์ ออกไปดำเนินการซ่อมบำรุงรักษา หรืออื่นๆ ภายนอก กทส.ฝน. จะต้องทำการถอด Hard Disk ออกก่อน และจัดเก็บในที่ปลอดภัย

๔.๑.๓ เมื่อต้องทำลายข้อมูล กทส.ฝน. จะต้องจัดทำเอกสารขออนุมัติทำลายสื่อบันทึกข้อมูลที่หมดอายุ เสื่อมสภาพเพื่อขออนุมัติทำลายข้อมูลด้านสารสนเทศ และได้รับการอนุมัติจากเจ้าของข้อมูล หรือผู้มีอำนาจก่อนทุกครั้ง

๔.๒ การทำลายข้อมูลขององค์กร

๔.๒.๑ อุปกรณ์สื่อบันทึกข้อมูลที่ยกเลิกการใช้งานแล้ว และถูกตัดออกจากระบบทรัพย์สินแล้ว เนื่องจากมีอายุการใช้งานค่อนข้างมาก เกินที่กำหนดไว้ เช่น มากกว่า ๕ ปี กทส.ฝน. จะต้องตรวจเช็คสภาพและทดสอบการใช้งานของ โดยการสุ่มเปิด Hard Disk Drive ของเครื่องคอมพิวเตอร์นั้น เพื่อกำหนดวิธีการทำลายต่อไป

๔.๒.๒.๑ กรณีพบว่า สื่อบันทึกข้อมูลยังสามารถใช้งานได้

(๑) เตรียมการลบทำลายข้อมูลที่อยู่ในสื่อบันทึกข้อมูลที่ต้องการ ด้วยโปรแกรม PC Disk Eraser หรือ โปรแกรม Seagate Disc Wizard โดย Boot จากแผ่นโปรแกรมที่เตรียมไว้

(๒) สุ่มทดสอบข้อมูล เพื่อให้แน่ชัดว่าไม่สามารถกู้คืนข้อมูลกลับมาได้ แล้วนำไปจัดเก็บ เพื่อรอการจำหน่ายหรือบริจาค หรือทำลาย

๔.๒.๒.๒ กรณีพบว่า สื่อบันทึกข้อมูลที่ชำรุด เสื่อมสภาพ หรือใช้งานไม่ได้แล้ว

(๑) ทำลายสื่อบันทึกโดยการใช้อุปกรณ์ทำลาย เช่น ค้อนทุบ เจาะด้วยสว่าน กระดาษทรายขัด หรือหักทำลาย เพื่อนำไปทิ้ง

(๒) ถ่ายภาพอุปกรณ์สื่อบันทึกเก็บไว้เป็นหลักฐานการดำเนินงาน

(๓) บันทึกผลการทำลายอุปกรณ์สื่อบันทึกข้อมูล จัดทำรายงานส่งให้ผู้บังคับบัญชารับทราบ