ประกาศสำนักงานประกันสังคม
เรื่อง นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๖๕

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ เลขาธิการสำนักงานประกันสังคมโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศสำนักงานประกันสังคม เรื่อง นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๕"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓ ให้ยกเลิกประกาศสำนักงานประกันสังคม เรื่อง นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ ๑๓ กุมภาพันธ์ พ.ศ. ๒๕๖๑

ข้อ ๔ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้ แบ่งเป็น ๒ ส่วน ได้แก่

ส่วนที่ ๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศต้องมีเนื้อหาอย่างน้อยครอบคลุม ตามข้อ ๕

ส่วนที่ ๒ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศต้องมีเนื้อหาอย่างน้อยครอบคลุม ตามข้อ ๖ – ๑๑

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๕.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของสำนักงานประกันสังคม

(๓) ผู้บริหารระดับสูงสุดเป็นผู้รับผิดชอบและผู้ดำเนินการให้เป็นไปตามประกาศนโยบายและข้อปฏิบัติดังกล่าว

(๔) มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๕.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบควบคุมการเข้าถึงข้อมูล ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

(๒) การจัดระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

มีนโยบายในการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่ การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้บริหาร ผู้ใช้งาน ทั้งภายในและภายนอก

ข้อ ๖ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานประกันสังคมให้เป็นไปตามเอกสารนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานประกันสังคม พ.ศ. ๒๕๖๕ ที่แนบท้ายประกาศ

ข้อ ๗ ตรวจสอบและประเมินด้านสารสนเทศอย่างสม่ำเสมอ โดยกำหนดให้มีการตรวจสอบและควบคุมระบบงานเทคโนโลยีสารสนเทศ และดำเนินการตรวจประเมินการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานประกันสังคม อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๘ สร้างความรู้ให้แก่ผู้ใช้งานของสำนักงานประกันสังคม เพื่อสร้างความตระหนัก ความเข้าใจถึงภัยด้านความมั่นคงปลอดภัยด้านสารสนเทศและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ ด้วยวิธีการ

(๑) เผยแพร่นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์ของสำนักงานประกันสังคม ให้แก่ผู้ใช้งานและบุคคลทั่วไปสามารถเข้าถึงได้

(๒) จัดฝึกอบรมให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Training) ให้แก่ผู้ใช้งาน เพื่อสร้างความตระหนัก ความเข้าใจถึงภัยด้านความมั่นคงปลอดภัยด้านสารสนเทศและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศและมาตรการเชิงป้องกันที่เหมาะสม อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และจะต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ โดยจัดหมวดหมู่เอกสารลับไว้ต่างหาก จัดเก็บแยก และต้องป้องกันให้มีความปลอดภัยอย่างพอเพียง เช่น การนำการเข้ารหัสการประยุกต์ใช้ เป็นต้น

ข้อ ๑๐ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงสุดเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๑๑ ให้สำนักบริหารเทคโนโลยีสารสนเทศ สำนักงานประกันสังคม เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้และให้มีการทบทวนนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒ ให้คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานประกันสังคม พิจารณาและสั่งการให้เกิดการดำเนินการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง เพื่อให้บรรลุตามวัตถุประสงค์ของการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ประกาศ ณ วันที่ ๒๒ พฤศจิกายน พ.ศ. ๒๕๖๕

(นายบุญสงค์ ทัพชัยยุทธ์)
เลขาธิการสำนักงานประกันสังคม

นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานประกันสังคม
พ.ศ. ๒๕๖๕

ฉบับที่	๓
วันที่	
เจ้าของเอกสาร	สำนักบริหารเทคโนโลยีสารสนเทศ สำนักงานประกันสังคม
ทบทวนโดย	คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานประกันสังคม
มีผลบังคับใช้กับ	สำนักงานประกันสังคม
อนุมัติโดย	เลขาธิการ สำนักงานประกันสังคม

ประวัติการแก้ไขเอกสาร

ครั้งที่	รายละเอียดการแก้ไข	วันที่มีผลบังคับใช้
๑	เพิ่มข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้สอดคล้องกับมาตรฐาน ISO/IEC 27001:2013 ดังนี้ เพิ่มเติม ส่วนที่ ๒ ข้อ ๑๗ การควบคุม กำกับ ดูแล การดำเนินงานของหน่วยงานภายนอก ข้อ ๑๘ การใช้งานอุปกรณ์พกพา เพิ่มเติม ส่วนที่ ๓ ข้อ ๗ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม ข้อ ๘ การแลกเปลี่ยนสารสนเทศ ข้อ ๙ การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ของผู้ดูแลระบบ ข้อ ๑๐ การควบคุมการใช้งานอุปกรณ์พกพา ข้อ ๑๑ การเข้ารหัสข้อมูล ข้อ ๑๒ การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ข้อ ๑๓ การพัฒนาระบบให้มีความมั่นคงปลอดภัย ข้อ ๑๔ การบริหารอุบัติการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ	บังคับใช้ตั้งแต่วันถัดจากวันประกาศนโยบายฯ พ.ศ. ๒๕๖๑
๒	- แก้ไขอ้างอิงมาตรฐานจาก ISO/IEC 27001:2005 เป็น ISO/IEC 27001:2013 - แก้ไขส่วนที่ ๒ ข้อ ๖ การใช้งานอินเทอร์เน็ต โดยเพิ่ม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ข้อ ๗ การใช้งานอินทราเน็ต โดยเพิ่ม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ข้อ ๑๒ การใช้งานอุปกรณ์พกพา เครื่องคอมพิวเตอร์แบบพกพา หรือเครื่องคอมพิวเตอร์โน้ตบุ้ค โดยเพิ่มมาตรการรักษาความมั่นคงปลอดภัยอุปกรณ์พกพา - แก้ไขส่วนที่ ๓ ข้อ ๙ การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ของผู้ดูแลระบบ โดยเพิ่ม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐	บังคับใช้ตั้งแต่วันถัดจากวันประกาศนโยบายฯ พ.ศ. ๒๕๖๕

บทนำ

ในปัจจุบันสารสนเทศถือเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานราชการ และเป็นสิ่งที่มีค่ายิ่งสำหรับองค์กรซึ่งจะต้องได้รับการป้องกันรักษาเช่นเดียวกับสินทรัพย์อื่น ทั้งนี้สารสนเทศอาจอยู่ได้ในหลายรูปแบบ ไม่ว่าจะเป็นเอกสารสิ่งพิมพ์หรือถูกเก็บไว้ในสื่ออิเล็กทรอนิกส์ ซึ่งในปัจจุบันมีการใช้งานกันอย่างกว้างขวาง เพราะด้วยความสะดวก รวดเร็ว ง่ายต่อการเข้าถึง ซึ่งก็เป็นผลเชิงบวกของเทคโนโลยีที่อำนวยความสะดวกให้กับการดำเนินงานราชการในยุคปัจจุบัน จากความสะดวกสบายนี้เองที่ทำให้มีภัยคุกคามที่อยู่ในวงกว้าง ซึ่งภัยเหล่านี้อาจก่อให้เกิดความเสียหายต่องานราชการหรือองค์กร ทั้งนี้เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคามและอีกทั้งถือเป็นหลักในการปฏิบัติเพื่อให้เกิดความมั่นคงปลอดภัย ความน่าเชื่อถือ และเป็นไปตามกฎหมาย จึงต้องกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศขึ้นมาใช้งาน

๑.๑ วัตถุประสงค์

การดำเนินนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ นอกจากจะเป็นการสร้างความน่าเชื่อถือมั่นคงและปลอดภัยแล้วยังประกอบด้วยวัตถุประสงค์อื่นอีก ซึ่งมีรายละเอียด ดังนี้

๑. เป็นบรรทัดฐานด้านความมั่นคงปลอดภัยในการดำเนินกิจกรรมอันเกี่ยวข้องกับระบบสารสนเทศเทคโนโลยีและการสื่อสาร

๒. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสารอ้างอิงตามมาตรฐาน ISO/IEC 27001:2013 และมีการปรับปรุงอย่างต่อเนื่อง

๓. เพื่อเกิดความเข้าใจในแนวทางเดียวกันสำหรับผู้ปฏิบัติ

๔. เพื่อใช้เป็นหลักในการพัฒนาและปรับปรุงคุณภาพด้านความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒ หลักการ

ระบบสารสนเทศ เทคโนโลยี และการสื่อสารที่ทางสำนักงานประกันสังคมได้จัดเตรียมให้ใช้งานจำเป็นจะต้องมีข้อกำหนดสำหรับการใช้งาน การดูแลรักษา และการป้องกันให้เหมาะสมกับลักษณะการดำเนินงาน ซึ่งการดูแลรักษาและการป้องกันมุ่งเน้นไปในทางความมั่นคงปลอดภัย โดยมีหลักการสำคัญ คือการธำรงไว้ซึ่งความสมบูรณ์พร้อมใช้ (Availability) ความถูกต้อง (Integrity) และความลับ (Confidentiality)

๑.๓ บทบังคับใช้

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ให้มีผลบังคับใช้กับสินทรัพย์สารสนเทศที่ได้แถลงไว้ในขอบเขต ผู้ทำหน้าที่ดูแลสินทรัพย์ ผู้ใช้สินทรัพย์ และผู้บริหารหรือฝ่ายบริหาร มีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการและปฏิบัติตามนโยบายอย่างเคร่งครัด ผู้ใช้งานที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลสินทรัพย์จะต้องให้ความร่วมมือในการดำเนินการตามนโยบายนี้ ผู้ฝ่าฝืนนโยบายนี้มีความผิดและจะต้องได้รับการดำเนินการตามระเบียบของสำนักงานประกันสังคม

๑.๔ การเผยแพร่และทบทวน

นโยบายนี้จะต้องทำการเผยแพร่โดยการประกาศเวียนในระบบอินทราเน็ต เพื่อให้เจ้าหน้าที่ทุกระดับในสำนักงานประกันสังคม ได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด นโยบายนี้ต้องถูกทบทวนทุก ๑ ปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ นโยบายนี้ต้องกำหนดการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้ง ต่อปี

คำนิยาม (คำจำกัดความ)
สำนักงานประกันสังคม

ลำดับที่	คำศัพท์	หมายถึง
๑)	สินทรัพย์ (Asset)	สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร เช่น ข้อมูล ระบบข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ระบบเครือข่าย เครื่องคอมพิวเตอร์แบบพกพาหรือตั้งโต๊ะ ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
๒)	สารสนเทศ (Information)	ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ โดยในที่นี้เรียกรวมว่า “ข้อมูล”
๓)	ระบบสารสนเทศ (Information System)	ระบบงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
๔)	ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)	ความมั่นคงปลอดภัยของระบบสารสนเทศ การป้องกันสินทรัพย์สารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำให้สูญหายทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ โดยมีความหมายรวมถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)
๕)	การรักษาความลับ (Confidentiality)	การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต
๖)	การรักษาความครบถ้วน (Integrity)	การดำเนินการเพื่อให้ข้อมูลสารสนเทศข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งาน ประมวลผล โอนหรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ
๗)	การรักษาสภาพพร้อมใช้งาน (Availability)	การจัดทำให้สินทรัพย์สารสนเทศ สามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ
๘)	มาตรฐาน (Standard)	บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

ลำดับที่	คำศัพท์	หมายถึง
๙)	วิธีการปฏิบัติ (Procedure)	รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
๑๐)	เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)	การเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
๑๑)	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของสำนักงานประกันสังคมถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
๑๒)	การเข้าถึง (Access) หรือการควบคุมการใช้งานสารสนเทศ	การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานหรือบุคคลภายนอก เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ
๑๓)	ผู้บริหารระดับสูงสุด (CEO)	เลขาธิการ สำนักงานประกันสังคม
๑๔)	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)	ผู้บริหารที่มีอำนาจหรือผู้ได้รับมอบอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงานประกันสังคมให้มีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของสำนักงานประกันสังคมหรือบริหารจัดการสำนักบริหารเทคโนโลยีสารสนเทศ
๑๕)	สำนักบริหารเทคโนโลยีสารสนเทศ	หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ภายในสำนักงานประกันสังคม
๑๖)	หน่วยงานภายนอก	บริษัทเอกชน หรือหน่วยงานราชการ ที่สำนักงานประกันสังคมอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
๑๗)	ผู้ใช้งาน (User)	ข้าราชการ พนักงานของรัฐ ผู้บริหารของสำนักงานประกันสังคม พนักงานหรือเจ้าหน้าที่ของสำนักงานประกันสังคม ลูกจ้างสำนักงานประกันสังคม ผู้ปฏิบัติงานตามสัญญาจ้างของสำนักงานประกันสังคม ผู้ดูแลระบบ ที่ปรึกษาหรือผู้เชี่ยวชาญของสำนักงานประกันสังคม ผู้รับบริการ และผู้ใช้งานทั่วไป
๑๘)	สิทธิของผู้ใช้งาน (User Right)	แบ่งสิทธิการใช้งานตามแบบลงทะเบียนผู้ขอใช้บริการแต่ละระบบ ดังนี้ ระดับปกติ ระดับปฏิบัติการ ระดับสูง และระดับสูงพิเศษ

บทบาทหน้าที่และความรับผิดชอบ
สำนักงานประกันสังคม

ลำดับที่	ตำแหน่ง/บทบาท	หน้าที่ความรับผิดชอบ
๑)	ผู้บริหารระดับสูงสุด (Chief Executive Officer: CEO)	▪ เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
๒)	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)	▪ ทำความเข้าใจ ยอมรับ อำนวยการและให้การสนับสนุนการปฏิบัติตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ▪ สนับสนุนทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการและวัตถุดิบที่พอเพียงต่อการบริหารจัดการด้านความมั่นคงปลอดภัยในแต่ละปีงบประมาณ ซึ่งรวมถึงแผนความมั่นคงปลอดภัยด้านสารสนเทศที่จะดำเนินการในปีงบประมาณนั้นด้วย ▪ อนุมัตินโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พร้อมทั้งประเมินประสิทธิผลและทบทวนเป็นประจำทุกปี
๓)	ผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ	▪ บริหารจัดการ และควบคุมการใช้งานระบบสารสนเทศ และการใช้งานของผู้ใช้งาน ให้เป็นไปตามข้อกำหนดของนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ▪ จัดสรรทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการและวัตถุดิบที่พอเพียงต่อการรักษาความมั่นคงปลอดภัยในแต่ละปีงบประมาณ ซึ่งรวมถึงแผนความมั่นคงปลอดภัยด้านสารสนเทศที่จะดำเนินการในปีงบประมาณนั้นด้วย ▪ อนุมัติและบังคับใช้ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พร้อมทั้งประเมินประสิทธิผลและทบทวนเป็นประจำทุกปี
๔)	ผู้ใช้งาน (User)	▪ ปฏิบัติตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และเอกสารอื่นที่เกี่ยวข้อง รวมถึงความตระหนักด้านความมั่นคงปลอดภัยด้านสารสนเทศในการปฏิบัติงานและใช้งานระบบสารสนเทศ ▪ รายงานเหตุการณ์ด้านความมั่นคงปลอดภัย หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ให้แก่ผู้รับผิดชอบของสำนักงานประกันสังคม

ลำดับที่	ตำแหน่ง/บทบาท	หน้าที่ความรับผิดชอบ
๕)	ผู้ดูแลระบบ	▪ ดูแลรักษาและปรับปรุงระบบสารสนเทศ เพื่อให้สามารถใช้งานได้ตามความชำนาญและความระมัดระวังตามวิชาชีพ รวมทั้งสอดส่องดูแลการใช้งานระบบสารสนเทศ เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย เครือข่ายคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ให้เป็นไปตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ▪ สำรองข้อมูลสำคัญทางธุรกิจที่อยู่ในระบบสารสนเทศ โปรแกรมระบบปฏิบัติการ (Operating System) โปรแกรมระบบงานสารสนเทศ (Application System) และ ชุดคำสั่ง (Source Code) ให้ครบถ้วนพร้อมใช้งานได้อย่างต่อเนื่อง รวมถึงมีการจัดเก็บสื่อบันทึกข้อมูลสำรองไว้นอกสถานที่ ▪ ต้องควบคุม จัดเก็บ ป้องกัน ข้อมูลคอมพิวเตอร์หรือสารสนเทศให้เป็นไปตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ▪ ระมัดระวังอย่างเหมาะสม เพื่อปกป้องความลับ ความสมบูรณ์ครบถ้วน และความพร้อมใช้ของสินทรัพย์ที่อยู่ภายใต้การดูแลและเตรียมการเพื่อสนับสนุนการบริหาร ▪ มีการดูแลรักษาการเข้าถึงสินทรัพย์ เพื่อเป็นการปกป้องสินทรัพย์อย่างเหมาะสม เพื่อให้สอดคล้องกับการกำหนดระดับชั้นการรักษาความปลอดภัยของสินทรัพย์

ส่วนที่ ๑
นโยบายการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้ผู้บริหารกำหนดทิศทางการบริหารด้านความมั่นคงปลอดภัยที่ต้องการให้เจ้าหน้าที่ยึดถือและนำมาใช้ปฏิบัติงาน โดยมีเป้าหมายเพื่อการปฏิบัติงานที่มีความมั่นคงปลอดภัยที่เพียงพอในปัจจุบันและอนาคต

ผู้รับผิดชอบ

ผู้บริหารระดับสูงสุดของหน่วยงาน (CEO)
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

อ้างอิงมาตรฐาน

- หมวดที่ ๑ นโยบายความมั่นคงปลอดภัย
- หมวดที่ ๒ โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร
- หมวดที่ ๓ ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร
- หมวดที่ ๔ การบริหารจัดการสินทรัพย์ขององค์กร
- หมวดที่ ๕ การควบคุมการเข้าถึง
- หมวดที่ ๖ การเข้ารหัส
- หมวดที่ ๗ ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- หมวดที่ ๘ ความมั่นคงปลอดภัยในการดำเนินงาน
- หมวดที่ ๙ ความมั่นคงปลอดภัยด้านการสื่อสาร
- หมวดที่ ๑๐ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ
- หมวดที่ ๑๑ ความสัมพันธ์กับผู้ให้บริการ
- หมวดที่ ๑๒ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร
- หมวดที่ ๑๓ การบริหารความต่อเนื่องในการดำเนินงานขององค์กร
- หมวดที่ ๑๔ การปฏิบัติตามข้อกำหนด

แนวนโยบาย

๑) ผู้บริหารระดับสูงสุดของสำนักงานประกันสังคมมีหน้าที่ทำความเข้าใจ ยอมรับ อำนวยการและให้การสนับสนุนการปฏิบัติตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พร้อมทั้งสนับสนุนทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่พอเพียงต่อการบริหารจัดการด้านความมั่นคงปลอดภัยในแต่ละปีงบประมาณ ซึ่งรวมถึงแผนความมั่นคงปลอดภัยด้านสารสนเทศที่จะดำเนินการในปีงบประมาณนั้นด้วย

๒) ในกรณีระบบคอมพิวเตอร์ ระบบสารสนเทศ หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูงสุดของสำนักงานประกันสังคมเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๓) นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศต้องจัดทำเป็นลายลักษณ์อักษรตามจุดประสงค์และขอบเขต ต้องได้รับการอนุมัติ เพื่อประกาศใช้และถือปฏิบัติในสำนักงานประกันสังคมโดยให้มีผลบังคับใช้กับบุคลากรในทุกระดับชั้นของสำนักงานประกันสังคม ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูลและสินทรัพย์สารสนเทศของสำนักงานประกันสังคม

๔) นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานประกันสังคม ที่จะต้องยึดถือปฏิบัติ จะประกอบไปด้วยหัวข้อ ดังนี้

๔.๑) นโยบายการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

การดำเนินการ การใช้งานและการกระทำใดๆ อันเกี่ยวข้องทั้งทางตรงและทางอ้อมกับสินทรัพย์สารสนเทศจะต้องเป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสินทรัพย์สารสนเทศนั้น ทั้งนี้นโยบายควรต้องได้รับการทบทวน ดูแล ปรับปรุงให้ตรงตามธุรกิจ กฎหมายและต้องได้รับการเผยแพร่ไปยังผู้ใช้งานหรือบุคคลที่เกี่ยวข้องด้วย

ในกรณีที่มีการฝ่าฝืนการปฏิบัติตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ถือเป็นความผิดที่ต้องได้รับการดำเนินการตามระเบียบของสำนักงานประกันสังคม และกฎหมายของราชอาณาจักรไทย

๔.๒) นโยบายการจัดโครงสร้างด้านความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักงานประกันสังคมจะต้องให้การรองรับ ส่งเสริม สนับสนุนกิจกรรมอันเกี่ยวข้องกับการดำเนินการด้านความมั่นคงปลอดภัยเพื่อให้เกิดความสำเร็จ โดยกิจกรรมเหล่านั้นควรต้องดำเนินการไปตามหลักธรรมาภิบาล นอกจากนี้กลุ่มธุรกิจหรือบุคคลภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อมกับสินทรัพย์สารสนเทศจะต้องถูกควบคุม ตรวจสอบ ประเมินผลอย่างสม่ำเสมอเพื่อเป็นการธำรงไว้ซึ่งความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานประกันสังคม

สำนักงานประกันสังคมต้องควบคุม กำกับ ติดตามให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานของบุคลากร เพื่อให้สามารถตรวจสอบการปฏิบัติงานของบุคลากรได้ รวมถึงต้องมีการกำหนดหน้าที่ความมั่นคงปลอดภัยด้านสารสนเทศของบุคลากรให้ชัดเจน เพื่อเป็นการลดความเสี่ยงด้านความมั่นคงปลอดภัยของโครงสร้างและระบบเทคโนโลยีสารสนเทศ จากการเข้าถึง หรือการเข้าไปแก้ไขเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการนำทรัพย์สินสารสนเทศไปใช้ในงานที่ผิดต่อวัตถุประสงค์

๔.๓) การบริหารจัดการสินทรัพย์

สินทรัพย์สารสนเทศซึ่งถือว่าเป็นสิ่งที่สำคัญควรต้องได้รับการจัดหมวดหมู่ จำแนกความสำคัญและมีวิธีการควบคุมดูแลเพื่อให้เกิดความถูกต้องเหมาะสม โปร่งใส ปลอดภัย และมีผู้รับผิดชอบ ทั้งนี้สำนักงานประกันสังคมต้องควบคุม กำกับ ติดตามการบริหารจัดการทรัพย์สินสารสนเทศ เพื่อให้มีการบันทึกรายการทรัพย์สินสารสนเทศของสำนักงานที่ครบถ้วน มีการกำหนดความรับผิดชอบในการดูแลทรัพย์สินทั้งหมด และมีการกำหนดระดับความสำคัญของข้อมูลสารสนเทศสำนักงาน เพื่อให้การดูแลรักษาข้อมูลสารสนเทศเป็นไปอย่างเหมาะสม

๔.๔) ความมั่นคงปลอดภัยทรัพยากรบุคคล

บุคลากรต้องได้รับการคัดสรรอย่างเหมาะสม สามารถปฏิบัติหน้าที่ความรับผิดชอบได้ตามบทบาทที่ได้รับมอบหมาย รวมถึงความรับผิดชอบต่อความมั่นคงปลอดภัยด้านสารสนเทศ

การอบรมให้ความรู้ที่เหมาะสมกับบทบาทหน้าที่ และหากพ้นหรือเปลี่ยนแปลงบทบาทหน้าที่ต้องมีการจัดการอย่างถูกต้องเหมาะสม การละเมิดนโยบายหรือการละเลยต่อความมั่นคงปลอดภัยต้องได้รับการดำเนินการอย่างเป็นทางการและเป็นไปด้วยความยุติธรรม

จัดให้มีการฝึกอบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Training) ให้แก่ผู้ใช้งาน เพื่อสร้างความตระหนักความเข้าใจถึงภัยด้านความมั่นคงปลอดภัยด้านสารสนเทศและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ และมาตรการเชิงป้องกันที่เหมาะสม อย่างน้อยปีละ ๑ ครั้ง

๔.๕) ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

สินทรัพย์สารสนเทศที่มีความสำคัญควรอยู่ในพื้นที่ควบคุมซึ่งมีความมั่นคงปลอดภัย ได้รับการป้องกันและควบคุมอย่างเหมาะสม เพื่อไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงได้ ตลอดจนป้องกันความเสียหายหรือการถูกรบกวนที่อาจเกิดได้

อุปกรณ์ที่เกี่ยวข้องรวมถึงอุปกรณ์ที่ใช้นอกสถานที่หรือสามารถเคลื่อนย้ายได้ ควรได้รับการป้องกันอย่างเหมาะสม เพื่อลดความเสี่ยงจากการโดนโจรกรรมหรือการเข้าถึงจากผู้ไม่มีสิทธิ

๔.๖) การบริหารจัดการด้านการสื่อสารและการดำเนินการ

การสื่อสารและการดำเนินการอันเกี่ยวข้องกับสินทรัพย์สารสนเทศควรได้รับการควบคุมดูแลความมั่นคงปลอดภัยด้านสารสนเทศ และเป็นไปตามกฎหมาย กระบวนการบริหารจัดการและหน้าที่ความรับผิดชอบควรต้องระบุถึงหน้าที่ที่ชัดเจน ควรมีการเฝ้าตรวจสอบและทดสอบอย่างเหมาะสม ควรมีการสำรองข้อมูลที่สำคัญ มีการควบคุมสื่อบันทึกข้อมูล มีการควบคุมการแลกเปลี่ยนข้อมูลให้เป็นไปตามนโยบายและข้อกำหนด

๔.๗) การควบคุมการเข้าถึง

การเข้าถึงข้อมูล ระบบสารสนเทศ ระบบเครือข่าย ระบบปฏิบัติการ และแอปพลิเคชันหรือสิ่งอื่นใดอันมีอยู่บนสินทรัพย์สารสนเทศ จะต้องได้รับการควบคุมบนพื้นฐานข้อกำหนดทางธุรกิจและความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้มั่นใจว่าเฉพาะมีผู้สิทธิเท่านั้นที่ได้รับอนุญาต พร้อมทั้งควบคุม กำกับ ติดตามการเข้าถึงระบบสารสนเทศและระบบเครือข่าย เพื่อติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายได้อย่างถูกต้อง และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้ไม่ประสงค์ดีที่ต้องการสร้างความเสียหายแก่ข้อมูลสารสนเทศหรือการทำงานของระบบสารสนเทศ หรือประสงค์ให้การให้บริการของระบบเครือข่ายต้องหยุดชะงัก

นอกจากนี้ กระบวนการลงทะเบียน การยกเลิก การอนุมัติสิทธิ์ควรได้รับการจัดทำประยุกต์ใช้ ปฏิบัติ การเคลียร์เอกสารสำคัญบนโต๊ะและการเคลียร์หน้าจอ การทำลายเอกสารสื่อบันทึกข้อมูลหรืออุปกรณ์ประมวลผลอาจพิจารณานำมาใช้เพื่อลดความเสี่ยงที่อาจเกิดขึ้นตามความเหมาะสม

๔.๘) การจัดหา การพัฒนาและบำรุงรักษาระบบสารสนเทศ

ระบบสารสนเทศ ข้อมูล ระบบปฏิบัติการ แอปพลิเคชันที่พัฒนามาเฉพาะงานหรือบริการ การออกแบบและการใช้ระบบข้อมูลสนับสนุนทางธุรกิจถือเป็นสิ่งสำคัญที่ควรมี

มาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ควรมีข้อกำหนด เกณฑ์การพิจารณาจัดซื้อจัดหาที่ชัดเจน การใช้งานแอปพลิเคชันควรได้รับการออกแบบ ควบคุมอย่างเหมาะสม เพื่อป้องกันความผิดพลาด สูญหาย การเปลี่ยนแปลงแก้ไข หรือการใช้ในทางที่ผิด นอกจากนี้ ควรมีการทบทวน ตรวจสอบระบบรักษาความมั่นคงปลอดภัย ควรมีการบริหารจัดการช่องโหว่ทางเทคนิคอย่างมีประสิทธิผล และเป็นระบบ

๔.๙) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย

เหตุการณ์ที่อาจมีผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศหรือจุดอ่อนที่เกี่ยวข้องกับสินทรัพย์สารสนเทศได้รับการรายงานและแก้ไขอย่างเป็นระบบ ทันต่อเวลา ทั้งนี้ การวางแผน การกำหนดหน้าที่และขั้นตอนวิธีการในการแก้ไขเหตุการณ์ที่เกิดขึ้นได้รับการดำเนินการ เพื่อให้สามารถแก้ไขเหตุการณ์ได้อย่างเหมาะสม ตลอดจนสอดคล้องกับระเบียบข้อบังคับหรือกฎหมาย และมีกระบวนการในการปรับปรุงเพื่อป้องกันเหตุการณ์อย่างต่อเนื่อง

๔.๑๐) การบริหารธุรกิจให้ดำเนินการได้อย่างต่อเนื่อง

สินทรัพย์สารสนเทศมีการบริหารจัดการความต่อเนื่องเพื่อลดผลกระทบที่อาจเกิดขึ้นกับสำนักงานประกันสังคม ซึ่งมีการลำดับความสำคัญและผลกระทบจากความเสียหายของสินทรัพย์เพื่อใช้ในการพิจารณาวิธีการสร้างความต่อเนื่อง

จัดให้มีระบบสารสนเทศและระบบสำรองซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยสนับสนุนและดำเนินการซ้อมแผนกู้คืนระบบหรือแผนการบริหารธุรกิจให้ดำเนินการได้อย่างต่อเนื่องอย่างน้อยปีละ ๑ ครั้ง พร้อมปรับปรุงแผนฯ ตามความเหมาะสม

๔.๑๑) การปฏิบัติตามข้อกำหนดและกฎหมาย

กฎเกณฑ์และสัญญาต่างๆ อันเกี่ยวข้องกับสินทรัพย์สารสนเทศควรได้รับการพิจารณาจัดทำให้เหมาะสม ข้อบังคับทางกฎหมายที่มีผลต่อสินทรัพย์ได้รับการปฏิบัติให้ถูกต้อง ทั้งนี้ การตรวจสอบการปฏิบัติได้รับการดำเนินการและการควบคุมการตรวจสอบนั้นด้วย

๕) ผู้ใช้งานจะต้องปฏิบัติตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างเคร่งครัด ในกรณีที่มีการฝ่าฝืนการปฏิบัติตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ถือเป็นความผิดที่ต้องได้รับการดำเนินการตามระเบียบของสำนักงานประกันสังคม และกฎหมายของราชอาณาจักรไทย

๖) การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานประกันสังคม จะดำเนินการตามแนวทางการบริหารจัดการความเสี่ยง โดยสินทรัพย์สารสนเทศจะต้องได้รับการประเมินความเสี่ยง วิเคราะห์ผลกระทบและความเสียหายต่อธุรกิจ โดยการประเมินความเสี่ยงจะต้องมีหลักการและวิธีการที่ชัดเจน ผลลัพธ์จากการประเมินต้องสามารถวัดค่าและนำไปเปรียบเทียบได้ ตลอดจนต้องมีการพิจารณายอมรับความเสี่ยงจากผลลัพธ์ที่ได้จากการประเมินและสามารถนำวิธีการประเมินความเสี่ยงนี้มาใช้ได้อีก โดยการประเมินความเสี่ยงต้องทำอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการปรับปรุงเปลี่ยนแปลงซึ่งส่งผลกระทบต่อระบบ การเปลี่ยนแปลงอุปกรณ์ การปรับกระบวนการควบคุมความเสี่ยงหรือการประกาศกฎหมายบังคับใช้ด้านคอมพิวเตอร์ การตรวจสอบและประเมินความเสี่ยงดำเนินการโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

๗) ความเสี่ยงที่ไม่สามารถรับได้จะต้องได้รับการจัดการอย่างเหมาะสม ไม่ว่าจะเป็นการหลีกเลี่ยงไม่ให้เกิด การยอมรับความเสี่ยงมีอยู่ การควบคุมความเสี่ยง การถ่ายโอนความเสี่ยง ซึ่งการจัดการกับความเสี่ยงเมื่อเลือกที่จะควบคุมจะต้องมีการกำหนดตัวชี้วัดประสิทธิผลเพื่อใช้ในการพิจารณาปรับปรุงต่อไป

๘) จัดให้มีการประเมินประสิทธิผลของการนำนโยบายไปใช้ในสำนักงานประกันสังคม เพื่อนำมาใช้ในการปรับปรุงเนื้อหานโยบายหรือแผนกลยุทธ์ในการนำนโยบาย ไปใช้ในสำนักงานประกันสังคมให้มีประสิทธิผลต่อไป

๙) จัดให้มีการสอบทานหรือตรวจสอบการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เป็นประจำอย่างน้อยปีละ ๑ ครั้ง เพื่อดำเนินการปรับปรุงหรือแก้ไขนโยบายอย่างสม่ำเสมอ หรือทุกครั้งหลังจากเกิดความเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความมั่นคงปลอดภัยของสำนักงานประกันสังคม เพื่อให้สอดคล้องกับการเปลี่ยนแปลงและแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยทางด้านสารสนเทศของสำนักงานประกันสังคม

ส่วนที่ ๒
ข้อปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศ และระบบเครือข่าย

วัตถุประสงค์

เพื่อให้ผู้ใช้งานมีข้อปฏิบัติในการใช้งานคอมพิวเตอร์และเครือข่าย ได้อย่างถูกต้องเหมาะสม สอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนการดูแลสินทรัพย์ ของสำนักงานประกันสังคม ให้มีความมั่นคงปลอดภัยจากการสูญหาย

ผู้รับผิดชอบ

ผู้ใช้งานของสำนักงานประกันสังคม

อ้างอิงมาตรฐาน

- หมวดที่ ๔ การบริหารจัดการสินทรัพย์ขององค์กร
- หมวดที่ ๕ การควบคุมการเข้าถึง
- หมวดที่ ๗ ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- หมวดที่ ๙ ความมั่นคงปลอดภัยด้านการสื่อสาร
- หมวดที่ ๑๔ การปฏิบัติตามข้อกำหนด

ข้อปฏิบัติ

๑. การบริหารจัดการสินทรัพย์ขององค์กร

๑.๑) ออกจากระบบงานในทันทีเมื่อใช้งานเสร็จ

๑.๒) ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เป็นประจำหลังเสร็จสิ้นการใช้งาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายให้บริการที่ต้องใช้งานตลอด ๒๔ ชั่วโมง

๑.๓) ทำการออกจากระบบปฏิบัติการ (Log Off) ของเครื่องคอมพิวเตอร์ทุกครั้งเมื่อผู้ใช้งานไม่ได้อยู่หน้าเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน

๑.๔) ในกรณีที่ต้องใช้งานระบบสารสนเทศจากภายนอกสำนักงานประกันสังคม ผู้ใช้งานจะต้องเป็นผู้ที่ได้รับอนุญาตจากผู้มีอำนาจในการอนุมัติเท่านั้น โดยต้องมีการเข้าถึงและยืนยันตัวตนผ่านระบบ SSL VPN เท่านั้น

๑.๕) ทำการจัดเก็บข้อมูล ดังนี้

๑.๕.๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

๑.๕.๑.๑) ข้อมูลสารสนเทศด้านการบริหาร

๑.๕.๑.๒) ข้อมูลสารสนเทศงานประกันสังคมที่ให้บริการ

๑.๕.๒) จัดแบ่งลำดับชั้นความลับของข้อมูล

๑.๕.๒.๑) ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

๑.๕.๒.๒) ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

๑.๕.๒.๓) ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๑.๕.๒.๔) ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๑.๕.๓) จัดแบ่งระดับชั้นการเข้าถึง

๑.๕.๓.๑) ระดับชั้นสำหรับผู้บริหาร สามารถเข้าถึงข้อมูลประเภทข้อมูลสารสนเทศด้านการบริการ และสามารถเข้าถึงข้อมูลในทุกระดับชั้นความลับ

๑.๕.๓.๒) ระดับชั้นสำหรับผู้ใช้งานทั่วไป สามารถเข้าถึงข้อมูลประเภทข้อมูลสารสนเทศงานประกันสังคมที่ให้บริการ และสามารถเข้าถึงข้อมูลชั้นความลับในระดับข้อมูลทั่วไป

๑.๕.๓.๓) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย สามารถเข้าถึงได้เฉพาะในส่วนที่ได้รับมอบหมายตามตำแหน่งหน้าที่ความรับผิดชอบของผู้ดูแลระบบนั้นๆ เท่านั้น

๑.๕.๔) การกำหนดเวลาที่สามารถเข้าถึง

๑.๕.๕) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

๑.๖) มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

๑.๖.๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

๑.๖.๒) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๑.๗) ทำการเก็บสินทรัพย์สารสนเทศ เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือข้อมูลสารสนเทศบนเครื่องคอมพิวเตอร์ จะต้องไม่เก็บสินทรัพย์บนหน้าจอเครื่องคอมพิวเตอร์ หรือสามารถเข้าถึงได้โดยง่ายจากหน้าจอเครื่องคอมพิวเตอร์

๑.๘) ขออนุมัติจากผู้มีอำนาจในการอนุมัติในการนำเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ต่างๆ ออกนอกสำนักงานประกันสังคม

๑.๙) ระมัดระวังและดูแลสินทรัพย์ขององค์กรที่ตนเองใช้งานหรือถือครองเสมือนเป็นสินทรัพย์ของตนเอง หากเกิดความสูญหายหรือเสียหายโดยประมาทเลินเล่อ ต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

๒. การลงทะเบียนการใช้งาน

๒.๑) ผู้ใช้งานจะต้องกรอกแบบฟอร์มลงทะเบียนผู้ขอใช้บริการระบบตามที่สำนักงานประกันสังคมกำหนดโดยขออนุมัติจากผู้มีอำนาจในการอนุมัติ

๒.๒) เข้าใช้งานระบบตามสิทธิที่ตนเองได้รับเท่านั้น

๒.๓) ในกรณีที่ผู้ใช้งานลาออก หรือปรับเปลี่ยนตำแหน่งภายในสำนักงานประกันสังคม กองบริหารทรัพยากรบุคคล และหรือหัวหน้าหน่วยงานต้นสังกัดที่ปฏิบัติงาน ต้องทำหนังสือแจ้งสำนักบริหารเทคโนโลยีสารสนเทศ เพื่อทราบและดำเนินการเพิกถอนหรือเปลี่ยนสิทธิจากระบบ

๓. การกำหนด ใช้งาน และป้องกันรหัสผ่าน

๓.๑) ต้องใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองเท่านั้น ในการเข้าถึงข้อมูล ระบบเครือข่าย ระบบปฏิบัติการ และโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

๓.๒) ต้องเก็บรักษารหัสผ่านไว้เป็นความลับ ห้ามเปิดเผยต่อผู้อื่น

๓.๓) กำหนดรหัสผ่านให้มีคุณสมบัติ ตามนโยบายการตั้งรหัสผ่าน

๓.๔) ต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านจะต้องประกอบด้วยตัวอักขระไม่น้อยกว่า ๘ ตัวอักขระ ซึ่งต้องประกอบด้วยตัวเลข ตัวอักษร และตัวอักขระพิเศษ โดยต้องไม่ตั้งรหัสผ่านด้วยชื่อ วันเดือนปีเกิด หรือข้อความใดที่ง่ายต่อการล่วงรู้

๓.๕) ห้ามไม่ให้ผู้ใช้งาน ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย ๕ รหัสผ่านที่เคยใช้งาน

๓.๖) เปลี่ยนรหัสผ่าน ทุกๆ ๙๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๓.๗) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่น

๓.๘) เปลี่ยนรหัสผ่านครั้งแรกทันที เมื่อได้รับชื่อผู้ใช้งาน

๓.๙) ในกรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเพื่อให้สามารถปฏิบัติงานแทนตนเองได้ หลังจากที่ทำงานนั้นเสร็จสิ้นแล้วให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๔. การป้องกันไวรัสบนเครื่องคอมพิวเตอร์

๔.๑) ทำการตรวจสอบเครื่องคอมพิวเตอร์ โปรแกรม หรือข้อมูลให้แน่ใจว่าไม่มีไวรัสคอมพิวเตอร์หรือโปรแกรมอันตรายแฝงอยู่ ก่อนนำซอฟต์แวร์หรือข้อมูลจากภายนอกมาใช้งานภายใน สำนักงานประกันสังคม

๔.๒) ทำการตรวจสอบการทำงานของโปรแกรมป้องกันไวรัส และการปรับปรุงฐานข้อมูลไวรัสอย่างสม่ำเสมอ อย่างน้อยวันละ ๑ ครั้ง หากพบว่าทำงานผิดปกติ ให้รีบแจ้งผู้ดูแลระบบที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยทันที

๕. การติดตั้งและถอดถอนระบบ อุปกรณ์ หรือโปรแกรมต่างๆ

๕.๑) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกเหนือจากที่สำนักงานประกันสังคมได้ติดตั้งไว้ให้ และห้ามติดตั้งโปรแกรมละเมิดลิขสิทธิ์ ในกรณีที่ต้องการติดตั้งหรือใช้งานโปรแกรมอรรถประโยชน์ จะต้องขออนุญาตและติดตั้งจากผู้ดูแลระบบของสำนักงานประกันสังคมเท่านั้น

๕.๒) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย ยกเว้นการติดตั้งเพื่อการปฏิบัติงานของผู้ดูแลระบบที่เกี่ยวข้อง

๕.๓) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ เครื่องคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์ที่ผู้ใช้งานเป็นเจ้าของบนระบบเครือข่ายของสำนักงานประกันสังคมยกเว้นได้รับการตรวจสอบจากผู้ดูแลระบบที่เกี่ยวข้องก่อนการใช้งาน

๕.๔) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครือข่ายของสำนักงานประกันสังคมเพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์นั้นหรือเครือข่ายของ สำนักงานประกันสังคม

๕.๕) ห้ามถอดถอนโปรแกรมรักษาความปลอดภัยที่ติดตั้งภายในเครื่องคอมพิวเตอร์และเครือข่าย เช่น โปรแกรมป้องกันไวรัส หรือโปรแกรมบริหารจัดการเครื่องคอมพิวเตอร์ ออกโดยมิได้รับอนุญาตจากสำนักบริหารเทคโนโลยีสารสนเทศ

๖. การใช้งานอินเทอร์เน็ต

๖.๑) ต้องใช้งานอินเตอร์เน็ตเพื่อปฏิบัติงานตามภารกิจของหน่วยงานหรือหน้าที่ความรับผิดชอบของตนเอง และต้องไม่ใช้อินเตอร์เน็ตและเครือข่ายคอมพิวเตอร์ของสำนักงานประกันสังคม เพื่อกระทำการที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ หรือแสวงหาประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเผยแพร่ข้อมูลที่ไม่เหมาะสม หรือเผยแพร่ข้อมูลที่เป็นความลับของสำนักงานประกันสังคม

๖.๒) ห้ามใช้อินเทอร์เน็ต เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อสำนักงานประกันสังคม

๖.๓) ห้ามใช้โปรแกรมประเภท Peer-to-peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bit Torrent), อีมูล (e-mule), ftp เป็นต้น

๖.๔) ห้ามเข้าเว็บไซต์ประเภท ลามก อนาจาร การพนัน การประมูล วิพากษ์วิจารณ์ที่เกี่ยวข้องกับชาติ ศาสนา พระมหากษัตริย์ และสิ่งที่ขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือเว็บไซต์ที่เป็นภัยต่อสังคม

๖.๕) ห้ามเล่นเกมส์ ดูภาพยนตร์ ฟังเพลง หรือความบันเทิงส่วนตัวในเวลาทำงาน เช่น ดาวน์โหลดเพลง เกมส์ โปรแกรม Hacking Tools หรือโปรแกรมขนาดใหญ่อื่นๆ ที่อาจทำให้ข้อมูลจราจรของเครือข่ายคอมพิวเตอร์ติดขัด

๖.๖) ห้ามแอบอ้างชื่อสำนักงานประกันสังคม หรือให้ข้อมูลเท็จ ซึ่งมีผลเสียต่อภาพลักษณ์หรือชื่อเสียงของสำนักงานประกันสังคม

๗. การใช้งานอินทราเน็ต

๗.๑) ต้องใช้งานอินทราเน็ตเพื่อปฏิบัติงานตามภารกิจของหน่วยงานหรือหน้าที่ความรับผิดชอบของตนเอง และต้องไม่ใช้อินทราเน็ตและเครือข่ายคอมพิวเตอร์ของสำนักงานประกันสังคม เพื่อกระทำการที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ หรือแสวงหาประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเผยแพร่ข้อมูลที่ไม่เหมาะสม หรือเผยแพร่ข้อมูลที่เป็นความลับของสำนักงานประกันสังคม

๗.๒) ห้ามใช้อินทราเน็ต เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมี ลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อสำนักงานประกันสังคม

๗.๓) ห้ามใช้โปรแกรมประเภท Peer-to-peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bit Torrent), อีมูล (e-mule), ftp เป็นต้น

๗.๔) ห้ามเล่นเกมส์ ดูภาพยนตร์ ฟังเพลง หรือความบันเทิงส่วนตัวในเวลาทำงาน เช่น ดาวน์โหลดเพลง เกมส์ โปรแกรม Hacking Tools, หรือโปรแกรมขนาดใหญ่อื่น ๆ ที่ อาจทำให้ข้อมูลจราจรของเครือข่ายคอมพิวเตอร์ติดขัด

๗.๕) ห้ามแอบอ้างชื่อสำนักงานประกันสังคม หรือให้ข้อมูลเท็จ ซึ่งมีผลเสียต่อภาพลักษณ์หรือชื่อเสียงของสำนักงานประกันสังคม

๘. การใช้งานเครือข่ายไร้สาย (Wireless)

๘.๑) ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในสำนักงานประกันสังคม จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับอนุมัติจากผู้มีอำนาจในการอนุมัติก่อนการใช้งาน

๘.๒) ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่าเสมอ

๘.๓) ผู้ดูแลระบบควรใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

๙. การใช้เครือข่ายสังคม (Social Networking)

๙.๑) ห้ามเผยแพร่ข้อมูลของสำนักงานประกันสังคม และต้องป้องกัน รักษาความลับของสำนักงานประกันสังคม ให้เหมาะสมตามระเบียบการรักษาความลับทางราชการ

๙.๒) ห้ามเข้าถึง หรือละเมิดข้อมูลส่วนบุคคลของผู้อื่น โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล

๙.๓) ห้ามแอบอ้างหรือกระทำการใดอันอาจทำให้ผู้อื่นเข้าใจผิดว่าเป็นการสื่อความในนามสำนักงานประกันสังคม

๙.๔) ห้ามใช้เครือข่ายสังคมในลักษณะที่หยาบคาย ก้าวร้าว หรือกล่าวโทษให้ผู้อื่นเกิดความเสียหาย หรือละเมิดต่อสิทธิของผู้อื่น ขัดต่อศีลธรรมอันดี ผิดต่อกฎหมาย หรือขัดต่อรัฐธรรมนูญ

๙.๕) ผู้ใช้งานต้องรับผิดชอบต่อข้อความที่จัดทำขึ้น หรือนำไปเผยแพร่ทั้งหมด

๙.๖) ห้ามแสดงความคิดเห็นอันก่อให้เกิดความเสียหายต่อเครื่องหมายการค้า หรือสิ่งที่มีการแจ้งจดทะเบียนลิขสิทธิ์ทั้งสิ้น

๙.๗) ห้ามแสดงความคิดเห็นในเรื่องใดๆ ที่เกี่ยวข้องกับประเด็นทางกฎหมาย หรือเกี่ยวข้องกับคู่กรณีที่สำนักงานประกันสังคมกำลังดำเนินการฟ้องร้องอยู่โดยเด็ดขาด

๙.๘) สำนักงานประกันสังคมขอสงวนสิทธิ์ในการเฝ้าระวังและบันทึกการใช้งานเครือข่ายสังคมผ่านระบบเครือข่ายของสำนักงานประกันสังคม

๑๐. การใช้งานจดหมายอิเล็กทรอนิกส์

๑๐.๑) ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของสำนักงานประกันสังคมเพื่อเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของสำนักงานประกันสังคมตลอดจนเป็นการรบกวนผู้ใช้งานอื่น

๑๐.๒) ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail) จดหมายลูกโซ่ (Chain Letter) จดหมายที่ละเมิดต่อกฎหมายสินทรัพย์ทางปัญญา หรือสิทธิของบุคคลอื่น จดหมายที่มีโปรแกรมไม่ประสงค์ดีไปให้กับบุคคลอื่นโดยเจตนา

๑๐.๓) ระบบจดหมายอิเล็กทรอนิกส์ของสำนักงานประกันสังคมมีวัตถุประสงค์เพื่อการใช้งานของสำนักงานประกันสังคม เท่านั้น ห้ามไม่ให้ผู้ใช้งานนำบัญชีจดหมายอิเล็กทรอนิกส์ (Email Account) ไปใช้นอกเหนือจากวัตถุประสงค์ที่สำนักงานประกันสังคม กำหนด

๑๐.๔) ห้ามไม่ให้ผู้ใช้งานส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มา อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น

๑๐.๕) ห้ามไม่ให้ผู้ใช้งานนำบัญชีจดหมายอิเล็กทรอนิกส์ (Email Account) ซึ่งเป็นของสำนักงานประกันสังคม ไปเผยแพร่สู่บุคคลอื่น ไม่ว่าจะเป็นทางใดก็ตาม เช่น การโพสต์ในเว็บบอร์ด ในชุดคำถามหรือแบบสอบถามจากผู้ค้า เป็นต้น เว้นแต่การเผยแพร่นั้นเป็นไปเพื่อผลประโยชน์ทางราชการของสำนักงานประกันสังคม หรือได้รับอนุญาตจากผู้มีอำนาจในการอนุมัติแล้วเท่านั้น

๑๐.๖) การส่งจดหมายอิเล็กทรอนิกส์ จะต้องระบุชื่อผู้รับ หัวข้อ ให้ชัดเจน ทั้งนี้เนื้อหาข้อความของจดหมายฯ จะต้องสุภาพ ไม่ขัดต่อจริยธรรม ไม่เป็นการปลุกปั่น ยั่วยุ เสียดสี หรือส่อไปในทางผิดกฎหมาย

๑๐.๗) ไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของสำนักงานประกันสังคม หรือก่อให้เกิดความเสียหายต่อสำนักงานประกันสังคม

๑๑. การป้องกันการใช้สินทรัพย์ผิดวัตถุประสงค์

๑๑.๑) ห้ามใช้สินทรัพย์กระทำการผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายต่อบุคคล

๑๑.๒) ห้ามใช้สินทรัพย์เพื่อการพาณิชย์ส่วนบุคคล

๑๑.๓) ห้ามไม่กระทำการอันมีลักษณะเป็นการละเมิดสินทรัพย์ทางปัญญา

๑๑.๔) ห้ามใช้สินทรัพย์เข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจากเจ้าของหรือผู้ที่มีสิทธิในข้อมูล

๑๒. การใช้งานอุปกรณ์พกพา เครื่องคอมพิวเตอร์แบบพกพา หรือเครื่องคอมพิวเตอร์โน้ตบุ้ค

๑๒.๑) อนุญาตให้ใช้อุปกรณ์พกพาที่สำนักงานได้จัดเตรียมไว้ให้ในการเชื่อมต่อเข้าสู่ระบบเทคโนโลยีสารสนเทศของสำนักงานเท่านั้น และไม่อนุญาตให้ใช้อุปกรณ์ส่วนตัวเชื่อมต่อ ประมวล หรือจัดเก็บข้อมูลของสำนักงาน

๑๒.๒) อนุญาตให้ใช้อุปกรณ์พกพาส่วนตัว ในกรณีที่พนักงานนำอุปกรณ์พกพาส่วนตัวมาใช้ในสำนักงานเพื่อ เชื่อมต่อ ประมวล หรือจัดเก็บข้อมูลได้ในกรณีที่อุปกรณ์นั้นได้มีการลงทะเบียนกับสำนักบริหารเทคโนโลยีสารสนเทศ และใช้มาตรการควบคุมตามที่สำนักงานได้กำหนดไว้เท่านั้น

๑๒.๓) สำนักบริหารเทคโนโลยีสารสนเทศต้องจัดทำข้อมูลบัญชีอุปกรณ์พกพาให้เข้าถึงเครือข่ายของสำนักงาน

๑๒.๔) สำนักบริหารเทคโนโลยีสารสนเทศต้องควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงานบนพื้นฐานของการจำกัดสิทธิตามความจำเป็นในการใช้งาน

๑๒.๕) ในกรณีที่มีการใช้งานอุปกรณ์พกพาในการเชื่อมต่อเข้าสู่ระบบเทคโนโลยีสารสนเทศของสำนักงาน จากเครือข่ายที่อยู่นอกเหนือการควบคุมของสำนักงาน ได้แก่ เครือข่ายระบบอินเทอร์เน็ต เป็นต้น ผู้ใช้งาน จะต้องปฏิบัติตามขั้นตอนและวิธีการที่กำหนด

๑๒.๖) ผู้ใช้งานต้องเพิ่มความระมัดระวังในการเก็บข้อมูลสำคัญบนอุปกรณ์คอมพิวเตอร์ประเภทพกพา จะต้องดำเนินการตามมาตรการควบคุมที่สำนักงานกำหนด

๑๒.๗) อุปกรณ์คอมพิวเตอร์ทุกเครื่องที่เชื่อมต่อกับระบบใดๆ ของสำนักงาน จะต้องติดตั้งซอฟต์แวร์ป้องกันไวรัส หรือซอฟต์แวร์อื่นๆ ที่สำนักงานกำหนด พร้อมทั้งอัปเดทให้เป็นปัจจุบันอยู่เสมอ และห้ามลบหรือยกเลิกการใช้งานโดยไม่ได้รับอนุญาตจากสำนักบริหารเทคโนโลยีสารสนเทศ

๑๒.๘) การยืม-คืนเครื่องคอมพิวเตอร์แบบพกพา หรือเครื่องคอมพิวเตอร์โน้ตบุ้คของสำนักงาน ต้องลงบันทึกก่อนนำไปใช้งาน

๑๒.๙) ตรวจสอบว่าเครื่องคอมพิวเตอร์แบบพกพา หรือเครื่องคอมพิวเตอร์โน้ตบุ้คได้รับการติดตั้งโปรแกรมตามมาตรฐานก่อนนำไปใช้งาน หากพบว่ายังไม่ได้รับการติดตั้งให้ติดต่อผู้ดูแลเพื่อขอรับการติดตั้ง

๑๒.๑๐) ระมัดระวังและรักษาเครื่องคอมพิวเตอร์แบบพกพา หรือเครื่องคอมพิวเตอร์โน้ตบุ้ค เมื่อมีการนำไปใช้งานนอกสถานที่ เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑๒.๑๑) ห้ามปล่อยทิ้งเครื่องไว้ในที่สาธารณะโดยไม่มีผู้ดูแล

๑๒.๑๒) เจ้าหน้าที่ใช้งานอุปกรณ์พกพาต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใดๆ จากการรั่วไหลของข้อมูลหรือผลกระทบต่อองค์กรจากการเชื่อมต่อของอุปกรณ์พกพานั้น ทั้งอุปกรณ์พกพาที่สำนักงานจัดเตรียมให้และอุปกรณ์พกพาส่วนตัวที่พนักงานนำมาใช้เองโดยนำมาใช้ภายในเครือข่ายของสำนักงาน

๑๒.๑๓) หากเจ้าหน้าที่ทำอุปกรณ์พกพาที่เป็นทรัพย์สินของสำนักงานประกันสังคมสูญหาย ถูกขโมย เลิกใช้ หรือจำหน่าย ต้องแจ้งต่อสำนักบริหารเทคโนโลยีสารสนเทศให้เร็วที่สุด เพื่อดำเนินการระงับหรือยกเลิกสิทธิตามความเหมาะสม

๑๓. การเข้าปฏิบัติงานในห้องเครื่องคอมพิวเตอร์แม่ข่าย

๑๓.๑) ห้ามเข้าไปในบริเวณห้องเครื่องโดยไม่มีภารกิจที่เกี่ยวข้องหรือจำเป็น

๑๓.๒) ผู้ใช้งานที่ได้รับอนุญาตต้องลงบันทึกการเข้าห้องเครื่องในสมุดบันทึกการเข้า-ออกห้องเครื่อง

๑๓.๓) หากผู้ใช้งานพบเห็นความผิดปกติในห้องเครื่อง เช่น มีสินทรัพย์หาย มีร่องรอยการบุกรุก เป็นต้น ให้รีบแจ้งผู้ดูแลห้องเครื่องที่เกี่ยวข้อง

๑๓.๔) ปฏิบัติตามคำแนะนำของเจ้าหน้าที่ที่ดูแลห้องเครื่องอย่างเคร่งครัด

๑๔. การจัดการสินทรัพย์สารสนเทศลับบนกระดาษ หรือบนสื่อบันทึกข้อมูลอิเล็กทรอนิกส์

๑๔.๑) การจัดเก็บสินทรัพย์สารสนเทศที่เป็นความลับ จะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ โดยจัดหมวดหมู่เอกสารลับไว้ต่างหาก จัดเก็บแยก และต้องป้องกันให้มีความปลอดภัยอย่างพอเพียง ให้นำการเข้ารหัสมาประยุกต์ใช้

๑๔.๒) ระมัดระวังเอกสารลับที่ถูกพิมพ์ออกมาทางเครื่องพิมพ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และจำกัดการสำเนาเอกสารลับเท่าที่จำเป็นต้องใช้งานเท่านั้น

๑๔.๓) ระมัดระวังการกระจายส่ง หรือแจกจ่ายเอกสารลับไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับทราบหรือใช้งานเอกสารนั้น

๑๔.๔) ยึดถือวิธีการปฏิบัติตามกฎหมายสำหรับการจัดส่งเอกสารลับทางไปรษณีย์

๑๕. การทำลายข้อมูลบนสื่อบันทึกข้อมูล

๑๕.๑) เมื่อมีความจำเป็นต้องการทำลายสื่อ ผู้ใช้งานต้องทำการคัดแยกเอกสารตามหมวดหมู่ประเภทเอกสาร และทำลายข้อมูลลับตามวิธีการที่สำนักงานประกันสังคมกำหนดเท่านั้น

๑๕.๒) ข้อมูลที่เป็นกระดาษ ให้ทำลายด้วยเครื่องย่อยกระดาษ

๑๕.๓) ข้อมูลที่อยู่บนซีดี ให้ทำลายด้วยเครื่องทำลายแผ่นซีดี

๑๕.๔) ข้อมูลที่อยู่ฮาร์ดดิสก์ ให้ทำลายข้อมูล โดยไม่สามารถกู้คืนข้อมูลได้ โดยการเลือกใช้โปรแกรมที่มีความสามารถในการลบข้อมูลตาม Algorithm ของกระทรวงกลาโหมของสหรัฐอเมริกากำหนด หรือโปรแกรมที่ได้รับการยอมรับในระดับสากล

๑๖. การแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัย

๑๖.๑) แจ้งผู้ดูแลระบบโดยทันที เมื่อพบเหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)

๑๖.๒) ให้ความร่วมมือในการตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น

๑๗. การควบคุม กำกับ ดูแล การดำเนินงานของหน่วยงานภายนอก

๑๗.๑) หน่วยงานของสำนักงานประกันสังคมซึ่งเป็นผู้ใช้บริการจากหน่วยงานภายนอก ต้องควบคุม กำกับ ดูแล ให้หน่วยงานภายนอก ดำเนินงานในการให้บริการแก่สำนักงานตามแนวทางปฏิบัติดังนี้

๑๗.๑.๑) บุคลากรของหน่วยงานภายนอก ไม่ว่าจะทำงานอยู่ภายในสำนักงาน หรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการรักษาความลับของข้อมูลสำนักงาน โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเครือข่าย และข้อมูลต่างๆ ของสำนักงาน

๑๗.๑.๒) ดูแล ตรวจสอบ และควบคุมให้หน่วยงานภายนอกที่มีการจ้างช่วงดำเนินการดูแลให้ผู้รับจ้างช่วงปฏิบัติหน้าที่ตามนโยบายและกฎระเบียบด้านความมั่นคงปลอดภัยที่สำนักงานประกันสังคมได้กำหนดไว้ และยึดถือปฏิบัติอย่างเคร่งครัด

๑๗.๑.๓) หน่วยงานภายนอกต้องปฏิบัติงานให้เป็นไปตามเงื่อนไขข้อตกลงการให้บริการ (Service Level Agreement - SLA) ตามที่ได้ระบุไว้ในสัญญาว่าจ้าง

๑๗.๒) หน่วยงานของสำนักงานประกันสังคมซึ่งเป็นผู้ใช้บริการจากผู้ให้บริการภายนอก ต้องดูแล ตรวจสอบ และทบทวนคุณภาพของการให้บริการให้เป็นไปตามสัญญา หรือข้อตกลงการให้บริการที่ระบุไว้

๑๗.๓) หน่วยงานของสำนักงานประกันสังคมซึ่งเป็นผู้ใช้บริการจากผู้ให้บริการภายนอก ต้องควบคุมสิทธิการเข้าถึงข้อมูลของผู้ให้บริการภายนอก ให้สามารถเข้าถึงข้อมูลเท่าที่จำเป็นต่อการปฏิบัติงานเพื่อให้งานเสร็จสมบูรณ์

ส่วนที่ ๓
ข้อปฏิบัติการบริหารจัดการระบบสารสนเทศและระบบเครือข่าย

วัตถุประสงค์

เพื่อให้บุคลากรด้านปฏิบัติการบริหารจัดการระบบสารสนเทศและระบบเครือข่ายมีแนวการปฏิบัติงานอย่างถูกต้อง ลดความผิดพลาดในการพัฒนาระบบ และสามารถควบคุมการติดตั้งระบบให้ใช้งานได้อย่างมีประสิทธิภาพและต่อเนื่อง

ผู้รับผิดชอบ

ผู้ดูแลระบบของสำนักบริหารเทคโนโลยีสารสนเทศ สำนักงานประกันสังคม ที่มีหน้าที่บริหารจัดการระบบสารสนเทศ ระบบปฏิบัติการ ระบบเครือข่ายคอมพิวเตอร์ ระบบฐานข้อมูล และแอปพลิเคชัน

อ้างอิงมาตรฐาน

- หมวดที่ ๒ โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร
- หมวดที่ ๕ การควบคุมการเข้าถึง
- หมวดที่ ๗ ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- หมวดที่ ๙ ความมั่นคงปลอดภัยด้านการสื่อสาร
- หมวดที่ ๑๐ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ
- หมวดที่ ๑๒ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร
- หมวดที่ ๑๓ การบริหารความต่อเนื่องในการดำเนินงานขององค์กร
- หมวดที่ ๑๔ การปฏิบัติตามข้อกำหนด

ข้อปฏิบัติ

๑. การบริหารจัดการการควบคุมการเข้าถึงและการควบคุมการใช้งานสารสนเทศ (Access Control)

๑.๑) ต้องมีระบบควบคุมการเข้าถึงข้อมูล ระบบเครือข่าย ระบบปฏิบัติการและโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ ทั้งทางกายภาพและทางระบบเครือข่าย

๑.๒) การขอสิทธิในการเข้าถึงระบบเครือข่ายเพื่อใช้งานระบบสารสนเทศจะต้องดำเนินการผ่านการกรอก “แบบลงทะเบียนผู้ขอใช้บริการ” ของสำนักบริหารเทคโนโลยีสารสนเทศ โดยแยกระบบการทำงานตามระบบหลัก ระดับการทำงาน แบ่งเป็น ปกติ และสูง และได้รับการอนุญาตจากผู้มีอำนาจในการอนุมัติเท่านั้น

๑.๓) ต้องจัดให้มีระบบบันทึกหรือติดตามการเข้าถึงข้อมูล ระบบเครือข่าย ระบบปฏิบัติการโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ โดยกำหนดระยะเวลา เปิดระบบ Online เวลา ๐๘.๐๐ น. และปิด Online ในเวลา ๑๘.๓๐ น.รวมทั้งกำหนดการเข้าใช้งานระบบอินทราเน็ตทุกคนเข้าได้ตลอดเวลา ส่วนการเข้าใช้งานระบบอินเทอร์เน็ตแบ่งเป็นเข้าได้ตลอดเวลา กับ ช่วงเวลา ๑๗.๐๐ น. ถึง ๐๘.๓๐ น. ของวันถัดไป และระบบตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

๑.๔) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบและการแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๑.๕) ผู้ดูแลระบบต้องไม่เข้าถึงข้อมูลของสำนักงานประกันสังคม หรือข้อมูลส่วนบุคคลของสมาชิกสำนักงานประกันสังคม โดยมิชอบ

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

๒.๑.๑) ต้องกำหนดสิทธิการเข้าถึงข้อมูล ระบบเครือข่าย ระบบปฏิบัติการและโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ ให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งานในการปฏิบัติงานก่อน รวมทั้งจัดให้มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

๒.๑.๒) การให้สิทธิในการเข้าถึงข้อมูล ระบบเครือข่าย ระบบปฏิบัติการและโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ จะต้องกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งานตามข้อมูลในแบบลงทะเบียนผู้ขอใช้บริการระบบเพื่อขอสิทธิในการเข้าสู่ระบบที่มีการลงนามอนุมัติเอกสารดังกล่าวจากเจ้าของข้อมูลหรือระบบ หรือผู้มีอำนาจในการอนุมัติเท่านั้น

๒.๑.๓) ผู้ดูแลระบบที่มีสิทธิจำเพาะ หรือสิทธิพิเศษ (Super User) ที่เกี่ยวข้องกับการเข้าถึงระบบ ซึ่งสามารถดำเนินการแก้ไขค่าพารามิเตอร์ หรือค่าคอนฟิกูเรชั่นของระบบที่สำคัญ จะต้องเป็นผู้ที่ได้รับมอบหมายจากผู้มีอำนาจในการอนุมัติ

๒.๑.๔) ในกรณีที่ผู้ใช้งานลาออก หรือปรับเปลี่ยนตำแหน่งภายในสำนักงานประกันสังคม ผู้ดูแลระบบจะต้องดำเนินการเพิกถอนสิทธิจากทะเบียนผู้ใช้งานหรือปรับเปลี่ยนสิทธิจากระบบ ภายใน ๓ วันทำการ นับจากได้รับเอกสารแจ้ง

๒.๑.๕) กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงเท่าที่ได้รับอนุญาตเท่านั้น

๒.๒) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๒.๒.๑) จัดให้มีระบบที่สามารถรองรับการกำหนดรหัสผ่านที่ประกอบด้วยตัวอักขระไม่น้อยกว่า ๘ ตัวอักขระ ซึ่งต้องประกอบด้วยตัวเลข ตัวอักษร และตัวอักขระพิเศษ พร้อมกำหนดห้ามไม่ให้ผู้ใช้งานใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย ๕ รหัสผ่านที่เคยใช้งาน และเปลี่ยนรหัสผ่านทุกๆ ๙๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๒.๒.๒) จัดให้ผู้ใช้งานที่ต้องการใช้บริการของระบบสารสนเทศหรือระบบเครือข่าย จะต้องมีการยืนยันตัวบุคคลของผู้ใช้งาน (Authentication) ผ่านระบบ Lightweight Directory Access Protocol (LDAP) ทุกครั้ง พร้อมจัดให้มีการบันทึกข้อมูลการเข้าถึงผ่านระบบ LDAP ทุกครั้ง

๒.๒.๓) ระบบการยืนยันตัวบุคคลของผู้ใช้งานจะต้องตั้งค่าระบบให้ห้ามใส่ทะเบียนผู้ใช้ (Username) หรือรหัสผ่าน (Password) ผิดเกินกว่า ๕ ครั้ง ในกรณีที่เกิน ระบบจะต้องทำการปฏิเสธการเข้าถึงของผู้ใช้งานท่านนั้น เป็นการชั่วคราว จนกว่าจะสามารถยืนยันตัวตนได้

๓. การบริหารจัดการระบบเครือข่าย (Network System)

๓.๑) จัดให้มีระบบการบริหารจัดการระบบเครือข่าย โดยกำหนดการใช้งานบริการเครือข่ายแยกตามสิทธิการเข้าถึงของผู้ใช้งาน และห้ามเข้าถึงบริการอื่นๆ ที่ไม่ได้รับอนุญาต

๓.๒) ต้องมีการออกแบบแบ่งแยกเครือข่าย (Segregation in networks) โดยกำหนดให้ทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ โซนผู้ใช้งานภายใน (Internal User Zone) โซนผู้ใช้งานภายนอก (External User Zone) และโซนเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๓.๓) การเข้าถึงระบบเครือข่าย หรือติดตั้งอุปกรณ์บนระบบเครือข่ายของสำนักงานประกันสังคม จะต้องได้รับอนุญาตจากผู้ดูแลระบบเครือข่ายเท่านั้น

๓.๔) การเข้าใช้งานระบบเครือข่ายของผู้ดูแลระบบ จะต้องตั้งค่าระบบการยืนยันตัวบุคคลของผู้ใช้งานของระบบเครือข่าย ห้ามใส่ทะเบียนผู้ใช้ (Username) หรือรหัสผ่าน (Password) ผิดเกินกว่า ๕ ครั้ง ในกรณีที่เกิน ระบบจะต้องทำการปฏิเสธการเข้าถึงของผู้ดูแลระบบท่านนั้นเป็นการชั่วคราว จนกว่าจะมีการยืนยันตัวตนได้

๓.๕) ในกรณีที่มีความจำเป็นจะต้องเข้าถึงระบบสารสนเทศจากภายนอกสำนักงาน จะต้องได้รับการอนุมัติจากผู้มีอำนาจในการอนุมัติเท่านั้น และต้องดำเนินการผ่านระบบเชื่อมต่อแบบ SSL VPN ของสำนักงานประกันสังคม และต้องมีการบริหารจัดการเพื่อจำกัดสิทธิ์การใช้งาน และควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๓.๖) การเข้าถึงระบบเครือข่ายผ่านระบบการสื่อสารไร้สาย (Wireless LAN) ผู้ดูแลระบบจะต้องกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย

๓.๗) การเข้าถึงบริการผ่านระบบการสื่อสารไร้สาย จะต้องผ่านอุปกรณ์รักษาความมั่นคงปลอดภัย เช่น อุปกรณ์ประเภท Firewall หรือ IPS เป็นต้น

๓.๘) การติดต่อสื่อสารผ่านระบบการสื่อสารไร้สายระหว่างเครื่องของผู้ใช้งานและ Access Point ต้องเป็นการเข้ารหัสข้อมูลแบบ WPA เป็นอย่างน้อย

๓.๙) ระบบเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อกันระหว่างสำนักงานประกันสังคมและหน่วยงานภายนอก จะต้องมีการควบคุมการเข้าถึงที่มีความมั่นคงปลอดภัย เชื่อมต่อผ่านอุปกรณ์ป้องกันประเภท Firewall และติดตั้งระบบที่ต้องเชื่อมต่อในเครือข่ายที่กำหนดไว้ (DMZ Zone)

๓.๑๐) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) จะดำเนินผ่านอุปกรณ์ที่ทำหน้าที่เป็นเกตเวย์หรืออุปกรณ์ที่สามารถควบคุมการไหลของข้อมูล จำกัดการเข้าถึงระบบเครือข่ายและปิดบังหมายเลขไอพีที่ได้ อุปกรณ์ประเภท Firewall หรือ Proxy

๓.๑๑) กำหนดให้มีการป้องกันพอร์ตที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบ ทั้งทางกายภายและทางเครือข่าย ด้วยการปิด (Disable) พอร์ตสำหรับตรวจสอบและปรับแต่งระบบที่ไม่ได้ใช้งาน ปิดประตูและล็อกตู้แร็คที่ติดตั้งอุปกรณ์และเครื่องคอมพิวเตอร์แม่ข่ายที่มีความสำคัญ รวมถึงกำหนดหมายเลขไอพีของเครื่องคอมพิวเตอร์ที่อนุญาตให้เข้าถึงพอร์ตสำหรับตรวจสอบและปรับแต่งระบบการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบจะต้องได้รับอนุญาตจากผู้มีอำนาจอนุมัติ

๓.๑๒) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Netwrok) จะดำเนินการโดยใช้บัญชีรายการอุปกรณ์บนระบบเครือข่าย (Inventory list) ประกอบกับผังเครือข่ายของสำนักงาน โดยบัญชีรายการอุปกรณ์ประกอบด้วยรายละเอียดของหมายเลขฮาร์ดแวร์ (MAC Address) หมายเลขไอพี (IP Address) ชื่อรุ่นอุปกรณ์ เป็นอย่างน้อย พร้อมทั้งดำเนินการ

ปรับปรุง ทบทวนความถูกต้องของบัญชีรายการอุปกรณ์และผังเครือข่ายทุก ๑ ปีหรือเมื่อมีการเปลี่ยนแปลงอุปกรณ์ภายในระบบเครือข่ายเพื่อให้ข้อมูลเป็นปัจจุบันอยู่เสมอ

๓.๑๓) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๓.๑๔) ต้องจัดให้มีระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสำนักงานประกันสังคมในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๓.๑๕) การติดตั้งอุปกรณ์บนเครือข่าย ต้องตรวจสอบและบันทึกหมายเลข MAC Address ของอุปกรณ์เพื่อใช้ในการตรวจสอบและการกำหนดสิทธิการใช้งานบนเครือข่าย

๓.๑๖) การใช้งาน Remote เพื่อตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration) ต้องผ่าน Firewall Policy เพื่อกำหนดสิทธิในการเข้าถึงให้สามารถใช้งานได้

๔. การบริหารจัดการระบบปฏิบัติการ (Operation System)

๔.๑) ต้องกำหนดผู้ดูแลระบบที่มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๔.๒) การเข้าถึงระบบปฏิบัติการจะต้องถูกควบคุมการเข้าถึงด้วยวิธีการยืนยันตัวบุคคลของผู้ใช้งาน (Authentication) ทุกครั้ง โดยใช้การลงทะเบียนผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นตัวควบคุม และต้องจัดให้มีระบบบันทึกการเข้าถึงข้อมูลเพื่อบันทึกข้อมูลการเข้าถึงทุกครั้ง

๔.๓) การเข้าถึงระบบปฏิบัติการหรือเครื่องคอมพิวเตอร์แม่ข่ายของผู้ดูแลระบบ จะต้องกำหนดการใช้งานแยกตามสิทธิการดูแลของผู้ดูแลระบบที่ได้รับมอบหมายจากผู้มีอำนาจในการอนุมัติ และห้ามเข้าถึงระบบปฏิบัติการหรือเครื่องคอมพิวเตอร์แม่ข่ายอื่นๆ ที่ไม่ได้รับอนุญาต

๔.๔) ต้องมีการทบทวนสิทธิในการเข้าถึงระบบปฏิบัติการหรือเครื่องคอมพิวเตอร์แม่ข่าย เป็นประจำอย่างสม่ำเสมอ ระยะเวลาอย่างน้อย ๑ ครั้งต่อปี หรือในกรณีที่ผู้ดูแลระบบลาออก หรือปรับเปลี่ยนตำแหน่งภายในสำนักงานประกันสังคม ผู้ดูแลระบบที่เหลือจะต้องดำเนินการเพิกถอนสิทธิจากทะเบียนผู้ดูแลระบบนั้น ภายใน ๗ วันหลังจากได้รับเอกสารแจ้ง

๔.๕) ระบบการยืนยันตัวบุคคลของผู้ดูแลระบบปฏิบัติการหรือเครื่องคอมพิวเตอร์แม่ข่าย ตามการอนุมัติของผู้บังคับบัญชาอย่างมีลายลักษณ์อักษร จะต้องตั้งค่าระบบให้ห้ามใส่ทะเบียนผู้ใช้ (Username) หรือรหัสผ่าน (Password) ผิดเกินกว่า ๕ ครั้ง ในกรณีที่เกินระบบจะต้องทำการปฏิเสธการเข้าถึงของผู้ดูแลระบบท่านนั้น เป็นการชั่วคราว จนกว่าจะสามารถยืนยันตัวตนได้โดยต้องติดต่อเจ้าหน้าที่ผู้รับผิดชอบดำเนินการต่อไป

๔.๖) การติดตั้งโปรแกรมอรรถประโยชน์ (System Utilities) บนเครื่องคอมพิวเตอร์แม่ข่าย จะต้องดำเนินการประเมินผลกระทบโดยผู้ดูแลระบบ และติดตั้งได้หลังจากรับการอนุมัติจากผู้มีอำนาจในการอนุมัติ

๔.๗) ต้องมีการกำหนดการยุติการใช้งานระบบปฏิบัติการ เมื่อมีการว่างเว้นจากการใช้งานเป็นระยะเวลาไม่เกิน ๒๐ นาที

๔.๘) ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น โดยตั้งปิดบริการที่ไม่จำเป็น เช่น telnet ftp หรือ ping เป็นต้น ทั้งนี้หากมีบริการที่จำเป็นต้องใช้ และมีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ผู้ดูแลระบบต้องมีมาตรการป้องกันเพิ่มเติมที่เหมาะสม และได้รับการอนุมัติจากผู้มีอำนาจในการอนุมัติเท่านั้น

๔.๙) ควรดำเนินการหาข้อมูลของเจ้าของผลิตภัณฑ์เกี่ยวกับช่องโหว่ของระบบปฏิบัติการและระบบซอฟท์แวร์ที่สำนักงานประกันสังคมใช้งานอยู่อย่างสม่ำเสมอ และประเมินความเสี่ยงที่อาจจะเกิดขึ้นถ้าดำเนินปรับปรุง (Update) ระบบปฏิบัติการและระบบซอฟท์แวร์ และในกรณีที่ความเสี่ยงต่ำหรือสามารถยอมรับได้ ควรดำเนินการปรับปรุง (Update) ระบบปฏิบัติการให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

๔.๑๐) การติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายใหม่พร้อมระบบปฏิบัติการ หรือติดตั้งระบบปฏิบัติการใหม่บนเครื่องคอมพิวเตอร์แม่ข่าย ผู้ดูแลระบบจะต้องปิดช่องโหว่ (System Hardening) ของระบบปฏิบัติการนั้นตามมาตรฐานด้านความมั่นคงปลอดภัยด้านสารสนเทศที่แนะนำโดยเจ้าของผลิตภัณฑ์นั้นทุกครั้ง ยกเว้นแต่ได้รับอนุญาตจากผู้มีอำนาจในการยกเว้นการปฏิบัติ

๕. การบริหารจัดการโปรแกรมประยุกต์ แอปพลิเคชัน ระบบงานสารสนเทศและสารสนเทศ (Application and Information)

๕.๑) ในกรณีระบบงานสารสนเทศ โปรแกรมประยุกต์ หรือสารสนเทศที่เป็นระบบที่ไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร จะต้องจัดวางบนระบบเครือข่ายที่แยกออกจากระบบอื่นๆ ของสำนักงานประกันสังคม และจัดให้มีการควบคุมการเข้าถึง (Access Control) และการรักษาความมั่นคงปลอดภัย (Security System) โดยเฉพาะอย่างเหมาะสม ในกรณีที่จะต้องมีการใช้งานจากภายนอกสำนักงานประกันสังคม จะต้องจัดหาช่องทางควบคุมการเข้าถึงจากภายนอกที่มีความมั่นคงปลอดภัยเพียงพอ เช่น ระบบการเชื่อมต่อแบบ SSL VPN

๕.๒) ระบบงานสารสนเทศที่มีการอนุญาตให้มีการเชื่อมต่อผ่านอุปกรณ์คอมพิวเตอร์แบบเคลื่อนที่ โทรศัพท์เคลื่อนที่ (Mobile) หรือคอมพิวเตอร์แบบพกพา (Tablet) จะต้องมีระบบควบคุมการเข้าถึงด้วยวิธีการยืนยันตัวบุคคลของผู้ใช้งานทุกครั้ง พร้อมทั้งจะต้องตั้งค่าระบบให้ห้ามใส่ทะเบียนผู้ใช้ (Username) หรือรหัสผ่าน (Password) ผิดเกินกว่า ๕ ครั้ง ในกรณีที่เกิน ระบบจะต้องทำการปฏิเสธการเข้าถึงของผู้ใช้งานหรือผู้ดูแลระบบท่านนั้น เป็นการชั่วคราว จนกว่าจะสามารถยืนยันตัวตนได้ โดยต้องติดต่อเจ้าหน้าที่ผู้รับผิดชอบดำเนินการต่อไป

๕.๓) ต้องมีการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับโปรแกรมประยุกต์ แอปพลิเคชัน หรือระบบงานสารสนเทศ ที่มีความเสี่ยงหรือมีความสำคัญสูง (Limitation of Connection Time) โดย

๕.๓.๑ ระยะเวลาที่จำกัดสามารถกำหนดได้ตามความเหมาะสมของลักษณะงาน แต่ไม่ควรเกินครั้งละ ๑๒๐ นาที

๕.๓.๒ สำหรับกรณีที่จ้างพัฒนาระบบ (Outsource) และเจ้าหน้าที่ผู้พัฒนาระบบเข้ามาแก้ปัญหาหลังจากการส่งมอบระบบต้องทำหนังสือแจ้งหน่วยงานที่รับผิดชอบพร้อมกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับโปรแกรมประยุกต์ แอปพลิเคชัน หรือระบบงานสารสนเทศไม่ควรเกินครั้งละ ๑๒๐ นาที

๕.๔) การพัฒนาระบบงานสารสนเทศให้เป็นไปตามมาตรฐานการพัฒนาระบบงานของสำนักงานประกันสังคม ดังนี้

๕.๔.๑) การพัฒนาระบบงาน ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น

๕.๔.๒) ในการพัฒนาระบบงานทุกครั้งจะต้องให้หน่วยงานที่ดูแลรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตรวจสอบความมั่นคงปลอดภัยของระบบสารสนเทศที่พัฒนาขึ้น เพื่อให้มั่นใจว่าตรงกับข้อกำหนดและมีความมั่นคงปลอดภัย

๕.๔.๓) ต้องมีการทดสอบระบบสารสนเทศที่ถูกปรับปรุงหรือพัฒนาขึ้น โดยต้องครอบคลุมความถูกต้องสมบูรณ์ครบถ้วนของข้อมูลที่นำเข้า การประมวลผล และข้อมูลที่ส่งออกให้เป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง (Production Environment) ต้องป้องกันและจำกัดสิทธิให้เฉพาะผู้ที่มีสิทธิเท่านั้น ที่สามารถเข้าถึงชุดคำสั่ง (Source Code) ของโปรแกรมได้ สำหรับบัญชีรายชื่อของผู้พัฒนาที่เป็น Outsource เมื่อส่งมอบงานแล้วจะถูกปิดการใช้งาน (Disable) และจะถูกเปิดการใช้งาน (Enable) เฉพาะกรณีที่มีการทำหนังสือแจ้งเพื่อเข้ามาปรับปรุงแก้ไข

๕.๔.๔) ควรดำเนินการหาข้อมูลของเจ้าของผลิตภัณฑ์เกี่ยวกับช่องโหว่ของโปรแกรมประยุกต์หรือแอปพลิเคชันที่สำนักงานประกันสังคมใช้งานอยู่อย่างสม่ำเสมอ และประเมินความเสี่ยงที่อาจจะเกิดขึ้นถ้าดำเนินปรับปรุง (Update) โปรแกรมประยุกต์หรือแอปพลิเคชัน และในกรณีที่ความเสี่ยงต่ำหรือสามารถยอมรับได้ ควรดำเนินการปรับปรุง (Update) เพื่อปิดช่องโหว่ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชันอย่างสม่ำเสมอ

๕.๔.๕) ต้องมีการควบคุมกรณีที่จ้างบุคคลภายนอกพัฒนาระบบ (Outsource) โดยกำหนดให้มีการแสดงหลักฐานที่สามารถระบุตัวบุคคลได้ การเข้าถึงระบบสารสนเทศต้องได้รับอนุมัติจากผู้มีอำนาจในการอนุมัติเท่านั้น ซอร์สโค้ดและเอกสารที่พัฒนาขึ้นให้เป็นกรรมสิทธิ์ของสำนักงานประกันสังคม และลงนามในข้อตกลงการไม่เปิดเผยข้อมูล

๖. การบริหารจัดการสร้างความต่อเนื่องทางธุรกิจ (Business Continuity Management)

๖.๑) การสร้างความต่อเนื่องทางธุรกิจสำหรับกระบวนการทางธุรกิจสำคัญ

๖.๑.๑) กำหนดกระบวนการทางธุรกิจสำคัญและระบบซึ่งสนับสนุนกระบวนการดังกล่าว

๖.๑.๒) ประเมินผลกระทบกรณีกระบวนการทางธุรกิจสำคัญและ/หรือระบบสนับสนุนเกิดการหยุดชะงักหรือไม่สามารถให้บริการได้ (Business Impact Analysis)

๖.๑.๓) ประเมินความเสี่ยง (Risk Assessment) และกำหนดแผนการลดความเสี่ยงสำหรับกระบวนการทางธุรกิจสำคัญและ/หรือระบบสนับสนุน

๖.๑.๔) จัดทำแผนสร้างความต่อเนื่องทางธุรกิจสำหรับกระบวนการทางธุรกิจสำคัญ

๖.๑.๕) จัดทำแผนกู้คืนระบบสนับสนุน

๖.๑.๖) ให้ความรู้แก่ผู้ที่เกี่ยวข้องทั้งหมด (ซึ่งรวมถึงทีมสร้างความต่อเนื่องทางธุรกิจ ทีมกู้คืนระบบ และผู้ให้บริการภายนอก) และสร้างความตระหนักแก่ผู้ใช้งานเพื่อให้คุ้นเคยกับการสร้างความต่อเนื่องทางธุรกิจ เข้าใจในบทบาทและหน้าที่ความรับผิดชอบของตนเอง รวมทั้งสามารถปฏิบัติได้อย่างถูกต้อง

๖.๑.๗) จัดให้มีการทบทวนและตรวจสอบรายละเอียดของแผนสร้างความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบสนับสนุนโดยผู้ตรวจสอบภายใน เพื่อนำไปสู่การปรับปรุงให้ดียิ่งขึ้น

๖.๑.๘) จัดให้มีการทำแผนการทดสอบ (การสร้างความต่อเนื่องทางธุรกิจและการกู้คืนระบบ) กำหนดสถานการณ์การทดสอบ ดำเนินการทดสอบตามแผนการทดสอบ บันทึกผลการทดสอบ สรุปผลและข้อเสนอแนะและนำเสนอต่อผู้บริหารระดับสูงเพื่อพิจารณาและให้ข้อคิดเห็นในการปรับปรุงตามความจำเป็น

๖.๑.๙) เตรียมการที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับกระบวนการทางธุรกิจสำคัญและการกู้คืนระบบสนับสนุน

๖.๑.๑๐) ทบทวนการดำเนินการในทุกรายการข้างต้นอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๖.๒) การสำรองและทดสอบการกู้คืนข้อมูล

๖.๒.๑) กำหนดระบบทั้งหมดที่มีความสำคัญ

๖.๒.๒) กำหนดผู้รับผิดชอบในการสำรองข้อมูล

๖.๒.๓) กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ ซึ่งอย่างน้อยต้องประกอบด้วย

๖.๒.๓.๑) ข้อมูลค่าคอนฟิกกูเรชัน (Configuration) สำหรับระบบ

๖.๒.๓.๒) ข้อมูลคู่มือการปฏิบัติงานสำหรับระบบ

๖.๒.๓.๓) ข้อมูลในฐานข้อมูลของระบบงาน (กรณีที่เป็นระบบงาน)

๖.๒.๓.๔) ข้อมูลซอฟต์แวร์ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงานและซอฟต์แวร์อื่นๆ เป็นต้น

๖.๒.๔) กำหนดความถี่ในการสำรองข้อมูลสำหรับระบบเหล่านั้น (ระบบที่มีการเปลี่ยนแปลงข้อมูลบ่อยควรมีความถี่ในการสำรองข้อมูลสูง)

๖.๒.๕) ทำการทดสอบกู้คืนข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ (ปีละ ๑ ครั้ง) เพื่อดูว่าข้อมูลยังคงสามารถใช้งานได้ตามปกติหรือไม่

๖.๒.๖) จัดทำหรือปรับปรุงขั้นตอนปฏิบัติในการสำรองและกู้คืนข้อมูล โดยให้มีการปฏิบัติตามแนวทางปฏิบัติ สำหรับการสำรองและทดสอบกู้คืนข้อมูล

๗. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๗.๑) ผู้ดูแลระบบ ต้องควบคุมหน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายเข้ามาในพื้นที่ศูนย์คอมพิวเตอร์ โดยจะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์และต้องมีผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมายลงนาม

๗.๒) ผู้ดูแลระบบ ต้องควบคุมการเข้าออกศูนย์คอมพิวเตอร์ของผู้ใช้งาน และบุคคลภายนอก โดยต้องกำหนดให้มีการเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ และบันทึกการเข้าออกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาผ่านเข้าออก และมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมออย่างน้อยเดือนละ ๑ ครั้ง

๗.๓) สำนักงานประกันสังคม ต้องกำหนดพื้นที่การส่งมอบสินค้า และพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าศูนย์คอมพิวเตอร์ เพื่อหลีกเลี่ยงการใช้งานพื้นที่ในศูนย์คอมพิวเตอร์โดยไม่ได้รับอนุญาต

๗.๔) สำนักงานประกันสังคม ต้องจัดหา ติดตั้ง และบำรุงรักษา อุปกรณ์หรือระบบสนับสนุนในการรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ เช่น อุปกรณ์ดับเพลิง อุปกรณ์สำรองไฟฟ้า ระบบควบคุมอุณหภูมิและความชื้น ระบบเตือนภัยน้ำรั่ว หรือระบบแจ้งเตือนเมื่ออุปกรณ์สารสนเทศทำงานผิดปกติ เป็นต้น

๗.๕) สำนักงานประกันสังคม ต้องควบคุม ตรวจสอบการติดตั้งและใช้งานระบบ อุปกรณ์และสายสัญญาณต่างๆ ในศูนย์คอมพิวเตอร์ ให้มีความปลอดภัยและสามารถทำงานได้อย่างต่อเนื่อง

๗.๖) สำนักงานประกันสังคม ต้องควบคุม การออกแบบและติดตั้งศูนย์คอมพิวเตอร์ โดยคำนึงถึงการป้องกันความมั่นคงปลอดภัยทางด้านกายภาพ ทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ

๘. การแลกเปลี่ยนสารสนเทศ

๘.๑) เจ้าของข้อมูล ต้องทำการตรวจสอบประเภทของข้อมูลสารสนเทศ และลำดับชั้นความลับของข้อมูลสารสนเทศที่จะดำเนินการแลกเปลี่ยนกับหน่วยงานอื่นตามที่ได้กำหนดไว้ เพื่อควบคุมการแลกเปลี่ยนสารสนเทศให้เหมาะสม และป้องกันข้อมูลสำคัญจากการถูกเข้าถึง การเปลี่ยนแปลงแก้ไข การสำเนา และการทำลายโดยไม่ได้รับอนุญาต รวมทั้งการแจกจ่ายหรือส่งผิดตัวผู้รับ

๘.๒) ผู้ดูแลระบบ ต้องควบคุมให้มีการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางที่ปลอดภัย ทั้งการแลกเปลี่ยนสื่อบันทึกข้อมูลทางกายภาพ และการแลกเปลี่ยนข้อมูลสารสนเทศผ่านระบบเครือข่าย โดยหากเป็นการแลกเปลี่ยนข้อมูลสารสนเทศผ่านระบบเครือข่าย ต้องให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมระหว่างการสื่อสารแลกเปลี่ยน เช่น การทำพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce) หรือการทำธุรกรรมทางออนไลน์ (Online Transaction) เพื่อไม่ให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือมีการรั่วไหลของข้อมูล หรือมีการแก้ไขข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๙. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ของผู้ดูแลระบบ

๙.๑) ผู้ดูแลระบบ ต้องจัดทำและปรับปรุงคู่มือการปฏิบัติงานให้ทันสมัยอยู่เสมอ และจัดเก็บคู่มือการปฏิบัติงานไว้ในสถานที่ที่มีความปลอดภัย

๙.๒) ผู้ดูแลระบบ ต้องการตรวจสอบข้อมูลความรู้ที่เกี่ยวข้องกับผลิตภัณฑ์ที่องค์กรใช้งานและความรู้ที่เกี่ยวกับความมั่นคงปลอดภัย โดยปฏิบัติดังนี้

๙.๒.๑) จัดเตรียมข้อมูลรายชื่อบุคคลและข้อมูลการติดต่อ เพื่อใช้ในการติดต่อระหว่างกันสำหรับเจ้าหน้าที่ทั้งภาครัฐและเอกชน ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และผู้ให้บริการภายนอกที่เกี่ยวข้อง

๙.๒.๒) ติดตาม ปรับปรุงข้อมูล แจ้งเวียนรายชื่อและช่องทางการติดต่อสื่อสาร เพื่อให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบ

๙.๓) ผู้ดูแลระบบ ต้องกำหนดความต้องการและวางแผนด้านขีดความสามารถของระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้รองรับความต้องการในอนาคต รวมทั้งมีการเฝ้าระวังและติดตามทรัพยากรของระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างต่อเนื่องเพื่อให้มีสภาพความพร้อมใช้งาน และประสิทธิภาพที่มีเพียงพอต่อการให้บริการ รวมถึงต้องจัดทำรายงานเพื่อนำเสนอผู้ที่เกี่ยวข้องอย่างสม่ำเสมอ

๙.๔) ผู้ดูแลระบบ ควบคุมให้มีการบันทึกการทำงาน (Log) ของระบบ ได้แก่ การทำงานของระบบคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย (Activity Log) การใช้งานระบบสารสนเทศของผู้ใช้งาน

(Application Log) และบันทึกการทำงานอื่นๆที่เป็นกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศและเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่างๆ เช่นการเข้าถึง (Access Log) โดยรายละเอียดการจัดเก็บบันทึก ต้องสอดคล้องกับข้อกำหนดในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ รวมทั้งป้องกันการแก้ไขเปลี่ยนแปลงบันทึก และจำกัดสิทธิ์การเข้าถึงบันทึก เพื่อป้องกันการเข้าถึง หรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต นอกจากนี้ ผู้ดูแลระบบ ต้องดำเนินการตรวจสอบวิเคราะห์บันทึกอย่างสม่ำเสมอ และดำเนินการจัดการและแก้ไขเหตุการณ์ที่พบตามความเหมาะสม

๙.๕) ผู้ดูแลระบบ ต้องตั้งค่าระบบเวลาของระบบคอมพิวเตอร์และระบบเครือข่ายที่ใช้ในสำนักงาน หรือในขอบเขตที่สำนักงานจะต้องรับผิดชอบดูแลด้านความมั่นคงปลอดภัยสารสนเทศ โดยต้องกำหนดให้มีความสอดคล้องกันของเวลา (Time Synchronization) โดยให้มีการตั้งค่าจากแหล่งเวลาที่เชื่อถือได้

๙.๖) ผู้ดูแลระบบ ต้องตรวจสอบและจัดหาทรัพยากรที่ใช้สำหรับการประมวลผลสารสนเทศอย่างเพียงพอ โดยจะต้องมีการออกแบบโครงสร้างหรือองค์ประกอบให้มีการรองรับในกรณีที่ทรัพยากรหลักไม่สามารถให้บริการได้ เพื่อให้เป็นไปตามข้อกำหนดด้านความพร้อมใช้ของระบบสารสนเทศ

๑๐. การควบคุมการใช้งานอุปกรณ์พกพา

๑๐.๑) สำนักงานประกันสังคม ต้องจัดทำแนวทางปฏิบัติสำหรับการใช้งานอุปกรณ์พกพา ในกรณีที่เจ้าหน้าที่นำอุปกรณ์พกพาส่วนตัวมาใช้ในสำนักงานเพื่อเชื่อมต่อ ประมวลผล หรือจัดเก็บข้อมูลของสำนักงาน จัดเก็บล็อกการเข้าถึงระบบเครือข่ายและระบบงานสารสนเทศ และทำการตรวจสอบการเข้าถึงอย่างสม่ำเสมอ

๑๑. การเข้ารหัสข้อมูล

๑๑.๑) ผู้ดูแลระบบ ต้องกำหนดให้มีการจัดประเภทของข้อมูลสารสนเทศและการสื่อสารที่จะต้องได้รับการเข้ารหัส

๑๑.๒) ผู้ดูแลระบบ ต้องกำหนดให้มีการใช้โปรแกรมที่มีความสามารถในการเข้ารหัสข้อมูล เพื่อให้บุคลากรใช้เป็นมาตรฐานเดียวกัน โดยโปรแกรมจะต้องทำหน้าที่ในการเข้ารหัสข้อมูลอย่างเหมาะสม เมื่อมีการเชื่อมต่อผ่านระบบเครือข่ายภายในและจากภายนอกสำนักงานประกันสังคมไปยังเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายต่างๆ ของประกันสังคม

๑๑.๓) ผู้ดูแลระบบ ต้องกำหนดให้มีแนวทางการบริหารจัดการกุญแจ (Key) ที่ใช้เข้ารหัสข้อมูล โดยให้มีการควบคุม กำกับ ติดตาม ให้ครอบคลุมตลอดทั้งวงจรในการนำกุญแจรหัสลับ ไปใช้งาน ได้แก่ การสร้างกุญแจรหัสลับ การจัดเก็บและดูแลรักษากุญแจรหัสลับ การนำกุญแจรหัสลับไปใช้ การกำหนดอายุของกุญแจรหัสลับ ตลอดจนการทำลายกุญแจรหัสลับเมื่อไม่ได้ใช้งาน

๑๒. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์

๑๒.๑) สำนักงานประกันสังคม ต้องจัดทำขั้นตอนปฏิบัติงานสำหรับการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศและระบบเครือข่าย อย่างเป็นลายลักษณ์อักษร รวมทั้งกำหนดเกณฑ์การประเมินผลกระทบทั้งในแง่ของการดำเนินงานของระบบสารสนเทศ และความมั่นคงปลอดภัยสารสนเทศ

๑๒.๒) สำนักงานประกันสังคม ต้องกำหนดผู้รับผิดชอบที่ทำหน้าที่ประเมินผลกระทบ ขออนุมัติ บันทึก และติดตามผลการเปลี่ยนแปลง รวมทั้งกำหนดผู้มีสิทธิอนุมัติ โดยให้พิจารณาจากระดับผลกระทบของแต่ละการเปลี่ยนแปลง

๑๒.๓) ผู้ดูแลระบบ และผู้พัฒนาระบบ ต้องจัดทำแผนเพื่อใช้ในการดำเนินการเปลี่ยนแปลง และแผนถอยกลับ (Fallback Plan) เพื่อใช้ในกรณีที่การดำเนินการเปลี่ยนแปลงไม่สำเร็จ รวมทั้งต้องทดสอบระบบหลังการเปลี่ยนแปลง โดยให้บุคลากรที่เกี่ยวข้องกับการใช้งานระบบมีส่วนร่วมในการทดสอบ

๑๓. การพัฒนาระบบให้มีความมั่นคงปลอดภัย

๑๓.๑) สำนักงานประกันสังคม ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศในการบริหารจัดการของโครงการที่เกี่ยวข้องกับงานด้านสารสนเทศ ลงในข้อตกลงหรือสัญญาทั้งโครงการที่เป็นโครงการภายในและโครงการที่จัดซื้อจัดจ้างผู้ให้บริการภายนอกเป็นผู้ดำเนินการ

๑๓.๒) ผู้พัฒนาระบบ ต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบ ดังต่อไปนี้

๑๓.๒.๑) การให้สิทธิต่ำที่สุด (Least Privilege) แก่บุคลากรผู้เข้ามาใช้งานระบบ เพื่อป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต

๑๓.๒.๒) การให้สิทธิเฉพาะที่จำเป็นในการปฏิบัติงาน (Need to Know) แก่บุคลากรผู้เข้ามาใช้งานระบบ เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ

๑๓.๒.๓) การออกแบบระบบให้สามารถป้องกันได้หลายระดับชั้น (Defense in-depth) เพื่อลดความเสี่ยงของการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑๓.๒.๔) การออกแบบในลักษณะเปิด (Open Design) เพื่อให้การพัฒนาระบบมีการใช้กลไกหรืออัลกอริทึม (Algorithm) ที่เป็นมาตรฐานและสามารถตรวจสอบการทำงานได้

๑๔. การบริหารอุบัติการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

๑๔.๑) สำนักงานประกันสังคม ต้องกำหนดขั้นตอนปฏิบัติสำหรับการรายงานเหตุการณ์ความมั่นคงปลอดภัย กำหนดหน่วยงานที่ทำหน้าที่ในการรับแจ้งเหตุการณ์ความมั่นคงปลอดภัย และกำหนดขั้นตอนการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น

๑๔.๒) ผู้ดูแลระบบ ต้องจัดทำบัญชีของระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ กำหนดผู้ที่มีหน้าที่รับผิดชอบ และกำหนดให้มีการจัดการกับช่องโหว่อย่างเหมาะสม

๑๔.๓) ผู้ดูแลระบบ ต้องดำเนินการแก้ไขช่องโหว่ที่มีระดับความสำคัญสูงหรือหามาตรการที่เหมาะสมเพื่อลดความเสี่ยงสำหรับช่องโหว่ที่พบ จัดลำดับความสำคัญเพื่อดำเนินการแก้ไขช่องโหว่ของระบบที่มีความเสี่ยงสูงก่อนระบบที่มีความเสี่ยงต่ำ และดำเนินการทดสอบโปรแกรมแก้ไขช่องโหว่ก่อนที่จะดำเนินการติดตั้งเพื่อป้องกัน

๑๔.๔) ผู้ดูแลระบบ ต้องดำเนินการควบคุมความปลอดภัยของข้อมูลสารสนเทศ ได้แก่ การติดตั้งโปรแกรมที่ใช้ซ่อมแซมจุดบกพร่องหรือปรับปรุงโปรแกรมคอมพิวเตอร์ (Patch) การติดตั้งโปรแกรมเพื่อป้องกันโปรแกรมไม่ประสงค์ดี เช่น ไวรัสคอมพิวเตอร์ ไม่ให้แพร่กระจายในระบบที่ให้บริการ เป็นต้น และควรจัดทำคู่มือในการป้องกันไวรัสให้แก่บุคลากรผู้ใช้งานระบบคอมพิวเตอร์เพื่อใช้เป็นแนวทางปฏิบัติ รวมทั้งแจ้ง และให้ความรู้แก่ผู้ใช้งานเกี่ยวกับไวรัสชนิดใหม่ๆ อย่างสม่ำเสมอ