ประกาศกรมอุตุนิยมวิทยา

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุตุนิยมวิทยา พ.ศ. 2558

โดยที่มาตรา 5 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ซึ่งออกโดยอาศัยอำนาจตามความในมาตรา 35 วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2544 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษรและทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอนั้น อธิบดีกรมอุตุนิยมวิทยาโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศดังต่อไปนี้

ข้อ 1 ประกาศนี้เรียกว่า "ประกาศกรมอุตุนิยมวิทยา เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุตุนิยมวิทยา พ.ศ. 2558"

ข้อ 2 ประกาศนี้ให้มีผลบังคับใช้ตั้งแต่บัดนี้เป็นต้นไป

ข้อ 3 ในประกาศนี้

กรม หมายถึง กรมอุตุนิยมวิทยา กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมอุตุนิยมวิทยา

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยา

ผู้ใช้งาน หมายถึง ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับผิดชอบ ผู้ใช้งานทั่วไป หน่วยงานภายนอก

ผู้บริหารระดับสูงสุด หมายถึง อธิบดีกรมอุตุนิยมวิทยา

ผู้บริหารด้านเทคโนโลยีสารสนเทศ หมายถึง อธิบดีกรมอุตุนิยมวิทยา หรือ ผู้ที่อธิบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของกรมอุตุนิยมวิทยา

/ผู้ดูแลระบบ .....

ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการข้อมูลและเครือข่ายคอมพิวเตอร์

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่กรมอุตุนิยมวิทยาอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของกรมอุตุนิยมวิทยา โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลอัตโนมัติ

ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของกรมอุตุนิยมวิทยา

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของกรมอุตุนิยมวิทยาที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง พื้นที่ที่กรมอุตุนิยมวิทยาอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

- พื้นที่ทำงานทั่วไป หมายถึง พื้นที่ที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
- พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย
- พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์
- พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นสูญหาย

/สินทรัพย์ .....

สินทรัพย์ (Asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

การสำรองข้อมูล (Backup) หมายถึง การสำเนาข้อมูลต่าง ๆ เก็บไว้ในอีกหน่วยความจำหนึ่ง (Media or Storage) เพื่อเป็นการป้องกันเมื่อเกิดความเสียหายของระบบคอมพิวเตอร์หรือของข้อมูลในหน่วยความจำที่ใช้งานอยู่

การกู้คืนข้อมูล (Data recovery) หมายถึง การฟื้นคืนสภาพข้อมูลที่ได้รับความเสียหายในระบบคอมพิวเตอร์ให้สามารถใช้งานได้จากสื่อบันทึกที่สำรองข้อมูลไว้ เช่นฐานข้อมูล ระบบงานคอมพิวเตอร์ เป็นต้น

จดหมายอิเล็กทรอนิกส์ (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อมูลข้อความระหว่างกันโดยใช้มาตรฐานการรับส่ง เช่น SMTP,POP3 และ IMAP เป็นต้น ผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน โดยผู้ส่งสามารถส่งไปยังผู้รับคนเดียวหรือหลายคนก็ได้

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ ในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

บัญชีผู้ใช้บริการ (Account) หมายถึง รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของหน่วยงาน

ชื่อเครื่องคอมพิวเตอร์ (Computer Name) หมายถึง ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

สื่อบันทึกพกพา หมายถึง สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น

โปรแกรมประสงค์ร้าย (Malware) หมายถึง โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือ สปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

การตั้งค่าระบบ (Configuration) หมายถึง ค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

เลขที่อยู่ไอพี (IP Address) หมายถึง ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย (IPv4 หรือ IPv6) ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน

/เลขที่อยู่ไอพีสาธารณะ .....

เลขที่อยู่ไอพีสาธารณะ (Public IP Address) หมายถึง เลขที่อยู่ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงาน หรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากัน หรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

แบนด์วิดท์ (Bandwidth) หมายถึง ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

ชื่อผู้ใช้ (Username) หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

ลงบันทึกเข้า (Login) หมายถึง กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

ลงบันทึกออก (Logout) หมายถึง กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

อัพเดท (Update) หมายถึง ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่าง ๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

ช่องโหว่ (Vulnerability) หมายถึง ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

การเข้ารหัส (Encryption) หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

อุปกรณ์กระจายสัญญาณ (Access Point) หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

SSID (Service Set Identifier) หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

WEP (Wired Equivalent Privacy) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

WPA (Wi-Fi Protected Access) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)

/ไฟร์วอลล์ .....

ไฟร์วอลล์ (Firewall) หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

IDS (Intrusion Detection System) หรือระบบตรวจจับการบุกรุก หมายถึง ระบบตรวจจับการบุกรุกของผู้ไม่ประสงค์ดีใช้วิเคราะห์และแจ้งเตือนหากข้อมูลที่ผ่านเข้า-ออกเครือข่ายมีลักษณะการทำงานที่เป็นความเสี่ยงต่อเครือข่าย

IPS (Intrusion Prevention System) หรือระบบตรวจสอบและโต้ตอบการบุกรุก หมายถึง ระบบที่มีลักษณะเช่นเดียวกับระบบ IDS แต่สามารถป้องกันข้อมูล ไม่ให้เข้ามาในเครือข่ายได้หากตรวจพบข้อมูลที่มีลักษณะที่เป็นความเสี่ยงต่อเครือข่าย

VPN (Virtual Private Network) หมายถึง เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

อุปกรณ์จัดเส้นทาง (Router) หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

อุปกรณ์เครือข่าย (Network Device) หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ-ส่งข้อมูลหรือควบคุมตรวจสอบการรับ-ส่งข้อมูล เช่น Switch, Router, Firewall หรือ IPS เป็นต้น

การพิสูจน์ยืนยันตัวตน (Authentication) หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

แผนผังระบบเครือข่าย (Network Diagram) หมายถึง แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

ข้อมูลจราจรทางคอมพิวเตอร์ หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิดต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการหรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

สิทธิ์ของผู้ใช้งาน หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาตการกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

/ความมั่นคงปลอดภัย.....

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

ข้อ 4 องค์ประกอบของนโยบาย

ส่วนที่ 1 การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์ เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันในการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์ อุปกรณ์เครือข่ายและระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของระบบเทคโนโลยีสารสนเทศและข้อมูล โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งาน ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและสื่อสารของกรมอุตุนิยมวิทยา

ส่วนที่ 2 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยา และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกและโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาได้อย่างถูกต้อง

ส่วนที่ 3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงาน เข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิ์ในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาได้อย่างถูกต้อง

ส่วนที่ 4 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อควบคุมและกำหนดมาตรการการปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมาย ที่เกี่ยวข้องกับข้อมูลสารสนเทศและบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมอุตุนิยมวิทยา เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

/ส่วนที่ 5 การควบคุม.....

ส่วนที่ 5 การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของกรมอุตุนิยมวิทยา โดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่ายในลักษณะแบบ VLAN

ส่วนที่ 6 การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงาน ให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

ส่วนที่ 7 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศของกรม และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกและโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบ ติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาได้อย่างถูกต้อง

ส่วนที่ 8 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของกรม โดยการกำหนดสิทธิของผู้ใช้ ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

ส่วนที่ 9 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อป้องกันความเสี่ยงต่อการเข้าถึงข้อมูล การถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาตจากการใช้บริการจากหน่วยงานภายนอก และเพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม เป็นไปอย่างมั่นคงปลอดภัย ให้กำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก

ส่วนที่ 10 ความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเตอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่น อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของกรมอุตุนิยมวิทยา ถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

ส่วนที่ 11 การสำรองและกู้คืนข้อมูล เพื่อกำหนดข้อปฏิบัติการสำรองข้อมูลและการกู้คืนระบบ (Backup and Recovery) โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่าย สามารถดำเนินการสำรองข้อมูลได้อย่างสมบูรณ์ ถูกต้อง และสามารถกู้คืนระบบได้ในกรณีที่จำเป็น

/ส่วนที่ 12 การใช้งาน.....

ส่วนที่ 12 การใช้งานจดหมายอิเล็กทรอนิกส์ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยา สามารถสนับสนุนการปฏิบัติงานและการบริหารงานของกรมอุตุนิยมวิทยาเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพและประสิทธิผล และเพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของกรมอุตุนิยมวิทยาและหน่วยงานเป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับของกรมอุตุนิยมวิทยา

ส่วนที่ 13 ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยา สามารถสนับสนุนการปฏิบัติงานของกรมอุตุนิยมวิทยา เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ และเพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยระบบจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของกรมอุตุนิยมวิทยาและหน่วยงานเป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของกรมอุตุนิยมวิทยาอุตุนิยมวิทยา

ส่วนที่ 14 การตรวจสอบและประเมินความเสี่ยง เพื่อให้มีมาตรการในการตรวจสอบประเมิน ควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร และป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ 15 การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

ข้อ 5 ตรวจสอบและประเมินความเสี่ยง จะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) อย่างน้อยปีละ 1 ครั้ง เพื่อให้ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

ข้อ 6 การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน โดยจัดอบรมให้ความรู้เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ รวมทั้งมาตรการการเข้าถึงจากผู้ซึ่งไม่ได้รับการอนุญาต

ข้อ 7 การกำหนดชั้นความลับของสารสนเทศให้เป็นไปตาม พ.ร.บ.ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 หรือข้อกำหนดอื่น ๆ ที่ได้ประกาศใช้ทดแทน

/ข้อ 8 กรณีระบบคอม.....

ข้อ 8 กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ ได้แก่ องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงสุดของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ 9 ให้สำนักสื่อสารและเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุตุนิยมวิทยา อย่างน้อยปีละ 1 ครั้ง

ข้อ 10 จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมฉุกเฉินในกรณีไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

ข้อ 11 รายละเอียดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุตุนิยมวิทยา ให้เป็นไปตามเอกสารแนบท้ายประกาศนี้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๙ กุมภาพันธ์ พ.ศ. 2559

(นายวันชัย ศักดิ์อุดมไชย)
อธิบดีกรมอุตุนิยมวิทยา

เอกสารแนบท้ายประกาศ
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๑
การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์
(Computing System Control Room Policy)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันในการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์อุปกรณ์เครือข่ายและระบบเทคโนโลยีสารสนเทศโดยพิจารณาตามความสำคัญของระบบเทคโนโลยีสารสนเทศข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับโดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งาน ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยา

๒. ผู้รับผิดชอบ

สำนักสื่อสารและเทคโนโลยีสารสนเทศ

๓. การควบคุมการเข้าออก

๓.๑. ต้องจำแนกและกำหนดพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่ายอุปกรณ์เครือข่ายระบบเทคโนโลยีสารสนเทศต่างๆ ในกรมอุตุนิยมวิทยาอย่างเหมาะสมโดยจัดทำเป็นเอกสาร“การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆที่อาจเกิดขึ้นได้

๓.๒ กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจนรวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน ในการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General working area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) เป็นต้น

๓.๓ ต้องกำหนดสิทธิ์ให้กับเจ้าหน้าที่ให้สามารถมีสิทธิ์ในการเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายประกอบด้วย

- ๓.๓.๑ จัดทำ “ทะเบียนผู้มีสิทธิ์เข้า-ออกพื้นที่” เพื่อปฏิบัติหน้าที่ตามสิทธิ์และหน้าที่ที่ได้รับมอบหมาย
- ๓.๓.๒ มีการบันทึกการเข้า-ออกโดยจัดทำเป็นเอกสาร“บันทึกการเข้า-ออกพื้นที่” และกำหนดผู้มีหน้าที่รับผิดชอบตรวจสอบการบันทึกดังกล่าว
- ๓.๓.๓ จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำและให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้า-ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารปีละ ๑ ครั้งเป็นอย่างน้อย

๓.๔ บุคคลภายนอกเข้ามาติดต่อจะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้า-ออกให้ถูกต้องและจะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา

๓.๕ บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

๔. ข้อปฏิบัติสำหรับผู้ติดต่อที่มาจากหน่วยงานภายนอก

๔.๑ ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร“บันทึกการเข้า-ออกพื้นที่”

๔.๒ ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในกรมอุตุนิยมวิทยามาปฏิบัติงานที่ห้องควบคุมระบบเครือข่ายต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการข้ออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร“บันทึกการเข้า-ออกพื้นที่”ให้ถูกต้องชัดเจน

๔.๓ เจ้าหน้าที่/ผู้ดูแลระบบต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเป็นประจำทุกเดือน

ส่วนที่ ๒
การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
(Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกและโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

ศูนย์เทคโนโลยีสารสนเทศ
ผู้ดูแลระบบที่ได้รับมอบหมาย
เจ้าของข้อมูล

๓. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

๓.๑ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๓.๒ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓.๓ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

๓.๔ ผู้ดูแลระบบต้องจัดให้มีระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

๓.๕ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆและการผ่านเข้าออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๔. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๔.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งาน สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น และการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ที่ได้รับอนุญาต

๔.๒ เจ้าของข้อมูลและเจ้าของระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้นเนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๔.๓ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๔.๔ การขอสิทธิ์ในการเข้าสู่ระบบจะต้องมีการทำเป็นเอกสารและมีการลงนามอนุมัติเอกสารดังกล่าวและต้องมีการจัดเก็บไว้เป็นหลักฐานด้วย

๕. ข้อกำหนดเกี่ยวกับประเภทข้อมูลลำดับชั้นความลับของข้อมูล

๕.๑ ประเภทข้อมูล

๑) ข้อมูลการพยากรณ์อากาศ ข้อมูลทั่วไป เข้าถึงได้ ๒๔. ช.ม. ผ่านเว็บไซต์

๒) ข้อมูลระบบงานสารบรรณข้อมูลภายใน เข้าถึงได้ ๒๔. ช.ม. ผ่านระบบงาน กำหนดสิทธิการเข้าถึง

๓) ข้อมูลระบบงานบุคลากร ข้อมูลส่วนบุคคลไม่เปิดเผย เข้าถึงได้ ๒๔. ช.ม. ผ่านระบบงาน กำหนดสิทธิการเข้าถึง

๔) ข้อมูลเว็บไซต์ของกรมอุตุนิยมวิทยาข้อมูลทั่วไป เข้าถึงได้ ๒๔. ช.ม. ผ่านเว็บไซต์

๕) ข้อมูลเว็บไซต์ภายในของกรมอุตุนิยมวิทยาข้อมูลทั่วไป เข้าถึงได้ ๒๔. ช.ม. ผ่านเว็บไซต์

๖) ฐานข้อมูลภูมิอากาศ ข้อมูลภายใน เข้าถึงได้ตามสิทธิ ผ่านระบบงาน

๗) ข้อมูลการส่งข่าวอัตโนมัติผ่านเครือข่าย ข้อมูลทั่วไป เข้าถึงได้ ๒๔. ช.ม. ผ่านเครือข่าย

๘) ข้อมูลเครือข่ายอุตุท้องถิ่นข้อมูลภายใน เข้าถึงผ่านระบบงาน

๙) ข้อมูลระบบ Web Portal เพื่อสนับสนุนการพยากรณ์อากาศข้อมูลทั่วไป เข้าถึงได้ ๒๔. ช.ม. ผ่านเว็บไซต์

๕.๒ การลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการพ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบถือว่าเป็นแนวทางที่เหมาะสมที่ในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

๕.๒.๑ การกำหนดชั้นความลับตามความสำคัญของข้อมูลในเอกสารกำหนดไว้ ๓ ระดับ ได้แก่ลับลับมากลับที่สุดและมีการกำหนดความรับผิดชอบให้แก่ผู้มีอำนาจกำหนดชั้นความลับเป็นผู้พิจารณากำหนดระดับชั้นความลับของเอกสารและการยกเลิกหรือปรับระดับชั้นความลับของเอกสารตามความจำเป็น

๕.๒.๒ การควบคุมเอกสารโดยกำหนดให้มีมาตรการควบคุมต่างๆคือการจัดทำทะเบียนการตรวจสอบการจัดทำเอกสารการสำเนาและการแปลการโอนการส่งและการรับการเก็บรักษาการยืมการทำลายการปฏิบัติในเวลาฉุกเฉินเวลาสูญหายรวมถึงการเปิดเผยข้อมูลในเอกสาร

๖. การบริหารจัดการการเข้าถึงของผู้ใช้

๖.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ของกรมอุตุนิยมวิทยาเพื่อให้มีสิทธิ์ต่างๆในการใช้งานตามความจำเป็น และต้องกำหนดให้มียกเลิกสิทธิ์การใช้งานเมื่อลาออกไปต้องทำภายใน ๒๔ ชั่วโมงหรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องทำภายใน ๗ วัน

๖.๒ กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญเช่นระบบคอมพิวเตอร์โปรแกรมประยุกต์(Application) จดหมายอิเล็กทรอนิกส์(e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ตเป็นต้นโดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๖.๓ ผู้ใช้ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

๖.๔ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

๖.๔.๑ ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้นๆต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบรวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในส่วนที่ ๓“การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๖.๔.๒ การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตามที่กำหนดไว้ในส่วนที่ ๓“การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๖.๔.๓ กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้หมายถึงผู้ใช้ที่มีสิทธิ์สูงสุดต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

๖.๔.๓.๑. ได้รับความเห็นชอบจากผู้ดูแลระบบงานนั้นๆโดยนำเสนอผู้บังคับบัญชาอนุมัติ

๖.๔.๓.๒. ควบคุมการใช้งานอย่างเข้มงวดเช่นกำหนดให้ใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

๖.๔.๓.๓. กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๖.๔.๓.๔. ต้องทำการเปลี่ยนรหัสผ่านอย่างเคร่งครัดโดยต้องทำการเปลี่ยนรหัสผ่านทุก๖เดือนเป็นอย่างน้อย

๖.๕ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๖.๕.๑ ผู้ดูแลระบบต้องกำหนดชั้นความลับให้กับข้อมูลวิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๖.๕.๒ เจ้าของข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้งเพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆที่ให้ไว้ยังคงมีความเหมาะสม

๖.๕.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User account) และรหัสผ่านเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๖.๕.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะต้องทำการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๖.๕.๕ กำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในส่วนที่ ๓“การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๖.๕.๖ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของกรมอุตุนิยมวิทยาเช่นส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนเป็นต้น

๗. การบริหารจัดการการเข้าถึงระบบเครือข่าย

๗.๑ ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งานกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศเช่นโซนภายใน (Internal zone) โซนภายนอก (External zone) เป็นต้นเพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

๗.๒ ผู้ดูแลระบบต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๗.๓ ผู้ดูแลระบบต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๗.๔ ผู้ดูแลระบบต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆได้และกำหนดบุคคลที่รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าParameter ต่างๆของระบบ

๗.๕ ต้องป้องกันเครือข่ายและอุปกรณ์ต่างๆที่เชื่อมต่อกับระบบเครือข่ายและทบทวนการกำหนดค่า Parameter ต่างๆอย่างน้อยปีละครั้งนอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งให้บุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๗.๖ ระบบเครือข่ายทั้งหมดของกรมอุตุนิยมวิทยาที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอกกรมต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่นการใช้ไฟร์วอล (firewall) หรือฮาร์ดแวร์อื่นๆรวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๗.๗ ให้ทำการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของกรมอุตุนิยมวิทยาในลักษณะที่ผิดปกติผ่านระบบเครือข่ายโดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๗.๘ การเข้าสู่ระบบงานเครือข่ายภายในกรมโดยผ่านทางอินเตอร์เน็ตจำเป็นต้องมีการล็อกอินและต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๗.๙ IP address ภายในของระบบงานเครือข่ายภายในของกรมอุตุนิยมวิทยาจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

๗.๑๐ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่างๆพร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๗.๑๑ การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๗.๑๒ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการ หรือควบคุมดูแลโดยกลุ่มเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศสำนักสื่อสารและเทคโนโลยีสารสนเทศเท่านั้น

๘. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๘.๑ ต้องกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่างๆของโปรแกรมระบบ (System Software) อย่างชัดเจน

๘.๒ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติจะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานโดยทันที

๘.๓ ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้นเช่น Telnet Ftp หรือ Ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย

๘.๔ ต้องดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่างๆของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอเช่น Web server เป็นต้น

๘.๕ ต้องทำการมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๘.๖ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการหรือควบคุมดูแลโดยกลุ่มเจ้าหน้าที่ด้านเทคโนโลยีและสารสนเทศสำนักสื่อสารและเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายเท่านั้น

๙. การบริหารจัดการการบันทึกและตรวจสอบ

๙.๑ ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่นบันทึกการเข้าออกระบบบันทึกการพยายามเข้าสู่ระบบบันทึกการใช้งาน command line และ firewall log เป็นต้นเพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

๙.๒ ต้องทำการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๙.๓ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆและจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๑๐. การควบคุมการเข้าใช้งานระบบจากภายนอก

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในกรมเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกโดยมีแนวทางปฏิบัติดังนี้

๑๐.๑ การเข้าสู่ระบบระยะไกล (Remote access) สู่ระบบเครือข่ายของกรมอุตุนิยมวิทยาต้องควบคุมบุคคลที่จะเข้าสู่ระบบของกรมอุตุนิยมวิทยาจากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๑๐.๒ วิธีการใดๆก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการสำนักสื่อสารและเทคโนโลยีสารสนเทศก่อนและมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของกรมอุตุนิยมวิทยาในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๑๐.๓ การให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกลผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับกรมอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๑๐.๔ ต้องมีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๑๐.๕ การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่เปิด Port ทิ้งไว้โดยไม่จำเป็นช่องทางดังกล่าว ต้องตัดการเชื่อมต่อเมื่อไม่ได้งานแล้วและจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๑๑. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของกรม

๑๑.๑ แสดงชื่อผู้ใช้งาน (Username)

๑๑.๒ ใส่รหัสผ่าน (Password)

ส่วนที่ ๓
การบริหารจัดการการเข้าถึงของผู้ใช้งาน
(User Access Management Policy)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งานมิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาตรวมทั้งจำกัดสิทธิ์ในการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาได้อย่างถูกต้อง

๒. การลงทะเบียนผู้ใช้งาน (User Registration)

๒.๑ ผู้ใช้งานกรอกแบบฟอร์มการลงทะเบียนผู้ใช้งานและต้องได้รับอนุมัติจากผู้มีอำนาจ

๒.๒ ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งานโดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๒.๓ ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๒.๔ ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศรวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

๒.๕ ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๒.๖ การลงทะเบียนผู้ใช้งานผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๓. การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management)

๓.๑ ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศโดยให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๓.๒ ผู้ดูแลระบบต้องกำหนดระดับสิทธิ์ในการเข้าถึงที่เหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศ

๓.๓ ผู้ดูแลระบบต้องมอบหมายสิทธิ์ที่มีความสอดคล้องกับนโยบายควบคุมการเข้าถึง

๓.๔ ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิ์แก่ผู้ใช้งานไว้เป็นหลักฐาน

๓.๕ ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่างๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกินกว่า ๑๐ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการลงบันทึกเข้า(Log in)ระบบสารสนเทศอีกครั้ง

๓.๖ กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุดโดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓.๗ ระบบเทคโนโลยีสารสนเทศที่มีการติดตั้งใช้งานแยกออกจากระบบเทคโนโลยีสารสนเทศของกรมและดูแลรับผิดชอบโดยส่วนราชการอื่นเช่น ระบบ GFMIS ให้ถือปฏิบัติตามหลักเกณฑ์และวิธีปฏิบัติตามที่ส่วนราชการนั้นๆกำหนดไว้

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๔.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตนโดยลงนามในเอกสารเพื่อแสดงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศของกรมอุตุนิยมวิทยา

๔.๒ การมอบบัญชีผู้ใช้งานให้กับผู้ใช้งานครั้งแรก ให้กำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่นและกำหนดรหัสผ่านที่แตกต่างกัน ให้กับผู้ใช้งาน เมื่อผู้ใช้งานได้รับรหัสผ่านแล้ว ให้เปลี่ยนรหัสผ่านนั้นเป็นรหัสผ่านของตนเอง

๔.๓ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันทีภายหลังจากที่ได้รับรหัสผ่านชั่วคราวและเปลี่ยนรหัสผ่านที่มีความยากต่อการเดาโดยผู้อื่น

๔.๔ ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งานโดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่งและกำหนดให้ผู้ใช้งานต้องตอบยืนยันการรับรหัสผ่านแล้ว

๔.๕ เมื่อมีผู้ใช้งานระบบสารสนเทศของหน่วยงานลาออก หรือไม่มีหน้าที่รับผิดชอบในระบบที่ขอสิทธิในการใช้งาน ให้หน่วยแจ้งผู้ดูแลระบบสารสนเทศทันที เพื่อเปลี่ยนสิทธิหรือถอดถอนสิทธิของผู้ใช้งานออกจากระบบทันทีที่ได้รับแจ้ง

๔.๖ ผู้ดูแลระบบต้องจัดทำระบบที่เอื้อให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านของตนเองได้

๔.๗ ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดได้ไม่เกิน ๓ ครั้ง

๕. การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review Of User Access Rights)

๕.๑ ผู้ดูแลระบบต้องดำเนินการทบทวนสิทธิ์การเข้าถึงของผู้ใช้อย่างน้อยปีละ ๑ ครั้ง

๕.๒ ผู้ดูแลระบบทบทวนสิทธิ์สำหรับผู้ที่มีสิทธิ์ในระดับสูงด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๕.๓ ผู้ดูแลระบบทบทวนสิทธิ์ตามรอบระยะเวลาที่กำหนดไว้หรือเมื่อมีการเปลี่ยนแปลงใดๆเกี่ยวกับการเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงานหรือสิ้นสุดการจ้างงาน

๕.๔ ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิ์ในระดับสูงเพื่อใช้ในการทบทวนในภายหลัง

ส่วนที่ ๔
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities Policy)

๑. วัตถุประสงค์

เพื่อควบคุมและกำหนดมาตรการการปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศและบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมอุตุนิยมวิทยาเพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๒. การใช้งานรหัสผ่าน (Password Use)

ผู้ใช้งานระบบเทคโนโลยีสารสนเทศต้องปฏิบัติตามข้อกำหนดการใช้งานรหัสผ่านดังนี้

๒.๑ ตั้งรหัสผ่านที่ยากต่อการคาดเดาโดยผู้อื่น

๒.๒ ไม่เปิดเผยรหัสผ่านของตนเอง

๒.๓ จัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

๒.๔ เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

๒.๕ ต้องตั้งรหัสผ่านที่มีความยาวอย่างน้อย ๘ ตัวอักษร หรือเกินกว่าขั้นต่ำกำหนดไว้

๒.๖ ตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

๒.๗ ไม่ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

๒.๘ หลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกันเช่น ๑๒๓ , abcdหรือกลุ่มของตัวอักขระที่เหมือนกันเช่น ๑๑๑ , aaaเป็นต้น

๒.๙ เปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด

๒.๑๐ เปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

๒.๑๑ เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการลงบันทึกเข้า (Login) เข้าสู่ระบบงาน

๒.๑๒ ไม่กำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้เพื่อความสะดวกของตนเองเมื่อทำการลงบันทึกเข้า (Login) ในภายหลัง

๒.๑๓ ไม่ใช้รหัสผ่านของตนร่วมกับผู้อื่น

๒.๑๔ หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆที่ใช้งาน

๓. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

๓.๑ ผู้ใช้งานต้องออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน

๓.๒ ผู้ใช้งานต้องล็อคอุปกรณ์ที่สำคัญ เมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ใช้งานชั่วคราว

๓.๓ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนเอง โดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานอุปกรณ์คอมพิวเตอร์

๓.๔ ผู้ดูแลระบบต้องกำหนดให้อุปกรณ์คอมพิวเตอร์ทุกเครื่อง ต้องทำการตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที และมีการใช้รหัสผ่านในการเข้าถึงใหม่อีกครั้ง

๔. การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy)

ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศเช่นเอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานดังนี้

๔.๑ ผู้ใช้งานต้องป้องกันทรัพย์สินของกรมและควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย

๔.๒ เครื่องคอมพิวเตอร์ต้องมีกลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

๔.๓ ต้องการป้องกันการใช้งานและควบคุมทรัพย์สิน ดังนี้

๔.๔.๑ ทุกคนต้องตระหนักและปฏิบัติการใดๆเพื่อป้องกันทรัพย์สินของกรม

๔.๔.๒ ลงชื่อออกจากระบบทันทีเมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

๔.๔.๓ จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย

๔.๔.๔ ล็อคเครื่องคอมพิวเตอร์เมื่อไม่ได้ใช้งาน

๔.๔.๕ ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาตได้แก่กล้องดิจิตอลเครื่องถ่ายสำเนาเอกสารเครื่องสแกนเอกสารเป็นต้น

๕. การเข้ารหัสข้อมูลที่เป็นความลับ

ให้ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับโดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการพ.ศ. ๒๕๔๔

๖. มาตรการทำลายสื่อบันทึกข้อมูลที่เป็นความลับ

สื่อบันทึกข้อมูล Removable Media และ Tape Backup ที่ใช้ในการจัดเก็บข้อมูล หรือสำรองข้อมูล ที่มีความสำคัญขององค์กรที่เป็นความลับต้องทำลายข้อมูลเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญ

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
กระดาษ	ใช้วิธีทำลายด้วยเครื่องทำลายเอกสาร
แผ่น CD/DVD	ใช้วิธีทำลายด้วยเครื่องทำลายแผ่น CD/DVD
เทป	ใช้วิธีทุบ หรือ บดให้เสียหาย หรือ เผาทำลาย
ฮาร์ดดิสก์ / Flash Drive	ให้ทำลายข้อมูลตามมาตรฐานสากล DoD 5220.2M, NIST 800-88

(ที่มาDoD 5220-22.M(http://www.dban.org/)

ส่วนที่ ๕
การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย
(Network Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงล่วงรู้แก้ไขเปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของกรมอุตุนิยมวิทยาโดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่างๆตามการแบ่งแยกเครือข่ายในลักษณะแบบ VLAN

๒. ผู้รับผิดชอบ

สำนักสื่อสารและเทคโนโลยีสารสนเทศ
ผู้ดูแลระบบที่ได้รับมอบหมาย
ผู้ใช้งาน

๓. การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

๓.๑ ข้อปฏิบัติสำหรับผู้ใช้งาน

๓.๑.๑ ห้ามผู้ใช้งานกระทำการใดๆเกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชนโดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆดังกล่าวย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของกรมอุตุนิยมวิทยา

๓.๑.๒ กรมอุตุนิยมวิทยาไม่อนุญาตให้ผู้ใช้งานกระทำการใดๆที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่ายเช่นการประกาศแจ้งความการซื้อหรือการจำหน่ายสินค้าการนำข้อมูลไปซื้อขายการให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๓.๑.๓ ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่นคือผู้ใช้งานจะต้องไม่อ่านเขียนลบเปลี่ยนแปลงหรือแก้ไขใดๆในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาตการบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่นการเผยแพร่ข้อความใดๆที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่นการใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือเป็นการละเมิดสิทธิ์ของผู้อื่นทั้งสิ้นผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียวกรมอุตุนิยมวิทยาไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๓.๑.๔ ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาตการบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

๓.๑.๕ กรมอุตุนิยมวิทยาให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้นผู้ใช้งานจะโอนหรือจ่ายแจกสิทธิ์นี้ให้กับผู้อื่นไม่ได้

๓.๑.๖ บัญชีผู้ใช้งาน (User Account) ที่กรมอุตุนิยมวิทยาให้กับผู้ใช้งานนั้นผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆอันอาจจะเกิดมีขึ้นรวมถึงผลเสียหายต่างๆที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้นๆเว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๒ ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๓.๒.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงได้เพียงบริการที่ได้รับอนุญาตเท่านั้น

๓.๒.๒ ผู้ดูแลระบบต้องกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึงโดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

๓.๒.๓ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ดังนี้

๓.๒.๓.๑ ผู้ดูแลระบบต้องกำหนดผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (identification) ด้วยชื่อผู้ใช้งาน (username) ทุกครั้ง

๓.๒.๓.๒ ผู้ดูแลระบบต้องกำหนดการพิสูจน์ตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password) ทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศ เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

๓.๒.๓.๓ การเข้าสู่ระบบจากระยะไกล (Remote Access) เพื่อเพิ่มความปลอดภัย จะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งานและต้องมีการใช้งานโปรโตคอลที่มีการเข้ารหัสข้อมูล ได้แก่ SSL

๓.๓ ข้อปฏิบัติสำหรับผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่ที่เกี่ยวข้อง

๓.๓.๑ ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องทำการกำหนดสิทธิ์บุคคลในการเข้าออกห้องควบคุมระบบเครือข่ายโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในและมีการบันทึก “ทะเบียนผู้มีสิทธิ์เข้า-ออกพื้นที่” เช่นเจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์(Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

๓.๓.๒ สิทธิ์ในการเข้าออกห้องต่างๆภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคนต้องได้รับการอนุมัติจากหัวหน้ากลุ่มงานด้านเทคโนโลยีและสารสนเทศเป็นลายลักษณ์อักษรโดยสิทธิ์ของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายห้องควบคุมระบบเครือข่าย

๓.๓.๓ ต้องจัดทำระบบเก็บบันทึกการเข้าออกกรมอุตุนิยมวิทยาตามกระบวนการที่ระบุไว้ในเอกสาร“บันทึกการเข้า-ออกพื้นที่”

๓.๓.๔ กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม

๓.๓.๕ การเข้าถึงห้องควบคุมระบบเครือข่ายต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร“บันทึกการเข้า-ออกพื้นที่”

๔. การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks)

๔.๑ ผู้ดูแลระบบต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๔.๒ ผู้ดูแลระบบจัดทำผังเครือข่ายและใช้ IP address และ MAC Address ในการระบุอุปกรณ์บนเครือข่าย

๔.๓ ผู้ดูแลระบบต้องควบคุมการใช้งานอย่างเหมาะสมและจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๕. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection)

ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๕.๑ ผู้ดูแลระบบต้องกำหนดการเปิด-ปิด พอร์ตที่ไม่ใช้งาน

๕.๒ การดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์ เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น

๕.๓ ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๖. การแบ่งแยกเครือข่าย (segregation in networks)

๖.๑ ต้องแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งานโดยแบ่งออกเป็น ๒ เครือข่ายคือเครือข่ายสำหรับผู้ใช้งานภายในและเครือข่ายสำหรับผู้ใช้งานภายนอกเพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ

๖.๒ มีระบบป้องการบุกรุก (Firewall) เพื่อป้องกันทางเข้าเครือข่าย จากผู้ไม่หวังดี

๗. การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control)

ผู้ดูแลระบบต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน ให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงดังนี้

๗.๑ ตรวจสอบการเชื่อมต่อเครือข่าย

๗.๒ จำกัดสิทธิความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

๗.๓ ระบุอุปกรณ์เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๗.๔ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

๗.๕ ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่ายโดยไม่ได้รับอนุญาต

๘. การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control)

ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจดังนี้

๘.๑ ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๘.๒ กำหนดให้มีการแปลงหมายเลขเครือข่ายเพื่อแยกเครือข่ายย่อย

๘.๓ กำหนดมาตรการการบังคับใช้เส้นทางเครือข่ายสามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้หรือจำกัดสิทธิในการใช้บริการเครือข่าย

ส่วนที่ ๖
การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการรวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัดอันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๒.๑. ผู้ใช้งานต้องกำหนดชื่อผู้ใช้และรหัสผ่านในการเข้าใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๒.๒. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver)หรือ ทำการล๊อคหน้าจอ (Lock screen) เพื่อทำการล็อคหน้าจอภาพเสมอเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๒.๓. ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้ง

๒.๔. ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๒.๕ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒.๖. ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๒.๗ ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๒.๘ จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

๒.๙ จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๓. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๓.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน

๓.๒ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้งการยืนยันว่าเป็นผู้ใช้งานที่ระบุถึง

๓.๓ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศเพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศหากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาดผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๓.๔ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่างๆอันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่ายเว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๕ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่นห้ามโอนจำหน่ายหรือจ่ายแจกให้ผู้อื่นโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๓.๖ ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเองและทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๔. การบริหารจัดการรหัสผ่าน (password management system)

ผู้ดูแลระบบต้องบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ กำหนดให้เปลี่ยนรหัสผ่านทันทีเมื่อเข้าใช้งานครั้งแรกและกำหนดบังคับให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

๕. การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities)

การใช้งานโปรแกรมอรรถประโยชน์ต้องจำกัดและควบคุมการใช้งานสำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญเนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการดังนี้

๕.๑ ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรม ประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือ หลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้

๕.๒ จำกัดสิทธิการเข้าถึงและกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๕.๓ กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

๕.๔ จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอกถ้าไม่ต้องใช้งานเป็นประจำ

๕.๕ มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๕.๖ กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๕.๗ ห้ามผู้ใช้งานลงโปรแกรมโดยไม่ได้รับอนุญาต หรือ ละเมิดลิขสิทธิ์

๖. เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

๖.๑ ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาทีเป็นอย่างน้อยหากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๕ นาทีตามความเหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๖.๒ ถ้าไม่มีการใช้งานระบบต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๖.๓ เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติหลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๗. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time)

ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๗.๑ การเชื่อมต่อระบบสารสนเทศสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูงกำหนดให้ใช้งานได้ ๓ ช.ม. ต่อการเชื่อมต่อหนึ่งครั้งกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น

๗.๒ การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๗.๓ กำหนดให้ระบบสารสนเทศเช่นระบบงานที่มีความสำคัญสูงระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) เป็นต้นมีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ส่วนที่๗
การควบคุมการเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ
(Application Information Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศของกรมและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกและโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

สำนักสื่อสารและเทคโนโลยีสารสนเทศ

ผู้ดูแลระบบที่ได้รับมอบหมาย

๓ การจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

๓.๑. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของกรมอุตุนิยมวิทยาต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งานเช่นการลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงานเป็นต้น

๓.๒. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญเช่นระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้นโดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๓.๓. ผู้ดูแลระบบ (SystemAdministrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๓.๓.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

๓.๓.๒ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัยเพื่อหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๓.๓.๓ กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

๓.๓.๔ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๓.๓.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งาน (Username) ต้องไม่ซ้ำกัน

๓.๓.๖ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาโดยมีการกำหนดระยะเวลาการใช้งานและ

ระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓.๔. ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับดังต่อไปนี้

๓.๔.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๓.๔.๒ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๓.๔.๓ ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๓.๔.๔ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากลเช่น SSL VPN หรือ XML Encryption เป็นต้น

๓.๔.๕ กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๓.๔.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงานเช่นส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมต้องทำการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนเป็นต้น

๔. การจัดการกับระบบที่ไวต่อการรบกวน

ระบบที่ไวต่อการรบกวนซึ่งมีผลกระทบต่อองค์การ ดังนี้

ระบบที่ไวต่อการรบกวนซึ่งมีผลกระทบต่อองค์การ	การจำกัดเข้าถึง	
	อุปกรณ์สื่อสารเคลื่อนที่	การปฏิบัติงานจากภายนอก
๑. ระบบพยากรณ์อากาศเชิงตัวเลข	ไม่ได้	ไม่ได้
๒. ระบบบริหารจัดการข้อมูลอุตุนิยมวิทยา	ได้	ไม่ได้
๓. ระบบบริการข้อมูลสถิติภูมิอากาศ	ไม่ได้	ไม่ได้
๔. ระบบสื่อสารข้อมูลอุตุนิยมวิทยา	ไม่ได้	ไม่ได้
๕. ระบบรับภาพถ่ายดาวเทียมอุตุนิยมวิทยา	ได้	ไม่ได้
๖. ระบบตรวจวัดรับ-ส่งข้อมูลอุตุนิยมวิทยาอุทกอัตโนมัติ	ได้	ไม่ได้
๗. ระบบตรวจวัดข้อมูลแผ่นดินไหว	ไม่ได้	ไม่ได้
๘. ระบบข้อมูลเครือข่ายอุตุนิยมวิทยาท้องถิ่น	ไม่ได้	ไม่ได้
๙. ระบบสารสนเทศเพื่อการพยากรณ์	ไม่ได้	ไม่ได้
๑๐. ระบบสารบรรณอิเล็กทรอนิกส์	ได้	ไม่ได้
๑๑. เว็บไซต์กรมอุตุนิยมวิทยา	ได้	ไม่ได้
๑๒. อินทราเน็ตกรมอุตุนิยมวิทยา	ไม่ได้	ไม่ได้
๑๓. ระบบสารสนเทศบุคลากร	ไม่ได้	ไม่ได้

๔.๑ ข้อปฏิบัติสำหรับระบบซึ่งไวต่อการรบกวน

๔.๑.๑ ผู้ดูแลระบบต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน

๔.๑.๒ ควบคุมสภาพแวดล้อมของตนเอง โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน ระบบสำรองไฟฟ้า เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบปรับอากาศและควบคุมความชื้น

๔.๑.๓ ต้องกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้น

๔.๒ ควบคุมการเข้าถึงผ่าน “อุปกรณ์สื่อสารเคลื่อนที่” และ “การปฏิบัติงานจากภายนอก” เกี่ยวข้องกับระบบที่ไวต่อการรบกวน ดังนี้

๔.๒.๑ ต้องได้รับการอนุมัติ/อนุญาต ก่อนปฏิบัติงาน โดยกำหนดสิทธิ และ ขอบเขตการทำงาน ชนิดของงาน และระบบงานอนุญาต

๔.๒.๒ ต้องกำหนดระยะเวลาการเข้าถึงและจัดให้มีการควบคุมการปฏิบัติงานและปรับปรุงสิทธิหลักจากการปฏิบัติงาน

๕. ข้อปฏิบัติในการการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

เพื่อป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์ คอมพิวเตอร์และสื่อสารเคลื่อนที่

๕.๑ ผู้ดูแลระบบต้องกำหนดมาตรการเพื่อป้องกันการเชื่อมต่อฝานอุปกรณ์เคลื่อนที่โดยไม่ได้รับอนุญาต

๕.๒ อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่จะต้องลงทะเบียนอุปกรณ์ก่อนใช้งาน

๕.๓ ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกรายการอุปกรณ์ในกรณีที่มีการ เข้า-ออกพื้นที่อย่างชัดเจน

๕.๔ ต้องจัดให้มีการสร้างความตระหนักเพื่อระมัดระวังและป้องกันการใช้งานอุปกรณ์เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่

๕.๕ ผู้ดูแลระบบต้องกำหนดให้มีการป้องกันข้อมูลที่สำรองไว้ในอุปกรณ์ จากการถูกขโมย สูญหาย หรือ เข้าถึงโดยไม่ได้รับอนุญาต

๖.ข้อปฏิบัติสำหรับการปฏิบัติงานจากภายนอกสำนักงาน (teleworking)

๖.๑ ผู้ใช้งานต้องได้รับการอนุญาตก่อนปฏิบัติงานจากระยะไกล

๖.๒ ผู้ดูแลระบบต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึกอาคารสำนักงานและสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานของกรม

๖.๓ ผู้ดูแลระบบจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกลการจัดเก็บข้อมูลและอุปกรณ์สื่อสารไว้ สำหรับผู้ปฏิบัติงานจากระยะไกลยกเว้นอุปกรณ์ที่กรมได้อนุญาต ให้ใช้งานได้เป็นกรณีไป

๖.๔ ผู้ดูแลระบบต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกลชั่วโมงการทำงานในสถานที่ดังกล่าวชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ ระบบงานและบริการต่างๆของกรมที่อนุญาตให้เข้าถึงได้จากระยะไกล

๖.๕ ผู้ดูแลระบบต้องยกเลิกการปฏิบัติงานจากระยะไกลการกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงานและการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

๗.การควบคุม outsource กรณีมีการจ้างเหมาดำเนินการ

๗.๑ ต้องกำหนดเรื่องสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๗.๒ ตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๗.๓ หลังจากการส่งมอบการพัฒนาซอฟแวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

๗.๔ ต้องระบุสัญญาจ้างว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด

๗.๕ ผู้รับจ้างพัฒนาระบบต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลและรักษาความลับของกรม

ส่วนที่ ๘
การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของกรม โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงานรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๒. ผู้รับผิดชอบ

สำนักสื่อสารและเทคโนโลยีสารสนเทศ

ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ข้อปฏิบัติสำหรับผู้ใช้งาน

๓.๑ ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของกรม จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตจากหัวหน้ากลุ่มงานด้านเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายจากหัวหน้ากลุ่มงานด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร

๓.๒ ผู้ใช้ที่ไม่ใช่บุคลากรของกรมอุตุนิยมวิทยา หรือผู้ที่ไม่เกี่ยวข้อง ที่จะขอเข้าใช้งานระบบเครือข่ายไร้สาย จะต้องลงทะเบียนขอใช้งาน โดยมีรายละเอียดเกี่ยวกับตัวบุคคล เช่นชื่อ และรหัสประจำตัวประชาชนเป็นอย่างน้อย และผู้ดูแลระบบ ต้องจัดการให้ใช้งานได้เฉพาะเครือข่ายอินเตอร์เน็ตเท่านั้น เพื่อช่วยป้องกันการเข้าถึงข้อมูลภายใน การโจมตี หรือการบุกรุกเครือข่ายภายในของกรมอุตุนิยมวิทยา

๔. ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๔.๑ ผู้ดูแลระบบ ต้องตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

๔.๒ ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๔.๓ ผู้ดูแลระบบ จะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๔.๔ ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

๔.๕ ผู้ดูแลระบบ ต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและสำรวจว่า สัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้ การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจ ช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

๔.๖ ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าปริยาย (default) มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

๔.๗ ผู้ดูแลระบบ ต้องเปลี่ยนค่าชื่อผู้ใช้และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและผู้ดูแลระบบต้องเลือกใช้ชื่อผู้ใช้และรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๔.๘ ผู้ดูแลระบบ ต้องกำหนดค่าใช้ WPAหรือ WPA2เป็นอย่างน้อย ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Clientและ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

๔.๙ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆของหน่วยงาน

๔.๑๐ ผู้ดูแลระบบ ต้องควบคุมการเข้าใช้งานระบบเครือข่ายไร้สาย เช่น เลือกใช้วิธีการควบคุม MAC address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย

๔.๑๑ ผู้ดูแลระบบ ต้องทำการติดตั้งไฟร์วอล (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในกรม

ส่วนที่ ๙
การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
(Third party Access Control Policy)

๑. วัตถุประสงค์

เพื่อป้องกันความเสี่ยงต่อการเข้าถึงข้อมูล การถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงาน โดยไม่ได้รับอนุญาตการใช้บริการจากหน่วยงานภายนอกและเพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมเป็นไปอย่างมั่นคงปลอดภัย ให้กำหนดแนวทางในการคัดเลือกควบคุมการปฏิบัติงานของหน่วยงานภายนอกเช่นการพัฒนาระบบการใช้บริการของที่ปรึกษาการใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกเป็นต้น

๒. ผู้รับผิดชอบ

สำนักสื่อสารและเทคโนโลยีสารสนเทศ
ผู้ดูแลระบบที่ได้รับมอบหมาย

๓.ข้อปฏิบัติ

๓.๑. หัวหน้ากลุ่มงานด้านเทคโนโลยีและสารสนเทศต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกและกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

๓.๒. การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

๓.๒.๑ บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อข้ออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศสำนักสื่อสารและเทคโนโลยีสารสนเทศ

๓.๒.๒ จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารซึ่งต้องมีรายละเอียดอย่างน้อยดังนี้

(๑) เหตุผลในการขอใช้
(๒) ระยะเวลาในการใช้
(๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
(๔) การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ
(๕) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๓.๒.๓ หน่วยงานภายนอกที่ทำงานให้กับกรมอุตุนิยมวิทยาทุกหน่วยงานไม่ว่าจะทำงานอยู่ภายในกรมอุตุนิยมวิทยาหรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของกรมอุตุนิยมวิทยาโดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๓.๒.๔ กรมอุตุนิยมวิทยาต้องพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอกทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เข้าไปปฏิบัติงาน

๓.๒.๕ เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๓.๒.๖ สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของกรมอุตุนิยมวิทยาผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้านคือการรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๓.๒.๗ กรมอุตุนิยมวิทยามีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้มั่นใจได้ว่ากรมอุตุนิยมวิทยาสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

๓.๒.๘ ต้องดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงานคู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้องรวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวดเพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

ส่วนที่ ๑๐
ความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต
(Internet Security Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเตอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. ๒๕๕๐ เช่น การส่งข้อมูลข้อความคำสั่งชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุขทำให้ระบบคอมพิวเตอร์ของกรมอุตุนิยมวิทยาถูกระงับชะลอขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. ผู้รับผิดชอบ

ผู้ใช้งาน
ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ข้อปฏิบัติสำหรับผู้ใช้งาน

๓.๑ ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านชองทางอื่นยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการข้ออนุญาตจากสำนักสื่อสารและเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

๓.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาก่อนทำการเชื่อมต่ออินเตอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ชองระบบปฏิบัติการเว็บเบราเซอร์

๓.๓ ผู้ใช้ต้องทำการ Update Patch และ Hot Fix อย่างสม่ำเสมอโดยสามารถ Download patch และ Hot Fix ต่างๆจากเจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่

๓.๔ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๓.๕ ผู้ใช้ต้องไม่ใช้เครือข่ายอินเตอร์เน็ตของกรมอุตุนิยมวิทยาเพื่อหาประโยชนในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสมเช่นเว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติศาสนาพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมเป็นต้น

๓.๖ ผู้ใช้จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของกรมอุตุนิยมวิทยา

๓.๗ ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับกรมอุตุนิยมวิทยา

๓.๘ ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมอุตุนิยมวิทยาที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเตอร์เน็ต

๓.๙ ผู้ใช้ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียงถูกดูหมิ่นถูกเกลียดชังหรือได้รับความอับอาย

๓.๑๐ หลังจากใช้งานอินเตอร์เน็ตเสร็จแล้วให้ทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๔. ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๔.๑ ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่กรมอุตุนิยมวิทยาจัดสรรไว้เท่านั้น โดยผ่าน Proxy, Firewall, IPS-IDS

ส่วนที่๑๑
การสำรองและกู้คืนข้อมูล
(Backup and Recovery Policy)

๑.วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติการสำรองข้อมูลและการกู้คืนระบบ(Backup and Recovery) โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถดำเนินการสำรองข้อมูลได้อย่างสมบูรณ์ถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น

๒. ผู้รับผิดชอบ

สำนักสื่อสารและเทคโนโลยีสารสนเทศ
ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ข้อปฏิบัติ

๓.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานสำรองข้อมูลและจัดทำระบบสารสนเทศสำรอง

๓.๒ ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

๓.๓ ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสมพร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูลสถานที่จัดเก็บ โดยรูปแบบการสำรองข้อมูลอาจแบ่งได้เป็นการสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๓.๔ การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึก รายละเอียดการสำรองข้อมูลได้แก่เวลาเริ่มต้นและสิ้นสุดชื่อผู้สำรองชนิดของข้อมูลที่บันทึกเป็นต้น

๓.๕ การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญโดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๓.๖ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อหัวหน้ากลุ่มงานด้านเทคโนโลยีสารสนเทศ

๓.๗ การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้นรวมทั้งวิธีการที่ใช้แก้ไขด้วย

๓.๘ นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนปฏิบัติ(Backup Procedure)โดยเคร่งครัด

๓.๙ ต้องทำการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๔. การปฏิบัติเกี่ยวกับการสำรองข้อมูล

๔.๑ ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการสำรองข้อมูลแต่ละรายการตามความถี่อย่างน้อยดังนี้

ที่	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๑	Mail servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในMail box	๑ ครั้งต่อเดือน
๒	Web servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลเผยแพร่บนเว็บไซต์	๑ ครั้งต่อเดือน
๓	Database servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในฐานข้อมูลของระบบ	๑ ครั้งต่อสัปดาห์
		ข้อมูล Log ของฐานข้อมูล	๑ ครั้งต่อสัปดาห์
๔	Firewall server	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูล Rule ของ Firewall	๑ ครั้งต่อเดือน
๕	Serverอื่นๆเช่น ระบบงานต่างๆ	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลบนServeอื่นๆ	๑ ครั้งต่อเดือน
หมายเหตุทุกรายการที่ปรากฏในตารางนี้จะใช้วิธีสำรองข้อมูลแบบ Full Backup ส่วนการสำรองข้อมูลแบบ Incremental Backup ให้พิจารณาตามความสำคัญของข้อมูล			

๔.๒ ผู้ดูแลระบบต้องทำการเก็บรักษาข้อมูลที่สำรองอย่างน้อย ๑ ชุดแยกสถานที่กัน เพื่อความมั่นคงปลอดภัย และใช้งานได้อย่างต่อเนื่อง

๔.๓ ผู้ดูแลระบบคอมพิวเตอร์ต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการสำรองข้อมูลตามรายละเอียดในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

๕. การกู้คืนระบบ(Data Recovery)

๕.๑ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายจะต้องทำการทดสอบการกู้คืนข้อมูลเป็นระยะเพื่อให้แน่ใจได้ว่าการสำรองข้อมูลนั้นทำได้อย่างครบถ้วนสมบูรณ์แล้ว

๕.๒ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไขรายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อหัวหน้ากลุ่มงานด้านเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายจากหัวหน้ากลุ่มงานด้านเทคโนโลยีสารสนเทศทราบ

๕.๓ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๕.๔ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบให้แจ้งผู้ใช้งานทราบทันทีพร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๖. การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) ต้องกำหนดบุคลากรที่เกี่ยวข้องและดำเนินการดังต่อไปนี้

๖.๑ กำหนดแผนเตรียมความพร้อม และกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติ

๖.๒ กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ

๖.๓ ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบติดขัดหรือไม่สามารถใช้งานได้อันเป็นผลจากภัยพิบัติที่กำหนดไว้

๖.๔ จัดทำแผนรับมือกับเหตุภัยพิบัติเพื่อให้สามารถกู้คืนระบบเทคโนโลยีสารสนเทศ ที่เสียหายให้สามารถใช้งานได้โดยเร็ว

๖.๕ ทดสอบการปฏิบัติตามแผนอย่างน้อยปีละ ๑ ครั้งโดยการจำลองสถานการณ์

๖.๕ ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูงอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๒
การใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail Policy)

๑. วัตถุประสงค์

๑.๑ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาสามารถสนับสนุนการปฏิบัติงานและการบริหารงานของกรมอุตุนิยมวิทยาเป็นไปอย่างถูกต้องสะดวกรวดเร็วทันสถานการณ์มีประสิทธิภาพและประสิทธิผล

๑.๒ เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของกรมอุตุนิยมวิทยาและหน่วยงานเป็นมาตรฐานอยู่ในกรอบของกฎหมายระเบียบคำสั่งข้อบังคับของกรมอุตุนิยมวิทยา

๒. ผู้รับผิดชอบ

ผู้ใช้งาน

ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ข้อปฏิบัติสำหรับผู้ใช้งาน

๓.๑ สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (default password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

๓.๒ รหัสจดหมายอิเล็กทรอนิกส์เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมาแต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น ‘x’ หรือ ‘o’ ในการพิมพ์แต่ละตัวอักษร

๓.๓ ผู้ใช้ต้องไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์

๓.๔ ผู้ใช้ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด โดยเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน

๓.๕ ผู้ใช้ต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อกรมอุตุนิยมวิทยาหรือละเมิดสิทธิ์สร้างความรำคาญต่อผู้อื่นหรือผิดกฎหมายหรือละเมิดศีลธรรมและไม่แสวงหาประโยชนหรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชนในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกรมอุตุนิยมวิทยา

๓.๖ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์(e-mail address) ของผู้อื่นเพื่ออ่านรับ-ส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆในจดหมายอิเล็กทรอนิกส์ของตน

๓.๗ ผู้ใช้ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาเพื่อการทำงานในภารกิจของกรมอุตุนิยมวิทยาเท่านั้น

๓.๘ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นต้องทำการลงบันทึกออก (Logout) จากระบบทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๓.๙ ผู้ใช้ต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file

๓.๑๐ ผู้ใช้ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๓.๑๑ ผู้ใช้ต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมข้อมูลอันอาจทำให้เสียชื่อเสียงของกรมอุตุนิยมวิทยา หรือข้อมูลที่ทำให้เกิดความแตกแยกในหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

๓.๑๒ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับไม่ต้องระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๒.๑๓ ผู้ใช้ต้องทำการตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ (Mail box) ของตนเองทุกวันและจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๒.๑๔ ผู้ใช้ต้องทำการลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๔. ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๓.๑ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอเช่นการลาออกเป็นต้น

๓.๒ ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายให้มีและรหัสผ่านสำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยา

๓.๓ ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง

๓.๔ ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ต้องทำการบันทึกออก (Logout) จากหน้าจอตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้เช่น ๑๐นาทีเมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

ส่วนที่ ๑๓
ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์
(Terms of Use and Disclaimer)

๑. วัตถุประสงค์

๑.๑ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาสามารถสนับสนุนการปฏิบัติงานของกรมอุตุนิยมวิทยาเป็นไปอย่างถูกต้องสะดวกรวดเร็วทันสถานการณ์มีประสิทธิภาพ

๑.๒ เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยระบบจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของกรมอุตุนิยมวิทยาและหน่วยงานเป็นมาตรฐานอยู่ในกรอบของกฎหมายระเบียบคำสั่งข้อบังคับคำแนะนำและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของกรมอุตุนิยมวิทยาอุตุนิยมวิทยา

๒. ข้อตกลงการใช้บริการ

๒.๑ ผู้ใช้บริการระบบจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาจะต้องไม่กระทำการอันละเมิดต่อกฎหมายระเบียบคำสั่งข้อบังคับคำแนะนำอย่างน้อยดังต่อไปนี้

๒.๑.๑ พระราชบัญญัติกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๕๐

๒.๑.๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ.๒๕๔๔

๒.๑.๓ พระราชบัญญัติข้อมูลข่าวสารของทางราชการพ.ศ.๒๕๔๐

๒.๑.๔ ระเบียบว่าด้วยการรักษาความลับของทางราชการพ.ศ.๒๕๔๔

๒.๑.๕ ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติพ.ศ.๒๕๑๗

๒.๑.๖ ระเบียบรักษาความปลอดภัยด้านการสื่อสารพ.ศ.๒๕๒๕

๒.๑.๗ ข้อตกลงเงื่อนไขการใช้บริการที่กรมอุตุนิยมวิทยากำหนด

๒.๒ หน่วยงาน/บุคคลผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาจะต้องใช้จดหมายอิเล็กทรอนิกส์นี้เพื่อผลประโยชน์ของทางราชการ

๒.๓ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาเพื่อการประกอบธุรกิจหรือแสวงหาผลประโยชน์ส่วนตน

๒.๔ ห้ามใช้บริการนี้ไปในการเผยแพร่อ้างอิงพาดพิงดูหมิ่นหรือการกระทำใดๆที่ก่อให้เกิดความเสียหายต่อสถาบันชาติศาสนาและพระมหากษัตริย์

๒.๕ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาในการประกอบอาชญากรรมทางคอมพิวเตอร์หรือการกระทำการใดๆซึ่งผิดกฎหมายคำสั่งระเบียบข้อบังคับและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารลับของทางราชการ

๒.๖ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาเพื่อการเผยแพร่ข้อมูลข่าวสารหรือภาพเสียงข้อความที่ไม่เหมาะสมหรือสร้างความเสื่อมเสียให้กับผู้อื่น

๒.๗ ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ไปแสดงข้อคิดเห็นส่วนตัวที่ส่งผลกระทบในทางลบหรือสร้างความเสื่อมเสียหรือเสียหายต่อบุคคลหรือกรมอุตุนิยมวิทยา

๒.๘ ห้ามกระทำการปลอมแปลงที่อยู่เป็นบุคคลอื่น (Impersonation)

๒.๙ ห้ามกระทำการที่สร้างปัญหาการใช้ทรัพยากรของระบบเช่น

(๑) การสร้างจดหมายลูกโซ่ (Chain mail)

(๒) การส่งจดหมายจำนวนมาก (Spam mail)

(๓) การส่งจดหมายต่อเนื่อง (Letter bomb)

(๔) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์

๒.๑๐ ห้ามผู้ใช้บริการกระทำการใดๆที่อาจจะนำมาซึ่งความเสื่อมเสียหรือก่อให้เกิดความเสียหายแก่ระบบเครื่องแม่ข่ายจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยา

๒.๑๑ ผู้ใช้ต้องรักษารหัสผ่าน(Password) ส่วนบุคคลหรือหน่วยงานของจดหมายอิเล็กทรอนิกส์เป็นไว้เป็นความลับ

๒.๑๒ ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับราชการของกรมอุตุนิยมวิทยา

๒.๑๓ การส่งข้อมูลข่าวสารที่เป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานนอกกรมอุตุนิยมวิทยาจะต้องเข้ารหัสข้อมูลข่าวสารนั้นอย่างเหมาะสม ตามวิธีปฏิบัติและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารตามที่กรมอุตุนิยมวิทยากำหนด

๒.๑๔ ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail address) และรหัสผ่าน(Password) ของหน่วยงานหรือบุคคลจะต้องเก็บรักษาไว้เป็นความลับหากสงสัยว่ารั่วไหลจะต้องดำเนินการเปลี่ยนรหัสผ่านทันทีโดยรหัสผ่านจะต้องกำหนดให้ยากแก่การคาดเดา (Strong Password)

๒.๑๕ ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาหรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์ (Email address) จะต้องศึกษาคู่มือการใช้งานระเบียบปฏิบัติคำแนะนำและข้อตกลงเงื่อนไขให้เข้าใจเพื่อใช้งานจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาได้อย่างถูกต้อง

๒.๑๖ กรณีได้รับการร้องเรียนร้องขอหรือพบเหตุอันไม่ชอบด้วยกฎหมายขอให้สงวนสิทธิ์ที่จะทำการยกเลิกหรือระงับบริการแก่สมาชิกนั้นๆเป็นการชั่วคราวเพื่อทำการสอบสวนและตรวจสอบหาสาเหตุของมูลเหตุนั้นๆ

๒.๑๗ การกระทำใดๆที่เกี่ยวกับการเผยแพร่ทั้งในรูปแบบของอีเมล์และ/หรือโฮมเพจของผู้ใช้บริการให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการสำนักสื่อสารและเทคโนโลยีสารสนเทศ ไม่มีส่วนเกี่ยวข้องใดๆ

ส่วนที่ ๑๔
การตรวจสอบและประเมินความเสี่ยง

๑.วัตถุประสงค์

เพื่อให้มีมาตรการในการตรวจสอบ ประเมิน ควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ผู้รับผิดชอบ

ศูนย์เทคโนโลยีสารสารสนเทศ

ผู้ตรวจสอบภายใน (internal auditor) หรือผู้ตรวจสอบจากภายนอก (external auditor)

ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ข้อปฏิบัติ

๓.๑ ตรวจสอบและประเมินความเสี่ยงในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๓.๒ ตรวจสอบและประเมินความเสี่ยง โดยคณะกรรมการหรือหน่วยงานหรือบุคคลที่กรมเห็นสมควร เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๓ การรักษาความมั่นคงปลอดภัยของข้อมูลและระบบข้อมูลจำเป็นต้องคำนึงถึงหลายด้านหลายมิติ แต่ละด้านก็มีความจำเป็นในการตรวจสอบและประเมินความเสี่ยงแตกต่างกัน โดยให้มีการดำเนินการดังต่อไปนี้

๑) การตรวจสอบและประเมินนโยบาย

๒) การตรวจสอบและประเมินความพร้อมทางด้านโครงสร้างองค์กร

๓) การตรวจสอบและประเมินด้านการบริหารทรัพย์สิน (ข้อมูลและระบบสารสนเทศ)

๔) การตรวจสอบและประเมินด้านบุคลากร

๕) การตรวจสอบและประเมินด้านกายภาพและสิ่งแวดล้อม

๖) การตรวจสอบและประเมินการสื่อสารและการปฏิบัติการ

๗) การตรวจสอบและประเมินการควบคุมการเข้าถึง

๘) การตรวจสอบและประเมินด้านการพัฒนาระบบ การจัดซื้อจัดหาระบบ การดูแลระบบ

๙) การตรวจสอบและประเมินด้านความพร้อมรับมือกับเหตุการณ์

๑๐) การตรวจสอบและประเมินด้านผลกระทบและความต่อเนื่องของการปฏิบัติภารกิจ

๑๑) การตรวจสอบและประเมินด้านการปฏิบัติตามกฎหมายและสัญญา

๓.๔ ระบุความเสี่ยง เหตุการณ์ความเสี่ยง และผลกระทบให้สอดคล้องตามแผนบริหารความเสี่ยงของกรมอุตุนิยมวิทยาดังนี้

๑) การลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

๒) การลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๓) การลงบันทึกเข้า (Login) สารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้บริการคนเดียวกันมากกว่าหนึ่งจุด

๔) การลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

๕) ความผิดพลาดของเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) ไวรัสคอมพิวเตอร์ (Computer Virus) ระบบไฟฟ้าขัดข้องความเสียหายจากเพลิงไหม้การโจรกรรมและการขโมยอุปกรณ์คอมพิวเตอร์

๓.๕ กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๓.๖ การประมาณความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

๑) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๒) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๓) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๓.๗ กำหนดมาตรการจัดการความเสี่ยง

๑) ดำเนินการทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan)

๒) จัดทำหลักเกณฑ์นโยบายกฎระเบียบในการใช้เครื่องคอมพิวเตอร์และเครือข่ายของกรมอุตุนิยมวิทยา

๓.๘ แนวทางการบริหารจัดการกับความเสี่ยงด้านสารสนเทศ ให้ปฏิบัติตามกระบวน PDCA (Plan-Do-Check-List)

ส่วนที่ ๑๕
การสร้างความตระหนัก
ในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้องได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

ศูนย์เทคโนโลยีสารสนเทศ
สถาบันอุตุนิยมวิทยา

๓. ข้อปฏิบัติ

๓.๑ จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอโดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่างๆตามแผนการฝึกอบรมของกรม

๓.๒ จัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัยและมีการเผยแพร่ทางเว็บไซต์ของกรม

๓.๓ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่ายซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอโดยการติดประกาศประชาสัมพันธ์แผ่นพับเผยแพร่ผ่านเว็บไซต์

๓.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับติดตามประเมินผลและสำรวจความต้องการของผู้ใช้บริการ

ภาคผนวก ก.

ตัวอย่างแบบฟอร์ม