ประกาศกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๖๐

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ จึงกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนการปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและสอดคล้องกับภารกิจของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ตามประกาศดังต่อไปนี้

๑. ประกาศนี้ เรียกว่า “ประกาศกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐”

๒. บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

๓. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ กำหนดให้มีการดำเนินการครอบคลุมประเด็นสำคัญดังต่อไปนี้

๓.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๓.๒ การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๔. รายละเอียดและองค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้บุคลากรของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ และบุคคลหรือหน่วยงานภายนอกที่เกี่ยวข้องรับทราบและถือปฏิบัติ ให้เป็นไปตามเอกสารแนบท้ายประกาศ เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๕. เอกสารนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่มีการประกาศใช้จะเผยแพร่ผ่านเว็บไซต์ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๖. กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่จะมีการทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงใดๆ ที่มีผลกระทบต่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๖.๑ การปรับปรุงแก้ไขหรือเปลี่ยนแปลงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ดำเนินการโดยการออกประกาศแก้ไขเพิ่มเติม หรือยกเลิกประกาศฉบับเดิมแล้วออกประกาศฉบับใหม่ทดแทนแล้วแต่กรณี

/๖.๒ การปรับปรุง...

๖.๒ การปรับปรุงแก้ไขแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ดำเนินการโดยคณะกรรมการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล ตามคำสั่งกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ที่ ๑๘๔/๒๕๕๘ ลงวันที่ ๑๔ สิงหาคม พ.ศ. ๒๕๕๘ เสนอความเห็นชอบต่ออธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ในการพิจารณา และเวียนแจ้งให้หน่วยงานที่เกี่ยวข้องรับทราบและถือปฏิบัติ

๗. อธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ในฐานะผู้บริหารสูงสุดของหน่วยงาน (chief executive officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๘. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๓๐ มีนาคม พ.ศ. ๒๕๖๐

(นายสมบูรณ์ ยินดียั่งยืน)
อธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

เอกสารแนบท้ายประกาศกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

พ.ศ. ๒๕๖๐

สารบัญ

คำนิยาม ๑

ความเป็นมา ๔

หมวดที่ ๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ๘

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ๘

ส่วนที่ ๒ ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirement for access control) ๑๑

ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ๑๑

ส่วนที่ ๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) ๑๓

ส่วนที่ ๕ การควบคุมการเข้าถึงระบบเครือข่าย (network access control) ๑๕

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (operation system access control) ๑๗

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) ๑๙

ส่วนที่ ๘ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (wireless access control) ๒๑

ส่วนที่ ๙ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ ๒๒

ส่วนที่ ๑๐ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย ๒๒

ส่วนที่ ๑๑ การบริหารจัดการสินทรัพย์ ๒๓

ส่วนที่ ๑๒ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และป้องกันโปรแกรมไม่ประสงค์ดี ๒๓

ส่วนที่ ๑๓ การควบคุมการใช้อินเตอร์เน็ต ๒๔

ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล ๒๕

ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา ๒๕

ส่วนที่ ๑๖ การใช้งานเครือข่ายสังคมออนไลน์ ๒๖

ส่วนที่ ๑๗ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ๒๖

หมวดที่ ๒ นโยบายการจัดทำระบบสำรองข้อมูลและการเตรียมความพร้อมกรณีฉุกเฉิน ๒๘

หมวดที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ๓๑

หมวดที่ ๔ หน้าที่และความรับผิดชอบ ๓๔

คำนิยาม

๑. **ผู้ใช้งาน** หมายถึง ข้าราชการ ลูกจ้าง พนักงานราชการ ผู้ดูแลระบบ ผู้บริหาร ผู้รับบริการ รวมถึง บุคคล และ/หรือ ผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

๒. **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยผู้บริหารหน่วยงานหรือผู้บริหารระดับสูงจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์หรือสารสนเทศ

๓. **สินทรัพย์** หมายถึง ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับหน่วยงาน

๔. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิ หรือมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ

๕. **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน โดยธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิดและความน่าเชื่อถือ

๖. **เหตุการณ์ด้านความมั่นคงปลดอดภัย** หมายถึง การเกิดเหตุการณ์ สภาพของบริการ หรือ เครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๗. **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๘. **หน่วยงาน** หมายถึง กรม สำนัก ศูนย์ กอง และหน่วยงานที่มีฐานะเทียบเท่า กรม/กอง รวมถึงหน่วยงานส่วนภูมิภาคที่อยู่ในสังกัด กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๙. **ผู้บริหารระดับสูงสุดของหน่วยงาน** หมายถึง อธิบดี หรือเทียบเท่า

๑๐. **ผู้บริหาร** หมายถึง ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน ได้แก่ อธิบดี หรือเทียบเท่า ผู้อำนวยการ สำนัก ศูนย์ กอง หรือเทียบเท่า

๑๑. **ผู้ดูแลระบบ** หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานให้มีหน้าที่รับผิดชอบดูแลรักษา หรือจัดการระบบคอมพิวเตอร์ และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

๑๒. **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรง หากข้อมูลเหล่านั้นเกิดสูญหาย

๑๓. **ระบบสารสนเทศ (Information System)** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น

๑๔. **ระบบเครือข่าย** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานได้ เช่น ระบบเครือข่ายแบบมีสาย ระบบเครือข่ายแบบไร้สาย ระบบอินทราเน็ต และระบบอินเทอร์เน็ต เป็นต้น

๑๕. **ระบบอินเทอร์เน็ต (internet)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

๑๖. **จดหมายอิเล็กทรอนิกส์ (e-mail)** หมายถึง ระบบรับส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเทคโนโลยีสารสนเทศ ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพนิ่ง ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน

๑๗. **สื่อบันทึกข้อมูล** หมายถึง สื่อทั้งที่เป็นอิเล็กทรอนิกส์และไม่เป็นอิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น CD, DVD, USB drive, portable hard drive, โทรศัพท์มือถือ กล้องถ่ายรูปดิจิตอล กล้องวิดีโอ หรือ เครื่องบันทึกเสียง เป็นต้น

๑๘. **ชื่อผู้ใช้ (user name)** หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่ได้กำหนดสิทธิการใช้งานไว้

๑๙. **รหัสผ่าน (password)** หมายถึง กลุ่มตัวอักษรหรือตัวเลขหรืออักขระที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล สารสนเทศ ระบบสารสนเทศ และระบบเครือข่าย

๒๐. **บัญชีผู้ใช้ (user account)** หมายถึง รายชื่อผู้ใช้และรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๒๑. **การเข้ารหัส (encryption)** หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๒๒. **อุปกรณ์จัดเส้นทาง (router)** หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

๒๓. **การพิสูจน์ยืนยันตัวตน (authentication)** หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (user name) และรหัสผ่าน (password)

๒๔. **อุปกรณ์กระจายสัญญาณ (access point)** หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

๒๕. **VPN (virtual private network)** หมายถึง เครือข่ายส่วนตัวเสมือน โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๒๖. **SSID (service set identifier)** หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

๒๗. **WEP (wire equivalent privacy)** หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สาย โดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันต้องรู้ค่าชุดตัวเลขนี้

๒๘. **WPA (Wi-Fi protected access)** หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

๒๙. **MAC Address (media access control address)** หมายถึง หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขที่จะมากับอีเทอร์เน็ตการ์ดโดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

๓๐. **ไฟล์วอลล์ (firewall)** หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

๓๑. **ข้อมูลจราจรทางคอมพิวเตอร์** หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

๓๒. **แผนผังระบบเครือข่าย** หมายถึง แผนผังหรือแผนภาพที่แสดงรูปแบบการจัดวางอุปกรณ์เครือข่ายในระบบเครือข่ายที่แสดงการเชื่อมโยง เพื่อให้เห็นเส้นทางการไหลเวียนของข้อมูลในเครือข่าย

๓๓. **หมายเลขไอพีแอดเดรส (IP address)** หมายถึง ตัวเลขประจำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายที่เชื่อมต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วน หรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

๓๔. **ระบบสำรอง (disaster recovery site : DR site)** หมายถึง ระบบคอมพิวเตอร์สำรองซึ่งประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่ายที่จำเป็น ที่สามารถทำงานได้ทันทีที่ระบบหลักมีปัญหา

๓๕. **IEEE ๘๐๒.๑x** หมายถึง มาตรฐานสำหรับการยืนยันอุปกรณ์ที่ต้องการเชื่อมต่อเข้ากับระบบเครือข่ายที่ใช้สาย และเครือข่ายไร้สาย

๓๖. **อุปกรณ์คอมพิวเตอร์** หมายถึง เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์โน้ตบุค อุปกรณ์จัดเก็บข้อมูลและอุปกรณ์ต่อพวง

๓๗. **สื่อสารเคลื่อนที่** หมายถึง อุปกรณ์โทรศัพท์ และอุปกรณ์แท็บเล็ต

ความเป็นมา

๑. หลักการและเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่างๆ มีความมั่นคงปลอดภัย เชื่อถือได้ กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ สามารถดำเนินงานได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถป้องกันภัยคุกคามต่างๆ รวมทั้งการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ตลอดจนการเตรียมความพร้อมในสภาวะฉุกเฉิน

๒. วัตถุประสงค์

กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมีวัตถุประสงค์ ดังต่อไปนี้

๒.๑. เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ทำให้การดำเนินงานเป็นไปได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒.๓. เพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหาร เจ้าหน้าที่ทุกระดับ ให้มีความรู้ ความเข้าใจและตระหนักถึงความสำคัญและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๔. เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และมีแผนเตรียมพร้อมกรณีฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

๒.๕. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๓. เป้าหมาย

เป้าหมายในการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ โดยมีรายละเอียดดังนี้

๓.๑. ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๓.๒. กำกับดูแลการดำเนินงาน เพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้อง สมบูรณ์และพร้อมใช้งานอยู่เสมอ

๓.๓. เผยแพร่ ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรและผู้เกี่ยวข้องทุกระดับ ทั้งของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ และหน่วยงานที่เกี่ยวข้อง

๓.๔. ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงที่เกิดขึ้น

๔. การมีส่วนร่วมในการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ

กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ได้มีคำสั่งแต่งตั้งคณะบุคคลเพื่อดำเนินการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

- คณะกรรมการในการรักษาความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล
- คณะทำงานในการรักษาความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล

รายละเอียดของแต่ละคณะบุคคล พร้อมทั้งหน้าที่ความรับผิดชอบ มีดังนี้

(๑) คณะกรรมการในการรักษาความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย

๑. อธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่	ประธานคณะกรรมการ
๒. รองอธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ (CIO)	รองประธานคณะกรรมการ
๓. รองอธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่	รองประธานคณะกรรมการ
๔. ผู้อำนวยการสำนักบริหารกลาง	กรรมการ
๕. ผู้อำนวยการกองบริหารยุทธศาสตร์	กรรมการ
๖. ผู้อำนวยการสำนักกฎหมาย	กรรมการ
๗. ผู้อำนวยการสำนักบริหารสิ่งแวดล้อม	กรรมการ
๘. ผู้อำนวยการสำนักโลจิสติกส์	กรรมการ
๙. ผู้อำนวยการสำนักวิศวกรรมและฟื้นฟูพื้นที่	กรรมการ
๑๐. ผู้อำนวยการสำนักเหมืองแร่และสัมปทาน	กรรมการ
๑๑. ผู้อำนวยการสำนักอุตสาหกรรมพื้นฐาน	กรรมการ
๑๒. ผู้อำนวยการสำนักตรวจและประสานราชการ	กรรมการ
๑๓. ผู้อำนวยการกลุ่มตรวจสอบภายใน	กรรมการ
๑๔. ผู้อำนวยการสำนักงานอุตสาหกรรมพื้นฐานและการเหมืองแร่ เขต ๑ – ๗	กรรมการ
๑๕. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	กรรมการ และเลขานุการ

โดยคณะกรรมการมีอำนาจดังนี้

๑. กำหนดกรอบ นโยบาย และยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน

๒. ให้คำปรึกษา และร่วมพิจารณากลั่นกรองแนะนำในประเด็นต่างๆ เกี่ยวกับปัญหาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

๓. พิจารณาและให้ความเห็นชอบ แผนการปฏิบัติงานของหน่วยงานความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

๔. ถ่ายทอดนโยบายสู่การปฏิบัติของบุคลากรในหน่วยงานอย่างเคร่งครัด รวมทั้งให้ความร่วมมือและสนับสนุนการดำเนินงานที่เกี่ยวข้องกับการดำเนินงานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

๕. ส่งเสริมให้มีการบูรณาการร่วมกันระหว่างกระบวนการทำงานและการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

๖. รับผิดชอบ กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

(๒) คณะทำงานในการรักษาความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย

๑. รองอธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ (CIO)	ประธานคณะทำงาน
๒. ผู้แทนสำนักบริหารกลาง	คณะทำงาน
๓. ผู้แทนกองบริหารยุทธศาสตร์	คณะทำงาน
๔. ผู้แทนสำนักกฎหมาย	คณะทำงาน
๕. ผู้แทนสำนักบริหารสิ่งแวดล้อม	คณะทำงาน
๖. ผู้แทนสำนักโลจิสติกส์	คณะทำงาน
๗. ผู้แทนสำนักวิศวกรรมและฟื้นฟูพื้นที่	คณะทำงาน
๘. ผู้แทนสำนักเหมืองแร่และสัมปทาน	คณะทำงาน
๙. ผู้แทนสำนักอุตสาหกรรมพื้นฐาน	คณะทำงาน
๑๐. ผู้แทนสำนักตรวจและประสานราชการ	คณะทำงาน
๑๑. ผู้แทนกลุ่มตรวจสอบภายใน	คณะทำงาน
๑๒. ผู้แทนสำนักงานอุตสาหกรรมพื้นฐานและการเหมืองแร่ เขต ๑ – ๗	คณะทำงาน
๑๓. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	คณะทำงานและเลขานุการ
๑๔. หัวหน้ากลุ่มพัฒนาระบบเครือข่ายและการสื่อสาร ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	ผู้ช่วยเลขานุการ
๑๕. หัวหน้ากลุ่มพัฒนาระบบสำนักงานอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	ผู้ช่วยเลขานุการ
๑๖. หัวหน้ากลุ่มแผนงานและส่งเสริมเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	ผู้ช่วยเลขนุการ

โดยคณะทำงานมีอำนาจดังนี้

๑. ศึกษา วิเคราะห์ และจัดทำร่างแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวนโยบายและแนวปฏิบัติการการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน

๒. ตรวจสอบ ปรับปรุง แก้ไข หรือเพิ่มเติม นโยบายและกระบวนการปฏิบัติอย่างสม่ำเสมอ เพื่อให้การปฏิบัติงานมีความเหมาะสมและมีประสิทธิภาพ

๓. ถ่ายทอดความรู้ ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคลให้แก่พนักงานและเจ้าหน้าที่ในหน่วยงาน

๔. ประสานงานระหว่างคณะกรรมการและหน่วยงานที่เกี่ยวข้อง เพื่อให้การดำเนินงานเป็นไปตามแผนปฏิบัติการที่กำหนดไว้ในกระบวนการรักษาความมั่นคงปลอดภัยสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

๕. ชี้แจงแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลให้กับหน่วยงานภายในกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๖. รายงาน และติดตามการละเมิดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคลให้แก่คณะกรรมการในการรักษาความมั่นคงปลอดภัยสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

หมวดที่ ๑
นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ต้องมีมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานระบบสารสนเทศ การเข้าถึงระบบคอมพิวเตอร์ อุปกรณ์เครือข่าย และการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้ายที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง และจะต้องเป็นไปโดยสอดคล้องกับภารกิจของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงาน

๒. เพื่อให้ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน และผู้เกี่ยวข้องได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control)

๑. ต้องจัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน เพื่อจำแนกกลุ่มทรัพยากรของระบบ หรือการทำงาน โดยกำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๒. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือ มอบอำนาจ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้

- อ่านได้อย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไขข้อมูล
- ลบข้อมูล
- อนุมัติ
- ไม่มีสิทธิ

(๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจให้เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งานที่กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงาน หรือ ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. การแบ่งประเภทข้อมูลและการจัดลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความมั่นคงปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

(๑) กำหนดแบ่งประเภทของข้อมูล

- ข้อมูลสารสนเทศด้านการบริหาร ประกอบด้วย ข้อมูลนโยบายด้านการบริหารจัดการอุตสาหกรรมแร่และอุตสาหกรรมพื้นฐาน ข้อมูลการเพิ่มความสามารถด้านการผลิตอุตสาหกรรมแร่และอุตสาหกรรมพื้นฐาน ข้อมูลการพัฒนาศักยภาพการค้าและการลงทุนอุตสาหกรรมแร่ในระดับภูมิภาคอาเซียน ข้อมูลการบริหารจัดการโลจิสติกส์และโซ่อุปทานของภาคอุตสาหกรรม ข้อมูลคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณ การเงินและบัญชี
- ข้อมูลสารสนเทศด้านการอนุญาตประทานบัตร ประกอบด้วย ข้อมูลประทานบัตร ข้อมูลอาชญาบัตร ข้อมูลผู้ประกอบการ ข้อมูลสถานประกอบการ ข้อมูลแหล่งแร่ ข้อมูลโรงโม่บดและย่อยหิน ข้อมูลโรงงานเกลือสินเธาว์ ข้อมูลใบอนุญาตขนแร่ ข้อมูลแหล่งหินอุตสาหกรรม ข้อมูลออกใบอนุญาตส่งแร่ออกนอกราชอาณาจักรและใบอนุญาตนำแร่เข้าในราชอาณาจักร ข้อมูลการจัดสรรค่าภาคหลวงแร่ ข้อมูลแหล่งแร่ในต่างประเทศ ข้อมูลสถานการณ์อุตสาหกรรมแร่ ข้อมูลราคาแร่และโลหะในตลาดต่างประเทศ ข้อมูลการนำเข้าแร่และโลหะ ข้อมูลการส่งออกแร่และโลหะ ข้อมูลสถิติแร่ ข้อมูลราคาแร่และโลหะ ข้อมูลการใช้แร่และโลหะภายในประเทศ ข้อมูลประกาศราคาแร่ และข้อมูลฟื้นฟูสิ่งแวดล้อม เป็นต้น

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับดังนี้

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผย หรือเผยแพร่ทั่วไปได้

(๔) จัดแบ่งระดับชั้นการเข้าถึงข้อมูลสารสนเทศ

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ปฏิบัติงานตามภาระหน้าที่

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย

(๕) เกณฑ์การแบ่งระดับการเข้าถึงข้อมูลและสารสนเทศ

- ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น
- ผู้ปฏิบัติงาน เข้าถึงได้ตามอำนาจหน้าที่ที่ได้รับมอบหมาย
- ผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ และสามารถดู เขียน แก้ไข และลบข้อมูลเฉพาะที่ตนเองสร้างเท่านั้น
- ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย มีสิทธิในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตามอำนาจหน้าที่
- การกำหนดสิทธิพิเศษสามารถดำเนินการได้ เมื่อได้รับอนุมัติจากผู้มีอำนาจ หรือเจ้าของข้อมูลเท่านั้น
- การมอบอำนาจในการเข้าถึงสามารถดำเนินการได้ เมื่อได้รับความยินยอมจากเจ้าของสิทธิหรือหน่วยงานหลักเท่านั้น

(๖) ระยะเวลาในการใช้งาน

- ระยะเวลาการเข้าถึงและการใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศ ผู้ใช้งานเข้าถึงและใช้งานได้ดังนี้
  - (ก) ระบบงานบริการ e-services (front office) สำหรับผู้ใช้งานภายนอกสามารถใช้งานได้ตลอดเวลา
  - (ข) ระบบงานภายใน (back office) สำหรับการใช้งานภายใน สามารถเข้าถึงระบบได้ตามช่วงเวลา ดังต่อไปนี้
    - ในเวลาราชการ ๘.๓๐ ถึง ๑๖.๓๐ น.
    - นอกเวลาราชการ หลัง ๑๖.๓๐ น. เป็นต้นไป
    - ช่วงวันหยุดราชการและวันหยุดนักขัตฤกษ์
    - ช่วงเวลาพิเศษเป็นรายครั้ง โดยระบุเป็นช่วงเวลา ระยะเวลาการเข้าถึง
- การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ
  - (ก) กำหนดให้ระบบสารสนเทศที่มีความเสี่ยงสูงหรือระบบที่มีข้อมูลสำคัญ ต้องตัดและหมดเวลาการใช้งานที่สั้นขึ้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
  - (ข) ต้องจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับระบบสารสนเทศความเสี่ยงสูงหรือระบบที่มีข้อมูลสำคัญ

(๗) ช่องทางการเข้าถึง

- ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)
- ระบบโทรศัพท์ (เข้าถึงได้ในเวลาราชการ)
- หนังสือหรือบันทึกข้อความ (เข้าถึงได้ทุกช่วงเวลา)
- ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)
- ระบบอินทราเน็ต (เข้าถึงได้ในเวลาราชการหรือนอกเวลาราชการ)
- ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)

- เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา หรือ ช่วงเวลาพิเศษที่กำหนดเวลา)

ส่วนที่ ๒ ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirement for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

๑. มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

๒. มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

๑. การสร้างความรู้ความเข้าใจให้แก่ผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม โดยปฏิบัติตามแนวทางดังนี้

(๑) ต้องกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ โดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

(๒) ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามเหมาะสม

(๓) จัดฝึกอบรมการใช้งานสารสนเทศของหน่วยงานอย่างสม่ำเสมอ หรือทุกครั้งที่มีการปรับปรุงหรือเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

(๔) จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน

(๕) ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจ และนำไปปฏิบัติได้ง่าย ซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ ได้แก่ การติดประกาศประชาสัมพันธ์ แผ่นพับ เผยแพร่ผ่านเว็บไซต์

(๖) ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติ ด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

๒. การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว โดยปฏิบัติตามแนวทางดังนี้

(๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานสำหรับระบบสารสนเทศ

(๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(๔) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานเป็นลายลักษณ์อักษร

(๕) มีการบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(๖) การอนุญาตให้เข้าถึงระบบสารสนเทศต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการหน่วยงานเจ้าของระบบสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๗) ต้องดำเนินการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและตัดออกจากทะเบียนผู้ใช้งานทันที เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง

๓. การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง โดยปฏิบัติตามแนวทางดังนี้

(๑) เมื่อเจ้าหน้าที่ของหน่วยงาน ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่เคยขอสิทธิการใช้งานไว้ ต้องรีบแจ้งเพื่อเปลี่ยนสิทธิ หรือถอดถอนสิทธิออกจากระบบทันที

(๒) การแจ้งขอใช้สิทธิ หรือเปลี่ยนแปลงสิทธิในการเข้าถึงและใช้งานข้อมูล สารสนเทศ และระบบสารสนเทศต้องทำเป็นลายลักษณ์อักษร ระบุเหตุผลและความจำเป็น

(๓) ให้อำนาจกับผู้ดูแลระบบในการระงับสิทธิ ในกรณีตรวจพบว่ามีการกระทำความผิดตามนโยบายการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

(๔) กรณีมีความจำเป็นต้องให้สิทธิกับผู้ใช้ ต้องพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้น อย่างรัดกุมเพียงพอ โดยต้องได้รับความเห็นชอบและอนุมัติจากอธิบดีหรือผู้ที่ได้รับมอบหมายจากอธิบดี โดยต้องควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว และต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้อย่างรัดกุม โดยปฏิบัติตามแนวทางดังนี้

(๑) กระบวนการจัดสรร หรือแจกจ่ายรหัสผ่านให้แก่ผู้ใช้งาน

- ผู้ดูแลระบบกำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้
- ผู้ดูแลระบบกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสชั่วคราว และเปลี่ยนรหัสผ่านที่มีความยากต่อการเดาโดยผู้อื่น
- ผู้ดูแลระบบต้องให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน ได้แก่ ลงนามเอกสารแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศของหน่วยงาน
- ผู้ดูแลระบบกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดา และกำหนดรหัสผ่านที่แตกต่างกัน
- ผู้ดูแลระบบจัดส่งรหัสผ่านชั่วคราวให้ผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นและการใช้จดหมายอิเล็กทรอนิกส์เป็นช่องทางในการจัดส่ง
- ผู้ดูแลระบบมีการแจ้งหน้าที่รับผิดชอบของผู้ใช้งานให้ดูแลรหัสผ่านและดูแลการใช้งานอีเมล์ในทางที่ถูกต้อง โดยไม่ผิดต่อพระราชบัญญัติที่ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
- หากผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องดูแล จดจำรหัสผ่านหลายตัว สามารถใช้รหัสผ่านเดียวที่มีคุณภาพ สำหรับการเข้าถึงทุกระบบได้ ซึ่งระบบเหล่านั้นต้องมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

- ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานปกติ

(๒) ขั้นตอนการเปลี่ยนรหัส

- ผู้ดูแลระบบอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง
- ผู้ใช้ต้องการเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะเปลี่ยนรหัสใหม่
- ผู้ใช้งานทำการล็อกอินเข้าใช้งานระบบงานครั้งแรกและทำการเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว
- ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเป็นระยะ หรือทุกครั้งที่มีการแจ้งเตือน หรือบังคับให้เปลี่ยนรหัสผ่านจากผู้ดูแลระบบ
- กรณีผู้ดูแลระบบตรวจพบว่ารหัสผ่านของผู้ใช้งานไม่มีความปลอดภัย หรือตรวจสอบได้ว่าถูกนำไปใช้โดยผู้อื่น ผู้ใช้งานรายนั้นจะถูกตัดสิทธิการใช้งานชั่วคราวจนกว่าจะดำเนินการเปลี่ยนรหัสผ่านเป็นที่เรียบร้อย

๕. การทบทวนสิทธิการเข้าถึง (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีอย่างน้อยปีละ ๑ ครั้ง หรือ เมื่อมีการเปลี่ยนแปลง ได้แก่ มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทางดังนี้

(๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน

(๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงาน เพื่อดำเนินการทบทวนรายชื่อและสิทธิการเข้าใช้งานว่าถูกต้องหรือไม่

(๓) ดำเนินการแก้ไขข้อมูลสิทธิต่างๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

(๔) ขั้นตอนการปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๓ วัน หรือเมื่อเปลี่ยนตำแหน่งภายในต้องดำเนินการภายใน ๗ วัน

ส่วนที่ ๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือ การลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีแนวปฏิบัติ ดังนี้

๑. การใช้งานรหัสผ่าน (password use)

(๑) เปลี่ยนรหัสผ่านชั่วคราวทันที เมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) กำหนดรหัสผ่านให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๓) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อ หรือนามสกุลของตนเอง หรือข้อมูลที่เกี่ยวข้องกับตนเองที่ผู้อื่นสามารถนำมาใช้เพื่อเดารหัสผ่านได้ หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๔) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๕) เก็บบัญชีและรหัสผ่านของตนเองไว้เป็นความลับ

(๖) ผู้ใช้ต้องทำการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้ และรหัสผ่าน โดยผู้ใช้แต่ละคนต้องมีบัญชีชื่อผู้ใช้ของตนเอง และห้ามทำการเผยแพร่แจกจ่าย หรือทำให้ผู้อื่นล่วงรหัสผ่าน

(๗) ผู้ใช้ต้องเปลี่ยนรหัสผ่านทันที เมื่อสงสัยว่ารหัสผ่านอาจถูกเปิดเผย หรือล่วงรู้

๒. การป้องกันอุปกรณ์ขณะไม่มีผู้ใช้งานที่อุปกรณ์

(๑) ผู้ใช้งานต้องตั้งค่าการใช้โปรแกรมถนอมหน้าจอ (screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งานหลังจากนั้น เมื่อต้องการใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

(๒) ผู้ดูแลระบบต้องสร้างความตระหนัก เพื่อให้ผู้ใช้งานเข้าใจมาตรการป้องกัน

(๓) ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(๔) ผู้ใช้งานต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งาน หรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๓. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy)

(๑) มีการป้องกันสินทรัพย์ของหน่วยงาน และควบคุมไม่ให้มีการทิ้งหรือปล่อยสินทรัพย์สารสนเทศที่สำคัญให้อยู่ในสถานที่ไม่ปลอดภัย โดยมีการจัดการบริเวณล้อมรอบ การควบคุมการเข้า-ออก การจัดบริเวณการเข้าถึงการส่งผลิตภัณฑ์โดยบุคคลภายนอก การวางอุปกรณ์และระบบสนับสนุนการทำงาน

(๒) มีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันสินทรัพย์ของหน่วยงาน
- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ หรือสื่อบันทึกข้อมูลที่เป็นสมบัติส่วนบุคคล
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน
- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

(๓) ควบคุมการเข้าถึงข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์ด้านสารสนเทศ โดยผู้เป็นเจ้าของ หรือผู้ที่ได้รับมอบหมายเท่านั้น

(๔) การลบ หรือเขียนข้อมูลทับบนข้อมูลที่สำคัญ ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูลก่อนที่จะอนุมัติให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เปลี่ยนทดแทน หรือ ทำลาย เพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญได้

(๕) สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๖) ในการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลาย ดังนี้

สื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
flash drive, thumb drive, USB drive,	- ใช้การทำลายข้อมูล โดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แม็ต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิกส์ของกระทรวงกลาโหมสหรัฐอเมริการ DOD ๕๒๒๐.๓๓-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย

(๗) การลบข้อมูลที่ไม่มีการใช้งานตั้งแต่ ๕ ปีขึ้นไปออกจากฐานข้อมูล และสำรองข้อมูลลงฮาร์ดดิกส์ภายนอก (external hard disk) หรือสื่อข้อมูลสำรอง (backup media) และจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล ทั้งนี้ การลบหรือทำลายข้อมูลอิเล็กทรอนิกส์ดังกล่าว ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติให้ทำลายสื่อบันทึกข้อมูลหรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูลทุกครั้ง

๔. ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ส่วนที่ ๕ การควบคุมการเข้าถึงระบบเครือข่าย (network access control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาตให้ดำเนินการอย่าง ดังนี้

๑. การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) การเข้าถึงระบบเครือข่ายต้องพิสูจน์ตัวตนผู้ใช้ด้วยบัญชีผู้ใช้ที่กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ออกให้

(๒) ผู้ใช้งานที่ได้รับอนุญาตเข้าถึงระบบเครือข่าย สามารถเข้าใช้ได้เฉพาะบริการในระบบเครือข่ายตามสิทธิที่ได้รับอนุญาตเท่านั้น

(๓) การเข้าถึงระบบเครือข่ายของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่จากภายนอกต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และต้องกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นเป็นพิเศษจากมาตรการเข้าถึงระบบเครือข่ายกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่จากภายใน

(๔) การใช้เครื่องมือต่างๆ เพื่อตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒. การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connection) ต้องยืนยันตัวบุคคลสำหรับการใช้งานด้วยชื่อผู้ใช้งานและรหัสผ่านกับระบบไฟล์วอลล์ หรือระบบ VPN ที่หน่วยงานจัดเตรียมไว้ให้ จึงจะสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๓. การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(๑) จัดทำบัญชีทะเบียนสินทรัพย์อุปกรณ์ที่เชื่อมต่อเข้ากับระบบเครือข่าย เพื่อการตรวจสอบยืนยันอุปกรณ์บนเครือข่าย

(๒) อุปกรณ์ที่เชื่อมต่อเข้ากับระบบเครือข่ายต้องมีการลงทะเบียน mac address ของอุปกรณ์และชื่อผู้ใช้งานอุปกรณ์

(๓) การตรวจสอบยืนยันอุปกรณ์บนเครือข่ายสามารถใช้ตรวจสอบได้จาก mac address หรือการตรวจสอบผ่านการตั้งค่าการใช้งาน IEEE ๘๐๒.๑x

๔. การป้องกันพอร์ตที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพ และทางเครือข่าย โดยปฏิบัติดังนี้

(๑) ควบคุมพอร์ตและหมายเลขไอพีแอดเดรสที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้เข้าถึงอุปกรณ์เครือข่ายอย่างรัดกุม

(๒) กำหนดรหัสผ่านสำหรับตรวจสอบและปรับแต่งอุปกรณ์เครือข่าย เมื่อใช้การเชื่อมต่อโดยตรงบนตัวอุปกรณ์

(๓) ไม่อนุญาตให้เชื่อมต่อพอร์ตโดยตรงจากเครือข่ายภายนอกกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ แต่ให้เชื่อมต่อผ่านช่องทาง VPN ที่กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่จัดเตรียมให้

(๔) อุปกรณ์เครือข่ายคอมพิวเตอร์ที่สำคัญต้องจัดเก็บในห้องอุปกรณ์เครือข่ายที่ควบคุมความปลอดภัย

(๕) ปิดพอร์ตหรือปิดบริการบนอุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

๕. การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ โดยปฏิบัติดังนี้

(๑) จัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตการแบ่งแยกเครือข่าย และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๒) แบ่งแยกเครือข่ายตามกลุ่มบริการ กลุ่มผู้ใช้งาน และระบบงานต่างๆ

(๓) ใช้ไฟร์วอลล์กันหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อยๆ

(๔) ใช้เกตเวย์ เพื่อควบคุมการเข้าถึงเครือข่ายทั้งจากภายในและภายนอกหน่วยงาน

๖. การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้งานร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง โดยต้องปฏิบัติดังนี้

(๑) การเชื่อมต่อระหว่างเครือข่าย อนุญาตให้มีการเชื่อมต่อผ่านหมายเลขไอพีแอดเดรสที่หน่วยงานกำหนดให้เท่านั้น

(๒) ผู้ใช้ต้องเชื่อมต่ออุปกรณ์ผ่านช่องทางที่หน่วยงานจัดเตรียมให้เท่านั้น

(๓) ไม่อนุญาตให้ผู้ใช้ติดตั้งอุปกรณ์กระจายสัญญาณเครือข่ายภายในหน่วยงาน

(๔) ใช้ระบบตรวจสอบจับผู้บุกรุกในระดับเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๗. การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ โดยปฏิบัติดังนี้

(๑) อนุญาตเส้นทางเครือข่ายเฉพาะกลุ่มหมายเลยไอพีแอดเดรสที่กำหนด

(๒) มีเกตเวย์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย

(๓) ควบคุมการไหลของข้อมูลผ่านเครือข่าย

(๔) ตรวจสอบหมายเลขไอพีแอดเดรสของต้นทางและปลายทาง

(๕) กำหนดเส้นทางการไหลของข้อมูลบนเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและการใช้งานบริการเครือข่าย

(๖) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อระงับการใช้จากเส้นทางอื่น

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (operation system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้อนุญาต โดยมีแนวปฏิบัติดังนี้

๑. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยปฏิบัติดังนี้

(๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(๒) หลังจากระบบติดตั้งเสร็จ ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

(๓) ผู้ใช้งานต้องตั้งค่าโปรแกรมพักหน้าจอ (screen saver) ให้มีรหัสผ่านเพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งานเกินกว่า ๕ นาที

(๔) ผู้ดูแลระบบต้องตั้งค่าไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(๕) ผู้ดูแลระบบต้องตั้งค่าให้ระบบยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดา รหัสผ่านจากเครื่องปลายทาง

(๖) ผู้ดูแลระบบต้องตั้งค่าให้มีการจำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

(๗) การเข้าใช้งานระบบปฏิบัติการ linux ผ่านระบบเครือข่ายอนุญาตให้ใช้เฉพาะ SSH เท่านั้น

(๘) การเข้าใช้งานระบบปฏิบัติการจากเครือข่ายภายนอก จะต้องผ่าน VPN ที่กำหนดให้เท่านั้น

(๙) ผู้ใช้งานต้องทำการลงบันทึกออก (logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒. การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ผู้ใช้งานต้องแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านสำหรับการใช้งานระบบสารสนเทศ ดังนี้

(๑) การพิสูจน์ตัวตนสำหรับผู้ใช้งาน ผู้ดูแลระบบต้องให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

(๒) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนโดยใช้ username และ password ของตนเองทุกครั้งก่อนใช้ระบบสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

(๓) ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้งานไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

(๔) ผู้ใช้งานต้องลงบันทึกเข้า (login) โดยใช้ชื่อบัญชีผู้ใช้งานของตนเอง และทำการลงบันทึกออก (logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๓. การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ โดยต้องปฏิบัติดังนี้

(๑) จำกัดระยะเวลาในการป้อนรหัสผ่าน หากผู้ใช้งานป้อนรหัสผ่านผิดเกินจำนวนครั้งที่กำหนด ระบบจะทำการล็อกสิทธิการเข้าถึงของผู้ใช้งาน ทำให้ไม่สามารถใช้งานได้จนกว่าผู้ดูแลระบบจะปลดล็อกให้

(๒) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีความพยายามในการเดารหัสผ่านจากเครื่องปลายทาง

(๓) มีระบบให้ผู้ใช้งานสามารถเปลี่ยนและยืนยันรหัสผ่านได้ด้วยตนเอง

(๔) จัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานแยกต่างหากจากข้อมูลของระบบงาน

(๕) ไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งานระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านของตนเอง แต่แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอแทน

(๖) เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้ที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๔. การใช้งานโปรแกรมอรรถประโยชน์

(๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(๔) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๕) ห้ามใช้งานโปรแกรมละเมิดลิขสิทธิ์

๕. การหมดเวลาใช้งานระบบสารสนเทศ (session time-out)

(๑) กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงสูงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๕ นาทีตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๒) ถ้าไม่มีการใช้งานระบบต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๖. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time)

(๑) จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอปพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานด้วยเครือข่ายภายในสามารถใช้งาน โดย

กำหนดให้ใช้งานได้ ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง และกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่เท่านั้น

(๒) จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอปพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานด้วยเครือข่ายภายนอกสามารถใช้งาน โดยกำหนดให้ใช้งานได้ ๓๐ นาทีต่อการเชื่อมต่อหนึ่งครั้ง และกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่เท่านั้น

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุมดังนี้

๑. จำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากร โดยกำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึง ดังนี้

(๑) การจำกัดการเข้าถึงของผู้ใช้งาน

- เข้าได้ตามสิทธิที่ได้รับอนุญาตเท่านั้น
- กำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคล
- บันทึกการออกจากระบบโดยทันทีที่ใช้งานเสร็จ

(๒) แบ่งกลุ่มบุคลากรที่ปฏิบัติงานด้านสารสนเทศของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ออกเป็น ๓ กลุ่ม คือ ผู้ดูแลระบบ ผู้พัฒนาระบบ และผู้ใช้งานระบบ

(๓) การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ ต้องบันทึกข้อมูลพฤติกรรมการใช้งาน การเข้าถึงระบบสารสนเทศที่สำคัญ ดังนี้

- ชื่อบัญชีผู้ใช้
- วันเวลาที่เข้าถึงระบบ
- วันเวลาที่ออกจากระบบ
- แสดงการใช้สิทธิ เช่น สิทธิของผู้ดูแลระบบ
- แสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น
- หมายเลขไอพีแอดเดรสที่เข้าถึง
- แสดงการหยุดการทำงานของระบบป้องกันการบุกรุก
- แสดงการหยุดการทำงานของระบบงานที่สำคัญ

(๔) การควบคุมผู้รับเหมาช่วง (outsource) กรณีมีการจ้างเหมาบำรุงรักษา ดูแล และพัฒนาระบบสารสนเทศ

- กำหนดคุณสมบัติของผู้รับเหมาช่วงที่ชัดเจน ต้องมีประสบการณ์ มีลูกค้าอ้างอิงน่าเชื่อถือ หรือใบรับรองทางด้านทักษะวิชาชีพตามมาตรฐานสากล มีความพร้อมด้านเทคโนโลยีของการรับเหมาช่วงทั้งในส่วนของ ฮาร์ดแวร์และซอฟท์แวร์ รวมถึงระบบสนับสนุนอื่นๆ เพื่อให้ได้ผู้รับเหมาช่วงที่มีคุณสมบัติตรงตามมาตรฐานที่หน่วยงานต้องการ
- มีข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้รับเหมาช่วง และต้องกำหนดขอบเขตและระดับการรับเหมาช่วงอย่างชัดเจน และต้องไม่เปิดเผยข้อมูลของหน่วยงานทั้งในช่วงของการว่าจ้างและเสร็จสิ้นการจ้างไปแล้ว

- หน่วยงานต้องเข้าไปตรวจสอบรายละเอียดของการปฏิบัติงานของผู้รับเหมาช่วงได้ ร่วมกำหนดวิธีการ การตรวจติดตามคุณภาพของผู้รับเหมาช่วงเป็นระยะๆ ตามที่กำหนดไว้ หรือการสุ่มตรวจสอบการปฏิบัติงานในจุดที่สำคัญ เพื่อพิจารณากระบวนการที่ผู้รับเหมาช่วงใช้ในการปฏิบัติงาน และเพื่อประเมินความสม่ำเสมอของผู้รับเหมาช่วงในการกระทำตามข้อกำหนดของหน่วยงาน
- ควบคุมการเข้าถึงของข้อมูลที่ชัดเจน มีระบบบันทึกการเข้าถึงข้อมูล และการสำรองข้อมูลทุกขั้นตอน จำกัดการเข้าถึงข้อมูลสำคัญหรือให้ใช้ข้อมูลจากชุดจำลองแทนข้อมูลจริง
- ตรวจรับงานที่ส่งมอบโดยผู้รับเหมาช่วงให้ชัดเจน เพื่อให้ได้งานตรงตามมาตรฐานที่กำหนด

๒. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการดังนี้

(๑) แยกระบบซึ่งไวต่อการรบกวนออกจากระบบอื่นๆ

(๒) ควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ โดยการติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่น ทำการป้องกันการมีทรัพยากรไม่เพียงพอ และเฝ้าระวังการเข้าถึงข้อมูลสำคัญโดยผู้ไม่ได้รับอนุญาต

(๓) กำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้น

(๔) ควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน

๓. การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(๑) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๒) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๔) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วยความรอบคอบ

(๕) เมื่อเกิดความเสียหายที่เกิดขึ้นจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๔. การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking)

(๑) ผู้ใช้งานระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

(๒) การรักษาความปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆ ภายในหน่วยงาน

(๓) ผู้ใช้ต้องระมัดระวังรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล เพื่อป้องกันการขโมยอุปกรณ์ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี

(๔) ผู้ใช้งานต้องไม่อนุญาตให้ครอบครัวหรือผู้อื่นเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน

(๕) ตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกลมีระบบป้องกันไวรัสและการใช้งานไฟร์วอลล์อย่างเหมาะสม

(๖) กำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้เข้าถึงสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงาน ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่างๆ ของหน่วยงานที่อนุญาตให้เข้าถึงจากระยะไกล

ส่วนที่ ๘ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (wireless access control)

๑. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงานต้องทำการลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒. ห้ามหน่วยงานหรือบุคลากรภายในกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ หรือบุคคลภายนอก ทำการติดตั้งอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบไร้สาย (wireless access point) ภายในกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๓. บุคลากรภายในกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ให้ใช้เฉพาะอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบไร้สายที่ทางกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่จัดเตรียมไว้เท่านั้น หากหน่วยงานหรือบุคลากรภายในกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ มีความประสงค์จะใช้งานอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบไร้สายเพิ่มเติมต้องแจ้งให้ทางศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ และเป็นผู้ดำเนินการติดตั้ง

๔. ผู้ดูแลระบบ (system administrator) ต้องดำเนินการต่อไปนี้

(๑) ทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(๒) ทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(๓) ควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๔) ทำการเปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่า default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

(๕) เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

(๖) กำหนดค่าการเข้ารหัสข้อมูลระหว่าง wireless LAN client และอุปกรณ์กระจายสัญญาณเพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

(๗) เลือกใช้วิธีการควบคุม MAC address และชื่อผู้ใช้ รหัสผ่านของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address และชื่อผู้ใช้ รหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

(๘) มีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

ส่วนที่ ๙ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์

๑. ผู้ใช้จะต้องลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) กับทางศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อนจึงจะสามารถใช้งานได้
๒. เมื่อผู้ใช้ได้รับรหัสผ่าน (password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ผู้ใช้ต้องเปลี่ยนรหัสผ่าน (password) โดยทันที
๓. ผู้ใช้ไม่ควรบันทึกหรือเก็บรหัสผ่าน (password) ไว้ในระบบคอมพิวเตอร์
๔. เปลี่ยนรหัสผ่าน (password) ทุกๆ ๓-๖ เดือน
๕. การใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ผู้ใช้ต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง
๖. การส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ให้กับผู้รับบริการ คู่สัญญา หรือตามภารกิจของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ผู้ใช้ควรใช้ระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงานเท่านั้น ไม่ควรใช้ระบบจดหมายอิเล็กทรอนิกส์ (e-mail) อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงานขัดข้อง
๗. ผู้ใช้ไม่ควรนำที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ซึ่งเป็นของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ไปเผยแพร่สู่บุคคลอื่น ไม่ว่าจะเป็นทางใดก็ตาม เช่น การโพสต์ในเว็บบอร์ดในชุดคำถามหรือแบบสอบถามจากผู้รับบริการ เป็นต้น เว้นแต่การเผยแพร่นั้นเป็นไปเพื่อผลประโยชน์ทางราชการของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ หรือได้รับอนุญาตจากผู้มีอำนาจแล้วเท่านั้น
๘. การส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ผู้ใช้ต้องระบุชื่อผู้รับ หัวข้อ ให้ชัดเจน และใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ปลุกปั่น ยั่วยุ เสียดสี หรือส่อในทางผิดกฎหมาย
๙. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องบันทึกการออกทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ของตน
๑๐. ก่อนส่งต่อ เปิดไฟล์ หรือคลิกลิ้งค์ที่แนบมา ต้องตรวจสอบให้แน่ใจก่อนว่าไม่ใช่จดหมายหลอกลวง

ส่วนที่ ๑๐ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (firewall control)

๑. ผู้ใช้สามารถใช้บริการการเชื่อมต่อเครือข่ายเฉพาะที่ไฟร์วอลล์อนุญาตให้ใช้งานเท่านั้น
๒. ทุกบริการ (services) และเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตาม policy จะต้องถูกบล็อก (block) โดย firewall
๓. การเข้าถึงอุปกรณ์ firewall สามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น
๔. ผู้ดูแลระบบหรือผู้ใช้ที่มีความจำเป็นต้องใช้งานเซิร์ฟเวอร์นอกเหนือจากบริการปกติจะต้องลงทะเบียนขออนุญาตการใช้งานเป็นลายลักษณ์อักษรก่อนจึงจะสามารถใช้งานได้
๕. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ firewall จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บไม่น้อยกว่า ๙๐ วัน
๖. กำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น
๗. มีการสำรองข้อมูลการกำหนดค่าต่างๆ ช่องอุปกรณ์ firewall เป็นประจำทุกสัปดาห์หรือทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า
๘. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ ภายในหน่วยงานที่มีลักษณะที่เป็นอินทราเน็ตจะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อให้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

๙. ผู้ละเมิดนโยบายด้านความปลอดภัยของ firewall จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

ส่วนที่ ๑๑ การบริหารจัดการสินทรัพย์

๑. ผู้ใช้งานต้องไม่เข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ที่มีการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและ/หรืออุปกรณ์บริหารจัดการเครือข่ายโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ
๒. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ
๓. ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ
๔. กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับมอบหมาย
๕. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน๊ตบุ๊ค ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน
๖. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน
๗. ทรัพย์สินและระบบสารสนเทศต่างๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อหน่วยงาน
๘. ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ ๗ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๑๒ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และป้องกันโปรแกรมไม่ประสงค์ดี

๑. กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่หน่วยงาน จัดหา หรืออนุญาตให้ใช้งาน หรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้สามารถขอให้งานได้ตามหน้าที่หรือตามความจำเป็น
๒. ซอฟต์แวร์ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้ ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ยกเว้นได้รับการอนุญาตจากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิในลิขสิทธิ์
๓. ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์หน่วยงาน ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว
๔. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (anti-virus) ตามที่หน่วยงานได้ประกาศให้ใช้เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน
๕. ผู้ใช้งานต้องทำการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีกับข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่น ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง
๖. ผู้ใช้งานต้องทำการอัพเดทโปรแกรมป้องกันไวรัส ให้เป็นปัจจุบันอยู่เสมอ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากไวรัส และโปรแกรมไม่ประสงค์ดี
๗. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

๘. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

๙. ผู้ใช้งานต้องระมัดระวัง และตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีจากการใช้งานสื่อบันทึกข้อมูลแบบพกพาต่างๆ เช่น ฟลอปปี้ดิสค์ (floppy disk) แฟลชไดรว์ (flash drive) หรือฮาร์ดดิสก์แบบพกพา เป็นต้น

๑๐. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ โปรแกรมไม่ประสงค์ดี หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายกับระบบสารสนเทศของหน่วยงาน

๑๑. ผู้ใช้งานต้องระมัดระวัง และต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนการใช้งาน

ส่วนที่ ๑๓ การควบคุมการใช้อินเทอร์เน็ต

๑. ผู้ใช้งานต้องเป็นบุคลากรสังกัดกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ที่ได้ลงทะเบียนชื่อผู้ใช้ (username) และรหัสผ่าน (password) ของระบบเมล์ที่ได้ลงทะเบียนไว้กับทางศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

๒. ผู้ใช้งานที่เป็นบุคคลภายนอกต้องลงทะเบียนกับทางศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ก่อนจึงจะสามารถใช้งานได้

๓. ผู้ใช้งานต้องตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลมาใช้งาน

๔. ผู้ใช้งานต้องใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ เช่น ไม่ดาวน์โหลดไฟล์ที่มีขนาดใหญ่ หากมีความจำเป็นให้ดำเนินการนอกเวลาทำงาน

๕. ห้ามเปิดหรือใช้งานโปรแกรมประเภท peer-to-peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (bit torrent) อีมูล (e-mule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

๖. ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

๗. ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีชื่อผู้ใช้ของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดสิทธิ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีต้องเป็นผู้รับผิดชอบ

๘. ห้ามผู้ใช้งานระบบอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล

๙. ห้ามผู้ใช้ทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

๑๐. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๑๑. ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลด การอัพเดท (update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

๑๒. ผู้ใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

๑๓. ผู้ใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

๑๔. หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดโปรแกรมเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๑. เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ผู้ใช้งานใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของหน่วยงาน

๒. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓. ไม่อนุญาตให้ ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

๔. การตั้งชื่อเครื่องคอมพิวเตอร์ (computer name) ส่วนบุคคลควรดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

๕. การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลเพื่อตรวจซ่อมควรจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือในกรณีที่หน่วยงานเจ้าของเครื่องคอมพิวเตอร์ส่วนบุคคลต้องการดำเนินการเองควรได้รับความเห็นชอบจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อนการดำเนินการ

๖. ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๗. เพื่อรักษาความปลอดภัยของคอมพิวเตอร์จากการใช้งานที่ไม่ถูกต้อง ผู้ใช้ควรมีการตั้งค่ารหัสผ่านในการเข้าใช้งาน และตั้งค่ารหัสผ่านการล็อคหน้าจอเมื่อไม่มีการใช้งานเกินกว่า ๑๐ นาที

๘. เมื่อผู้ใช้งานใช้งานคอมพิวเตอร์ส่วนบุคคลเสร็จแล้วหรือมีความจำเป็นต้องลุกจากเครื่องคอมพิวเตอร์ ผู้ใช้ควรทำการออกจากระบบ (logoff) หรือ ล็อคหน้าจอเพื่อป้องกันการใช้งานจากบุคคลอื่น

ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๑. เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ผู้ใช้งานใช้งานเป็นทรัพย์สินของหน่วยงาน ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานของหน่วยงาน

๒. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาขององค์กรต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓. การตั้งชื่อเครื่องคอมพิวเตอร์ (computer name) แบบพกพา ควรดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

๔. การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาเพื่อตรวจซ่อมควรจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือในกรณีที่หน่วยงานเจ้าของเครื่องคอมพิวเตอร์แบบพกพาต้องการดำเนินการเองควรได้รับความเห็นชอบจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อนการดำเนินการ

๕. ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๖. ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๗. ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น
๘. ห้ามใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้
๙. การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดควรปิดเครื่องคอมพิวเตอร์ เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
๑๐. หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอให้เป็นรอยขีดข่วนหรือทำให้จอของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
๑๑. ห้ามวางของทับบนหน้าจอและแป้นพิมพ์
๑๒. การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
๑๓. ห้ามเคลื่อนย้ายเครื่องในขณะที่ฮาร์ดดิสก์กำลังทำงาน
๑๔. ห้ามใช้ หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่างๆ เป็นต้น
๑๕. ห้ามใช้ หรือวางเครื่องคอมพิวเตอร์แบบพกพาในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า ๓๕ องศาเซลเซียส
๑๖. ห้ามวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น
๑๗. ห้ามติดตั้ง หรือวางคอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่
๑๘. การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอที่มีรอยขีดข่วนได้

ส่วนที่ ๑๖ การใช้งานเครือข่ายสังคมออนไลน์ (social network)

๑. การใช้งานเครือข่ายสังคมออนไลน์ ต้องใช้งานเพื่อประโยชน์ของทางราชการเป็นสำคัญ
๒. ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น
๓. ผู้ใช้งานต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอและต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์
๔. หากเกิดปัญหาจากการใช้งานเครือข่ายออนไลน์ ที่อาจมีผลกระทบกับหน่วยงาน ผู้ใช้งานต้องแจ้งต่อศูนย์เทคโนโลยีสารสนเทศและการสื่อสารโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม
๕. การใช้งานเครือข่ายออนไลน์ ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

ส่วนที่ ๑๗ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (log)

๑. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง
๒. ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT auditor) และบุคคลที่หน่วยงานมอบหมาย
๓. มีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๔. มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

หมวดที่ ๒
นโยบายการจัดทำระบบสำรองข้อมูลและการเตรียมความพร้อมกรณีฉุกเฉิน

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่มีสภาพพร้อมใช้และให้บริการได้อย่างต่อเนื่อง
๒. เพื่อกำหนดแนวปฏิบัติการจัดทำระบบสำรอง การสำรองข้อมูล การกู้คืนข้อมูล และการเตรียมความพร้อมกรณีฉุกเฉิน ให้ผู้ดูแลระบบเครือข่าย ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายและผู้ดูแลระบบสารสนเทศหน่วยงานถือปฏิบัติ
๓. เพื่อให้มั่นใจได้ว่ามีระบบสำรองที่สามารถทำงานแทนระบบหลักได้ในกรณีที่ระบบหลักมีปัญหา ต้องสำรองข้อมูลและสามารถกู้คืนข้อมูลได้ในกรณีที่จำเป็น

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญ และจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้
   ๑.๑. จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศที่สำคัญที่ต้องมีระบบสำรอง และทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง
   ๑.๒. ระบบสำรองต้องอยู่ในห้อง หรือพื้นที่ที่ต่างจากระบบหลัก และมีการควบคุม ดังนี้
      (๑) มีระบบการควบคุมการเข้าถึงที่อนุญาตเฉพาะผู้มีหน้าที่เกี่ยวข้อง
      (๒) มีระบบไฟฟ้าสำรอง
      (๓) มีระบบปรับอากาศและความชื้นที่เหมาะสม
      (๔) มีระบบป้องกันอัคคีภัย
      (๕) มีระบบแสงสว่างที่เหมาะสม
      (๖) มีระบบสื่อสารหรือระบบเครือข่ายสำรอง
      (๗) มีระบบแจ้งเตือนกรณีที่ระบบสนับสนุนทำงานผิดปกติหรือหยุดการทำงาน
   ๑.๓. มีแผนบำรุงรักษาระบบสำรองทุกระบบอย่างต่อเนื่อง
   ๑.๔. การสำรองข้อมูล (data backup)
      (๑) จัดทำขั้นตอนปฏิบัติสำหรับการสำรองข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติอย่างสม่ำเสมอ
      (๒) จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานที่จะทำการสำรองข้อมูลและทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง

(๓) กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ

(๔) กำหนดความถี่ในการสำรองข้อมูล ระบบที่มีความสำคัญสูง หรือระบบที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น

(๕) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สถานการณ์ทำงานสำเร็จ/ไม่สำเร็จ เป็นต้น

(๖) ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล และข้อมูลการตั้งค่าระบบและอุปกรณ์ต่างๆ เป็นต้น

(๗) จัดเก็บข้อมูลสำรองไว้ในระบบสำรอง

(๘) ดำเนินการป้องกันทางกายภายอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลสำรอง

๑.๕. การกู้คืนข้อมูล (data recovery)

(๑) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติอย่างสม่ำเสมอ

(๒) ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(๓) ให้ใช้ข้อมูลทันสมัยที่สุด (latest update) ที่ได้สำรองไว้ หรือตามความเหมาะสม เพื่อกู้คืนระบบ

(๔) ทดสอบการกู้คืนข้อมูลที่ได้ทำการสำรองไว้อย่างสม่ำเสมอ อย่างน้อยเดือนละ ๑ ครั้ง

๒. จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

๒.๑. จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น

(๓) กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) กำหนดช่องทางในการติดต่อกับผู้บริการภายนอก ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ และซอฟท์แวร์ เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) สร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๒.๒. ทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. มีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์

๔. มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๕. ความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้

๖. การติดตามและรายงานผล กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบเป็นประจำเดือน เพื่อรายงานสรุปให้ผู้บริหารระดับสูงสุดของหน่วยงาน (chief executive officer : CEO) ทราบและหากมีเหตุฉุกเฉินร้ายแรงต้องรายงานให้ผู้บริหารระดับสูงสุดของหน่วยงานทราบทันที

หมวดที่ ๓
นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ
๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ตรวจสอบภายใน (internal auditor) หรือผู้ตรวจสอบจากภายนอก (external auditor)
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้
   ๑.๑. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง มีวิธีการปฏิบัติ ดังนี้
   - มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ
   - มีการวางแผนสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
   - มีการตรวจสอบและประเมินความเสี่ยงของระบบให้บริการ
   - มีการตรวจประเมินระบบสารสนเทศ (information system audit considerations) อย่างน้อย ๑ ครั้งต่อปี เพื่อให้มั่นใจได้ว่าการตรวจประเมินมีประสิทธิภาพและผลการตรวจสอบเป็นที่น่าเชื่อถือได้

   ๑.๒. ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ มีวิธีการปฏิบัติ ดังนี้
   - กำหนดให้มีคณะทำงานตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ซึ่งประกอบด้วยหน่วยตรวจสอบภายในของหน่วยงาน (internal auditor) เป็นผู้ตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศ และให้ตรวจสอบและประเมินความเสี่ยงอย่างน้อย ๑ ครั้งต่อปี
   - มีข้อตกลงร่วมกันสำหรับขอบเขตการตรวจสอบระหว่างผู้ตรวจสอบกับผู้รับการตรวจ
   - มีข้อจำกัดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้ในลักษณะที่อ่านได้เพียงอย่างเดียว
   - มีวิธีการที่ปลอดภัยสำหรับการอนุญาตให้ผู้ตรวจสามารถเข้าถึงข้อมูล ชนิดที่สามารถเขียนหรือบันทึกข้อมูลได้

- มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบทำงานบนข้อมูลสำเนา
- มีการทำลาย หรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ
- มีวิธีการแบบผลอดภัยสำหรับการเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจสอบ
- มีการกำหนดหน้าที่ความรับผิดชอบของผู้ตรวจสอบและขั้นตอนปฏิบัติสำหรับการตรวจสอบ
- มีการกำหนดเจ้าหน้าที่ที่ทำหน้าที่เป็นผู้ตรวจสอบให้เป็นเอกเทศ จากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ (ผู้ตรวจสอบจะต้องไม่ตรวจสอบกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่ตนดูแล หรือรับผิดชอบ)

๒. มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึงอย่างน้อยดังนี้

๒.๑. แนวทางในการตรวจสอบและประเมินความเสี่ยง

- มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง
- มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง
- มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายการพร้อมข้อเสนอแนะ ให้ผู้บริหารพิจารณาระดับความเสี่ยงที่เป็นอยู่และกำหนดแนวทางการปรับปรุง และแจ้งให้หน่วยงานภายในที่เกี่ยวข้องทราบเพื่อนำไปปฏิบัติ

๒.๒. มาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

- ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว
- ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งดำเนินการทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้ โดยมีการป้องกันเป็นอย่างดี
- มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
- มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ
- ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ต้องแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓. รายการที่สอบทาน

- การป้องกันการบุกรุกระบบ
- การสำรองข้อมูล
- การควบคุมการเข้าห้องควบคุมระบบเครือข่าย
- การซ้อมรับสถานการณ์ฉุกเฉิน
- สอบทานการเข้าถึงระบบสารสนเทศ
- สอบทานการกำหนดการใช้งานตามภารกิจ

๒.๔. การกำกับดูแลการปฏิบัติตามด้านเทคนิค

- ผู้บริหารต้องกำกับดูแลเพื่อให้มั่นใจว่าเจ้าหน้าที่ทราบถึงความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและได้มีการปฏิบัติในทางที่เหมาะสม
- สอบทานและตรวจสอบการควบคุมทางด้านเทคนิคของระบบสารสนเทศ เพื่อตรวจสอบว่ามีความเพียงพอและเหมาะสมหรือไม่
- ในระบบสารสนเทศโดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูง ต้องมีการทดสอบระดับมาตรฐานความปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ เพื่อตรวจสอบถึงจุดเปราะบางของระบบและประสิทธิผลของการควบคุมด้านปลอดภัย
- เครื่องมือที่ใช้ในการตรวจสอบระบบคอมพิวเตอร์ทั้งหมด ซึ่งรวมถึงซอฟต์แวร์ระบบงานและเอกสาร ที่จำเป็นสำหรับงานตรวจสอบระบบคอมพิวเตอร์ ต้องได้รับการปกป้อง จากการลักลอบใช้งานหรือใช้งานหรือใช้ในทางที่ผิดวัตถุประสงค์ และการควบคุมจำกัดการเข้าใช้งานให้เฉพาะแผนกที่เกี่ยวข้องกับการตรวจสอบเท่านั้น

หมวดที่ ๔
หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

๑. ระดับนโยบาย ผู้รับผิดชอบ ได้แก่
   (๑) ผู้บริหารสูงสุด
   (๒) ผู้บริหารเทคโนโลยีสารสนเทศ ระดับสูง
   (๓) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเทียบเท่าระดับผู้อำนวยการ โดยมีหน้าที่ดังนี้
   - รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ
   - รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กร หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ระดับบริหาร ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการ หรือเทียบเท่า หัวหน้ากลุ่ม หรือเทียบเท่าหัวหน้ากลุ่ม โดยมีหน้าที่ ดังนี้
   - รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ
   - รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล
   - รับผิดชอบ วางแผน ทบทวน ติดตาม กำกับ ดูแล แผนสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๓. ระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าส่วนราชการกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ เช่น นักวิชาการคอมพิวเตอร์ วิศวกรเหมืองแร่ นักวิเคราะห์นโยบายและแผน เจ้าหน้าที่เครื่องคอมพิวเตอร์ โดยมีหน้าที่ ดังนี้
   - ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
   - ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ
   - รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
   - ทำการสำรองข้อมูลและเรียกคืนข้อมูล (backup and recovery) ตามรอบระยะเวลาที่กำหนด

- ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (hacker) โดยไม่ได้รับอนุญาต
- รับผิดชอบในการรักษาความปลอดภัย ระบบอินเทอร์เน็ต
- ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่