ประกาศองค์การอุตสาหกรรมป่าไม้

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ขององค์การอุตสาหกรรมป่าไม้

---

๑. วัตถุประสงค์และขอบเขต

ด้วยองค์การอุตสาหกรรมป่าไม้ (อ.อ.ป.) ได้นำระบบเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติงาน เพื่ออำนวยความสะดวกให้กับพนักงานในการปฏิบัติงาน ดังนั้น เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกภัยคุกคามจากภัยต่างๆ และเพื่อทำให้ระบบเทคโนโลยีสารสนเทศมีความปลอดภัย สามารถดำเนินงานได้ต่อเนื่องและมีประสิทธิภาพ จึงเห็นสมควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ครอบคลุมถึงประเด็นสำคัญ ดังนี้

๑.๑ การรักษาความลับ (Confidentiality) คือ การรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ ผู้มีสิทธิเท่านั้นที่จะเข้าถึงข้อมูลนั้นได้ และไม่ถูกเปิดเผยสู่บุคคลหรือหน่วยงานอื่นที่ไม่มีสิทธิ

๑.๒ การรักษาความสมบูรณ์ (Integrity) คือ การรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา ข้อมูลจะคงอยู่อย่างถูกต้องและสมบูรณ์ ตลอดขั้นตอนการประมวลผลและขั้นตอนการเก็บรักษา

๑.๓ การพร้อมใช้ (Availability) คือ การรับรองว่าข้อมูลและบริการการสื่อสารต่างๆ พร้อมที่จะใช้ได้ในเวลาที่ต้องการใช้งาน

๑.๔ การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) คือ วิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้น ทั้งผู้รับและผู้ส่งจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวภายหลัง

๒. องค์ประกอบของนโยบาย

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ อ.อ.ป. ได้ใช้แนวทางและกระบวนการสร้างความมั่นคงปลอดภัย โดยอ้างอิงจากพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ รวมถึงมาตรฐานการรักษาความมั่นคงปลอดภัยในการ

/ประกอบ...

ประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี ๒๕๕๐ และมาตรฐาน ISO/IEC ๒๗๐๐๑ ซึ่งประกอบด้วย ๑๒ หมวด ตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศดังต่อไปนี้

หมวด ๑ นโยบายความมั่นคงปลอดภัย (Security Policy) มีวัตถุประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับการใช้งานระบบเทคโนโลยีสารสนเทศของ อ.อ.ป. เพื่อให้สอดคล้องกับข้อกำหนดทางราชการ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งจัดทำเป็นลายลักษณ์อักษร โดยที่ฝ่ายบริหารเห็นชอบและอนุมัติและเผยแพร่ให้ “พนักงาน” ทุกระดับได้รับรู้ โดยนโยบายความมั่นคงปลอดภัยได้ครอบคลุมการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารใน ๔ ด้าน คือ

๑. การเข้าถึงระบบสารสนเทศ

๒. การเข้าถึงระบบเครือข่าย

๓. การเข้าถึงระบบปฏิบัติการ

๔. การเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

รวมถึงให้มีการประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง และจัดเตรียมระบบสำรองข้อมูลสารสนเทศและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินเพื่อรองรับการบริหารความต่อเนื่องในการดำเนินงาน กรณีเกิดสถานการณ์ที่ไม่สามารถดำเนินงานได้อย่างปกติของระบบเทคโนโลยีสารสนเทศขององค์การอุตสาหกรรมป่าไม้

หมวด ๒ โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security) มีวัตถุประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ อ.อ.ป. ที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับประชาชนหรือหน่วยงานภายนอก โดยจัดให้มีคณะทำงานและบุคลากรเฉพาะด้านความมั่นคงปลอดภัย มีการประสานงานความรับผิดชอบประเมินความเสี่ยง และตรวจสอบการทำงานด้านความมั่นคงปลอดภัย รวมทั้งประสานงานกับหน่วยงานภายนอกและผู้ใช้งานระบบเทคโนโลยีสารสนเทศจากภายนอก โดยมีการระบุและจัดทำข้อกำหนดที่ชัดเจนในการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์การอุตสาหกรรมป่าไม้

หมวด ๓ การบริหารจัดการสินทรัพย์ (Asset Management) มีวัตถุประสงค์เพื่อป้องกันสินทรัพย์ของ อ.อ.ป. จากความเสียหายที่อาจเกิดขึ้นได้ และกำหนดระดับของการป้องกันสารสนเทศอย่างเหมาะสม โดยมีการจัดทำบัญชีสินทรัพย์ ระบุผู้เป็นเจ้าของสินทรัพย์และกำหนดหลักเกณฑ์การใช้งานสินทรัพย์ที่เหมาะสม มีการจัดหมวดหมู่สินทรัพย์ตามระดับชั้นความลับและจัดทำป้ายชื่อ เพื่อการบริหารจัดการสินทรัพย์ตามที่ได้จัดหมวดหมู่ไว้

/หมวด ๔...

หมวด ๔ ความมั่นคงปลอดภัยทางด้านทรัพยากรบุคคล (Human Resource Security) มีวัตถุประสงค์เพื่อให้ "พนักงาน" ผู้ที่ อ.อ.ป. ทำสัญญาจ้างและ "บุคคลภายนอก" เข้าใจถึงบทบาทหน้าที่ความรับผิดชอบของตน ทั้งก่อนการจ้างงาน ระหว่างการจ้างงานและการสิ้นสุดหรือการเปลี่ยนการจ้างงาน ซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมายและตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกงและการใช้อุปกรณ์ผิดวัตถุประสงค์ รวมทั้งลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

หมวด ๕ ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) มีวัตถุประสงค์เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ป้องกันสินทรัพย์ไม่ให้เกิดการสูญหาย ถูกขโมย เกิดความเสียหาย เกิดการก่อกวนหรือแทรกแซง ป้องกันการถูกเปิดเผยโดยไม่ได้รับอนุญาตและป้องกันไม่ให้กิจกรรมการดำเนินงานต่างๆ ของ อ.อ.ป. เกิดการติดขัดหรือหยุดชะงัก ได้แก่ การมีระบบกระแสไฟฟ้าสำรอง การมีระบบสื่อสารสำรอง เป็นต้น

หมวด ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงาน (Communications and Operations Management) มีวัตถุประสงค์เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้อง รักษาระดับความมั่นคงปลอดภัยในการปฏิบัติหน้าที่ของหน่วยงานภายนอกให้เป็นไปตามข้อตกลง ลดความเสี่ยงจากความล้มเหลวของระบบ ป้องกันซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี ป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย ป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายสินทรัพย์โดยไม่ได้รับอนุญาต รักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกัน สร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

หมวด ๗ การควบคุมการเข้าถึง (Access Control) มีวัตถุประสงค์เพื่อควบคุมการเข้าถึงหรือควบคุมการใช้งานสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ สร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

หมวด ๘ การจัดหา การพัฒนาและการบำรุงรักษาระบบเทคโนโลยีสารสนเทศ (Information System Acquisition, Development and Maintenance) มีวัตถุประสงค์เพื่อให้การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศได้มีการพิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐาน

/ที่สำคัญ...

ที่สำคัญ ได้แก่ เป็นการป้องกันความผิดพลาดการสูญหายและการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาตหรือการใช้งานสารสนเทศผิดวัตถุประสงค์ การรักษาความลับของข้อมูล การยืนยันตนของผู้ส่งข้อมูล การรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยวิธีการเข้ารหัสข้อมูล การสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สารสนเทศและแฟ้มข้อมูลต่างๆ ของระบบที่ให้บริการ ทั้งนี้เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ

หมวด ๙ การบริหารจัดการสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Information Security Incident Management) มีวัตถุประสงค์เพื่อให้สถานการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบเทคโนโลยีสารสนเทศของ อ.อ.ป. ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสมและให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศของ อ.อ.ป.

หมวด ๑๐ การบริหารความต่อเนื่องในการดำเนินงาน (Continuity Management) มีวัตถุประสงค์เพื่อป้องกันการติดขัดหรือหยุดชะงักของกิจกรรมต่างๆ และกระบวนการทำงานที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบเทคโนโลยีสารสนเทศ และให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

หมวด ๑๑ การปฏิบัติตามข้อกำหนด (Compliance) มีวัตถุประสงค์เพื่อป้องกันการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ และเพื่อให้การตรวจประเมินระบบเทคโนโลยีสารสนเทศมีประสิทธิภาพสูงสุด และมีการแทรกแซงหรือทำให้หยุดชะงักต่อการปฏิบัติงานน้อยที่สุด

หมวด ๑๒ การควบคุมข้อมูลส่วนบุคคล (Privacy Statement) มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดหลักเกณฑ์การเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานให้เป็นไปตามที่กฎหมายบัญญัติ รวมทั้งกำหนดกลไกในการกำกับดูแล

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศแต่ละหมวดที่กล่าวมาข้างต้นจะประกอบด้วยวัตถุประสงค์ในการดำเนินการที่เกี่ยวข้องกับหมวดนั้น และมีรายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และวิธีปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของ อ.อ.ป. เพื่อลดความเสียหายต่อการปฏิบัติงาน ทำให้ อ.อ.ป. เป็นหน่วยงานที่ได้รับการยอมรับจากองค์กรต่างๆ

/ในการ...

ในการปฏิบัติงานได้อย่างมั่นคงปลอดภัยตามมาตรฐานสากล ซึ่งนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ อ.อ.ป. นี้จัดเป็นมาตรฐานความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของ อ.อ.ป. ซึ่งพนักงานของ อ.อ.ป. และบุคคลภายนอกหรือหน่วยงานภายนอกจะต้องปฏิบัติอย่างเคร่งครัด

กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูงจักเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นและกำหนดให้ฝ่ายสารสนเทศ สำนักวิจัยพัฒนาการจัดการป่าไม้เศรษฐกิจอย่างยั่งยืนเป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ รวมถึงกำหนดให้มีการปฏิบัติที่ชัดเจนและให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๓๐ ธันวาคม พ.ศ. ๒๕๖๔

(นายสุกิจ จันทร์ทอง)
รองผู้อำนวยการองค์การอุตสาหกรรมป่าไม้
รักษาการแทนผู้อำนวยการองค์การอุตสาหกรรมป่าไม้