แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสวัสดิการและคุ้มครองแรงงาน

สำนักพัฒนามาตรฐานแรงงาน
กรมสวัสดิการและคุ้มครองแรงงาน

คำนำ

ปัจจุบันระบบเครือข่ายคอมพิวเตอร์เป็นสิ่งสำคัญสำหรับหน่วยงาน ซึ่งช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่าง ๆ ของหน่วยงานที่เชื่อมต่อเครือข่ายในระบบอินเทอร์เน็ต เช่น การรับส่งไปรษณีย์อิเล็กทรอนิกส์ และการมีเว็บไซต์ของหน่วยงานสำหรับเป็นช่องทางการประชาสัมพันธ์ข่าวสารต่าง ๆ เป็นต้น ทั้งนี้ระบบเครือข่ายดังกล่าวแม้จะมีประโยชน์และช่วยอำนวยความสะดวกก็ตาม ในขณะเดียวกันก็มีความเสี่ยง และอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติราชการได้เช่นกัน เพราะการใช้งานระบบเครือข่ายคอมพิวเตอร์เปรียบเสมือนการเปิดประตูเพื่อติดต่อกับโลกภายนอก ซึ่งมีโอกาสถูกบุกรุกได้มากขึ้น อาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการโจมตีทางระบบเครือข่ายเพื่อก่อกวนไม่ให้ระบบสามารถให้บริการได้ รวมถึงการขโมยหรือทำลายข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก และส่งผลให้เกิดความสูญเสียชื่อเสียงหรือภาพพจน์ของหน่วยงาน ดังนั้น ผู้ให้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความจำเป็นต้องตระหนักถึงการให้บริการ การดูแลบำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง

สำนักพัฒนามาตรฐานแรงงานได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสวัสดิการและคุ้มครองแรงงาน เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตาม การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ จากทุกหน่วยงาน และต้องกระทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอและปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว สำนักพัฒนามาตรฐานแรงงานจึงหวังเป็นอย่างยิ่งว่า แนวนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของกรมสวัสดิการและคุ้มครองแรงงานในการดูแลรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมสวัสดิการและคุ้มครองแรงงาน ต่อไป

สำนักพัฒนามาตรฐานแรงงาน
กรมสวัสดิการและคุ้มครองแรงงาน

สารบัญ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมสวัสดิการและคุ้มครองแรงงาน

หลักการและเหตุผล

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ สำนักพัฒนามาตรฐานแรงงานจึงได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสวัสดิการและคุ้มครองแรงงาน เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นเครื่องมือที่สำคัญในการปฏิบัติงานและการบริหารราชการต่อไป

วัตถุประสงค์

๑. เพื่อให้มีแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสวัสดิการและคุ้มครองแรงงาน ซึ่งเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒. เพื่อกำหนดแนวทางและวิธีการปฏิบัติให้บุคลากรและบุคคลที่ปฏิบัติงานให้กับหน่วยงาน การยืนยันตัวบุคคล การเข้าถึงและควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

๓. เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ เพื่อรักษาความถูกต้องสมบูรณ์ความพร้อมใช้ระบบเทคโนโลยีสารสนเทศอยู่เสมอ และการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

๔. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๕. เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ ความเข้าใจและให้การอบรมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศให้แก่บุคลากรและบุคคลที่เกี่ยวข้อง

แนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสวัสดิการและคุ้มครองแรงงาน

๑. ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของหน่วยงาน

๒. มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไขหรือบทลงโทษตามความเหมาะสมหากมีการละเมิด หรือฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๓. เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๔. เผยแพร่ความรู้ ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานเองและหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

/ ๕. ติดตาม ...

๕. ติดตาม ตรวจสอบการดำเนินงานและปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสวัสดิการและคุ้มครองแรงงาน

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสวัสดิการและคุ้มครองแรงงาน จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยแบ่งแนวปฏิบัติออกเป็นส่วน ๆ ดังนี้

ส่วนที่ ๑. แนวปฏิบัติการการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ส่วนที่ ๒. แนวปฏิบัติการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย

ส่วนที่ ๓. แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย

ส่วนที่ ๔. แนวปฏิบัติของผู้ดูแลระบบ

ส่วนที่ ๕. แนวปฏิบัติการสำรองข้อมูล

ส่วนที่ ๖. แนวปฏิบัติการประเมินความเสี่ยง

ส่วนที่ ๗. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

“หน่วยงาน” หมายความว่า กรมสวัสดิการและคุ้มครองแรงงาน

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่นระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

“ความมั่นคงปลอดภัย” หมายความว่า ความมั่นคงและปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

“ระบบแลน (Local Area Network: LAN)” และ “ระบบอินทราเน็ต (Intranet)” หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

“ระบบอินเทอร์เน็ต (Internet)” หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายสากล

“ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศ

/ ที่หน่วยงาน ...

ที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

"เครื่องคอมพิวเตอร์" หมายความว่า เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ เครื่องคอมพิวเตอร์แบบพกพา และหมายความรวมถึงอุปกรณ์ติดต่อสื่อสารประเภทเคลื่อนที่ (Mobile Device) ที่สามารถเชื่อมต่อระบบเครือข่ายของหน่วยงานได้

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

"สารสนเทศ (Information)" หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่น ๆ

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมสวัสดิการและคุ้มครองแรงงาน

"ผู้ใช้บริการ" หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างตามสัญญาจ้าง ในสังกัดหน่วยงาน และให้หมายความรวมถึงบุคคลที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

"ผู้ดูแลระบบ (System Administrator)" หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบ ดูแลรักษาหรือจัดการระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศ

"หน่วยงานภายนอก" หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล

"พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร" หมายความว่า พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

(๑) พื้นที่ทำงานทั่วไป (general working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน

(๒) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)

(๓) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)

(๔) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)

(๕) พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

"ทรัพย์สิน" หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย ซอฟต์แวร์ลิขสิทธิ์ เป็นต้น

"จดหมายอิเล็กทรอนิกส์ (e-mail)" หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นตัวอักษร ภาพถ่าย ภาพกราฟฟิก

/ ภาพเคลื่อนไหว ...

ภาพเคลื่อนไหวและเสียง ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 หรือ IMAP เป็นต้น

"รหัสผ่าน (Password)" หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ

"บัญชีผู้ใช้บริการ (Account)" หมายความว่า รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของหน่วยงาน

"โปรแกรมประสงค์ร้าย (Malware)" หมายความว่า โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาโดยมีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหาย ไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์ หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) สปายแวร์ (Spyware) หนอน (Worm) ฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

"ชื่อเครื่องคอมพิวเตอร์ (Computer Name)" หมายความว่า ชื่อที่กำหนดเฉพาะให้เครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

"สื่อบันทึกพกพา" หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Thumb Drive หรือ Handy Drive หรือ External Hard Disk หรือ Floppy Disk เป็นต้น

"การตั้งค่าระบบ (Configuration)" หมายความว่า ค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

"เลขที่อยู่ไอพี (IP Address)"หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ติดต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วน หรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

"เลขที่อยู่ไอพีสาธารณะ (Public IP Address)" หมายความว่า เลขที่อยู่ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงาน หรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากันหรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

"แบนด์วิดท์ (Bandwidth)" หมายความว่า ปริมาณข้อมูลที่ผ่านเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

"ชื่อผู้ใช้ (Username)" หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

"ลงบันทึกเข้า (Login)" หมายความว่า กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้น ตามเงื่อนไขที่ตั้งไว้ เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

"ลงบันทึกออก (Logout)" หมายความว่า กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

"อัพเดท (Update)" หมายความว่า ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่าง ๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

/ "ช่องโหว่ ...

"ช่องโหว่ (Vulnerability)" หมายความว่า ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

"อุปกรณ์กระจายสัญญาณ (Access Point)" หมายความว่า อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

"SSID (Service Set Identifier)" หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน

"MAC Address (Media Access Control Address)" หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้ถูกกำหนดจากผู้ผลิตอุปกรณ์ที่มีหมายเลขไม่ซ้ำกัน โดยอยู่ในรูปของเลขฐาน ๑๖ จำนวน ๖ คู่

"ไฟร์วอลล์ (Firewall)" หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

"ชื่อโดเมนย่อย (Sub Domain Name)" หมายความว่า ส่วนย่อยที่ขยายให้ทราบถึงกลุ่มต่าง ๆ ภายในโดเมนนั้น ๆ ซึ่งเป็นชื่อที่ระบุให้กับผู้ใช้ที่เข้ามายังเว็บไซต์ของตน หรืออาจจะใช้ที่อยู่เว็บไซต์แทนก็ได้

"อุปกรณ์จัดการเส้นทาง (Router)" หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทาง และค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

"อุปกรณ์กระจายสัญญาณข้อมูล (Switch)" หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ ทำหน้าที่รับ-ส่งข้อมูล

"การพิสูจน์ยืนยันตัวตน (Authentication)" หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

"ผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor)" หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่ตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ (Log) และรับผิดชอบให้สามารถเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์

"เวลาอ้างอิงสากล (Stratum 0)" หมายความว่า การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์กับเวลามาตรฐานสากล ซึ่งในประเทศไทยสามารถอ้างอิงกับหน่วยงานมาตรฐาน (เช่น กรมอุทกศาสตร์กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ เป็นต้น) เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"ข้อมูลจราจรทางคอมพิวเตอร์ (Log)" หมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการที่เกี่ยวข้อง ในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

/ การบังคับใช้ ...

การบังคับใช้และแนวทางปฏิบัติ

ในการพิจารณาว่าเจ้าหน้าที่ได้ปฏิบัติให้เป็นไปตามนโยบายและแนวปฏิบัติฯ หรือไม่นั้น กรมจะใช้แนวทางปฏิบัติเป็นเกณฑ์ในการพิจารณา ประกอบด้วย

๑. แนวปฏิบัติที่ต้องถือปฏิบัติตาม และมีบทลงโทษ

๒. แนวทางที่แนะนำให้ปฏิบัติ โดยไม่มีบทลงโทษ

๓. แนวทางที่แจ้งให้ทราบเพื่อปฏิบัติตามนโยบายข้ออื่นๆ หรือเป็นเรื่องที่ผู้ดูแลระบบมีสิทธิขาดในการดำเนินการ

มาตรการสำหรับผู้ฝ่าฝืน

หากมีผู้ฝ่าฝืนนโยบายและแนวปฏิบัติฯ นี้ สำนักพัฒนามาตรฐานแรงงานในฐานะผู้ดูแลระบบจะรายงานกรมเพื่อพิจารณาระงับสิทธิ์การใช้งานอินเทอร์เน็ตตามความเหมาะสม

เงื่อนไขการดำเนินงาน

๑. เจ้าหน้าที่ต้องปฏิบัติตามนโยบายและแนวปฏิบัติฯ ที่จัดทำขึ้นอย่างไม่มีเงื่อนไข โดยจะอ้างว่าไม่ทราบนโยบายและแนวปฏิบัติฯ มิได้

๒. มาตรการนี้ไม่สามารถยกเว้นความรับผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๓. ผู้ดูแลระบบมีสิทธิกระทำการใดๆ เพื่อดำเนินการตามมาตรการที่กำหนดไว้ต่อเจ้าหน้าที่ที่ละเมิดหรือพยายามจะล่วงละเมิดนโยบายและแนวปฏิบัติฯ นี้

๔. เจ้าหน้าที่ต้องยินยอมให้ผู้ดูแลระบบมีสิทธิกระทำการใดๆ เพื่อให้เกิดความปลอดภัยและเป็นไปตามนโยบายและแนวปฏิบัติฯ ที่ประกาศไว้ โดยไม่ถือว่าเป็นการกระทำผิดต่อกฎหมาย

ส่วนที่ ๑ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

เพื่อกำหนดเป็นมาตรฐานในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวกับการเข้าใช้งาน หรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน จึงกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมดังนี้

๑. ให้สำนักพัฒนามาตรฐานแรงงานเป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๒. ให้สำนักพัฒนามาตรฐานแรงงานเป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

/ ๓. บุคคลหรือ ...

๓. บุคคลหรือหน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

ส่วนที่ ๒ แนวปฏิบัติการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย

เพื่อให้ผู้ใช้บริการได้ทราบถึงหน้าที่ และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ จึงกำหนดแนวปฏิบัติการใช้ระบบคอมพิวเตอร์และระบบเครือข่ายดังนี้

๑. ผู้ใช้บริการจะต้องไม่ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายโดยมีวัตถุประสงค์ดังต่อไปนี้

๑.๑ ทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๑.๒ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

๑.๓ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

๑.๔ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

๑.๕ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

๑.๖ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๑.๗ เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตามข้อ ๑.๑ ๑.๒ ๑.๓ ๑.๔ ๑.๕ หรือ ๑.๖

๒. ผู้ใช้บริการจะต้องไม่สนับสนุน หรือยินยอมให้มีการกระทำความผิดตามข้อ ๑ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

๓. ผู้ใช้บริการจะต้องไม่กระทำการดังต่อไปนี้

๓.๑ เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน

๓.๒ นำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดขึ้นเป็นการเฉพาะไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

๓.๓ กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูล

/ คอมพิวเตอร์ ...

คอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะ หรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

๓.๔ ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

๓.๕ กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

๓.๖ ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลง แหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

๓.๗ กระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

๓.๘ จำหน่ายหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะ เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามข้อ ๓.๑ ๓.๒ ๓.๓ ๓.๔ ๓.๕ ๓.๖ หรือ ๓.๗

๔. การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย ผู้ใช้บริการควรปฏิบัติดังต่อไปนี้

๔.๑ ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานอย่างมีประสิทธิภาพ และเกิดประโยชน์สูงสุดแก่ทางราชการ

๔.๒ ไม่คัดลอกโปรแกรมต่าง ๆ ที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมายนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๔.๓ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ของหน่วยงานจะต้องกำหนดโดยเจ้าหน้าที่ของสำนักพัฒนามาตรฐานแรงงานเท่านั้น

๔.๔ ไม่ทำการปรับแต่งหรือตั้งค่าระบบ (Configuration) อื่นใดที่อาจส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ อันเป็นเหตุให้ไม่สามารถเปิดเครื่องใช้งานได้เป็นปกติ

๔.๕ ไม่ทำการเปลี่ยนแปลงเลขที่อยู่ไอพี (IP Address) ของเครื่องคอมพิวเตอร์ภายในหน่วยงาน

๔.๖ หากผู้ใช้บริการที่มีความประสงค์จะขอใช้เลขที่อยู่ไอพีสาธารณะ (Public IP Address) จะต้องทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการสำนักพัฒนามาตรฐานแรงงาน

๔.๗ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการสำนักพัฒนามาตรฐานแรงงาน

๔.๘ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงาน เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์บนระบบเครือข่ายของหน่วยงานได้ เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการสำนักพัฒนามาตรฐานแรงงาน

๔.๙ ไม่ใช้บริการบนระบบอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์ (Bandwidth) เป็นจำนวนมากหรือเป็นเวลานาน ในระหว่างเวลาทำงาน

๕. แนวปฏิบัติการใช้งานบัญชีผู้ใช้บริการ (Account)

/ ๕.๑ ผู้ใช้บริการ ...

๕.๑ ผู้ใช้บริการที่เป็นเจ้าของบัญชีผู้ใช้บริการ ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๕.๒ ผู้ใช้บริการจะต้องเก็บรักษาบัญชีผู้ใช้บริการไว้เป็นความลับ และห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่นโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๕.๓ ผู้ใช้บริการจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือจัดการใช้งานชั่วคราว

๖. แนวปฏิบัติการใช้รหัสผ่าน (Password) สำหรับเครื่องคอมพิวเตอร์

๖.๑ รหัสผ่าน ควรมีความยาวไม่น้อยกว่า ๖ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ต่าง ๆ ด้วย

๖.๒ ไม่ควรกำหนดรหัสผ่านจากชื่อ หรือสกุลของผู้ใช้บริการ ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตน หรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์

๖.๓ ควรเปลี่ยนรหัสผ่าน เพื่อใช้งานเครื่องคอมพิวเตอร์ของทุกหน่วยงานทุก ๓ – ๖ เดือน หรือเปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

๖.๔ ผู้ใช้บริการจะต้องเก็บรักษารหัสผ่าน สำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่ได้มา โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๗. แนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย (Malware)

๗.๑ เครื่องคอมพิวเตอร์ที่ใช้งานภายในหน่วยงานต้องติดตั้งโปรแกรมป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๗.๒ ผู้ใช้บริการควรทำการอัพเดท (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๗.๓ ห้ามมิให้ผู้ใช้บริการทำการปิด หรือยกเลิก หรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้าย (Malware) ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้ดูแลระบบ

๗.๔ หากผู้ใช้บริการพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย ห้ามมิให้ผู้ใช้บริการเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้าย ไปยังเครื่องคอมพิวเตอร์อื่น ๆ

๗.๕ ก่อนการใช้งานสื่อบันทึกพกพา ควรทำการตรวจสอบเพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย

๗.๖ ในการรับส่งข้อมูลคอมพิวเตอร์ หรือสารสนเทศ (Information) ผ่านทางระบบเครือข่าย ผู้ใช้บริการต้องทำการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้ายก่อนการรับส่งทุกครั้ง

๘. แนวปฏิบัติการใช้งานระบบอินเทอร์เน็ต (Internet)

๘.๑ ผู้ใช้บริการต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น และห้ามผู้ใช้บริการทำการเชื่อมต่อระบบคอมพิวเตอร์

/ ผ่านช่องทาง ...

ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการสำนักพัฒนามาตรฐานแรงงานเป็นลายลักษณ์อักษรแล้ว

๘.๒ ผู้ใช้บริการต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของหน่วยงาน และต้องไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงานเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหาย ให้กับหน่วยงาน เป็นต้น

๘.๓ ห้ามผู้ใช้บริการเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๘.๔ ผู้ใช้บริการต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการอัพเดทโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๘.๕ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้บริการต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

๘.๖ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้บริการต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

๘.๗ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ผู้ใช้บริการต้องปิดโปรแกรมเว็บเบราเซอร์ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๙. แนวปฏิบัติการใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

๙.๑ แนวปฏิบัติการใช้งานสำหรับผู้ใช้บริการ

๙.๑.๑ ผู้ใช้บริการที่ต้องการขอลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ของหน่วยงาน และยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิ์บัญชีผู้ใช้บริการรายใหม่และรหัสผ่าน

๙.๑.๒ ผู้ใช้บริการที่ได้รับรหัสผ่านครั้งแรกสำหรับการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์เมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นจะต้องเปลี่ยนรหัสผ่านโดยทันที

๙.๑.๓ ผู้ใช้บริการไม่ควรบันทึก หรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๙.๑.๔ ผู้ใช้บริการควรเปลี่ยนรหัสผ่านทุก ๓ – ๖ เดือน

๙.๑.๕ ผู้ใช้บริการไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๙.๑.๖ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้บริการควรทำการลงบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ของตน

/ ๙.๑.๗ ในกรณี ...

๙.๑.๗ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้บริการไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๙.๑.๘ ผู้ใช้บริการมีหน้าที่จะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๙.๒ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ

๙.๒.๑ ต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงานให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบ และหน้าที่ความรับผิดชอบของผู้ใช้บริการ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก การโอนย้าย เป็นต้น

๙.๒.๒ ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้บริการใส่รหัสผ่านผิดพลาดได้ไม่เกิน ๓ ครั้ง

ส่วนที่ ๓ แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายของหน่วยงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้ระบบงานสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง จึงกำหนดแนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายดังนี้

๑. ให้สำนักพัฒนามาตรฐานแรงงาน กำหนดมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการสำนักพัฒนามาตรฐานแรงงาน

๒. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๓. ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

๔. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไข เปลี่ยนแปลงสิทธิ์ต่าง ๆ การผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบ

๕. แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบสารสนเทศ

๕.๑ ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของสำนักพัฒนามาตรฐานแรงงาน ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งภายในหน่วยงาน เป็นต้น

๕.๒ ผู้ดูแลระบบต้องกำหนดให้มีการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องมีการทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

/ ๕.๓ ผู้ดูแลระบบ ...

๕.๓ ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังนี้

๕.๓.๑ กำหนดการเปลี่ยนแปลงและยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๕.๓.๒ ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๕.๓.๓ ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน

๕.๓.๔ ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๕.๓.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๕.๓.๖ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษให้กับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๕.๔ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทตามชั้นความลับ ดังต่อไปนี้

๕.๔.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งโดยการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๕.๔.๒ ต้องกำหนดรายชื่อผู้ใช้ และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๕.๔.๓ ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๕.๔.๔ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารับรหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๕.๔.๕ ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๕.๔.๖ ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๖. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๖.๑ ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point)ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๖.๒ ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSIS (Service Set Identifier) ที่ถูกกำหนดเป็น ค่าปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

/ ๖.๓ ผู้ดูแลระบบ ...

๖.๓ ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าไม่ให้แสดงชื่อระบบเครือข่ายไร้สาย

๖.๔ ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (User name) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address ชื่อผู้ใช้ และรหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้

๖.๕ ผู้ดูแลระบบควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

๖.๖ ผู้ดูแลระบบควรกำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Vertual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

๖.๗ ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย ในกรณีที่ตรวจสอบพบการใช้งานเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานต่อผู้อำนวยการสำนักพัฒนามาตรฐานแรงงานทราบทันที

๖.๘ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

๗. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๗.๑ ให้สำนักพัฒนามาตรฐานแรงงานกำหนดมาตรการควบคุมการเข้า-ออก ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๗.๒ ผู้ใช้บริการที่จะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้อำนวยการสำนักพัฒนามาตรฐานแรงงาน และต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๗.๓ การขออนุญาตใช้งานพื้นที่เว็บไซต์ (Web Server) และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องมีหนังสือขออนุญาตต่อผู้อำนวยการสำนักพัฒนามาตรฐานแรงงาน และต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ใช้บริการอื่น ๆ

๗.๔ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือกระทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๗.๕ ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อให้สามารถบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๗.๕.๑ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๗.๕.๒ ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๗.๕.๓ ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น ๆ ได้

/๗.๕.๔ ระบบเครือข่าย ...

๗.๕.๔ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นภายนอกหน่วยงาน ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้ายด้วย

๗.๕.๕ ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System /Intrustion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๗.๕.๖ เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

๗.๕.๗ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๗.๕.๘ การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

๗.๕.๙ การใช้เครื่องมือต่าง ๆ เพื่อตรวจสอบระบบเครือข่าย ต้องได้รับการอนุญาตจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๗.๖ ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ

๗.๗ ให้สำนักพัฒนามาตรฐานแรงงานกำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุได้ถึงตัวบุคคล โดยควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึงข้อมูล และผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน หรือบุคคลที่หน่วยงานมอบหมาย

๗.๘ ให้สำนักพัฒนามาตรฐานแรงงานกำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก ตามแนวทางดังต่อไปนี้

๗.๘.๑ บุคคลจากภายนอกหน่วยงานที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงาน จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขอนุญาตจากผู้อำนวยการสำนักพัฒนามาตรฐานแรงงาน

๗.๘.๒ มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๗.๘.๓ วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุญาตจากผู้อำนวยการสำนักพัฒนามาตรฐานแรงงาน

๗.๘.๔ การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

๗.๘.๕ การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

/ ส่วนที่ ๔ ...

ส่วนที่ ๔ แนวปฏิบัติของผู้ดูแลระบบ

เพื่อกำหนดหน้าที่และแนวปฏิบัติของผู้ดูแลระบบ (System Administrator) ในการบริหารจัดการ กำกับ ดูแลเครื่องคอมพิวเตอร์และระบบเครือข่ายให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งการสอดส่องดูแลการใช้งานของผู้ใช้บริการให้เป็นไปตามแนวนโยบาย จึงกำหนดแนวปฏิบัติของผู้ดูแลระบบดังนี้

๑. ผู้ดูแลระบบมีหน้าที่ดังต่อไปนี้

๑.๑ ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้บริการที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ใช้บริการผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และในกรณีที่จำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงาน ให้ผู้ดูแลระบบพิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้บริการดังกล่าวได้ทันที

๑.๒ ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

๑.๓ ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย

๑.๔ ลบข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์แม่ข่ายอย่างถาวร หรือทำลายข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานของหน่วยงานบนเครื่องคอมพิวเตอร์และระบบเครือข่ายเมื่อหมดความจำเป็นในการใช้งาน

๑.๕ ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

๑.๖ ดูแลรักษาและปรับปรุงบัญชีจดหมายอิเล็กทรอนิกส์ (e-mail) ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิ์การใช้งานของผู้ใช้บริการที่พ้นสภาพการเป็นผู้ใช้บริการ

๑.๗ ตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้บริการให้มีการกำหนดรหัสผ่าน รวมทั้งการเก็บรักษารหัสผ่าน

๑.๘ ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

๑.๙ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์ หรือข้อมูลส่วนบุคคลที่จัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

๑.๑๐ ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๑.๑๑ เมื่อผู้ดูแลระบบพ้นจากหน้าที่จะต้องคืนทรัพย์สินของหน่วยงานที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้ผู้อำนวยการสำนักพัฒนามาตรฐานแรงงานหรือผู้ที่ได้รับมอบหมายตรวจสอบการคืนทรัพย์สิน

๒. ผู้ดูแลระบบจะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็น เพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับแต่การใช้บริการสิ้นสุดลง การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังนี้

/ ๒.๑ เก็บในสื่อ ...

๒.๑ เก็บในสื่อที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้

๒.๒ มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่นผู้ตรวจสอบระบบสารสนเทศของหน่วยงานหรือบุคคลที่หน่วยงานมอบหมาย

๒.๓ ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์นั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้

๒.๔ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริง ผู้ให้บริการต้องตั้งค่านาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

ส่วนที่ ๕ แนวปฏิบัติการสำรองข้อมูล

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม จึงกำหนดแนวปฏิบัติการสำรองข้อมูลดังนี้

๑. จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปน้อย

๒. มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนการปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

๓. จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการระบุข้อความบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่จัดเก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๔. ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

ส่วนที่ ๖ แนวปฏิบัติการประเมินความเสี่ยง

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ระบุความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ จึงกำหนดแนวปฏิบัติการประเมินความเสี่ยงดังนี้

๑. ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อประเมินความเสี่ยงนั้น ดังต่อไปนี้

๑.๑ ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต

๑.๒ ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

/ ๑.๓ ความเสี่ยง ...

๑.๓ ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๑.๔ ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) สารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้บริการคนเดียวกันมากกว่าหนึ่งจุด

๒. กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๓. การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

๓.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๓.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดสถานการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๓.๓ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๓.๔ ผลการประเมินภาพรวมของความเสี่ยงที่ระบุ ต้องจัดทำเป็นคะแนนโดยมีคะแนนเต็มเป็น ๑๐๐ คะแนน และกำหนดให้มีเกณฑ์ในการพิจารณาว่าความเสี่ยงที่ระบุนั้น ต้องมีการบริหารจัดการลดความเสี่ยงนั้นหรือไม่ โดยให้เกณฑ์เป็น ๘๐ คะแนนขึ้นไป

ส่วนที่ ๗ แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง จึงกำหนดแนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศดังนี้

๑. ส่งเสริมความรู้ การปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยอาจอยู่ในรูปแบบการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับการฝึกอบรมหลักสูตรต่าง ๆ ตามแผนการฝึกอบรม หรือแผนการสัมมนาของหน่วยงาน

๒. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๓. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผลและสำรวจความต้องการของผู้ใช้บริการ
