ระเบียบสำนักงานเศรษฐกิจการเกษตร

ว่าด้วยการใช้งานระบบเครือข่ายคอมพิวเตอร์ขององค์กรอย่างปลอดภัย

พ.ศ. ๒๕๕๓

ด้วยสำนักงานเศรษฐกิจการเกษตร ได้พัฒนาระบบเครือข่ายคอมพิวเตอร์และระบบฐานข้อมูลสารสนเทศขึ้นเพื่อเป็นประโยชน์ต่อการปฏิบัติงานของบุคลากรในสำนักงาน ดังนั้นเพื่อให้การใช้งานเครือข่ายคอมพิวเตอร์และระบบฐานข้อมูลสารสนเทศเป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์ ในลักษณะที่ไม่ถูกต้อง และเพื่อควบคุมการใช้งานให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ สำนักงานเศรษฐกิจการเกษตรเห็นสมควรให้มีนโยบายการใช้งานอย่างปลอดภัย (Acceptable Use Policy) โดยวางระเบียบไว้ดังต่อไปนี้

หมวดที่ ๑ บททั่วไป

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบการใช้งานระบบเครือข่ายคอมพิวเตอร์ขององค์กรอย่างปลอดภัย พ.ศ.๒๕๕๓”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่วันถัดจากเลขาธิการสำนักงานเศรษฐกิจการเกษตร ลงนาม

ข้อ ๓ บรรดาระเบียบ คำสั่ง และข้อบังคับในส่วนที่มีประกาศไว้แล้วในระเบียบนี้หรือขัดแย้งกับบทแห่งระเบียบนี้ให้ใช้ระเบียบนี้แทน

ข้อ ๔ ในระเบียบนี้

“สำนักงาน” หมายความถึง สำนักงานเศรษฐกิจการเกษตร กระทรวงเกษตรและสหกรณ์

“เครือข่ายคอมพิวเตอร์” หมายความถึง เครือข่ายคอมพิวเตอร์ของสำนักงานเศรษฐกิจการเกษตร

“ศูนย์” หมายความถึง ศูนย์สารสนเทศการเกษตร

“ผู้บังคับบัญชา” หมายความถึง ผู้มีอำนาจสั่งการตามโครงสร้างของสำนักงานเศรษฐกิจการเกษตร

“ผู้ใช้” หมายความถึง ข้าราชการ พนักงานราชการและลูกจ้างของสำนักงานเศรษฐกิจการเกษตร รวมถึงบุคคลอื่นที่สำนักงานเศรษฐกิจมอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลง หรือใบสั่งซื้อ

“ข้อมูล” หมายความถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการอื่นใด และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศ” หมายความถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

“ระบบสารสนเทศ” หมายความถึง ระบบที่มีการนำคอมพิวเตอร์มาช่วยในการรวบรวม จัดเก็บ หรือจัดการกับข้อมูลข่าวสาร เพื่อให้ข้อมูลนั้นสามารถนำไปใช้ประกอบการดำเนินงานและตัดสินใจได้

ข้อ ๕ ให้ผู้บริหารเทคโนโลยีระดับสูงของสำนักงานเศรษฐกิจการเกษตร รักษาการตามระเบียบนี้

หมวดที่ ๒ ข้อปฏิบัติในการใช้งานเครือข่ายคอมพิวเตอร์

ข้อ ๑ ผู้ใช้มีสิทธิใช้เครือข่ายคอมพิวเตอร์ได้ภายใต้ข้อกำหนดแห่งระเบียบนี้ การฝ่าฝืนข้อกำหนดและก่อหรืออาจก่อให้เกิดความเสียหายแก่สำนักงาน หรือบุคคลหนึ่งบุคคลใด สำนักงานจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ใช้ที่ฝ่าฝืนตามความ เหมาะสมต่อไป

ข้อ ๒ ผู้ใช้พึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ เช่น ไม่ดาวน์โหลดไฟล์ที่มีขนาดใหญ่โดยไม่จำเป็น และไม่ควรปฏิบัติในระหว่างเวลาทำงานซึ่งมีการใช้เครือข่ายอย่างหนาแน่น เช่น ในช่วงเวลา ๐๘.๓๐ – ๑๒.๐๐ น. และ ๑๓.๐๐ – ๑๖.๓๐ น.

ข้อ ๓ ผู้ใช้พึงใช้ข้อความที่สุภาพและถูกต้องตามธรรมเนียมปฏิบัติในการใช้เครือข่าย อาทิเช่น ไม่ใช้การส่งอีเมล์ แบบกระจายถึงทุกคนที่เป็นสมาชิกเครือข่ายโดยไม่จำเป็น หรือ การใช้ข้อความที่สุภาพชนทั่วไปพึงใช้ในข้อความที่ส่งไปถึงบุคคลอื่น เป็นต้น

ข้อ ๔ ผู้ใช้ต้องใช้บัญชีผู้ใช้ในโดเมนที่สำนักงานกำหนดให้ ก่อนใช้ระบบคอมพิวเตอร์และเครือข่ายทุกครั้ง และมีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งไม่อนุญาตให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้ของตนเอง

ข้อ ๕ เพื่อประโยชน์ในการใช้รหัสผ่านส่วนบุคคล ผู้ใช้จะต้อง

(๑) ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้งานเครื่องคอมพิวเตอร์ที่ผู้ใช้ครอบครองใช้งานอยู่ โดยรหัสผ่านส่วนบุคคลดังกล่าวต้องมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน แต่ไม่ควรกำหนด

รหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๒) ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๓) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้ครอบครองอยู่

(๔) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือบันทึกไว้ในระบบคอมพิวเตอร์ ระบบอิเล็กทรอนิกส์

ข้อ ๖ ผู้ใช้จะต้องไม่ใช้เครือข่ายคอมพิวเตอร์โดยมีวัตถุประสงค์ดังต่อไปนี้

(๑) เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

(๒) เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

(๓) เพื่อการพาณิชย์ และการแสวงหาผลประโยชน์อันมิชอบ

(๔) เพื่อการเปิดเผยข้อมูลที่เป็นความลับ หรือปกปิด ซึ่งได้มาจากการปฏิบัติให้แก่สำนักงาน ไม่ว่าจะเป็นข้อมูลของสำนักงาน หรือบุคคลภายนอกก็ตาม

(๕) เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของสำนักงานหรือของบุคคลอื่น

(๖) เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

(๗) เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่สำนักงาน เช่น การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับหรือส่งข้อมูลที่ได้รับจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิด ต่อกฎหมายหรือสิทธิของบุคคลอื่นไปยังผู้ใช้หรือบุคคลอื่น เป็นต้น

(๘) เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของสำนักงาน หรือของผู้ใช้อื่นของสำนักงาน หรือเพื่อให้เครือข่ายคอมพิวเตอร์ของสำนักงาน ไม่สามารถใช้งานได้ตามปกติ

(๙) เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของสำนักงานไปยังที่อยู่เว็บ (web site) ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

(๑๐) เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ของสำนักงาน หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่สำนักงาน

ข้อ ๗ เพื่อความปลอดภัยในการใช้เครือข่ายคอมพิวเตอร์โดยส่วนรวม ผู้ใช้จะต้อง

(๑) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น

(๒) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาก่อน

(๓) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ส่วนบุคคลของสำนักงาน เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนั้นหรือเครือข่ายคอมพิวเตอร์ของสำนักงานได้

(๔) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้ครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องบริการ (Server) ที่ต้องใช้งานตลอด ๒๔ ชั่วโมง

(๕) ตรวจสอบข้อมูลที่ได้รับจากภายนอกสำนักงาน ทุกครั้งด้วยโปรแกรมคอมพิวเตอร์สำหรับตรวจสอบกำจัดไวรัส โทรจันและหนอนคอมพิวเตอร์ที่สำนักงาน จัดให้ และหากตรวจพบไวรัสโทรจันและหนอนคอมพิวเตอร์ฝังตัวอยู่ในข้อมูลส่วนใดจะต้องรีบจัดการทำลายไวรัสโทรจันและหนอนคอมพิวเตอร์ หรือข้อมูลนั้นโดยเร็วที่สุด

(๖) สำนักงานและศูนย์ ได้จัดเตรียมพื้นที่สำหรับจัดเก็บข้อมูลที่ใช้ร่วมกัน แต่ขอสงวนสิทธิในการบริหารจัดการข้อมูลโดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า

(๗) ลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตน จากเครื่องให้บริการอิเล็กทรอนิกส์เมล์ และเครื่องให้บริการไฟล์ เพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

(๘) การนำเครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วงที่เป็นของส่วนตัวมาใช้ในเครือข่ายคอมพิวเตอร์ของสำนักงาน ต้องแจ้งให้ศูนย์ทราบก่อนดำเนินการทุกครั้ง

(๙) ใช้โปรแกรมคอมพิวเตอร์ที่มีการเข้ารหัสข้อมูลซึ่งสำนักงานจัดให้สำหรับใช้ในการติดต่อกับเครือข่ายคอมพิวเตอร์จากภายนอกสถานที่ทำการของสำนักงาน

(๑๐) ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศ หรือผู้ที่ได้รับมอบหมายให้ดำเนินการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลของผู้ใช้และเครือข่ายคอมพิวเตอร์ รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชา ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

(๑๑) ระมัดระวังการใช้งานและสงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์เหมือนเช่นบุคคลทั่วไปจะพึงปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์ แล้วแต่กรณี

(๑๒) ไม่เข้าไปในสถานที่ตั้งของระบบเครือข่ายคอมพิวเตอร์ก่อนได้รับอนุญาต

ข้อ ๘ คืนทรัพย์สินอันเกี่ยวข้องกับการใช้งานเครือข่ายคอมพิวเตอร์ที่เป็นของสำนักงาน เช่น ข้อมูล และสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้าหรือออก ฯลฯ ให้แก่สำนักงาน รวมทั้งขอรับข้อมูลส่วนบุคคลที่อยู่บนเครือข่ายคอมพิวเตอร์คืนจากสำนักงาน ภายในกำหนด ๗ วันนับแต่วันพ้นสภาพการเป็นผู้ใช้

ข้อ ๙ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศที่ฝ่าฝืนข้อกำหนดในระเบียบนี้ และก่อหรืออาจก่อให้เกิดความเสียหายแก่สำนักงาน หรือบุคคลหนึ่งบุคคลใด สำนักงานจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศนั้น ตามความเหมาะสมต่อไป

หมวดที่ ๓ ข้อปฏิบัติของผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศ

ข้อ ๑ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศจะต้องดูแลรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งจะต้องสอดส่องดูแลการใช้เครือข่ายคอมพิวเตอร์ของผู้ใช้เพื่อให้เป็นไปตามระเบียบนี้

หากผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศพบว่าผู้ใช้ผู้ใดมีพฤติการณ์ส่อไปในทางที่จะละเมิดข้อกำหนดการใช้เครือข่ายคอมพิวเตอร์แห่งระเบียบนี้ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศจะต้องรายงานให้ผู้อำนวยการศูนย์สารสนเทศการเกษตร ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปทราบโดยเร็วที่สุด และในกรณีจำเป็นเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นแก่สำนักงาน ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศมีอำนาจในการระงับการใช้งานเครือข่าย คอมพิวเตอร์ของผู้ใช้ดังกล่าวได้ทันที

ข้อ ๒ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศมีหน้าที่ในการเสนอความเห็นและข้อสังเกตต่อผู้บังคับบัญชาที่เหนือขึ้นไปเพื่อพิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพและการบริหารเครือข่ายคอมพิวเตอร์ หรือปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ตามที่ผู้บังคับบัญชามอบหมาย

ข้อ ๓ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศมีหน้าที่ในการติดตั้งอุปกรณ์ ซอฟต์แวร์ ระบบการเข้ารหัสข้อมูลอัตโนมัติหรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาให้สามารถใช้งานได้ดีอยู่เสมอ

ข้อ ๔ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศจะต้องไม่ใช้อำนาจหน้าที่ของตนไปในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึง ข้อมูลนั้น และจะต้องไม่เปิดเผยข้อมูลที่ตนได้รับมาจากหรือเนื่องจากการปฏิบัติหน้าที่ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผย ให้บุคคลหนึ่งบุคคลใดทราบ

ข้อ ๕ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศมีสิทธิตรวจสอบข้อมูลทุกประเภท ตามความจำเป็นในการซ่อมแซมแก้ไขบำรุงรักษาระบบ หรือการสืบสวนเกี่ยวกับการใช้งานระบบอย่างไม่ถูกต้อง

ข้อ ๖ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศมีหน้าที่ดำเนินการควบคุมดูแลการใช้งานอุปกรณ์คอมพิวเตอร์ทั้งหมดของสำนักงาน

ข้อ ๗ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศมีหน้าที่ดำเนินการควบคุมและตรวจสอบการติดตั้งโปรแกรมเข้าสู่ระบบคอมพิวเตอร์ทั้งหมดของหน่วยงาน ให้เป็นไปตามความมุ่งหมายของสำนักงาน

ข้อ ๘ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศมีหน้าที่ดำเนินการตามที่ผู้บังคับบัญชามอบหมายและจัดทำรายงานเกี่ยวกับการปฏิบัติตามระเบียบนี้เสนอต่อผู้บังคับบัญชา

ข้อ ๙ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศมีอำนาจหน้าที่ที่จะเพิกถอนสิทธิ์การใช้ระบบต่อผู้ใช้ที่ฝ่าฝืนระเบียบนี้

ข้อ ๑๐ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศมีหน้าที่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า เกี่ยวกับวันเวลาที่จะปิดระบบคอมพิวเตอร์และเครือข่ายเพื่อบำรุงรักษา ปรับปรุง หรือเปลี่ยนแปลงระบบ ซึ่งส่งผลให้ต้องหยุดให้บริการในช่วงเวลาหนึ่ง เว้นแต่ในกรณีฉุกเฉินผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศสามารถปิดระบบได้ทันทีโดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า

ข้อ ๑๑ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศมีสิทธิบีบอัด ลดขนาดแฟ้มข้อมูลที่มีขนาดใหญ่ รวมถึงมีสิทธิ์ในการยุติการทำงานที่สร้างภาระให้ระบบโดยไม่จำเป็นหรือเกินขนาดได้โดยแจ้งให้ผู้ใช้ทราบล่วงหน้า

ข้อ ๑๒ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศมีหน้าที่สำรองข้อมูลในระบบสารสนเทศ และตรวจสอบความสามารถการในการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

ข้อ ๑๓ เมื่อผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศจะต้องคืนทรัพย์สินอันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นของสำนักงาน เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ ให้แก่สำนักงาน ในทันทีที่พ้นหน้าที่และให้คณะกรรมการรักษาความมั่นคงปลอดภัยข้อมูลระบบเทคโนโลยีสารสนเทศและการสื่อสารดำเนินการตรวจสอบการคืนทรัพย์สินของผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศที่พ้นจากหน้าที่โดยละเอียดเพื่อความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์

ข้อ ๑๔ ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศที่ฝ่าฝืนข้อกำหนดในระเบียบนี้ และก่อหรืออาจก่อให้เกิดความเสียหายแก่สำนักงาน หรือบุคคลหนึ่งบุคคลใด สำนักงานจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศนั้น ตามความเหมาะสมต่อไป

หมวด ๔ ว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

ข้อ ๑ บรรดากฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบ ของสำนักงานถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวดที่ ๕ การรักษาความปลอดภัยอุปกรณ์คอมพิวเตอร์

ข้อ ๑ อุปกรณ์คอมพิวเตอร์ในระบบคอมพิวเตอร์ของสำนักงานทุกหน่วย หรือทุกชุด ต้องมีการกำหนดผู้รับผิดชอบ และจัดทำรายละเอียดที่จำเป็น เช่น ผู้ที่ได้รับอนุญาตให้เข้าใช้ การใช้งานตลอดจนระดับของการป้องกัน

ข้อ ๒ ให้ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศตรวจสอบอุปกรณ์ที่นำมาติดตั้งทุกครั้ง และให้ตรวจสอบบำรุงรักษาอย่างสม่ำเสมอ

ข้อ ๓ การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เข้า-ออกนอกสำนักงาน หรือการเคลื่อนย้ายที่มีผลทำให้สภาวะการทำงานของอุปกรณ์เปลี่ยนแปลงไป จะต้องแจ้งและขออนุญาตตามลำดับชั้น ก่อนการเคลื่อนย้ายทุกครั้ง

ข้อ ๔ ก่อนนำอุปกรณ์คอมพิวเตอร์ไปซ่อมบำรุง หรือจำหน่ายซากให้บุคคลภายนอกสำนักงานต้องทำลายข้อมูลทั้งหมดที่อยู่ในอุปกรณ์ดังกล่าวไม่ให้สามารถกู้คืนมาใช้งานได้อีก

ข้อ ๕ ให้หน่วยงานระดับสำนัก / ศูนย์ / กอง / สศข. ทำบัญชีครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงเพื่อจัดทำเป็นบัญชีครุภัณฑ์รวมของสำนักงาน

ข้อ ๖ ให้มีการเก็บบันทึกการเข้าออกห้องเครื่องแม่ข่ายจากบุคคลภายนอก โดยในบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาเข้าออก และให้มีการตรวจสอบบันทึกดังกล่าวอยู่เสมอ

ข้อ ๗ เครื่องคอมพิวเตอร์ทุกเครื่องของสำนักงานต้องติดตั้งโปรแกรมที่จัดหาให้สำหรับป้องกันโปรแกรมที่ไม่พึงประสงค์ เช่น ไวรัส โทรจัน และหนอนคอมพิวเตอร์

หมวดที่ ๖ การควบคุมการเข้าถึงระบบสารสนเทศ

ข้อ ๑ ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบฐานข้อมูลสารสนเทศ เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๒ ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๓) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๔) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๓ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

(๕) ควรกำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ ๔ การให้สิทธิและการถอดถอนสิทธิในการเข้าถึงระบบสารสนเทศตามความจำเป็นในการใช้งานของผู้ใช้ โดยต้องได้รับการอนุมัติจากผู้บังคับบัญชาของผู้ใช้

ข้อ ๕ ผู้ที่สามารถเข้าถึงระบบสารสนเทศได้ต้องเป็นผู้ที่มีสิทธิในการเข้าถึงระบบผ่านขั้นตอนการพิสูจน์ตัวตน พิสูจน์สิทธิอย่างถูกต้อง และระบุตัวตนของตนเองได้ในเวลาเข้าถึงแล้วเท่านั้น

ข้อ ๖ การให้สิทธิต้องมีการแบ่งแยกระดับสิทธิการเข้าถึงในแต่ละระบบสารสนเทศ เช่น แบ่งตามความจำเป็นตามหน้าที่ของผู้ใช้งานเป็น ผู้ใช้งาน ผู้ปฏิบัติงาน และผู้ควบคุมระบบสารสนเทศ

ข้อ ๗ การเข้าถึงระบบสารสนเทศต้องสามารถตรวจสอบย้อนหลังได้

ข้อ ๘ เมื่อผู้ใช้หมดหน้าที่ในการใช้ระบบสารสนเทศนั้น ต้องแจ้งผู้มีอำนาจตามระบบสารสนเทศนั้น เพื่อระงับสิทธิการเข้าถึง

ข้อ ๙ ในกรณีที่มีความจำเป็นต้องให้สิทธิในการเข้าถึงระบบสารสนเทศชั่วคราวต้องได้รับอนุมัติจากผู้มีอำนาจตามระบบสารสนเทศนั้น โดยต้องระบุเหตุผล มีกำหนดระยะเวลาการใช้งาน และระงับทันทีเมื่อพ้นกำหนดระยะเวลาที่กำหนดไว้

ข้อ ๑๐ การแชร์ทรัพยากรคอมพิวเตอร์เช่น ข้อมูล เครื่องพิมพ์ ผู้ใช้ต้องกำหนดสิทธิการเข้าถึงให้กับผู้ที่เกี่ยวข้องกับการใช้ทรัพยากรเท่านั้น และให้ยกเลิกการแชร์เมื่อเสร็จสิ้นภารกิจ

ข้อ ๑๑ การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ จัดให้มีการป้องกันการเข้าถึงเอกสารระบบ หรือข้อมูลที่เกี่ยวกับระบบงานจากผู้ที่ไม่มีสิทธิในการเข้าถึงซึ่งควรประกอบด้วยรายละเอียดดังนี้

(๑) เอกสารระบบต้องเก็บในบริเวณที่มีความมั่นคงปลอดภัย

(๒) ผู้เป็นเจ้าของระบบงานต้องเป็นผู้กำหนดสิทธิในการเข้าถึงเอกสารระบบ และจำกัดคนที่มีสิทธิในการเข้าถึงให้น้อยที่สุด

(๓) เอกสารระบบเครือข่าย ต้องได้รับการจัดเก็บโดยมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

หมวด ๗ ว่าด้วยการบริหารจัดการข้อมูลองค์กร

ข้อ ๑ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของสำนักงาน หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๒ ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของสำนักงาน ถือเป็นทรัพย์สินของสำนักงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๓ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของสำนักงาน หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๔ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ ๕ ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร สำนักงานจะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่สำนักงาน ต้องการตรวจสอบข้อมูลหรือ คาดว่าข้อมูลนั้นเกี่ยวข้องกับสำนักงาน ซึ่งสำนักงานอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวดที่ ๘ การรับ-ส่งจดหมายอิเล็กทรอนิกส์

ข้อ ๑ เจ้าหน้าที่ต้องลงทะเบียนเพื่อขอใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) จากผู้ดูแลระบบก่อน

ข้อ ๒ เจ้าหน้าที่ที่ได้รับอนุญาตให้ใช้งาน E-mail ได้ จะได้รับ Account ซึ่งประกอบด้วย รหัสผู้ใช้งาน และรหัสผ่าน (Password) เพื่อเข้าใช้งาน E-mail

ข้อ ๓ ห้ามเจ้าหน้าที่ใช้ E-mail ที่สำนักงานจัดสรรให้ ในการรับ-ส่ง หรือ ใช้งาน E-mail โดยมีวัตถุประสงค์ดังต่อไปนี้

(๑) เพื่อก่อให้เกิดความเสียหายแก่สำนักงาน และบุคคลอื่นหรือละเมิดสิทธิ หรือสร้างความรำคาญต่อผู้อื่น เช่น การจงใจส่งข้อมูลที่มีไวรัสให้กับผู้อื่น การส่งข้อความดูหมิ่นผู้อื่น การส่งจดหมายลูกโซ่ การส่ง Spam mail เป็นต้น

(๒) เพื่อใช้ประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือการพาณิชย์

(๓) เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน เช่น การส่งภาพลามกให้กับผู้อื่น เป็นต้น

(๔) เพื่อการเปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ได้รับอนุญาตซึ่งได้มาจากองค์กรหรือ ผู้ที่มีสิทธิในข้อมูลดังกล่าว

ข้อ ๔ หากเจ้าหน้าที่ต้องการส่ง E-mail ถึงเจ้าหน้าที่ทุกคนในสำนักงาน หรือกลุ่มของหน่วยงาน ควรแจ้งผู้ดูแลระบบให้ดำเนินการจัดส่งให้

ข้อ ๕ เจ้าหน้าที่ไม่ควรนำ E-mail ที่สำนักงานจัดสรรให้ไปให้ผู้อื่นใช้งาน ดังนั้น สศก. จะไม่รับผิดชอบผลเสียหายต่างๆ อันจะเกิดขึ้นจากการยินยอมให้ผู้อื่นใช้ E-mail นั้น ยกเว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้น เกิดจากการกระทำของผู้อื่น นอกจากนี้ เจ้าหน้าที่ (ผู้อนุญาตและผู้ได้รับอนุญาต) จะต้องได้รับโทษตามนโยบายข้อที่กระทำผิดเช่นเดียวกัน

ข้อ ๖ ห้ามเจ้าหน้าที่นำ E-mail ไปใช้งานบนเว็บไซต์ซึ่งเสี่ยงต่อการเกิด Spam mail เช่น การนำ E-mail ไปลงทะเบียนเพื่อสมัครงานบนเว็บไซต์สมัครงาน การระบุ E-mail เพื่อแสดงความคิดเห็นบนเว็บไซต์ขายสินค้า เป็นต้น

ข้อ ๗ เจ้าหน้าที่ไม่ควรเปิดหรือส่งต่อ E-mail ที่ไม่ทราบแหล่งที่มาหรือไม่น่าเชื่อถือ เช่น E-mail โฆษณา ขายสินค้า E-mail ให้สินเชื่อ E-mail เสนอให้รางวัล เป็นต้น

ข้อ ๘ เจ้าหน้าที่ต้องตรวจสอบไวรัสกับไฟล์ที่แนบมาพร้อม E-mail ทุกครั้งเสมอ ถึงแม้ว่าจะมาจากผู้ส่งที่รู้จัก

หมวดที่ ๙ การป้องกันไวรัสและภัยคุกคามในการใช้งานคอมพิวเตอร์

ข้อ ๑ เจ้าหน้าที่ควรทำการสำรองข้อมูลสำคัญที่อยู่บนเครื่องคอมพิวเตอร์ไว้ เช่น CD หรือ Flash Drive เพื่อลดปัญหาการกู้คืนข้อมูลที่ถูกทำลายโดยไวรัสคอมพิวเตอร์

ข้อ ๒ ห้ามเจ้าหน้าที่ปรับแต่ง หรือยกเลิกการทำงานของซอฟต์แวร์ป้องกันไวรัสที่สำนักงานติดตั้งให้

ข้อ ๓ เจ้าหน้าที่ควรมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้ โดยตรวจสอบว่ามีการ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอยู่เสมอ และแจ้งให้ส่วนเทคโนโลยีสารสนเทศ (สทส.) หน่วยงานในศูนย์สารสนเทศการเกษตร ทราบ หากไม่สามารถ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

ข้อ ๔ เจ้าหน้าที่ต้องแจ้งให้ สทส.ทราบ เมื่อพบว่าคอมพิวเตอร์หรือซอฟต์แวร์ที่ใช้มีพฤติกรรมผิดไปจากปกติ หรือเมื่อสงสัยว่ามีการติดไวรัส

ข้อ ๕ เจ้าหน้าที่ต้องตรวจสอบข้อมูลหรือโปรแกรมที่ได้รับจากผู้อื่นทุกครั้งเมื่อมีการติดตั้งหรือใช้งาน ด้วยซอฟต์แวร์ป้องกันไวรัส และหากตรวจพบไวรัสจะต้องรีบจัดการทำลายไวรัสโดยเร็วที่สุด หากไม่สามารถกำจัดไวรัสที่ติดมากับข้อมูลหรือโปรแกรมนั้น ห้ามทำการเปิดข้อมูลหรือติดตั้งโปรแกรมลงไปบนเครื่องที่ใช้งานอยู่

หมวดที่ ๑๐ การใช้งานเครือข่ายไร้สาย

ข้อ ๑ การจัดทำ Wireless Policy ต้องครอบคลุมทุกโฮสต์ในเครือข่ายของสำนักงาน และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง Wireless Policy อาจมีการเปลี่ยนแปลงตามเทคโนโลยีใหม่ และกระบวนการที่สอดคล้องและเหมาะสมในอนาคต

ข้อ ๒ สทส. มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าการเชื่อมต่อ และการเชื่อมต่อเครื่องไร้สายทั้งหมด

ข้อ ๓ การจัดการจุดเชื่อมต่อไร้สายในพื้นที่สำนักงาน จะต้องถูกตรวจสอบอุปกรณ์ติดตั้ง และกำหนดค่าโดย สทส. เท่านั้น

ข้อ ๔ ทุกจุดเชื่อมต่อเครือข่ายไร้สาย และอุปกรณ์ที่เกี่ยวข้อง เช่น Access Point จุดเชื่อมต่อสายสัญญาณ Switch จะต้องมีความปลอดภัย มีรูปแบบในการจัดเก็บ และเข้าถึงอุปกรณ์

ข้อ ๕ ฟังก์ชันที่ใช้ในการตั้งค่าของจุดเชื่อมต่อจะต้องสามารถเข้าถึงได้เฉพาะผู้ที่มีหน้าที่ในการดูแลระบบ

ข้อ ๖ จุดเชื่อมต่อจะต้องมีการกำหนดค่า Gateway ที่เป็นค่าที่กำหนดไว้ของเครือข่ายส่วนนั้นเท่านั้น

ข้อ ๗ SSID, User name, Login Password ของผู้ดูแลระบบและผู้ใช้ การเข้ารหัส หรือการตั้งค่าพื้นฐานอื่นๆ ที่สำคัญจะต้องเปลี่ยนจากค่าเริ่มต้น

ข้อ ๘ SSID ที่กำหนดจะต้องถูกต้องตามรูปแบบที่ สทส. กำหนดไว้ และจะต้องไม่มีการบ่งบอกหรือแสดงตำแหน่งของสายที่จุดเชื่อม LAN หรือ ชื่ออื่นๆ ระบุ

ข้อ ๙ SSID จะต้องถูกยกเลิกค่าการ Broadcast ยกเว้น จุดที่ สทส. อนุญาต

ข้อ ๑๐ อุปกรณ์จะไม่สามารถเชื่อมต่อกับเครือข่ายไร้สายได้จนกว่าจะสามารถระบุ SSID ที่ถูกต้องในกรณีที่มีการยกเลิกค่าการ Broadcast

ข้อ ๑๑ เลือกใช้เทคโนโลยี Authentication และมีการกำหนดค่าการเข้ารหัสในการเชื่อมต่อ

ข้อ ๑๒ อุปกรณ์ที่ใช้ในการเข้าถึงเครือข่ายของสำนักงาน จะต้องรองรับมาตรฐาน IEEE 802.11g การเชื่อมต่อจะมีซอฟต์แวร์ป้องกันไวรัส

ข้อ ๑๓ ทุกจุดเชื่อมจะต้องกำหนดรหัสผ่านเพื่อเข้าใช้งาน คุณลักษณะการจัดการรหัสผ่านนี้ จะถูกเก็บไว้และส่งในรูปแบบที่เข้ารหัส

ข้อ ๑๔ SNMP จะต้องถูกยกเลิกหากไม่จำเป็นสำหรับการบริหารจัดการเครือข่าย หากมีความจำเป็นต้องใช้ จะต้องมีการเปลี่ยนค่า Community String

ข้อ ๑๕ อุปกรณ์เครือข่ายไร้สายทั้งหมดต้องผ่านความเห็นชอบจาก สทส.

ข้อ ๑๖ ห้ามไม่ให้เจ้าหน้าที่ หรือทีมงานเครือข่ายบอกค่าติดตั้งของเครือข่ายไร้สายกับผู้ใช้งาน หรือบุคคลภายนอก

ข้อ ๑๗ สทส. มีสิทธิในการยุติการเชื่อมต่อเครือข่ายไร้สายของอุปกรณ์ทุกชนิด ที่ไม่เป็นไปตามนโยบาย หรือมีความเสี่ยงต่อระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้ล่วงหน้า

ข้อ ๑๘ ผู้ละเมิดนโยบายด้านความปลอดภัยของเครือข่ายไร้สายจะถูกระงับการใช้งานอินเทอร์เน็ตทันที

ข้อ ๑๙ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของสำนักงาน

หมวดที่ ๑๑ ด้านความปลอดภัยของไฟร์วอลล์

ข้อ ๑ สทส. มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

ข้อ ๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

ข้อ ๓ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อกโดยไฟร์วอลล์

ข้อ ๔ ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login account ก่อนการใช้งานทุกครั้ง

ข้อ ๕ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

ข้อ ๖ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่าที่กฎหมายกำหนด และอย่างน้อย ๙๐ วัน

ข้อ ๗ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทาง สทส. อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความความยินยอมจาก สทส.

ข้อ ๘ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ ๙ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ ๑๐ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๑ สทส. มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบายหรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ ๑๒ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจาก สทส.

ข้อ ๑๓ ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

หมวดที่ ๑๒ นโยบายด้านความปลอดภัยของระบบตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy: IDS/IPS Policy)

ข้อ ๑ IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายใน สศก. ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ ๒ IDS/IPS Policy ครอบคลุมทุกโฮสต์ในเครือข่ายของ สศก. และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๓ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ ๔ ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๕ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ ๖ มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

ข้อ ๗ มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๘ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๙ เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ ๑๐ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จจะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

ข้อ ๑๑ พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

ข้อ ๑๒ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๓ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ ๑๔ สทส. มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้ล่วงหน้า

ข้อ ๑๕ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของ สศก. การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบ ของ สศก. จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ประกาศ ณ วันที่ พ.ศ. ๒๕๕๓

เลขาธิการสำนักงานเศรษฐกิจการเกษตร