ประกาศกรมอุตุนิยมวิทยา
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุตุนิยมวิทยา
พ.ศ. ๒๕๖๖

โดยที่มาตรา ๕ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ซึ่งออกโดยอาศัยอำนาจตามความในมาตรา ๓๕ วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๔ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษรและทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอนั้น อธิบดีกรมอุตุนิยมวิทยาจึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า " ประกาศกรมอุตุนิยมวิทยา เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุตุนิยมวิทยา พ.ศ. ๒๕๖๖ "

ข้อ ๒ ประกาศนี้ให้มีผลบังคับใช้ตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ในประกาศนี้

กรม หมายถึง กรมอุตุนิยมวิทยา กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมอุตุนิยมวิทยา

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยา

ผู้ใช้งาน หมายถึง ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับผิดชอบ ผู้ใช้งานทั่วไป หน่วยงานภายนอก

ผู้บริหารสูงสุด หมายถึง อธิบดีกรมอุตุนิยมวิทยา

ผู้บริหารด้านเทคโนโลยีสารสนเทศ หมายถึง อธิบดีกรมอุตุนิยมวิทยา หรือผู้ที่อธิบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของกรมอุตุนิยมวิทยา

ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการข้อมูลและเครือข่ายคอมพิวเตอร์

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่กรมอุตุนิยมวิทยา อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของกรมอุตุนิยมวิทยา โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

/ข้อมูล...

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

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

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลอัตโนมัติ

ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ 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 ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นสูญหาย

สินทรัพย์ (Asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

การสำรองข้อมูล (Backup) หมายถึง การสำเนาข้อมูลต่างๆ เก็บไว้ในอีกหน่วยความจำหนึ่ง (Media or Storage) เพื่อเป็นการป้องกันเมื่อเกิดความเสียหายของระบบคอมพิวเตอร์หรือของข้อมูลในหน่วยความจำที่ใช้งานอยู่

การกู้คืนข้อมูล (Data recovery) หมายถึง การฟื้นคืนสภาพข้อมูลที่ได้รับความเสียหายในระบบคอมพิวเตอร์ให้สามารถใช้งานได้จากสื่อบันทึกที่สำรองข้อมูลไว้ เช่น ฐานข้อมูล ระบบงานคอมพิวเตอร์ เป็นต้น

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

/รหัสผ่าน...

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

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 หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

การตั้งค่าระบบ (Configuration) หมายถึง ค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

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

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 การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

/ช่องโหว่...

ช่องโหว่ (Vulnerability) หมายถึง ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

การเข้ารหัส (Encryption) หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

อุปกรณ์กระจายสัญญาณ (Access Point) หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

SSID (Service Set Identifier) หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

WEP (Wired Equivalent Privacy) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

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

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 ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

/แผนผัง...

แผนผังระบบเครือข่าย (Network Diagram) หมายถึง แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

ข้อมูลจราจรทางคอมพิวเตอร์ หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิดต้นทางปลายทางเส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการหรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

สิทธิ์ของผู้ใช้งาน หมายถึง สิทธิ์ทั่วไปสิทธิ์จำเพาะสิทธิ์พิเศษและสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาตการกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

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

เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๔ องค์ประกอบของนโยบาย

หมวด ๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

ส่วนที่ ๑ การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์ เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันในการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์ อุปกรณ์เครือข่ายและระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของระบบเทคโนโลยีสารสนเทศและข้อมูล โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งาน ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและสื่อสารของกรมอุตุนิยมวิทยา

ส่วนที่ ๒ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยา และป้องกันการบุกรุกผ่านระบบเครือข่าย จากผู้บุกรุกและโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาได้อย่างถูกต้อง

ส่วนที่ ๓ การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ เพื่อกำหนดมาตรการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศของกรมอุตุนิยมวิทยา และการปรับปรุงเพื่อให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศของกรมอุตุนิยมวิทยา

/ส่วนที่ ๔

ส่วนที่ ๔ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่เกี่ยวข้องในการทำงาน เข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิ์ในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาได้อย่างถูกต้อง

ส่วนที่ ๕ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อควบคุมและกำหนดมาตรการการปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมาย ที่เกี่ยวข้องกับข้อมูลสารสนเทศและบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมอุตุนิยมวิทยา เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

ส่วนที่ ๖ การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของกรมอุตุนิยมวิทยา โดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่างๆ ตามการแบ่งแยกเครือข่ายในลักษณะแบบ VLAN

ส่วนที่ ๗ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงาน ให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

ส่วนที่ ๘ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศของกรมอุตุนิยมวิทยาและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกและโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาได้อย่างถูกต้อง

ส่วนที่ ๙ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของกรม โดยการกำหนดสิทธิของผู้ใช้ ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

ส่วนที่ ๑๐ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อป้องกันความเสี่ยงต่อการเข้าถึงข้อมูล การถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาตจากการใช้บริการจากหน่วยงานภายนอก และเพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยา เป็นไปอย่างมั่นคงปลอดภัย ให้กำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก

ส่วนที่ ๑๑ ความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเตอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ เช่น การส่งข้อมูล ข้อความ คำสั่ง

/ชุดคำสั่ง...

ชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่น อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของกรมอุตุนิยมวิทยา ถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

ส่วนที่ ๑๒ การใช้งานจดหมายอิเล็กทรอนิกส์ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยา สามารถสนับสนุนการปฏิบัติงานและการบริหารงานของกรมอุตุนิยมวิทยาเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพและประสิทธิผล และเพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของกรมอุตุนิยมวิทยาและหน่วยงานเป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับของกรมอุตุนิยมวิทยา

ส่วนที่ ๑๓ ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยา สามารถสนับสนุนการปฏิบัติงานของกรมอุตุนิยมวิทยา เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ และเพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยระบบจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของกรมอุตุนิยมวิทยาและหน่วยงานเป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของกรมอุตุนิยมวิทยา

หมวด ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองสารสนเทศ

ส่วนที่ ๑๔ การสำรองและกู้คืนข้อมูล เพื่อกำหนดข้อปฏิบัติการสำรองข้อมูลและการกู้คืนระบบ (Backup and Recovery) โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถดำเนินการสำรองข้อมูลได้อย่างสมบูรณ์ ถูกต้องและสามารถกู้คืนระบบได้ ในกรณีที่จำเป็น

หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๑๕ การตรวจสอบและประเมินความเสี่ยง เพื่อให้มีมาตรการในการตรวจสอบ ประเมิน ควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

หมวด ๔ การสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ ๑๖ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

ข้อ ๕ ตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

ข้อ ๖ การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน โดยจัดอบรมให้ความรู้เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ รวมทั้งมาตรการการเข้าถึงจากผู้ซึ่งไม่ได้รับการอนุญาต

ข้อ ๗ การกำหนดชั้นความลับของสารสนเทศให้เป็นไปตาม พ.ร.บ. ข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ หรือข้อกำหนดอื่นๆ ที่ได้ประกาศใช้ทดแทน

/ข้อ ๘...

ข้อ ๘ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ ได้แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้อธิบดีกรมอุตุนิยมวิทยาเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๙ ให้กองบริการดิจิทัลอุตุนิยมวิทยา เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุตุนิยมวิทยา อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๐ รายละเอียดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุตุนิยมวิทยา ให้เป็นไปตามเอกสารแนบท้ายประกาศนี้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ **๒๗** มิถุนายน พ.ศ. ๒๕๖๖

(นางสาวชมภารี ชมภูรัตน์)
อธิบดีกรมอุตุนิยมวิทยา

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมอุตุนิยมวิทยา
ประจำปี พ.ศ. ๒๕๖๖

คำนำ

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลายมากขึ้นในการให้ได้มาซึ่งข้อมูลสารสนเทศที่เป็นประโยชน์ต่อการดำเนินชีวิตของประชาชน การบริหารและการตัดสินใจในการดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชน รวมถึงการนำสารสนเทศมาใช้ในการกำหนดนโยบายและการพัฒนาประเทศ ขณะเดียวกันปัญหาความไม่น่าเชื่อถือของสารสนเทศอันเนื่องมาจากความไม่ทันสมัย ความไม่ถูกต้องครบถ้วนเพียงพอ โดยหัวใจสำคัญของความมั่นคงปลอดภัยของข้อมูลสารสนเทศประกอบด้วย หลักแนวคิด CIA ประกอบด้วย Confidentiality (ความลับ) โดยข้อมูลระบบสารสนเทศจะต้องเข้าถึงได้โดยผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น ข้อมูลและระบบสารสนเทศ จึงต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เพียงพอในการรักษาความลับของข้อมูลนั้น Integrity (ความถูกต้อง ความสมบูรณ์) รวมถึงความถูกต้องครบถ้วนของข้อมูล Availability (ความพร้อมใช้) ระบบสารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้น

ปัจจุบันพบปัญหาความมั่นคงปลอดภัยในระบบสารสนเทศที่มีรูปแบบหลากหลาย ส่งผลทวีความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ ซึ่งเกิดปัญหาเนื่องมาจากช่องโหว่ หรือจุดอ่อนของระบบสารสนเทศ การขาดนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยที่ชัดเจน และการนำมาตรการไปปฏิบัติอย่างมีประสิทธิภาพ

โดยคณะอนุกรรมการความมั่นคงปลอดภัยภายใต้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ขึ้น เพื่อเป็นแนวทางให้หน่วยงานของภาครัฐได้ใช้จัดทำแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อช่วยให้การดำเนินกิจกรรมหรือการให้บริการต่างๆ ของหน่วยงานภาครัฐมีความมั่นคงปลอดภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

กรมอุตุนิยมวิทยา จึงได้จัดทำนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมอุตุนิยมวิทยา ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ ขึ้น เพื่อเผยแพร่ให้ทุกหน่วยงานในกรมอุตุนิยมวิทยา เพื่อให้บุคลากรทุกคนในกรมอุตุนิยมวิทยา มีความรู้ เข้าใจในนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมอุตุนิยมวิทยา และสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

กรมอุตุนิยมวิทยา

สารบัญ

๑. บทนำ

๑.๑ หลักการ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ในมาตรา ๕ *"หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้"* และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ข้อมูลถือเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานราชการ และเป็นสิ่งที่มีค่ายิ่งสำหรับองค์กร ซึ่งจะได้รับการป้องกันรักษาให้มีความมั่นคงปลอดภัย เช่นเดียวกับสินทรัพย์อื่น ซึ่งข้อมูลดังกล่าวอาจอยู่ในรูปแบบสิ่งพิมพ์ สื่ออิเล็กทรอนิกส์ และในระบบสารสนเทศที่มีความสะดวกรวดเร็ว ง่ายต่อการเข้าถึง แต่ก็คงมีความเสี่ยงของภัยคุกคามที่อยู่ในวงกว้าง และอาจก่อให้เกิดความเสียหายต่อข้อมูล หรือมีการลักลอบนำข้อมูลไปใช้ในทางมิชอบ สร้างความเสียหายต่อองค์กรได้

ความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศจึงมีสำคัญอย่างยิ่งต่อองค์กรที่จะต้องมีการวางแผนและมีกระบวนการบริหารด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงจากภัยคุกคามที่เข้ามาในระบบสารสนเทศ องค์กรจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับกฎหมายและมาตรฐานสากล เพื่อเป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้แก่บุคลากรในองค์กร และบุคลากรอื่นที่เกี่ยวข้อนำไปปฏิบัติอย่างเคร่งครัด เพื่อให้บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรต่อไป

๑.๒ วัตถุประสงค์

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุตุนิยมวิทยาฉบับนี้มีวัตถุประสงค์เพื่อ

1) กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุตุนิยมวิทยา ที่สอดคล้องกับบริบทองค์กรและกฎหมายที่เกี่ยวข้อง

2) จัดทำเป็นบรรทัดฐานด้านความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศเทคโนโลยีและการสื่อสารของบุคลากรในองค์กร และบุคลากรอื่นที่มีส่วนเกี่ยวข้องกับกิจกรรมอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศขององค์กร

๓) เพื่อให้มั่นใจได้ว่าข้อมูลและระบบสารสนเทศของกรมอุตุนิยมวิทยา มีมาตรการในการรักษาความมั่นคงปลอดภัย ลดผลกระทบ ลดความเสียหายที่อาจจะเกิดขึ้นในระบบสารสนเทศ กรมอุตุนิยมวิทยา และใช้เป็นแนวทางเพื่อการพัฒนาและปรับปรุงคุณภาพการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมอุตุนิยมวิทยา

๑.๓ องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมอุตุนิยมวิทยา โดยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ อ้างอิงตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๕ และมาตรา ๗ ซึ่งกำหนดให้หน่วยงานภาครัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยแนวทางปฏิบัตินี้ประกอบด้วย วัตถุประสงค์ ผู้เกี่ยวข้องและรายละเอียด หรือขั้นตอนแนวปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมอุตุนิยมวิทยา

๑.๔ บทบังคับใช้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ให้มีผลบังคับใช้ครอบคลุมข้อมูลและระบบสารสนเทศของกรมอุตุนิยมวิทยา บุคลากรที่เกี่ยวข้องมีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ภายใต้การสนับสนุน และติดตามการประยุกต์ใช้ โดยผู้บริหารระดับสูง

กรณีข้อมูลหรือระบบสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูง (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

๑.๕ การเผยแพร่และทบทวน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมอุตุนิยมวิทยา ฉบับนี้ จัดทำขึ้นและมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง โดยนโยบายและแนวปฏิบัติได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายใน (Intranet) กรมอุตุนิยมวิทยา จัดพิมพ์เผยแพร่เพื่อให้บุคลากรกรมอุตุนิยมวิทยา และบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒. คำนิยาม

๑. กรม หมายถึง กรมอุตุนิยมวิทยา กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมอุตุนิยมวิทยา

๓. การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยา

๔. ผู้ใช้งาน หมายถึง ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับผิดชอบ ผู้ใช้งานทั่วไป หน่วยงานภายนอก

๕. ผู้บริหารสูงสุด หมายถึง อธิบดีกรมอุตุนิยามวิทยา

๖. ผู้บริหารด้านเทคโนโลยีสารสนเทศ หมายถึง อธิบดีกรมอุตุนิยมวิทยา หรือผู้ที่อธิบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของกรมอุตุนิยมวิทยา

๗. ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการข้อมูลและเครือข่ายคอมพิวเตอร์

๘. หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่กรมอุตุนิยมวิทยา อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของกรมอุตุนิยมวิทยา โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

๙. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๐. สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

๑๑. ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลอัตโนมัติ

๑๒. ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของกรมอุตุนิยมวิทยา

๑๓. ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึงระบบงานของกรมอุตุนิยมวิทยาที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่นระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

๑๔. พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง พื้นที่ที่กรมอุตุนิยมวิทยาอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

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

๑๕. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นสูญหาย

๑๖. สินทรัพย์ (Asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

๑๗. การสำรองข้อมูล (Backup) หมายถึง การสำเนาข้อมูลต่างๆ เก็บไว้ในอีกหน่วยความจำหนึ่ง (Media or Storage) เพื่อเป็นการป้องกันเมื่อเกิดความเสียหายของระบบคอมพิวเตอร์หรือของข้อมูลในหน่วยความจำที่ใช้งานอยู่

๑๘. การกู้คืนข้อมูล (Data recovery) หมายถึง การฟื้นคืนสภาพข้อมูลที่ได้รับความเสียหายในระบบคอมพิวเตอร์ให้สามารถใช้งานได้จากสื่อบันทึกที่สำรองข้อมูลไว้ เช่น ฐานข้อมูล ระบบงานคอมพิวเตอร์ เป็นต้น

๑๙. จดหมายอิเล็กทรอนิกส์ (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อมูล ข้อความระหว่างกันโดยใช้มาตรฐานการรับส่ง เช่น SMTP, POP3 และ IMAP เป็นต้น ผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน โดยผู้ส่งสามารถส่งไปยังผู้รับคนเดียวหรือหลายคนก็ได้

๒๐. รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ ในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๒๑. บัญชีผู้ใช้บริการ (Account) หมายถึง รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของหน่วยงาน

๒๒. ชื่อเครื่องคอมพิวเตอร์ (Computer Name) หมายถึง ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

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

๒๔. โปรแกรมประสงค์ร้าย (Malware) หมายถึง โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือ สปายแวร์

(Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

๒๕. ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือ ปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๒๖. การตั้งค่าระบบ (Configuration) หมายถึง ค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

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

๒๘. เลขที่อยู่ไอพีสาธารณะ (Public IP Address) หมายถึง เลขที่อยู่ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงานหรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากัน หรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

๒๙. แบนด์วิดท์ (Bandwidth) หมายถึง ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

๓๐. ชื่อผู้ใช้ (Username) หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

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

๓๒. ลงบันทึกออก (Logout) หมายถึง กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

๓๓. อัพเดท (Update) หมายถึง ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

๓๔. ช่องโหว่ (Vulnerability) หมายถึง ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยขอบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓๕. การเข้ารหัส (Encryption) หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๓๖. อุปกรณ์กระจายสัญญาณ (Access Point) หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

๓๗. SSID (Service Set Identifier) หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

๓๘. WEP (Wired Equivalent Privacy) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

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

๔๐. ไฟร์วอลล์ (Firewall) หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

๔๑. IDS (Intrusion Detection System) หรือระบบตรวจจับการบุกรุกหมายถึง ระบบตรวจจับการบุกรุกของผู้ไม่ประสงค์ดีใช้วิเคราะห์และแจ้งเตือนหากข้อมูลที่ผ่านเข้า-ออกเครือข่ายมีลักษณะการทำงานที่เป็นความเสี่ยงต่อเครือข่าย

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

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

๔๔. อุปกรณ์จัดเส้นทาง (Router) หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

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

๔๖. การพิสูจน์ยืนยันตัวตน (Authentication) หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

๔๗. แผนผังระบบเครือข่าย (Network Diagram) หมายถึง แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

๔๘. ข้อมูลจราจรทางคอมพิวเตอร์ หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิดต้นทางปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

๔๙. สิทธิ์ของผู้ใช้งาน หมายถึง สิทธิ์ทั่วไปสิทธิ์จำเพาะสิทธิ์พิเศษและสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๕๐. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาตการกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพรวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๕๑. ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่นได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๕๒. เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๕๓. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

หมวดที่ ๑ นโยบายการเข้าถึง และการควบคุมการใช้งานสารสนเทศ

ส่วนที่ ๑
การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์
(Computing System Control Room Policy)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน ในการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์ อุปกรณ์เครือข่ายและระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งาน ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยา

๒. ผู้รับผิดชอบ

กองบริการดิจิทัลอุตุนิยมวิทยา

๓. แนวปฏิบัติการควบคุมการเข้าออก

๓.๑ ต้องจำแนกและกำหนดพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบเทคโนโลยีสารสนเทศต่างๆ ในกรมอุตุนิยมวิทยาอย่างเหมาะสม โดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

๓.๒ กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน 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-ออกให้ถูกต้องและเจ้าหน้าที่จะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา

๓.๕ บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

๔. แนวปฏิบัติสำหรับผู้ติดต่อที่มาจากหน่วยงานภายนอก

๔.๑ ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่”

๔.๒ ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในกรมอุตุนิยมวิทยามาปฏิบัติงานที่ห้องควบคุมระบบเครือข่ายต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการข้ออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่” ให้ถูกต้องชัดเจน

๔.๓ เจ้าหน้าที่/ผู้ดูแลระบบต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเป็นประจำทุกเดือน

ส่วนที่ ๒

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาต เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยา และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกและโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

ศูนย์เทคโนโลยีสารสนเทศ
ผู้ดูแลระบบที่ได้รับมอบหมาย
เจ้าของข้อมูล

๓. แนวปฏิบัติ

๓.๑ กระบวนการหลักในการควบคุมการเข้าถึงระบบ

๓.๑.๑ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๓.๑.๒ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓.๑.๓ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

๓.๑.๔ ผู้ดูแลระบบควรจัดให้มีระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

๓.๑.๕ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๓.๒ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๓.๒.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งาน สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น และการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ที่ได้รับอนุญาต

๓.๒.๒ เจ้าของข้อมูลและเจ้าของระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๓.๒.๓ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๓.๒.๔ การขอสิทธิ์ในการเข้าสู่ระบบจะต้องมีการทำเป็นเอกสารและมีการลงนามอนุมัติเอกสารดังกล่าวและต้องมีการจัดเก็บไว้เป็นหลักฐานด้วย

๓.๓ ข้อกำหนดเกี่ยวกับประเภทข้อมูลลำดับชั้นความลับของข้อมูล

๓.๓.๑ ประเภทข้อมูล

๑) ข้อมูลการพยากรณ์อากาศ ข้อมูลทั่วไป เข้าถึงได้ ๒๔ ชม. ผ่านเว็บไซต์

๒) ข้อมูลระบบงานสารบรรณ ข้อมูลภายใน เข้าถึงได้ ๒๔ ชม. ผ่านระบบงาน กำหนดสิทธิการเข้าถึง

๓) ข้อมูลระบบงานบุคลากร ข้อมูลส่วนบุคคลไม่เปิดเผย เข้าถึงได้ ๒๔ ชม. ผ่านระบบงานกำหนดสิทธิการเข้าถึง

๔) ข้อมูลเว็บไซต์ของกรมอุตุนิยมวิทยา ข้อมูลทั่วไป เข้าถึงได้ ๒๔ ชม. ผ่านเว็บไซต์

๕) ข้อมูลเว็บไซต์ภายในของกรมอุตุนิยมวิทยา ข้อมูลทั่วไป เข้าถึงได้ ๒๔ ชม. ผ่านเว็บไซต์

๖) ฐานข้อมูลภูมิอากาศ ข้อมูลภายใน เข้าถึงได้ตามสิทธิ ผ่านระบบงาน

๗) ข้อมูลการส่งข่าวอัตโนมัติผ่านเครือข่าย ข้อมูลทั่วไป เข้าถึงได้ ๒๔ ชม. ผ่านเครือข่าย

๘) ข้อมูลเครือข่ายอุตุท้องถิ่น ข้อมูลภายใน เข้าถึงผ่านระบบงาน

๙) ข้อมูลระบบ Web Portal เพื่อสนับสนุนการพยากรณ์อากาศ ข้อมูลทั่วไป เข้าถึงได้ ๒๔ ชม. ผ่านเว็บไซต์

๓.๓.๒ การลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบถือว่าเป็นแนวทางที่เหมาะสมที่ในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

๑) การกำหนดชั้นความลับตามความสำคัญของข้อมูลในเอกสารกำหนดไว้ ๓ ระดับ ได้แก่ ลับ/ลับมาก/ลับที่สุด และมีการกำหนดความรับผิดชอบให้แก่ผู้มีอำนาจ

กำหนดชั้นความลับเป็นผู้พิจารณากำหนดระดับชั้นความลับของเอกสารและการยกเลิกหรือปรับระดับชั้นความลับของเอกสารตามความจำเป็น

๒) การควบคุมเอกสารโดยกำหนดให้มีมาตรการควบคุมต่างๆ คือการจัดทำทะเบียนการตรวจสอบการจัดทำเอกสารการสำเนา และการแปล การโอน การส่ง และการรับ การเก็บรักษาการยืมการทำลายการปฏิบัติในเวลาฉุกเฉินเวลาสูญหายรวมถึงการเปิดเผยข้อมูลในเอกสาร

๓.๔ การบริหารจัดการการเข้าถึงของผู้ใช้

๓.๔.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ของกรมอุตุนิยมวิทยาเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งานเช่นเมื่อลาออกไปต้องทำภายใน ๒๔ ชั่วโมงหรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องทำภายใน ๗ วัน

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

๓.๔.๓ ผู้ใช้ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

๓.๔.๔ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

๑) ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในส่วนที่ ๓ “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๒) การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตามที่กำหนดไว้ในส่วนที่ ๓ “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๓) กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้หมายถึงผู้ใช้ที่มีสิทธิ์สูงสุดต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

(๑) ได้รับความเห็นชอบจากผู้ดูแลระบบงานนั้นๆ โดยนำเสนอผู้บังคับบัญชาอนุมัติ

(๒) ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) ต้องทำการเปลี่ยนรหัสผ่านอย่างเคร่งครัดเช่นทุกครั้ง หลังหมดความจำเป็นในการใช้งานหรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๓.๕ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๓.๕.๑ ผู้ดูแลระบบต้องกำหนดชั้นความลับให้กับข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๓.๕.๒ เจ้าของข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้งเพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๓.๕.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User account) และรหัสผ่านเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๓.๕.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากลหรืออ้างอิงตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

๓.๕.๕ กำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในส่วนที่ ๓ “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๓.๕.๖ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของกรมอุตุนิยมวิทยา เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๓.๖ การบริหารจัดการการเข้าถึงระบบเครือข่าย

๓.๖.๑ ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งานกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal zone) โซนภายนอก (External zone) เป็นต้น เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

๓.๖.๒ ผู้ดูแลระบบต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๓.๖.๓ ผู้ดูแลระบบควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๓.๖.๔ ผู้ดูแลระบบต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆ ได้ และกำหนดบุคคลที่รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบ

๓.๖.๕ ต้องป้องกันเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายและควรทบทวนการกำหนดค่า Parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๓.๖.๖ ระบบเครือข่ายทั้งหมดของกรมอุตุนิยมวิทยาที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกกรมควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอล (firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๓.๖.๗ ควรมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของกรมอุตุนิยมวิทยาในลักษณะที่ผิดปกติผ่านระบบเครือข่ายโดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๓.๖.๘ การเข้าสู่ระบบงานเครือข่ายภายในกรมโดยผ่านทางอินเตอร์เน็ตจำเป็นต้องมีการล๊อกอินและต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๓.๖.๙ IP address ภายในของระบบงานเครือข่ายภายในของกรมอุตุนิยมวิทยาจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

๓.๖.๑๐ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่างๆ พร้อม มีการทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์อย่างน้อยปีละ ๑ ครั้งและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๓.๖.๑๑ การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๓.๖.๑๒ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการ หรือควบคุมดูแลโดยกลุ่มเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศกองสื่อสารและเทคโนโลยีสารสนเทศเท่านั้น

๓.๗ การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๓.๗.๑ ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๓.๗.๒ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานโดยทันที

๓.๗.๓ ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น Telnet Ftp หรือ Ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย

๓.๗.๔ ควรดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web server เป็นต้น

๓.๗.๕ ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๓.๗.๖ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการหรือควบคุมดูแลโดยกลุ่มเจ้าหน้าที่ด้านเทคโนโลยีและสารสนเทศกองสื่อสารและเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายเท่านั้น

๓.๘ การบริหารจัดการการบันทึกและตรวจสอบ

๓.๘.๑ ควรกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบบันทึกการพยายามเข้าสู่ระบบบันทึกการใช้งาน command line และ firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้ อย่างน้อย ๓ เดือน

๓.๘.๒ ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๓.๘.๓ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๓.๙ การควบคุมการเข้าใช้งานระบบจากภายนอก

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในกรมเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติดังนี้

๓.๙.๑ การเข้าสู่ระบบระยะไกล (Remote access) สู่ระบบเครือข่ายของกรมอุตุนิยมวิทยา ต้องควบคุมบุคคลที่จะเข้าสู่ระบบของกรมอุตุนิยมวิทยาจากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๓.๙.๒ วิธีการใดๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับการอนุมัติจากผู้อำนวยการกองสื่อสารและเทคโนโลยีสารสนเทศก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของกรมอุตุนิยมวิทยาในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๓.๙.๓ การให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับกรมอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๓.๙.๔ ต้องมีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๓.๙.๕ การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port ทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๓.๑๐ การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร

๓.๑๐.๑ แสดงชื่อผู้ใช้งาน (Username)

๓.๑๐.๒ ใส่รหัสผ่าน (Password)

ส่วนที่ ๓

การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

(Business Requirements for Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศของกรมอุตุนิยมวิทยา และการปรับปรุงเพื่อให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศของกรมอุตุนิยมวิทยา

๒. ผู้รับผิดชอบ

ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติ

๒.๑ การควบคุมการเข้าถึงสารสนเทศ

๒.๑.๑ กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศของผู้ใช้งานให้สอดคล้องกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้งานระบบสารสนเทศของกรมอุตุนิยมวิทยา

๒.๑.๒ กำหนดชื่อผู้ใช้งานต้องไม่ซ้ากัน

๒.๑.๓ กำหนดให้ผู้ใช้งานเก็บรักษารหัสผ่านให้เป็นความลับเฉพาะตนเท่านั้น

๒.๒ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒.๒.๑ ทบทวนสิทธิการเข้าถึงระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อได้รับเอกสารแจ้งจากหน่วยงานต้นสังกัดของผู้ใช้งานระบบ เพื่อปรับปรุงการให้สิทธิแก่ผู้ใช้งานให้สอดคล้องกับการปฏิบัติงานที่เปลี่ยนไป เช่น เมื่อเปลี่ยนแปลงตำแหน่งงาน ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงานภายในองค์กร เป็นต้น

๒.๒.๒ หน่วยงานต้นสังกัดของผู้ใช้งานต้องแจ้งเอกสารอย่างเป็นทางการแก่ผู้ดูแลระบบให้กำหนดสิทธิตามหน้าที่ความรับผิดชอบในการปฏิบัติงานเมื่อมีผู้ใช้งานใหม่เข้ามาปฏิบัติงาน หรือยกเลิกสิทธิต่างๆ ในการเข้าใช้ระบบสารสนเทศเมื่อมีผู้ใช้งานโยกย้าย หรือลาออก เป็นต้น

ส่วนที่ ๔

การบริหารจัดการการเข้าถึงของผู้ใช้งาน

(User Access Management Policy)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงาน เข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิ์ในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติ

๓.๑ การลงทะเบียนผู้ใช้งาน (User Registration)

๓.๑.๑ ผู้ใช้งานกรอกแบบฟอร์มการลงทะเบียนผู้ใช้งาน และต้องได้รับอนุมัติจากผู้มีอำนาจ

๓.๑.๒ ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๓.๑.๓ ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๓.๑.๔ ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

๓.๑.๕ ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันที เมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๓.๑.๖ การลงทะเบียนผู้ใช้งานผู้ดูแลระบบ ต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๓.๒ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management)

๓.๒.๑ ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๓.๒.๒ ผู้ดูแลระบบต้องกำหนดระดับสิทธิ์ในการเข้าถึงที่เหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศ

๓.๒.๓ ผู้ดูแลระบบต้องมอบหมายสิทธิ์ที่มีความสอดคล้องกับนโยบายควบคุมการเข้าถึง

๓.๒.๔ ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิ์แก่ผู้ใช้งานไว้เป็นหลักฐาน

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

๓.๒.๖ กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓.๒.๗ ระบบเทคโนโลยีสารสนเทศที่มีการติดตั้งใช้งานแยกออกจากระบบเทคโนโลยีสารสนเทศของกรม และดูแลรับผิดชอบโดยส่วนราชการอื่น เช่น ระบบ GFMIS ให้ถือปฏิบัติตามหลักเกณฑ์และวิธีปฏิบัติตามที่ส่วนราชการนั้นๆ กำหนดไว้

๓.๓ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๓.๓.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารเพื่อแสดงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศของกรมอุตุนิยมวิทยา

๓.๓.๒ ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๓.๓.๓ ผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราวและควรเปลี่ยนรหัสผ่านที่มีความยากต่อการเดาโดยผู้อื่น

๓.๓.๔ ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่นและควรกำหนดรหัสผ่านที่แตกต่างกัน

๓.๓.๕ ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งานโดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่งและควรกำหนดให้ผู้ใช้งานตอบกลับหลังจากที่ได้รับรหัสผ่านแล้ว

๓.๔ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

๓.๔.๑ ผู้ดูแลระบบดำเนินการทบทวนสิทธิ์การเข้าถึงของผู้ใช้อย่างน้อยปีละ ๑ ครั้ง

๓.๔.๒ ผู้ดูแลระบบทบทวนสิทธิ์สำหรับผู้ที่มีสิทธิ์ในระดับสูง เช่น สิทธิ์ในระดับผู้ดูแลระบบด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๓.๔.๓ ผู้ดูแลระบบทบทวนสิทธิ์ตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใด เช่น การเลื่อนตำแหน่งลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

๓.๔.๔ ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิ์ในระดับสูงเพื่อใช้ในการทบทวนในภายหลัง

ส่วนที่ ๕

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

(User Responsibilities Policy)

๑. วัตถุประสงค์

เพื่อควบคุมและกำหนดมาตรการการปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศ และบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมอุตุนิยมวิทยา เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๒. ผู้รับผิดชอบ

ผู้ดูแลระบบที่ได้รับมอบหมาย

ผู้ใช้งาน

๓. แนวปฏิบัติ

๓.๑ การใช้งานรหัสผ่าน (Password Use)

ผู้ใช้งานต้องปฏิบัติตามข้อกำหนด การใช้งานรหัสผ่าน ดังนี้

๓.๑.๑ ตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

๓.๑.๒ ไม่เปิดเผยรหัสผ่านของตนเอง

๓.๑.๓ จัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

๓.๑.๔ เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

๓.๑.๕ ผู้ใช้งานควรตั้งรหัสผ่านที่มีความยาวอย่างน้อย ๘ ตัวอักษร หรือเกินกว่าขั้นต่ำกำหนดไว้

๓.๑.๖ ตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

๓.๑.๗ ไม่ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

๓.๑.๘ หลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกันเช่น ๑๒๓, abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน เช่น ๑๑๑, aaa เป็นต้น

๓.๑.๙ เปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด

๓.๑.๑๐ เปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

๓.๑.๑๑ เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการลงบันทึกเข้า (Login) เข้าสู่ระบบงาน

๓.๑.๑๒ ไม่กำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้เพื่อความสะดวกของตนเองเมื่อทำการลงบันทึกเข้า (Login) ในภายหลัง

๓.๑.๑๓ หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ใช้งาน

๓.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

๓.๒.๑ ผู้ใช้งานต้องไม่ปล่อยให้สื่อบันทึกข้อมูลหรืออุปกรณ์ทิ้งไว้โดยไม่ได้ดูแล

๓.๒.๒ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน

๓.๒.๓ ผู้ดูแลระบบควรกำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

๓.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy)

ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่นเอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

๓.๓.๑ ผู้ใช้งานต้องป้องกันทรัพย์สินของกรมและควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย

๓.๓.๒ เครื่องคอมพิวเตอร์ต้องมีกลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

๓.๓.๓ ต้องการป้องกันการใช้งานและควบคุมทรัพย์สิน ดังนี้

๑) ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของกรม

๒) ลงชื่อออกจากระบบทันทีเมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

๓) จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย

๔) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ หรือสื่อบันทึกข้อมูลที่เป็นสมบัติส่วนบุคคล

๕) ล็อคเครื่องคอมพิวเตอร์เมื่อไม่ได้ใช้งาน

๖) ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องถ่ายสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น

๗) ข้อมูลสำคัญที่บันทึกไว้ในกระดาษ สื่อบันทึกข้อมูลแฟลชไดร์ฟ หรือฮาร์ดดิสก์ เมื่อไม่ใช้งาน ต้องจัดเก็บไว้ในที่ปลอดภัย ไม่ทิ้งวางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

๘) นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๓.๔ การเข้ารหัสข้อมูลที่เป็นความลับ

ให้ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

๓.๕ 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 ๕๒๒๐.๒M, NIST ๘๐๐-๘๘

(ที่มา DoD ๕๒๒๐-๒๒.M (http://www.dban.org/)

ส่วนที่ ๖

การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

(Network Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของกรมอุตุนิยมวิทยา โดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่างๆ ตามการแบ่งแยกเครือข่ายในลักษณะแบบ VLAN

๒. ผู้รับผิดชอบ

กองบริการดิจิทัลอุตุนิยมวิทยา

กองสื่อสาร

ผู้ดูแลระบบที่ได้รับมอบหมาย

ผู้ใช้งาน

๓. แนวปฏิบัติ

๓.๑ การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

๓.๑.๑ ข้อปฏิบัติสำหรับผู้ใช้งาน

๑) ห้ามผู้ใช้งานกระทำการใดๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆ ดังกล่าวย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของกรมอุตุนิยมวิทยา

๒) กรมอุตุนิยมวิทยาไม่อนุญาตให้ผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความการซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขายการให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๓) ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น คือผู้ใช้งานจะต้องไม่อ่านเขียนลบเปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาตการบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่นการเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพ หรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิ์ของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียวกรมอุตุนิยมวิทยาไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๔) ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาตการบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

๕) กรมอุตุนิยมวิทยาให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธิ์นี้ให้กับผู้อื่นไม่ได้

๖) บัญชีผู้ใช้งาน (User Account) ที่กรมอุตุนิยมวิทยาให้กับผู้ใช้งานนั้นผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ อันอาจจะเกิดมีขึ้นรวมถึงผลเสียหายต่างๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๑.๒ ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๑) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงได้เพียงบริการที่ได้รับอนุญาตเท่านั้น

๒) ผู้ดูแลระบบต้องกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึงโดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

๓) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่าย และระบบสารสนเทศของหน่วยงานได้ดังนี้

๓.๑ ผู้ดูแลระบบต้องกำหนดผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (identification) ด้วยชื่อผู้ใช้งาน (username) ทุกครั้ง

๓.๒ ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูลโดยจะต้องมีวิธีการยืนยันตัวบุคคล (authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงเช่นการใช้รหัสผ่าน (password) หรือการใช้สมาร์ทการ์ดหรือการใช้ USB token ที่มีความสามารถ PKI เป็นต้น

๓.๑.๓ ข้อปฏิบัติสำหรับผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่ที่เกี่ยวข้อง

๑) ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องทำการกำหนดสิทธิ์บุคคลในการเข้าออกห้องควบคุมระบบเครือข่ายโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในและมีการบันทึก “ทะเบียนผู้มีสิทธิ์เข้า-ออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

๒) สิทธิ์ในการเข้าออกห้องต่างๆ ภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคนต้องได้รับการอนุมัติจากหัวหน้ากลุ่มงานด้านเทคโนโลยีและสารสนเทศเป็นลายลักษณ์อักษร โดยสิทธิ์ของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายห้องควบคุมระบบเครือข่าย

๓) ต้องจัดทำระบบเก็บบันทึกการเข้าออกกรมอุตุนิยมวิทยาตามกระบวนการที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่”

๔) กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม

๕) การเข้าถึงห้องควบคุมระบบเครือข่ายต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร“บันทึกการเข้า-ออกพื้นที่”

๓.๒ การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks)

๓.๒.๑ ผู้ดูแลระบบต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๓.๒.๒ ผู้ดูแลระบบจัดทำผังเครือข่ายและใช้ IP address และ MAC Address ในการระบุอุปกรณ์บนเครือข่าย

๓.๒.๓ ผู้ดูแลระบบต้องควบคุมการใช้งานอย่างเหมาะสมและจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๓.๓ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection)

ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๑) ผู้ดูแลระบบต้องกำหนดการเปิด-ปิด พอร์ตที่ไม่ใช้งาน

๒) การดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์ เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น

๓) ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๓.๔ การแบ่งแยกเครือข่าย (segregation in networks)

๑) ต้องแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งานโดยแบ่งออกเป็น ๒ เครือข่ายคือเครือข่ายสำหรับผู้ใช้งานภายในและเครือข่ายสำหรับผู้ใช้งานภายนอกเพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ

๒) มีระบบป้องการบุกรุก (Firewall) เพื่อป้องกันทางเข้าเครือข่าย จากผู้ไม่หวังดี

๓.๕ การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control)

ผู้ดูแลระบบต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน ให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

๑) ตรวจสอบการเชื่อมต่อเครือข่าย

๒) จำกัดสิทธิความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

๓) ระบุอุปกรณ์เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๔) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

๕) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่ายโดยไม่ได้รับอนุญาต

๓.๖ การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control)

ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจดังนี้

๑) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๒) กำหนดให้มีการแปลงหมายเลขเครือข่ายเพื่อแยกเครือข่ายย่อย

๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่ายสามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้หรือจำกัดสิทธิในการใช้บริการเครือข่าย

ส่วนที่ ๗

การควบคุมการเข้าถึงระบบปฏิบัติการ

(Operating System Access Control Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. ผู้รับผิดชอบ

ผู้ดูแลระบบที่ได้รับมอบหมาย

ผู้ใช้งาน

๓. แนวปฏิบัติ

๓.๑ การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๓.๑.๑ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้ และรหัสผ่านในการเข้าใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๓.๑.๒ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) หรือทำการล๊อคหน้าจอ (Lock screen) เพื่อทำการล็อคหน้าจอภาพเสมอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๓.๑.๓ ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้ง

๓.๑.๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๓.๑.๕ ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๓.๑.๖ ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๓.๑.๗ ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๓.๑.๘ จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

๓.๑.๙ จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๓.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๓.๒.๑ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาดผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๓.๒.๒ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๒.๓ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับ และห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอนจำหน่ายหรือจ่ายแจกให้ผู้อื่นโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

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

๓.๓ การบริหารจัดการรหัสผ่าน (password management system)

มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ กำหนดให้เปลี่ยนรหัสผ่านทันทีเมื่อเข้าใช้งานครั้งแรก และกำหนดบังคับให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

๓.๔ การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities)

ควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

๓.๔.๑ จำกัดสิทธิการเข้าถึงและกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๓.๔.๒ กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

๓.๔.๓ จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอกถ้าไม่ต้องใช้งานเป็นประจำ

๓.๔.๕ มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๓.๔.๖ กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๓.๔.๗ ห้ามผู้ใช้งานลงโปรแกรมโดยไม่ได้รับอนุญาต หรือละเมิดลิขสิทธิ์

๓.๔.๘ ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือ หลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้

๓.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

๓.๕.๑ ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาที เป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้

งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๕ นาที ตามความเหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๓.๕.๒ ถ้าไม่มีการใช้งานระบบต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๓.๕.๓ เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูง ต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติหลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๓.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time)

ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๓.๖.๑ กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศสำหรับระบบสารสนเทศ หรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ ๓ ชม. ต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น

๓.๖.๒ การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๓.๖.๓ กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูงระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ส่วนที่ ๘

การควบคุมการเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ
(Application Information Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศของกรม และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกและโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

กองบริการดิจิทัลอุตุนิยมวิทยา

ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติ

๓.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

๓.๑.๑ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของกรมอุตุนิยมวิทยา ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๓.๑.๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๓.๑.๓ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

๒) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัยควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๓) ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

๔) ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๕) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งาน (Username) ต้องไม่ซ้ำกัน

๖) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓.๑.๔ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับดังต่อไปนี้

๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๓.๒ การจัดการกับระบบที่ไวต่อการรบกวน

๓.๒.๑ ผู้ดูแลระบบต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน

๓.๒.๒ ต้องควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

๓.๒.๓ ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบ

๓.๓ ข้อปฏิบัติในการการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

เพื่อป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์ คอมพิวเตอร์และสื่อสารเคลื่อนที่

๓.๓.๑ ผู้ดูแลระบบต้องกำหนดมาตรการเพื่อป้องกันการเชื่อมต่อฝานอุปกรณ์เคลื่อนที่โดยไม่ได้รับอนุญาต

๓.๓.๒ อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่จะต้องลงทะเบียนอุปกรณ์ก่อนใช้งาน

๓.๓.๓ ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกรายการอุปกรณ์ในกรณีที่มีการ เข้า-ออกพื้นที่อย่างชัดเจน

๓.๓.๔ ต้องจัดให้มีการสร้างความตระหนักเพื่อระมัดระวังและป้องกันการใช้งานอุปกรณ์เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่

๓.๓.๕ ผู้ดูแลระบบต้องกำหนดให้มีการป้องกันข้อมูลที่สำรองไว้ในอุปกรณ์ จากการถูกขโมย สูญหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต

๓.๔ ข้อปฏิบัติสำหรับการปฏิบัติงานจากภายนอกสำนักงาน (teleworking)

๓.๔.๑ ผู้ใช้งานต้องได้รับการอนุญาตก่อนปฏิบัติงานจากระยะไกล

๓.๔.๒ ผู้ดูแลระบบต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึกอาคารสำนักงานและสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานของกรม

๓.๔.๓ ผู้ดูแลระบบจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกลการจัดเก็บข้อมูลและอุปกรณ์สื่อสารไว้ สำหรับผู้ปฏิบัติงานจากระยะไกลยกเว้นอุปกรณ์ที่กรมได้อนุญาต ให้ใช้งานได้เป็นกรณีไป

๓.๔.๔ ผู้ดูแลระบบต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกลชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ ระบบงานและบริการต่างๆ ของกรมที่อนุญาตให้เข้าถึงได้จากระยะไกล

๓.๔.๕ ผู้ดูแลระบบต้องยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงานและการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

ส่วนที่ ๙

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

(Wireless LAN Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของกรมโดยการกำหนดสิทธิของผู้ใช้ ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๒. ผู้รับผิดชอบ

กองบริการดิจิทัลอุตุนิยมวิทยา

กองสื่อสาร

ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติ

๓.๑ ข้อปฏิบัติสำหรับผู้ใช้งาน

๓.๑.๑ ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของกรม จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตจากหัวหน้ากลุ่มงานด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากหัวหน้ากลุ่มงานด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร

๓.๑.๒ ผู้ใช้ที่ไม่ใช่บุคลากรของกรมอุตุนิยมวิทยา หรือผู้ที่ไม่เกี่ยวข้อง ที่จะขอเข้าใช้งานระบบเครือข่ายไร้สาย จะต้องลงทะเบียนขอใช้งานโดยมีรายละเอียดเกี่ยวกับตัวบุคคล เช่น ชื่อและรหัสประจำตัวประชาชนเป็นอย่างน้อย และผู้ดูแลระบบควรจัดให้ใช้งานได้เฉพาะเครือข่ายอินเตอร์เน็ตเท่านั้น เพื่อช่วยป้องกันการเข้าถึงข้อมูลภายใน การโจมตี หรือการบุกรุกเครือข่ายภายในของกรมอุตุนิยมวิทยา

๓.๒ ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๓.๒.๑ ผู้ดูแลระบบ ต้องตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

๓.๒.๒ ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓.๒.๓ ผู้ดูแลระบบ จะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๓.๒.๔ ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตี สามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

๓.๒.๕ ผู้ดูแลระบบ ควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

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

๓.๒.๗ ผู้ดูแลระบบ ต้องเปลี่ยนค่าชื่อผู้ใช้และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและผู้ดูแลระบบต้องเลือกใช้ชื่อผู้ใช้และรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตี ไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๓.๒.๘ ผู้ดูแลระบบ ต้องกำหนดค่าใช้ WPA หรือ WPA๒ เป็นอย่างน้อย ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Clientและ AP เพื่อให้ยากต่อการดักจับจะช่วยให้ปลอดภัยมากยิ่งขึ้น

๓.๒.๙ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

๓.๒.๑๐ ผู้ดูแลระบบ ควรควบคุมการเข้าใช้งานระบบเครือข่ายไร้สาย เช่น เลือกใช้วิธีการควบคุม MAC address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย

๓.๒.๑๑ ผู้ดูแลระบบ ควรจะมีการติดตั้งไฟร์วอล (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในกรม

ส่วนที่ ๑๐

การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(Third party Access Control Policy)

๑. วัตถุประสงค์

เพื่อป้องกันความเสี่ยงต่อการเข้าถึงข้อมูล การถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงาน โดยไม่ได้รับอนุญาตการใช้บริการจากหน่วยงานภายนอก และเพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมเป็นไปอย่างมั่นคงปลอดภัย ให้กำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบการใช้บริการของที่ปรึกษาการใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

๒. ผู้รับผิดชอบ

กองบริการดิจิทัลอุตุนิยมวิทยา

ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติ

๓.๑ หัวหน้ากลุ่มงานด้านเทคโนโลยีและสารสนเทศต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ และการสื่อสารหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

๓.๒ การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

๓.๒.๑ บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตุนิยมวิทยาจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อข้ออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ กองสื่อสารและเทคโนโลยีสารสนเทศ

๓.๒.๒ จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารซึ่งต้องมีรายละเอียดอย่างน้อยดังนี้

(๑) เหตุผลในการขอใช้

(๒) ระยะเวลาในการใช้

(๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

(๔) การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

(๕) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๓.๒.๓ หน่วยงานภายนอกที่ทำงานให้กับกรมอุตุนิยมวิทยาทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในกรมอุตุนิยมวิทยาหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของกรมอุตุนิยมวิทยา โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๓.๒.๔ กรมอุตุนิยมวิทยาควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เข้าไปปฏิบัติงาน

๓.๒.๕ เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๓.๒.๖ สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของกรมอุตุนิยมวิทยาผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือการรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๓.๒.๗ กรมอุตุนิยมวิทยามีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มั่นใจได้ว่ากรมอุตุนิยมวิทยาสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

๓.๒.๘ ควรดำเนินการให้ผู้ให้บริการหน่วยงานภายนอก จัดทำแผนการดำเนินงานคู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

ส่วนที่ ๑๑
ความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต
(Internet Security Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเตอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่น อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของกรมอุตุนิยมวิทยา ถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. ผู้รับผิดชอบ

ผู้ใช้งาน

ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติ

๓.๑ ข้อปฏิบัติสำหรับผู้ใช้งาน

๓.๑.๑ ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านชองทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็น และทำการข้ออนุญาตจากกองสื่อสารและเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

๓.๑.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเตอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ชองระบบปฏิบัติการเว็บเบราเซอร์

๓.๑.๓ ผู้ใช้ควรหมั่น Update Patch และ Hot Fix อย่างสม่ำเสมอโดยสามารถ Download patch และ Hot Fix ต่างๆ จากเจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่

๓.๑.๔ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ต จะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๓.๑.๕ ผู้ใช้ต้องไม่ใช้เครือข่ายอินเตอร์เน็ตของกรมอุตุนิยมวิทยาเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาที่ขัดต่อ ชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๓.๑.๖ ผู้ใช้จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่าย และความปลอดภัยทางข้อมูลของกรมอุตุนิยมวิทยา

๓.๑.๗ ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับกรมอุตุนิยมวิทยา

๓.๑.๘ ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมอุตุนิยมวิทยาที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเตอร์เน็ต

๓.๑.๙ ผู้ใช้ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียงถูกดูหมิ่นถูกเกลียดชังหรือได้รับความอับอาย

๓.๑.๑๐ หลังจากใช้งานอินเตอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๓.๒ ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๓.๒.๑ ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่กรมอุตุนิยมวิทยาจัดสรรไว้เท่านั้น โดยผ่าน Proxy, Firewall, IPS-IDS

ส่วนที่ ๑๒
การใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail Policy)

๑. วัตถุประสงค์

๑.๑ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยา สามารถสนับสนุนการปฏิบัติงานและการบริหารงานของกรมอุตุนิยมวิทยา เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพและประสิทธิผล

๑.๒ เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของกรมอุตุนิยมวิทยาและหน่วยงานเป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบ คำสั่งข้อบังคับของกรมอุตุนิยมวิทยา

๒. ผู้รับผิดชอบ

ผู้ใช้งาน

ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติ

๓.๑ ข้อปฏิบัติสำหรับผู้ใช้งาน

๓.๑.๑ สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (default password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์ และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

๓.๑.๒ รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น ‘x’ หรือ ‘o’ ในการพิมพ์แต่ละตัวอักษร

๓.๑.๓ ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์

๓.๑.๔ ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดเช่นควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน

๓.๑.๕ ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อกรมอุตุนิยมวิทยาหรือละเมิดสิทธิ์สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมายหรือละเมิดศีลธรรมและไม่แสวงหาประโยชนหรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชนในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกรมอุตุนิยมวิทยา

๓.๑.๖ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านรับ-ส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๓.๑.๗ ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาเพื่อการทำงานในภารกิจของกรมอุตุนิยมวิทยาเท่านั้น

๓.๑.๘ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควรทำการลงบันทึกออก (Logout) จากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๓.๑.๙ ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์ โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file

๓.๑.๑๐ ผู้ใช้ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๓.๑.๑๑ ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมข้อมูลอันอาจทำให้เสียชื่อเสียงของกรมอุตุนิยมวิทยา หรือข้อมูลที่ทำให้เกิดความแตกแยกในหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

๓.๑.๑๒ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๓.๑.๑๓ ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ (Mail box) ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๓.๑.๑๔ ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๓.๒ ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๓.๒.๑ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

๓.๒.๒ ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้ ให้มีและรหัสผ่านสำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยา

๓.๓.๓ ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง

๓.๓.๔ ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ควรมีการลงบันทึกออก (Logout) จากหน้าจอตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้เช่น ๑๐ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

ส่วนที่ ๑๓

ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์

(Terms of Use and Disclaimer)

๑. วัตถุประสงค์

๑.๑ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยา สามารถสนับสนุนการปฏิบัติงานของกรมอุตุนิยมวิทยาเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ

๑.๒ เพื่อให้การติดต่อสื่อสาร โดยการรับ-ส่งข้อมูลข่าวสารด้วยระบบจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของกรมอุตุนิยมวิทยาและหน่วยงานเป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบคำสั่ง ข้อบังคับ คำแนะนำและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของกรมอุตุนิยมวิทยาอุตุนิยมวิทยา

๒. ผู้รับผิดชอบ

ผู้ใช้บริการ

๓. แนวปฏิบัติ

๓.๑ ข้อตกลงการใช้บริการ

๓.๑.๑ ผู้ใช้บริการระบบจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาจะต้องไม่กระทำการอันละเมิดต่อกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำ อย่างน้อยดังต่อไปนี้

๑) พระราชบัญญัติกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

๒) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔

๓) พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐

๔) ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

๕) ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗

๖) ระเบียบรักษาความปลอดภัยด้านการสื่อสาร พ.ศ.๒๕๒๕

๗) ข้อตกลงเงื่อนไขการใช้บริการที่กรมอุตุนิยมวิทยากำหนด

๓.๑.๒ หน่วยงาน/บุคคลผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยา จะต้องใช้จดหมายอิเล็กทรอนิกส์นี้เพื่อผลประโยชน์ของทางราชการ

๓.๑.๓ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยา เพื่อการประกอบธุรกิจหรือแสวงหาผลประโยชน์ส่วนตน

๓.๑.๔ ห้ามใช้บริการนี้ไปในการเผยแพร่อ้างอิงพาดพิงดูหมิ่นหรือการกระทำใดๆ ที่ก่อให้เกิดความเสียหายต่อสถาบัน ชาติ ศาสนา และพระมหากษัตริย์

๓.๑.๕ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาในการประกอบอาชญากรรมทางคอมพิวเตอร์หรือการกระทำการใดๆ ซึ่งผิดกฎหมายคำสั่งระเบียบข้อบังคับและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารลับของทางราชการ

๓.๑.๖ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยา เพื่อการเผยแพร่ข้อมูลข่าวสารหรือภาพเสียงข้อความที่ไม่เหมาะสมหรือสร้างความเสื่อมเสียให้กับผู้อื่น

๓.๑.๗ ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ไปแสดงข้อคิดเห็นส่วนตัวที่ส่งผลกระทบในทางลบหรือสร้างความเสื่อมเสียหรือเสียหายต่อบุคคลหรือกรมอุตุนิยมวิทยา

๓.๑.๘ ห้ามกระทำการปลอมแปลงที่อยู่เป็นบุคคลอื่น (Impersonation)

๓.๑.๙ ห้ามกระทำการที่สร้างปัญหาการใช้ทรัพยากรของระบบ เช่น

(๑) การสร้างจดหมายลูกโซ่ (Chain mail)

(๒) การส่งจดหมายจำนวนมาก (Spam mail)

(๓) การส่งจดหมายต่อเนื่อง (Letter bomb)

(๔) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์

๓.๑.๑๐ ห้ามผู้ใช้บริการกระทำการใดๆ ที่อาจจะนำมาซึ่งความเสื่อมเสียหรือก่อให้เกิดความเสียหายแก่ระบบเครื่องแม่ข่ายจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยา

๓.๑.๑๑ ผู้ใช้ต้องรักษารหัสผ่าน (Password) ส่วนบุคคลหรือหน่วยงานของจดหมายอิเล็กทรอนิกส์เป็นไว้เป็นความลับ

๓.๑.๑๒ ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับราชการของกรมอุตุนิยมวิทยา

๓.๑.๑๓ การส่งข้อมูลข่าวสารที่เป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานนอกกรมอุตุนิยมวิทยาจะต้องเข้ารหัสข้อมูลข่าวสารนั้นอย่างเหมาะสม ตามวิธีปฏิบัติและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารตามที่กรมอุตุนิยมวิทยากำหนด

๓.๑.๑๔ ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail address) และรหัสผ่าน (Password) ของหน่วยงานหรือบุคคลจะต้องเก็บรักษาไว้เป็นความลับ หากสงสัยว่ารั่วไหลจะต้องดำเนินการเปลี่ยนรหัสผ่านทันที โดยรหัสผ่านจะต้องกำหนดให้ยากแก่การคาดเดา (Strong Password)

๓.๑.๑๕ ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยา หรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์ (Email address) จะต้องศึกษาคู่มือการใช้งานระเบียบปฏิบัติคำแนะนำและข้อตกลงเงื่อนไขให้เข้าใจเพื่อใช้งานจดหมายอิเล็กทรอนิกส์ของกรมอุตุนิยมวิทยาได้อย่างถูกต้อง

๓.๑.๑๖ กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอให้สงวนสิทธิ์ที่จะทำการยกเลิกหรือระงับบริการแก่สมาชิกนั้นๆ เป็นการชั่วคราว เพื่อทำการสอบสวนและตรวจสอบหาสาเหตุของมูลเหตุนั้นๆ

๓.๑.๑๗ การกระทำใดๆ ที่เกี่ยวกับการเผยแพร่ทั้งในรูปแบบของอีเมล์และ/หรือโฮมเพจของผู้ใช้บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการ กองสื่อสารและเทคโนโลยีสารสนเทศ ไม่มีส่วนเกี่ยวข้องใดๆ

๓.๑.๑๘ กรณีที่ผู้ใช้งานมีการใช้งาน ระบบการสื่อสารแบบรวมศูนย์ (workD Communication Platform) ต้องปฏิบัติตามข้อกำหนดของผู้ให้บริการด้วย https://workd.go.th/files/terms-and-conditions_UC_280466.pdf

หมวดที่ ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองของสารสนเทศ

ส่วนที่ ๑๔
การสำรองและกู้คืนข้อมูล
(Backup and Recovery Policy)

๑. วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติการสำรองข้อมูลและการกู้คืนระบบ (Backup and Recovery) โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่าย สามารถดำเนินการสำรองข้อมูลได้อย่างสมบูรณ์ถูกต้องและสามารถกู้คืนระบบได้ ในกรณีที่จำเป็น

๒. ผู้รับผิดชอบ

กองบริการดิจิทัลอุตุนิยมวิทยา

ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติ

๓.๑ ระบบสำรอง

๓.๑.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสม ให้อยู่ในสภาพพร้อมใช้งานสำรองข้อมูล และจัดทำระบบสารสนเทศสำรอง

๓.๑.๒ ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

๓.๑.๓ ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูลสถานที่จัดเก็บ โดยรูปแบบการสำรองข้อมูลอาจแบ่งได้เป็นการสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๓.๑.๔ การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึก รายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น

๓.๑.๕ การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๓.๑.๖ ในกรณีที่พบปัญหาในการสำรองข้อมูล จนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อหัวหน้ากลุ่มงานด้านเทคโนโลยีสารสนเทศ

๓.๑.๗ การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้นรวมทั้งวิธีการที่ใช้แก้ไขด้วย

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

๓.๑.๙ ต้องทำการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๓.๒ การสำรองข้อมูล

๓.๒.๑ ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่าย ต้องทำการสำรองข้อมูลแต่ละรายการตามความถี่อย่างน้อย ดังนี้

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
หมายเหตุ ทุกรายการที่ปรากฏในตารางนี้จะใช้วิธีสำรองข้อมูลแบบ Full Backup ส่วนการสำรองข้อมูลแบบ Incremental Backup ให้พิจารณาตามความสำคัญของข้อมูล			

๓.๒.๒ ผู้ดูแลระบบต้องทำการเก็บรักษาข้อมูลที่สำรองอย่างน้อย ๑ ชุด แยกสถานที่กัน เพื่อความมั่นคงปลอดภัยและใช้งานได้อย่างต่อเนื่อง

๓.๒.๓ ผู้ดูแลระบบคอมพิวเตอร์ต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเอง ว่าการสำรองข้อมูลตามรายละเอียดในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

๓.๓ การกู้คืนระบบ (Data Recovery)

๓.๓.๑ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย จะต้องทำการทดสอบการกู้คืนข้อมูลเป็นระยะเพื่อให้แน่ใจได้ว่าการสำรองข้อมูลนั้นทำได้อย่างครบถ้วนสมบูรณ์แล้ว

๓.๓.๒ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่าย จนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไขรายงานผลการแก้ไข พร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อหัวหน้า

กลุ่มงานด้านเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายจากหัวหน้ากลุ่มงานด้านเทคโนโลยีสารสนเทศทราบ

๓.๓.๓ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๓.๓.๔ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๓.๔ การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) ต้องกำหนดบุคลากรที่เกี่ยวข้องและดำเนินการ ดังต่อไปนี้

๓.๔.๑ กำหนดแผนเตรียมความพร้อม และกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติ

๓.๔.๒ กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ

๓.๔.๓ ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบติดขัดหรือไม่สามารถใช้งานได้อันเป็นผลจากภัยพิบัติที่กำหนดไว้

๓.๔.๔ จัดทำแผนรับมือกับเหตุภัยพิบัติเพื่อให้สามารถกู้คืนระบบเทคโนโลยีสารสนเทศที่เสียหายให้สามารถใช้งานได้โดยเร็ว

๓.๔.๕ ทดสอบการปฏิบัติตามแผนอย่างน้อยปีละ ๑ ครั้งโดยการจำลองสถานการณ์

๓.๔.๖ ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูงอย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๑๕
การตรวจสอบและประเมินความเสี่ยง

๑. วัตถุประสงค์

เพื่อให้มีมาตรการในการตรวจสอบ ประเมิน ควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ผู้รับผิดชอบ

ศูนย์เทคโนโลยีสารสารสนเทศ

ผู้ตรวจสอบภายใน (internal auditor) หรือผู้ตรวจสอบจากภายนอก (external auditor)

ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติ

๓.๑ ตรวจสอบและประเมินความเสี่ยงในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 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)

หมวดที่ ๔ การสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ ๑๖
การสร้างความตระหนัก
ในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้องได้มีความรู้ ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

ศูนย์เทคโนโลยีสารสนเทศ

สถาบันอุตุนิยมวิทยา

๓. แนวปฏิบัติ

๓.๑ จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของกรม

๓.๒ จัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัยและมีการเผยแพร่ทางเว็บไซต์ของกรม

๓.๓ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย ซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ โดยการติดประกาศประชาสัมพันธ์แผ่นพับเผยแพร่ผ่านเว็บไซต์

๓.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติ ด้วยการกำกับติดตามประเมินผลและสำรวจความต้องการของผู้ใช้บริการ