สำนักงานการบินพลเรือนแห่งประเทศไทย
The Civil Aviation Authority of Thailand

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) และแนวปฏิบัติที่เกี่ยวข้อง

อนุมัติโดย

นายสุทธิพงษ์ คงพูล
ผู้อำนวยการสำนักงานการบินพลเรือนแห่งประเทศไทย
วันที่อนุมัติใช้: 13 พฤษภาคม 2567

0. สารบัญ

0.1 รายละเอียดการปรับปรุงเอกสาร

เวอร์ชัน	วันที่มีผลบังคับใช้	รายละเอียด
1.0	23 มิถุนายน 2565	เอกสารฉบับแรก
2.0	13 พฤษภาคม 2567	ปรับปรุงเนื้อหาให้สอดคล้องตามข้อกำหนด ISO27001:2022

1. วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ สำนักงานจึงเห็นสมควรกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนการปฏิบัติ (Procedure) วิธีการปฏิบัติ (Work Instruction) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังนี้

1. เพื่อให้สำนักงานมีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยมีความสอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง
2. เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอ้างอิงตามนโยบายมาตรฐานที่สำนักงานปรับใช้ และนโยบายอื่นๆที่เกี่ยวข้อง
3. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้คณะกรรมการ ผู้อำนวยการ รองผู้อำนวยการ ผู้จัดการฝ่าย พนักงาน ลูกจ้าง ผู้ดูแลระบบและบุคลากรภายนอกที่ปฏิบัติงานให้สำนักงานตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและปฏิบัติตามอย่างเคร่งครัด
4. เพื่อใช้เป็นหลักในการพัฒนาและปรับปรุงคุณภาพด้านความมั่นคงปลอดภัยสารสนเทศของสำนักงาน

2. ขอบเขต

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) และแนวปฏิบัติที่เกี่ยวข้องฉบับนี้มีผลบังคับใช้กับระบบสารสนเทศของสำนักงาน ผู้ทำหน้าที่ดูแล สินทรัพย์ ผู้ใช้สินทรัพย์ คณะกรรมการ ผู้อำนวยการ รองผู้อำนวยการ ผู้จัดการฝ่าย พนักงาน และลูกจ้าง โดยมีหน้าที่สนับสนุนดำเนินการและปฏิบัติตามนโยบายอย่างเคร่งครัด ผู้ใช้งานอื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลสินทรัพย์จะต้องให้ความร่วมมือในการดำเนินการตามนโยบายนี้ ผู้ฝ่าฝืนนโยบายนี้จะมีความผิดและต้องได้รับการดำเนินการตามระเบียบของสำนักงาน

นโยบายนี้จะต้องทำการเผยแพร่โดยการประกาศเวียนในระบบ Intranet จดหมายอิเล็กทรอนิกส์ (e-mail) และเว็บไซต์ของสำนักงาน เพื่อให้พนักงานทุกระดับในสำนักงานได้รับทราบ และพนักงานทุกคนจะต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด นโยบายนี้ต้องถูกทบทวนอย่างสม่ำเสมอหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

3. คำนิยาม

คำศัพท์	ความหมาย
การเข้าถึง	การเข้าสถานที่ การใช้งานทางอิเล็กทรอนิกส์หรือกายภาพ รวมถึงการรับรู้ซึ่งข้อมูล
การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	การตรวจสอบ การอนุมัติ และการกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ การเพิกถอนหรือการยกเลิกสิทธิการเข้าถึง
การควบคุมการเข้าถึง	การอนุญาต การกำหนดสิทธิ การเปลี่ยนแปลง การเพิกถอนหรือการยกเลิกสิทธิการเข้าถึง
การจัดการทรัพยากรระบบ (Capacity Management)	การบริหารจัดการทรัพยากรและการกำหนดค่าขีดความสามารถของเจ้าหน้าที่ แผนการดำเนินงาน และอื่น ๆ
การบริหารจัดการการเปลี่ยนแปลง (Change Management)	กระบวนการควบคุมการเปลี่ยนแปลงระบบสารสนเทศ ซึ่งการเปลี่ยนแปลงดังกล่าวจะมีผลกระทบต่อฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ระบบ (System Software) ซอฟต์แวร์ประยุกต์ (Application Software) และระบบเครือข่าย (Network System) เป็นต้น
การประเมินความเสี่ยง	กระบวนการทั้งหมดในการวิเคราะห์และประเมินความเสี่ยง
ข้อมูลจำกัด (Restricted)	ข้อมูลข่าวสารที่ถูกจำกัดทั้งหมดหรือบางส่วนสามารถเปิดเผยได้เฉพาะกลุ่มที่เกี่ยวข้องเท่านั้น
ข้อมูลลับ (Confidential)	ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ ซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอก เว้นแต่จะได้รับการอนุญาตจากเจ้าของข้อมูล หรือการเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
ข้อมูลลับมาก (Secret)	ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง ซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอก เว้นแต่จะได้รับการอนุญาตจากเจ้าของข้อมูล หรือการเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
ข้อมูลลับที่สุด (Top Secret)	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด ซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอก เว้นแต่จะได้รับการอนุญาตจากเจ้าของข้อมูล หรือการเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง

คำศัพท์	ความหมาย
ข้อมูลทางการ (Official)	ข้อมูลที่มีการจัดทำภายในสำนักงาน แบ่งออกเป็น 2 ระดับชั้น ดังนี้ ● Internal - ข้อมูลที่ใช้เฉพาะภายในสำนักงานเท่านั้น ● Public - ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่แก่สาธารณะได้
ข้อมูล (Data)	สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ไม่ว่าการสื่อความหมายนั้นจะทำได้ โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของซีดี (CD) ดีวีดี (DVD) Hard Disk Thumb drive เอกสาร แฟ้ม รายงาน หนังสือ แผนที่ แผนผัง ภาพวาด ภาพถ่าย การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)	การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
ความต่อเนื่องในการดำเนินงานของสำนักงาน (Business Continuity Management : BCM)	แนวทางในการบริหารจัดการธุรกิจได้อย่างต่อเนื่อง เมื่อสำนักงานอยู่ภายใต้สภาวะวิกฤตและเหตุฉุกเฉินต่าง ๆ ทำให้มั่นใจได้ว่า ขั้นตอนการดำเนินงานและระบบสารสนเทศต่าง ๆ ของสำนักงานที่สำคัญ ได้รับการวางแผนความต่อเนื่องในการดำเนินงานของสำนักงาน (Business Continuity Plan หรือ BCP) และแผนสำรองฉุกเฉิน (Disaster Recovery Plan หรือ DRP) อย่างเหมาะสม
คลาวด์คอมพิวติ้ง (Cloud Computing)	บริการที่ครอบคลุมถึงการประมวลผล หน่วยจัดเก็บข้อมูล และระบบออนไลน์ต่างๆจากผู้ให้บริการคลาวด์ ซึ่งครอบคลุมการใช้บริการประเภท Cloud Infrastructure as a Service (IaaS) Platform as a Service (PaaS) และ Software as a Service (SaaS)
เจ้าของข้อมูล (Information Owner)	ผู้ซึ่งรับผิดชอบข้อมูลของสำนักงานซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยเจ้าของข้อมูลเป็นผู้ที่รับผิดชอบข้อมูลนั้น ๆ หรือเป็นผู้ได้รับผลกระทบโดยตรง หากข้อมูลเหล่านั้นเกิดสูญหาย
เจ้าของระบบงาน (System Owner)	ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ในสำนักงาน
นิสิตและนักศึกษาฝึกงาน	นิสิตและนักศึกษาที่สำนักงานอนุญาตให้เข้ามาทดลองปฏิบัติงาน โดยมีช่วงระยะเวลาที่กำหนดไว้
โปรแกรมประยุกต์ หรือแอปพลิเคชัน (Application)	โปรแกรมประเภทหนึ่งที่ถูกสร้างขึ้นสำหรับใช้งานเฉพาะทาง ได้แก่ ระบบ eHRM ระบบ Intranet ระบบ e-DOC ระบบ e-Service ระบบ e-Saraban เป็นต้น

คำศัพท์	ความหมาย
แผนการจัดการทรัพยากรระบบ (Capacity Plan)	แผนการจัดการทรัพยากรระบบของบริการในการติดตามสถานะปัจจุบันของทรัพยากรที่ใช้งาน และวางแผนทรัพยากรสำหรับอนาคตอย่างเพียงพอ
พนักงาน	บุคคลผู้ที่สำนักงานบรรจุและแต่งตั้งเป็นพนักงาน
ผู้จัดการฝ่าย	ผู้จัดการฝ่าย/สำนัก ตามโครงสร้างของสำนักงานการบินพลเรือนแห่งประเทศไทย
ผู้ใช้งาน (User)	คณะกรรมการ ผู้อำนวยการ รองผู้อำนวยการ ผู้จัดการฝ่าย พนักงาน ลูกจ้าง บุคคลที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามาใช้งาน บริหารหรือดูแลรักษาระบบสารสนเทศของสำนักงานตามสิทธิและหน้าที่ความรับผิดชอบ
ผู้ให้บริการ	ผู้ให้บริการคลาวด์คอมพิวติ้ง (Cloud Computing)
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง(Chief Information Officer : CIO)	รองผู้อำนวยการสำนักงานการบินพลเรือนแห่งประเทศไทยที่ได้รับมอบหมายให้ทำหน้าที่ผู้บริหาร
คณะกรรมการ	คณะกรรมการกำกับสำนักงานการบินพลเรือนแห่งประเทศไทย
ผู้อำนวยการ	ผู้อำนวยการสำนักงานการบินพลเรือนแห่งประเทศไทย
พื้นที่ใช้งานระบบสารสนเทศ (Information System Workspaces)	พื้นที่ที่สำนักงานอนุญาตให้มีการใช้งานระบบสารสนเทศ โดยแบ่งเป็น - พื้นที่มั่นคงปลอดภัย (Secure Area) คือ พื้นที่ที่มีการควบคุมการเข้าถึงและมีระบบการป้องกันจากภัยคุกคามต่าง ๆ - พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator / Operator Area) คือ พื้นที่สำหรับพนักงานดูแลระบบใช้ในการปฏิบัติงานในการดูแลระบบสารสนเทศของสำนักงาน - ห้องปฏิบัติงานทั่วไป (Working Area) ห้องประชุม เช่น พื้นที่ปฏิบัติงานทั่วไปของพนักงาน - พื้นที่ทั่วไป (General Area) คือ พื้นที่สำหรับใช้รับรองบุคคลที่มาติดต่อสำนักงาน
ระบบเครือข่าย (Network System)	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือส่งข้อมูลระหว่าง ระบบคอมพิวเตอร์ ได้แก่ ระบบ LAN (Local Area Network) ระบบ WLAN (Wireless LAN) ระบบ Intranet และระบบ Internet เป็นต้น
ระบบเครือข่ายไร้สาย (Wireless LAN : WLAN)	ระบบเครือข่ายที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ รวมถึง การติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่าย โดยปราศจากการใช้สายสัญญาณในการเชื่อมต่อ แต่จะใช้คลื่นวิทยุเป็นช่องทางการสื่อสารแทน
ระบบสารสนเทศ (Information System)	ระบบงานที่นำเทคโนโลยีมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งประกอบด้วยเทคโนโลยีคอมพิวเตอร์และ

คำศัพท์	ความหมาย
	เทคโนโลยีการสื่อสารโทรคมนาคม ได้แก่ ระบบคอมพิวเตอร์ (Computer System) ระบบเครือข่าย (Network System) ซอฟต์แวร์ (Software) ข้อมูล (Data) และสารสนเทศ (Information) เป็นต้น
ระบบ Intranet	เป็นระบบเครือข่ายที่สามารถเข้าถึงได้โดยผู้ใช้งานภายในสำนักงานเท่านั้น โดยมีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในสำนักงาน
ระบบ Internet	ระบบเครือข่ายที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ของสำนักงานเข้ากับระบบคอมพิวเตอร์ทั่วโลก
ระบบ LAN	ระบบเครือข่ายแบบเชื่อมต่อคอมพิวเตอร์เข้าด้วยกันในระยะจำกัด เช่น ในอาคารเดียวกัน หรือบริเวณเดียวกันที่สามารถลากสายถึงกันได้โดยตรง
ลูกจ้าง	บุคคลผู้ที่สำนักงานบรรจุและแต่งตั้งเป็นลูกจ้าง โดยมีสัญญาจ้างให้ปฏิบัติงานเป็นการชั่วคราวและมีกำหนดระยะเวลาและสิ้นสุดที่แน่นอน
สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)	สถานการณ์ซึ่งมีแนวโน้มทำให้ระบบของสำนักงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
สารสนเทศ (Information)	ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
สำนักงาน	สำนักงานการบินพลเรือนแห่งประเทศไทย
สิทธิของผู้ใช้งาน	สิทธิและหน้าที่ตามบทบาท (Role) ที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน มีดังนี้ - สิทธิใช้งานทั่วไป หมายถึง คณะกรรมการ ผู้อำนวยการ รองผู้อำนวยการ ผู้จัดการฝ่าย พนักงาน ลูกจ้าง บุคคลที่ใช้งานระบบสารสนเทศพื้นฐานของสำนักงาน ผู้ใช้งานต้องขออนุญาตจากผู้จัดการฝ่าย โดยให้ใช้แบบฟอร์มเพื่อขออนุมัติตามที่สำนักงานกำหนด - สิทธิพิเศษ หมายถึง สิทธิที่ได้รับมอบหมายเพิ่มเติมจากผู้บังคับบัญชาเป็นกรณีพิเศษ ผู้ใช้งานต้องได้รับมอบหมายจากผู้บังคับบัญชาเป็นครั้งคราว
สื่อสังคมออนไลน์ (Social Media)	สังคมออนไลน์ที่ผู้ใช้อินเทอร์เน็ตสามารถแลกเปลี่ยนประสบการณ์ซึ่งกันและกัน โดยใช้สื่อต่าง ๆ เป็นตัวแทนในการสนทนา โดยได้มีการจัดแบ่งประเภทของ Social Media ออกเป็นหลายประเภท ได้แก่ - ประเภทสื่อสิ่งพิมพ์ (Publish) เช่น Wikipedia, Wordpress, Bloggang, Blogger, OKnation ฯลฯ

คำศัพท์	ความหมาย
	- ประเภทสื่อสนทนาและส่งข้อความ (Discuss/SMS/Instant Messaging) เช่น G-chat, Line, Skype, Facebook Messenger ฯลฯ - ประเภทเครือข่ายสังคมออนไลน์ (Social Network) เช่น Facebook, LinkedIn, Instagram, Twitter ฯลฯ - ประเภทบริการวิดีโอออนไลน์ (Online Video) เช่น YouTube, Flickr, SlideShare, MSN, Yahoo ฯลฯ - ประเภทบริการฝากรูปภาพ (Photo Sharing) เช่น Flickr, Photobucket ฯลฯ
หน่วยงานภายนอก/ ผู้ให้บริการภายนอก/ บุคคลภายนอก	ผู้ให้บริการภายนอก (Third Party) หรือบุคคลภายนอก ที่ใช้งานระบบสารสนเทศของสำนักงาน ได้เป็นครั้งคราวหรือตามสัญญา
เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event)	กรณีที่เกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
อุปกรณ์เคลื่อนที่ (Mobile Device)	อุปกรณ์ประมวลผลแบบพกพา ที่มีขนาดเล็กสามารถใช้เพียงมือเดียวในการใช้งาน ส่วนของการรับข้อมูลเป็นแบบสัมผัส โดยไม่ต้องใช้ Keyboard และสามารถเชื่อมต่อเครือข่ายแบบไร้สาย เครือข่ายโทรศัพท์ได้ เช่น Smartphone, Tablet เป็นต้น
อุปกรณ์ประมวลผล (Computing Device)	อุปกรณ์ที่มีหน่วยประมวลผล หน่วยความจำ ส่วนบันทึกข้อมูล ส่วนการเชื่อมต่อเครือข่าย ส่วนรับข้อมูล และส่วนแสดงผล ได้แก่ - คอมพิวเตอร์แบบตั้งโต๊ะ เช่น Desktop Computer เป็นต้น - คอมพิวเตอร์แบบพกพา เช่น Notebook, Netbook เป็นต้น

4. นโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศ

4.1 นโยบายความมั่นคงปลอดภัย (Security Policy)

<u>วัตถุประสงค์</u>

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) และแนวปฏิบัติที่เกี่ยวข้องฉบับนี้ถูกจัดทำขึ้น เพื่อกำหนดทิศทาง หลักการและกรอบของข้อกำหนดในการป้องกันทรัพย์สินที่เกี่ยวข้องกับสารสนเทศให้ปลอดภัยจากภัยคุกคามที่อาจก่อให้เกิดความเสียหายต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลและระบบงานสารสนเทศ เพื่อผลักดันให้มีการควบคุมภายในด้านสารสนเทศที่รัดกุมตามแนวความเสี่ยง (Risk Based Approach) ที่สอดคล้องกับมาตรฐานสากล และเพื่อสนับสนุนให้ผู้ใช้งานตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศรวมถึงความสำคัญในการบริหารจัดการความเสี่ยงด้านสารสนเทศ

<u>แนวนโยบายและแนวทางปฏิบัติ</u>

4.1.1 ผู้อำนวยการเป็นผู้รับผิดชอบความเสี่ยง ความเสียหายต่อระบบสารสนเทศของสำนักงาน ซึ่งเกิดจากการละเลย ละเว้นการควบคุมความมั่นคงปลอดภัยสารสนเทศ

4.1.2 ผู้อำนวยการต้องให้การสนับสนุนการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) และแนวปฏิบัติที่เกี่ยวข้อง

4.1.3 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) ของสำนักงานต้องจัดให้มีการประเมินความเสี่ยงอย่างสม่ำเสมอหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ โดยการประเมินความเสี่ยงดังกล่าวต้องพิจารณาถึงบริบทภายใน (Internal Context) บริบทภายนอก (External Context) ผู้ที่มีส่วนได้ส่วนเสีย (Interested Party) วิสัยทัศน์ พันธกิจที่สำนักงานกำหนด

4.1.4 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) ของสำนักงานต้องกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้และความเสี่ยงที่ยอมรับไม่ได้ เพื่อใช้เป็นแนวทางในการบริหารจัดการความเสี่ยงที่เกิดขึ้นในการประเมินความเสี่ยงที่เกิดขึ้น

4.1.5 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) ของสำนักงานต้องจัดให้มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) และแนวปฏิบัติที่เกี่ยวข้องอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของบริบทภายใน (Internal Context) บริบทภายนอก (External Context) ผู้ที่มีส่วนได้ส่วนเสีย (Interested Party) วิสัยทัศน์ พันธกิจ และแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยทางด้านสารสนเทศของสำนักงาน

4.1.6 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) ของสำนักงานต้องประเมินผลสัมฤทธิ์ของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) และแนวปฏิบัติที่เกี่ยวข้องที่ประกาศใช้ เพื่อนำมาปรับปรุงแก้ไขแผนกลยุทธ์ให้สอดคล้องกับภัยคุกคามในปัจจุบัน และที่อาจเกิดขึ้นในอนาคต

4.1.7 นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) และแนวปฏิบัติที่เกี่ยวข้องต้องจัดทำเป็นลายลักษณ์อักษรตามวัตถุประสงค์และขอบเขต ต้องได้รับการอนุมัติ เพื่อประกาศใช้และถือปฏิบัติทั่วทั้งสำนักงาน โดยให้มีผลบังคับใช้กับบุคลากรในทุกระดับชั้นของสำนักงาน ตั้งแต่คณะกรรมการ ผู้อำนวยการ รองผู้อำนวยการ ผู้จัดการฝ่าย พนักงาน ลูกจ้าง ผู้ใช้งานอื่น ตลอดจนหน่วยงานหรือบุคคลภายนอก (External Party) ที่เกี่ยวข้องกับการใช้ข้อมูลและสินทรัพย์สารสนเทศของสำนักงาน

4.1.8 ผู้อำนวยการต้องจัดให้มีทรัพยากร ด้านงบประมาณ ทรัพยากรบุคคล การบริหารจัดการเทคโนโลยีที่เพียงพอต่อการบริหารจัดการด้านความมั่นคงปลอดภัย

4.1.9 ผู้อำนวยการต้องสนับสนุนให้มีการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อย ปีละ 1 ครั้ง

4.1.10 การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) และแนวปฏิบัติที่เกี่ยวข้อง จะต้องได้รับการตรวจสอบโดยผู้ตรวจสอบภายในอย่างน้อยปีละ 1 ครั้ง และรายงานผลการตรวจสอบให้ผู้อำนวยการทราบ ทั้งนี้ ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) ของสำนักงาน เป็นผู้รับผิดชอบในการติดตามผลการปรับปรุงหรือแก้ไขปัญหาที่พบจากการตรวจสอบนั้น

4.1.11 ผู้ใช้งานมีสิทธิ์ใช้ระบบสารสนเทศตามอำนาจหน้าที่ที่ได้รับมอบหมาย ภายใต้ข้อกำหนดตามนโยบายและคู่มือการปฏิบัติ หากมีการฝ่าฝืนจนเป็นเหตุให้เกิดความเสียหายแก่สำนักงานหรือบุคคลหนึ่งบุคคลใด สำนักงานจะพิจารณาดำเนินการทางวินัยตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ที่มีผลบังคับใช้ และกฎหมายประกอบอื่น ๆ แก่พนักงานที่ฝ่าฝืนตามความเหมาะสม

4.1.12 สำนักงานสงวนสิทธิ์ในการเข้าตรวจสอบ เก็บหลักฐาน และดำเนินการอันสมควร หากพบว่ามีการละเมิดนโยบายการใช้งาน

ผู้รับผิดชอบ

คณะกรรมการ ผู้อำนวยการ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง รองผู้อำนวยการ ผู้จัดการฝ่าย พนักงาน ลูกจ้าง ผู้ใช้งานอื่น ตลอดจนหน่วยงานหรือบุคคลภายนอก (External Party) ซึ่งเกี่ยวข้องกับการใช้ข้อมูลหรือสินทรัพย์สารสนเทศของสำนักงานตามสิทธิและหน้าที่ความรับผิดชอบ

4.2 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับสำนักงาน (Organization of Information Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม กำกับและติดตามการปฏิบัติหน้าที่ในด้านการรักษาความมั่นคงสารสนเทศสำหรับหน่วยงานต่าง ๆ ภายในสำนักงาน และเพื่อเป็นแนวทางการควบคุมอุปกรณ์ประมวลผลและการปฏิบัติงานจากภายนอก ให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

แนวนโยบายและแนวทางปฏิบัติ

4.2.1 การจัดโครงสร้างภายในองค์กร (Internal Organization)

4.2.1.1 แนวนโยบาย

เพื่อกำหนดบทบาทหน้าที่ และความรับผิดชอบในการใช้ระบบสารสนเทศอย่างเหมาะสมและปลอดภัย

4.2.1.2 แนวทางปฏิบัติ

4.2.1.2.1 การกำหนดบทบาท และหน้าที่ความรับผิดชอบในด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Roles and Responsibilities) ผู้อำนวยการต้องกำหนดรายละเอียดหน้าที่ความรับผิดชอบในด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับพนักงานในหน่วยงาน เป็นลายลักษณ์อักษร และให้เป็นไปตามนโยบายความมั่นคงปลอดภัย ตามข้อ 4.1

4.2.1.2.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (duties allocation)
ผู้จัดการฝ่ายต้องกำหนดรายละเอียดหน้าที่ความรับผิดชอบในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศในหน่วยงานของตนอย่างชัดเจน เพื่อให้มีการสอบทานระหว่างกันได้

4.2.1.3 ผู้รับผิดชอบ
4.2.1.3.1 ผู้อำนวยการ
4.2.1.3.2 ผู้จัดการฝ่าย

4.2.2 นโยบายการควบคุมอุปกรณ์ประมวลผลและการปฏิบัติงานจากภายนอก (Computing Device and Teleworking Policy)
4.2.2.1 แนวนโยบาย
เพื่อรักษาความมั่นคงปลอดภัยสำหรับอุปกรณ์ประมวลผลและการปฏิบัติงานจากภายนอกสำนักงาน
4.2.2.2 แนวทางปฏิบัติ
4.2.2.2.1 อุปกรณ์ประมวลผลและอุปกรณ์เคลื่อนที่ (Computing Device and Mobile Device)
เพื่อเป็นมาตรการในการควบคุมบริหารจัดการความเสี่ยงสำหรับการใช้งานอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของสำนักงาน และของส่วนตัว ต้องปฏิบัติดังนี้

ก) การใช้งานทั่วไปและการดูแลรักษา
- อุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของสำนักงานถือเป็นสินทรัพย์ของสำนักงานโดยใช้เพื่อการดำเนินงานของสำนักงานเท่านั้น
- การคืน หรือส่งซ่อมอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของสำนักงานให้ลบข้อมูลอย่างปลอดภัย ตามระดับความลับของข้อมูลที่อยู่ในอุปกรณ์นั้น
- ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไข Configuration หรือส่วนประกอบของอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของสำนักงานโดยไม่ได้รับอนุญาต
- ไม่ใช้อุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของสำนักงานผิดวัตถุประสงค์ และหลีกเลี่ยงการใช้อุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ในสภาวะแวดล้อมที่มีผลกระทบต่ออุปกรณ์
- หากมีความจำเป็นต้องใช้งานอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ส่วนตัวมาใช้เชื่อมต่อเครือข่ายภายในของสำนักงาน รวมทั้งเข้าถึงระบบงานภายในต้องได้รับการอนุญาตจากผู้บังคับบัญชาและต้องนำอุปกรณ์ส่วนตัวไปขึ้นทะเบียนกับสำนักงาน และต้องปฏิบัติตามขั้นตอนการใช้งานที่สำนักงานกำหนด

ข) ความปลอดภัยทางด้านกายภาพของอุปกรณ์ประมวลผลและอุปกรณ์เสริมของสำนักงาน
- ต้องจัดเก็บในที่ปลอดภัย ไม่วางทิ้งไว้ในที่เสี่ยงต่อการสูญหาย

- ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ในกรณีที่อุปกรณ์ประมวลผลสูญหายหรือเสียหาย ผู้ใช้งานต้องแจ้งฝ่ายบริหารเทคโนโลยีดิจิทัล โดยทันที
- หากผู้ใช้งานพ้นสภาพจากการเป็นผู้ปฏิบัติงานแล้วต้องส่งอุปกรณ์ประมวลผลและอุปกรณ์เสริมทั้งหมดที่เคยได้รับคืนให้สำนักงาน

ค) การบริหารจัดการข้อมูล

ข้อมูลของสำนักงานที่มีชั้นความลับซึ่งถูกจัดเก็บไว้ในอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ทั้งของสำนักงาน และของส่วนตัว ต้องบริหารจัดการตามระดับชั้นความลับของข้อมูลอย่างเคร่งครัด

ง) การบริหารจัดการรหัสผ่าน (Password)

- ผู้ใช้งานต้องปฏิบัติตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy) สำหรับอุปกรณ์ประมวลผล
- ผู้ใช้งานต้องตั้งค่า Password ที่เป็นรหัสที่เดาสุ่มได้ยาก ความยาวอย่างน้อย 8 ตัวเลข หรือใช้วิธีการยืนยันตัวตนก่อนใช้งานเครื่องที่ดีกว่า เช่น PIN, Fingerprint หรือ Face Scan เป็นต้น

จ) การเก็บข้อมูลสำรอง (Backup Data)

ผู้ใช้งานต้องปฏิบัติตามนโยบายการสำรองข้อมูล (Backup Policy)

ฉ) การป้องกันซอฟต์แวร์ที่ไม่พึงประสงค์ (Malware)

- ฝ่ายบริหารเทคโนโลยีดิจิทัล มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของสำนักงาน และผู้ใช้งานต้องรับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับอุปกรณ์ส่วนตัวเอง
- ห้ามผู้ใช้งานทำการปิด ยกเลิก กระทำการใด ๆ ที่อาจส่งผลต่อระบบการป้องกันไวรัสหรือระบบป้องกันมัลแวร์อื่นใด ที่ติดตั้งอยู่บนอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของสำนักงาน
- หากพบว่าโปรแกรมป้องกันไวรัสในอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ ทำงานผิดพลาด หรือไม่ทำงาน หรือสงสัยว่าอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของสำนักงาน ติดมัลแวร์ หรือพบข้อมูลภัยคุกคาม ผู้ใช้งานต้องยุติการเชื่อมต่อเครื่องเข้ากับระบบเครือข่าย และให้แจ้งฝ่ายบริหารเทคโนโลยีดิจิทัลทันที
- ต้องตรวจสอบหาไวรัสจากสื่อบันทึกข้อมูลต่าง ๆ ได้แก่ External Harddisk, Flash Drive ก่อนนำมาใช้งาน
- ต้องตรวจสอบไฟล์ที่แนบมากับ E-mail หรือไฟล์ที่ Download มาจากอินเทอร์เน็ต ด้วยโปรแกรมตรวจสอบไวรัสก่อนใช้งาน
- ไม่ครอบครอง หรือพัฒนาโปรแกรมไวรัส หรือโปรแกรมที่ก่อกวน หรือโปรแกรมที่ส่งผลต่อระบบของสำนักงานหรือองค์กรอื่น ๆ โดยไม่ได้รับอนุญาต

- ไม่ติดตั้ง หรือใช้งานโปรแกรมเพิ่มเติม โดยไม่ได้รับอนุญาตในอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของสำนักงาน และไม่ติดตั้งหรือใช้งานโปรแกรมที่สุ่มเสี่ยงกับการกระทำผิดกฎหมาย และละเมิดลิขสิทธิ์ในอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ส่วนตัว

4.2.2.2.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ก) การควบคุมการเข้าถึงการปฏิบัติงานภายนอกสำนักงาน ในกรณีที่ผู้ให้บริการภายนอก (Third Party) มีการ Remote Desktop เช่น ERP, Support เพื่อปฏิบัติงานชั่วคราว ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Third Party Relationship Policy) โดยควบคุมและตรวจสอบการใช้งาน หรือการเข้าถึงระบบตามสิทธิที่ได้รับอย่างเคร่งครัด

ข) การเชื่อมต่อจากภายนอกสำนักงาน จะต้องมีการดำเนินการที่ได้รับการอนุมัติและเชื่อมต่อผ่านระบบ Virtual Private Network (VPN) ที่สำนักงานจัดหาให้เท่านั้น

ค) สิทธิในการใช้งาน Remote Access เพื่อปฏิบัติงานชั่วคราวเป็นสิทธิที่สำนักงานจะให้เฉพาะผู้ใช้งาน ผู้ให้บริการภายนอกเป็นการชั่วคราวเท่านั้น ไม่สามารถถ่ายโอน กันได้

ง) ผู้ใช้งานจะต้องขออนุมัติจากผู้บังคับบัญชาก่อนเข้ามาใช้งาน Remote Access เข้าสู่ระบบสารสนเทศ ผู้ใช้งานจะต้องระบุวัตถุประสงค์ วิธีการเข้าถึง และขอบข่ายของการเข้าถึงที่แน่ชัด และจะต้องทำการอนุมัติให้เป็นรายครั้ง หรือเป็นช่วงระยะเวลาจำกัดแล้วแต่กรณีและความจำเป็น

จ) สำนักงานมีสิทธิเรียกร้องค่าเสียหายจากผู้ใช้งาน หรือผู้ให้บริการภายนอก หากระบบคอมพิวเตอร์ของสำนักงานได้รับความเสียหาย เช่น การติดไวรัสคอมพิวเตอร์ จงใจหรือประมาทเลินเล่อ หรือไม่มีความรู้ความชำนาญ กระทำหรืองดเว้นการกระทำใดๆ จากการใช้งาน Remote Access ในการปฏิบัติงานชั่วคราว

4.2.2.3 ผู้รับผิดชอบ

4.2.2.3.1 ผู้จัดการฝ่าย

4.2.2.3.2 พนักงานฝ่ายบริหารเทคโนโลยีดิจิทัล

4.2.2.3.3 ผู้ใช้งาน

4.2.2.3.4 ผู้ให้บริการภายนอก

4.3 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับทรัพยากรบุคคล (Human Resource Security Policy)

วัตถุประสงค์

เพื่อให้สำนักงานมีกระบวนการในการคัดเลือกบุคลากร ฝึกอบรมและควบคุมการปฏิบัติงานของบุคลากรในสำนักงานอย่างเหมาะสมตลอดระยะเวลาการจ้างงานและเพื่อให้เข้าใจถึงหน้าที่ความรับผิดชอบของตนในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักงาน

แนวนโยบายและแนวทางปฏิบัติ

4.3.1 ก่อนการจ้างงาน

4.3.1.1 สำนักงานต้องกำหนดหน้าที่ความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในคุณสมบัติของบุคลากรตามหน้าที่งานที่ได้รับมอบหมาย

4.3.1.2 ฝ่ายบริหารทุนมนุษย์ ต้องตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นบุคลากรของสำนักงาน จะต้องมีการตรวจสอบประวัติอาชญากรรม หรืออื่น ๆ ตามเงื่อนไขที่เกี่ยวข้อง

4.3.1.3 การกำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment) ฝ่ายบริหารทุนมนุษย์ ต้องกำหนดเงื่อนไขการจ้างงาน ที่รวมถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของสำนักงาน

4.3.1.5 ฝ่ายบริหารทุนมนุษย์ ต้องเตรียมข้อมูลที่เกี่ยวข้องกับ นโยบายความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน เพื่อให้พนักงานและผู้ใช้งานที่เข้ามาใหม่ได้ศึกษาและลงนามรับทราบ รวมถึงยอมรับสัญญาในการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับตำแหน่งหน้าที่ความรับผิดชอบตามนโยบายเหล่านั้น

4.3.1.6 เพื่อให้การบริหารจัดการ User ID เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด ฝ่ายบริหารทุนมนุษย์ ต้องแจ้งให้หน่วยงานที่รับผิดชอบทราบทันทีเมื่อมีการดำเนินการดังต่อไปนี้

4.3.1.6.1 การว่าจ้างงาน

4.3.1.6.2 การเปลี่ยนแปลงสภาพการว่าจ้างงาน

4.3.1.6.3 การลาออกหรือการสิ้นสุดการเป็นบุคลากรของสำนักงาน

4.3.1.6.4 การโอนย้ายหน่วยงาน

4.3.1.6.5 การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

4.3.1.7 คณะกรรมการ ผู้อำนวยการ รองผู้อำนวยการ ผู้จัดการฝ่าย พนักงาน และลูกจ้างใหม่ทุกคนที่ปฏิบัติงานในสำนักงาน ต้องลงนามรับทราบและยินยอมปฏิบัติตามสัญญาการรักษาข้อมูลที่เป็นความลับของสำนักงาน และเอกสารอื่น ๆ ที่เกี่ยวข้อง ก่อนอนุญาตให้เริ่มงานหรือเข้าถึงและใช้งานข้อมูลสารสนเทศของสำนักงาน

4.3.2 ระหว่างการจ้างงาน

4.3.2.1 การให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยให้แก่เจ้าหน้าที่ (Information Security Education and Training)

4.3.2.1.1 ฝ่ายบริหารเทคโนโลยีดิจิทัลต้องจัดให้มีการสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานอย่างสม่ำเสมอ

4.3.2.1.2 พนักงานใหม่ของสำนักงาน ต้องได้รับการอบรมเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ โดยจัดเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการบันทึกการอบรมและเก็บรวบรวมไว้ในระบบ

4.3.2.1.3 ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบสารสนเทศของสำนักงาน

4.3.2.2 กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary Process)

สำนักงานจัดให้มีมาตรการดำเนินการกับผู้ฝ่าฝืนหรือละเมิดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานที่เป็นความผิดทางวินัยภายใต้ระเบียบ ข้อบังคับของสำนักงาน

4.3.3 การเปลี่ยนตำแหน่งหรือการสิ้นสุดการจ้างงาน

4.3.3.1 ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องดำเนินการเปลี่ยนแปลง/เพิกถอน/ยกเลิก/ระงับสิทธิของผู้ใช้งานที่เกี่ยวกับการใช้งานระบบสารสนเทศเพื่อให้สอดคล้องกับการเปลี่ยนแปลงสถานะของการว่าจ้าง

4.3.3.2 เมื่อสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน ผู้ใช้งานจะต้องคืนสินทรัพย์อันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นของสำนักงาน ได้แก่ อุปกรณ์ระบบสารสนเทศ ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ

4.3.4 ผู้รับผิดชอบ

4.3.4.1 ฝ่ายบริหารทุนมนุษย์

4.3.4.2 ฝ่ายบริหารเทคโนโลยีดิจิทัล

4.3.4.3 ผู้ใช้งาน

4.4 การบริหารจัดการสินทรัพย์ (Asset Management)

<u>วัตถุประสงค์</u>

เพื่อให้มีการระบุสินทรัพย์ของสำนักงานและกำหนดหน้าที่ความรับผิดชอบในการปกป้องสินทรัพย์จากภัยคุกคาม ช่องโหว่ ผู้บุกรุก การถูกขโมย และสิ่งที่สร้างความเสียหายที่อาจเกิดขึ้นอย่างเหมาะสม

<u>แนวนโยบายและแนวทางปฏิบัติ</u>

4.4.1 นโยบายการบริหารจัดการสินทรัพย์ (Asset Management Policy)

4.4.1.1 แนวนโยบาย

เพื่อให้มีการระบุสินทรัพย์ของสำนักงานและกำหนดหน้าที่ความรับผิดชอบในการปกป้องสินทรัพย์อย่างเหมาะสม

4.4.1.2 แนวทางปฏิบัติ

4.4.1.2.1 หน้าที่ความรับผิดชอบต่อสินทรัพย์ (Responsibility for Assets)

ก) กองจัดซื้อและพัสดุจะต้องทำบัญชีสินทรัพย์สำนักงาน ซึ่งรวมถึงบัญชีครุภัณฑ์คอมพิวเตอร์ เพื่อใช้ในการกำหนดมูลค่าสินทรัพย์ โดยระบุ

ผู้เป็นเจ้าของสินทรัพย์แต่ละชนิดตามที่กำหนดไว้ และต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ตามระยะเวลาที่กำหนดอย่างน้อยปีละ 1 ครั้ง

ข) ในกรณีที่มีการใช้ซอฟต์แวร์ที่ใช้เพื่อการดำเนินงานของสำนักงานซึ่งไม่มีค่าลิขสิทธิ์ หากฝ่ายใดมีการใช้งาน ให้ฝ่ายนั้นทำทะเบียนการใช้งานไว้ที่ฝ่ายและให้ส่งสำเนาดังกล่าวให้ฝ่ายบริหารเทคโนโลยีดิจิทัลในการจัดการข้อมูลเพื่อประโยชน์ในการค้นหาติดตามและสำรวจช่องโหว่ที่อาจมีผลกระทบต่อความมั่นคงปลอดภัยในระบบสารสนเทศ

ค) อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ซอฟต์แวร์ หรือระบบงานคอมพิวเตอร์ที่สำนักงานเช่ามาใช้งาน ต้องกำหนดให้มีผู้รับผิดชอบจัดทำบัญชีรายการของอุปกรณ์ ซอฟต์แวร์ หรือระบบงานคอมพิวเตอร์ที่เช่ามาใช้งาน

ง) การใช้งานสินทรัพย์ต้องใช้งานด้วยความระมัดระวัง บำรุงรักษาให้เหมาะสมกับการใช้งาน ตามประกาศสำนักงาน

จ) เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลง พนักงาน ลูกจ้าง หรือหน่วยงานภายนอกที่ใช้สินทรัพย์ของสำนักงานต้องคืนสินทรัพย์ของสำนักงานทั้งหมดที่ตนเองถือครองให้ครบถ้วน รวมถึงการเปลี่ยนแปลง/เพิกถอน/ยกเลิก/ระงับสิทธิของผู้ใช้งานที่เกี่ยวกับการใช้งานระบบสารสนเทศ

ฉ) กำหนดให้มีการติดตามและพิจารณาลบข้อมูลสำคัญ ข้อมูลส่วนบุคคลที่มีการจัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์ หรือสื่อบันทึกข้อมูลใด ๆ ด้วยวิธีการที่มั่นคงปลอดภัยตามระยะเวลาการจัดเก็บข้อมูลที่กำหนด หรือเมื่อไม่มีความจำเป็นต้องใช้งานอีกต่อไปพร้อมทั้งจัดเก็บบันทึกการลบข้อมูลนั้นไว้เป็นหลักฐาน (Information deletion)

ช) กำหนดให้มีมาตรการควบคุมเพื่อป้องกันข้อมูลรั่วไหล สำหรับระบบเครือข่าย และอุปกรณ์ที่ใช้ในการประมวลผล จัดเก็บ และรับส่งข้อมูลสำคัญ (Data leakage prevention)

4.4.1.3 การจัดการสินทรัพย์สารสนเทศ (Handling)

การจัดการสินทรัพย์สารสนเทศ (Handling) ต้องจัดทำ และปฏิบัติตามขั้นตอนในการปฏิบัติการจัดระดับชั้นความลับ การระบุชั้นความลับ และการจัดการกับระบบสารสนเทศ

4.4.1.4 ผู้รับผิดชอบ

4.4.1.4.1 ผู้จัดการฝ่ายบัญชีและการเงิน (กองจัดซื้อและพัสดุ)

4.4.1.4.2 ฝ่ายบริหารเทคโนโลยีดิจิทัล

4.4.1.4.3 ผู้ใช้งาน

4.4.2 นโยบายการจัดชั้นความลับของสารสนเทศ (Information Classification Policy)

4.4.2.1 แนวนโยบาย

เพื่อให้สารสนเทศได้รับการปกป้องที่เหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศนั้น ๆ ที่มีต่อสำนักงาน

4.4.2.2 แนวทางปฏิบัติ

4.4.2.2.1 ชั้นความลับของสารสนเทศ (Classification of Information)

ก) การจัดระดับชั้นความลับต้องพิจารณาถึงข้อกำหนดทางด้านกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหวเพื่อป้องกันมิให้ข้อมูลถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต โดยให้ปฏิบัติอย่างเหมาะสมตามระดับชั้นความลับของข้อมูล

ข) ผู้จัดการฝ่ายต้องกำหนดประเภทของข้อมูล ระดับความสำคัญ ลำดับชั้นความลับของข้อมูล รวมทั้ง ระดับชั้นการเข้าถึง และช่องทางการเข้าถึงเป็นลายลักษณ์อักษรและมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ

ค) แนวทางการแบ่งประเภทของข้อมูล

- ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร และข้อมูลงบประมาณการเงินและบัญชี
- ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลบริการต่าง ๆ
- ข้อมูลสารสนเทศด้านการบินต่าง ๆ

ง) แนวทางการจัดแบ่งระดับชั้นการเข้าถึง

- ลับที่สุด
- ลับมาก
- ลับ
- ข้อมูลจำกัด
- ข้อมูลทางการ แบ่งออกเป็น 2 ประเภท ได้แก่ ข้อมูลใช้ภายใน และข้อมูลสาธารณะ

จ) จัดแบ่งระดับชั้นการเข้าถึง

- การเข้าถึงและการใช้งานข้อมูลแต่ละระดับชั้นความลับต้องสอดคล้องกับขั้นตอนในการปฏิบัติการจัดระดับชั้นความลับ การระบุชั้นความลับ และการจัดการกับระบบสารสนเทศ
- กำหนดให้มีการพิจารณามาตรการปิดบังข้อมูล (Data Masking) สำหรับข้อมูลสำคัญหรือข้อมูลส่วนบุคคล สอดคล้องกับนโยบายการควบคุมการเข้าถึง ความต้องการทางธุรกิจ กฎหมาย และกฎระเบียบที่เกี่ยวข้อง ด้วยการทำเครื่องหมายหรือแทนที่ข้อมูลเพื่อไม่ให้สามารถอ้างถึงข้อมูลตัวตนของบุคคลได้

4.4.2.2.2 การบ่งชี้สารสนเทศ (Labeling of Information)

ต้องมีการจัดทำการบ่งชี้สารสนเทศ มีการสื่อสาร และปฏิบัติตามที่สอดคล้องกับขั้นตอนการปฏิบัติที่สำนักงานกำหนดไว้และให้เหมาะสมกับชั้นความลับที่กำหนดไว้

4.4.2.3 ผู้รับผิดชอบ

4.4.2.3.1 ผู้จัดการฝ่าย

4.4.2.3.2 ฝ่ายบริหารเทคโนโลยีดิจิทัล

4.4.2.3.3 ผู้ใช้งาน

4.4.3 นโยบายการจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media Handling Policy)

4.4.3.1 แนวนโยบาย

เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายสินทรัพย์สารสนเทศโดยไม่ได้รับอนุญาต

4.4.3.2 แนวทางปฏิบัติ

4.4.3.2.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)

ก) ข้อมูลที่มีชั้นความลับ ต้องกำหนดให้มีการทำลายเมื่อไม่มีการใช้งานแล้ว

ข) ในกรณีที่สื่อบันทึกข้อมูลนั้นไม่ได้ถูกนำมาใช้งานแล้ว ก่อนที่จะนำออกไปจากสำนักงาน ต้องมั่นใจว่าข้อมูลที่อยู่ในสื่อดังกล่าวไม่สามารถกู้คืนกลับมาใช้งานได้อีก

ค) สื่อบันทึกข้อมูลทั้งหมดจะต้องถูกจัดเก็บอย่างปลอดภัย อยู่ในสภาพแวดล้อมที่ไม่เป็นอันตรายต่อสื่อบันทึกข้อมูล

ง) ในการจัดเก็บสื่อบันทึกข้อมูลที่สำคัญ ต้องมีการป้องกันการรั่วไหลหรือเปิดเผยข้อมูล

จ) ห้ามไม่ให้นำสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ไปใช้เพื่อกิจการอื่นซึ่งไม่เกี่ยวกับภารกิจของสำนักงาน

4.4.3.2.2 การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

การทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งาน ต้องทำให้ไม่สามารถกู้คืนข้อมูลเดิมกลับมาใช้ได้อีก และให้มีการจัดทำบันทึกการทำลายอย่างเหมาะสมตามขั้นตอนการทำลายสื่อบันทึกข้อมูล

4.4.3.2.3 ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information Handling Procedures)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์ ผู้ใช้งานต้องปฏิบัติตามขั้นตอนในการปฏิบัติการจัดระดับชั้นความลับ การระบุชั้นความลับ และการจัดการกับระบบสารสนเทศ

4.4.3.2.4 การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ (Security of System Documentation)

ก) จัดเก็บอย่างมั่นคงปลอดภัย ตามระดับชั้นความลับของข้อมูล

ข) มีการกำหนดบุคคลที่มีสิทธิเข้าถึงเอกสารระบบสารสนเทศให้น้อยที่สุด หรือเป็นไปตามนโยบายการจัดชั้นความลับของสารสนเทศ (Information Classification Policy)

ค) ไม่จัดเก็บเอกสารระบบสารสนเทศที่มีความสำคัญไว้ในเครือข่ายสาธารณะ หากจำเป็นต้องใช้งานเครือข่ายสาธารณะ จะต้องมีระบบการป้องกันที่เหมาะสม

4.4.3.2.5 การส่งสื่อบันทึกข้อมูลออกไปภายนอกสำนักงาน (Physical Media Transfer) การจัดส่งแต่ละรูปแบบต้องคำนึงถึงความปลอดภัยเป็นสำคัญ และสอดคล้องตามขั้นตอนในการปฏิบัติการจัดระดับชั้นความลับ การระบุชั้นความลับ และการจัดการกับระบบสารสนเทศ

4.4.3.3 ผู้รับผิดชอบ

4.4.3.3.1 เจ้าของระบบงาน

4.4.3.3.2 ฝ่ายบริหารเทคโนโลยีดิจิทัล

4.4.3.3.3 ผู้ดูแลระบบ

4.4.3.3.4 ผู้ใช้งาน

4.5 การควบคุมการเข้าถึง (Access Control)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรได้อย่างถูกต้อง

<u>แนวนโยบายและแนวทางปฏิบัติ</u>

4.5.1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Information System Access Control Policy)

4.5.1.1 แนวนโยบาย

เพื่อให้ผู้รับผิดชอบและผู้ที่มีส่วนเกี่ยวข้องกับการปฏิบัติงาน รับทราบ เข้าใจ และตระหนักถึงความสำคัญของการควบคุมการเข้าถึงข้อมูลและการใช้งานระบบสารสนเทศให้เป็นตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและสามารถปฏิบัติตามแนวทางที่กำหนดอย่างเคร่งครัด ซึ่งจะเป็นทางหนึ่งในการปกป้องข้อมูลและสารสนเทศจากการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต

4.5.1.2 แนวทางปฏิบัติ

ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล หรือผู้ที่มีอำนาจควบคุมดูแล ต้องจัดให้มีคู่มือปฏิบัติงาน (Documented Operating Procedures) โดยมีการดำเนินการอย่างน้อยดังต่อไปนี้

4.5.1.2.1 ผู้ที่เข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงาน เท่านั้น

4.5.1.2.2 ผู้ดูแลระบบต้องมีการจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มเข้าใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

4.5.1.2.3 ผู้ดูแลระบบต้องมีการกำหนดสิทธิการใช้งานและการเข้าถึงตามระดับความสำคัญของผู้ใช้งานซึ่งเห็นชอบ โดยผู้บริหารของหน่วยงานต้นสังกัด

4.5.1.2.4 ผู้ดูแลระบบต้องมีการกำหนดสิทธิในการเข้าใช้งานแก่ผู้ใช้งานให้ตรงตามหน้าที่ความรับผิดชอบ โดยสามารถตรวจสอบสิทธิได้

4.5.1.2.5 การเข้าถึงระบบด้วย VPN ต้องได้รับการอนุญาตและสิทธิการเข้าใช้งานระบบจากผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.5.1.2.6 ผู้ดูแลระบบสามารถควบคุมหรือตัดสิทธิการใช้งานของผู้ใช้งานได้ตามความเหมาะสม หากผู้ใช้งานกระทำการใด ๆ ในทางที่ผิดตามประกาศของสำนักงาน

4.5.1.2.7 ผู้ดูแลระบบต้องจัดทำบัญชีทรัพย์สินจำแนกตามกลุ่มทรัพย์สินของระบบหรือการทำงาน

4.5.1.2.8 ผู้ดูแลระบบต้องกำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

ก) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น อ่านอย่างเดียว สร้างข้อมูล ป้อนข้อมูล แก้ไข อนุมัติ

ข) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

ค) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องได้รับการอนุมัติจากผู้จัดการต้นสังกัด และได้รับการพิจารณาอนุมัติจากผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล หรือผู้ดูแลระบบที่ได้รับมอบหมาย

4.5.1.3 ผู้รับผิดชอบ

4.5.1.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.5.1.3.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

4.5.2 การบริหารจัดการการเข้าถึง (Access Management)

4.5.2.1 แนวนโยบาย

เพื่อควบคุมการเข้าถึงและใช้งานระบบสารสนเทศและการสื่อสารของสำนักงาน ครอบคลุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย ระบบปฏิบัติการ รวมถึงระบบงานหรือโปรแกรมประยุกต์และสารสนเทศ เฉพาะผู้ที่ได้รับอนุญาต โดยมีการควบคุมและจัดการสิทธิการเข้าถึงและใช้งานอย่างเหมาะสม รวมถึงสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิด

จากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

4.5.2.2 แนวทางปฏิบัติ

4.5.2.2.1 การลงทะเบียนใช้งาน (Access Registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติที่เหมาะสม เมื่อมีการอนุญาตให้เข้าถึงระบบ สารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการยกเลิก เพิกถอนการอนุญาตดังกล่าว

4.5.2.2.2 การบริหารจัดการสิทธิ (Access Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิ เพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตาม ความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึงตามความเหมาะสม

4.5.2.2.3 การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูลผู้ละเมิดจะถูกลงโทษตาม พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

4.5.2.2.4 ผู้ใช้มีสิทธิเข้าใช้งานผ่านระบบเครือข่าย ระบบงาน และระบบปฏิบัติการตามที่ผู้ดูแลระบบกำหนด

4.5.2.2.5 ผู้ดูแลระบบต้องมีการควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต และมีการกำหนดเวลาตัดการเชื่อมต่อหรือการจำกัดระยะเวลาการเชื่อมต่อ

4.5.2.2.6 ผู้ดูแลระบบต้องมีการทบทวนสิทธิการเข้าถึง (Review Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึง โดยผู้ดูแลระบบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการปรับเปลี่ยน เช่น การย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ หรือการยกเลิก การจ้าง เป็นต้น

4.5.2.2.7 การกำหนดสิทธิพิเศษควรได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เพื่อมั่นใจได้ว่าไม่มีการได้สิทธิพิเศษกับผู้ใช้งานที่ไม่ได้รับมอบอำนาจ

4.5.2.2.8 การเปลี่ยนแปลงของผู้ได้รับสิทธิพิเศษควรถูกบันทึกเพื่อการทบทวน

4.5.2.3 ผู้รับผิดชอบ

4.5.2.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.5.2.3.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

4.5.3 การกำหนดหน้าที่ความรับผิดชอบ (Responsibilities)

4.5.3.1 แนวนโยบาย

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและ การลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยได้กำหนดหน้าที่ความรับผิดชอบของทุกคนในสำนักงาน

4.5.3.2 แนวทางปฏิบัติ

4.5.3.2.1 การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งาน ในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

4.5.3.2.2 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว ควรกำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

4.5.3.2.3 สร้างให้ทุกคนต้องตระหนักและเอาใจใส่ต่อการป้องกันและดูแลอุปกรณ์คอมพิวเตอร์และเครือข่ายของหน่วยงานตลอดเวลา เพื่อไม่ให้เกิดความเสียหายหรือสูญหาย หรือมีผู้ไม่พึงประสงค์เข้าถึงระบบและอุปกรณ์ต่าง ๆ โดยไม่ได้รับอนุญาต

4.5.3.2.4 ภายหลังการใช้งานเครื่องแม่ข่ายหรือระบบคอมพิวเตอร์เสร็จสิ้น จะต้องทำการ Log Off ทุกครั้งเสมอ

4.5.3.2.5 ติดตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา 10 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

4.5.3.2.6 ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่มีการดูแลชั่วคราว

4.5.3.2.7 ผู้บริหารมอบหมายหน่วยงานผู้รับผิดชอบ หรือแต่งตั้งผู้มีส่วนเกี่ยวข้องในการควบคุมดูแลบริหารทรัพย์สินของหน่วยงานไม่ให้เกิดความเสียหาย หรือสูญหาย หรือถูกบุกรุกข้อมูลสารสนเทศ

4.5.3.2.8 การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน มีข้อปฏิบัติ ดังนี้

ก) ผู้ที่ใช้งานคอมพิวเตอร์และอุปกรณ์ หรือระบบเครือข่าย หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ที่ใช้งานที่ได้รับอนุญาตจากหน่วยงานเท่านั้น

ข) หน่วยงานผู้รับผิดชอบจะต้องจัดหาสถานที่ที่ใช้ในการจัดเก็บเอกสาร สื่อบันทึก ข้อมูล เครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องให้มีความเหมาะสม ไม่ให้ได้รับความเสี่ยง

ค) บุคลากรของสำนักงานทุกคนอนุญาตให้เข้าใช้พื้นที่และอุปกรณ์ต่าง ๆ ได้ตามสิทธิที่หน่วยงานกำหนดเท่านั้น

ง) ต้องตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

จ) ต้องจัดเก็บสื่อการบันทึกเหตุการณ์ไว้ในที่ที่ปลอดภัยและมีการตรวจสอบระบบอย่างสม่ำเสมอ

ฉ) ต้องจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งาน

ช) ต้องตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น ชื่อผู้ใช้งาน และรหัสผ่าน

ซ) ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับ ระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่านระบบ Active Directory (AD)

4.5.3.3 ผู้รับผิดชอบ

4.5.3.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.5.3.3.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

4.5.4 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

4.5.4.1 แนวนโยบาย

เพื่อป้องกันการเข้าถึงระบบเครือข่ายของสำนักงานโดยไม่ได้รับอนุญาต

4.5.4.2 แนวทางปฏิบัติ

4.5.4.2.1 เจ้าของระบบงานต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational Procedures and Responsibilities) ได้แก่

ก) เจ้าของระบบงานต้องจัดทำคู่มือและขั้นตอนการปฏิบัติงานของระบบงานนั้นๆ โดยมีเนื้อหาที่สำคัญเกี่ยวกับการใช้งาน

ข) ในกรณีที่มีการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ ต้องปฏิบัติตามขั้นตอนการบริหารจัดการการเปลี่ยนแปลง

ค) เจ้าของระบบงานต้องกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานของผู้ที่เกี่ยวข้องไว้อย่างชัดเจน

ง) เจ้าของระบบงานต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัยตามขั้นตอนการปฏิบัติการแก้ไขเหตุการณ์ไม่พึงประสงค์

จ) เจ้าของระบบงานต้องแยกเครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบสารสนเทศออกจากเครื่องที่ทำงานจริงหรือเครื่องให้บริการ

ฉ) ผู้ดูแลระบบเครือข่ายต้องรับผิดชอบในการตรวจสอบและดูแลอุปกรณ์ที่เกี่ยวข้องในระบบเครือข่ายทั้งหมด รวมทั้งอุปกรณ์ที่ใช้สำหรับการเข้าถึงระยะไกล (Remote Equipment)

ช) การดำเนินการใด ๆ ภายในระบบเครือข่าย ต้องอยู่ภายในการควบคุมดูแลและการรับผิดชอบของผู้ดูแลระบบเครือข่าย และต้องรายงานต่อผู้บังคับบัญชา เพื่อควบคุมการใช้งานระบบเครือข่ายให้มีประสิทธิภาพสูงสุด และให้มีความสอดคล้องโดยทั่วกัน

4.5.4.2.2 การบริหารจัดการเครือข่าย (Network Management)

ก) อุปกรณ์ที่ทำหน้าที่เชื่อมโยงกับระบบเครือข่าย เพื่อการทำงานภายในสำนักงาน ได้แก่ Router และ Switch มีข้อปฏิบัติ ดังนี้

- อุปกรณ์ที่ทำหน้าที่ขยายการเชื่อมโยงเครือข่าย ต้องปิด Service Port ที่ไม่จำเป็นและการส่งข้อมูลการทำงานของอุปกรณ์เครือข่ายจะต้องไม่ใช้ค่า Default Community, Default Username และ Default Password

- กรณีเชื่อมโยงเครือข่ายโดยพลการแล้วทำให้เกิดความเสียหายกับระบบเครือข่ายจะต้องถูกลงโทษตามที่กำหนดไว้
- ผู้ดูแลระบบเครือข่ายต้องมีแผนดำเนินการบำรุงรักษาและปรับปรุงระบบเครือข่าย เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง
- ผู้ดูแลระบบจะต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่รับหรือส่งผ่านระบบเครือข่าย ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น

ข) อุปกรณ์ที่ทำหน้าที่ Remote Access เพื่อการควบคุมระบบจากระยะไกล ได้แก่ Virtual Private Network (VPN) มีข้อปฏิบัติดังนี้

- ต้องมีการปรับปรุงช่องโหว่อย่างสม่ำเสมอ และสำรองค่า Configuration ของอุปกรณ์ทุกครั้งที่ติดตั้ง หรือมีการเปลี่ยนแปลงหรือตามระยะเวลาที่กำหนด
- เมื่อมีการทดสอบการเข้าใช้งานระบบสารสนเทศระยะไกลเสร็จสิ้นให้ลบบัญชีผู้ใช้งานที่ใช้ในการทดสอบออกจากระบบเพื่อไม่ให้ผู้ไม่มีสิทธิเข้ามาใช้
- ต้องไม่มีการตั้งค่า Default Community, Default Username และ Default Password หรือทำการเปลี่ยนค่าดังกล่าวเพื่อความปลอดภัย

ค) เครื่องแม่ข่ายและอุปกรณ์ที่ติดตั้งเพื่อการทำงานภายในสำนักงาน มีข้อปฏิบัติดังนี้

- ต้องมีการปรับปรุงช่องโหว่อย่างสม่ำเสมอ และต้องมีการสำรองค่า Configuration ของเครื่องแม่ข่ายทุกครั้งที่ติดตั้ง หรือมีการเปลี่ยนแปลงหรือตามระยะเวลาที่กำหนด
- ต้องไม่เปิดเผย OS Version, Service Port, IP Address และ Service Patch Version ให้บุคคลที่ไม่เกี่ยวข้องทราบ
- ออกจากระบบทุกครั้งเมื่อเลิกใช้งาน
- ผู้ดูแลระบบต้องสำรองข้อมูลและระบบปฏิบัติการตามความเหมาะสมและทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง โดยสอดคล้องกับความสำคัญของระบบ
- อุปกรณ์แม่ข่ายและอุปกรณ์เครือข่ายต้องได้รับการตั้งค่าให้มีความมั่นคงปลอดภัยก่อนนำมาติดตั้งบนระบบเครือข่าย เช่น การกำหนดรหัสผ่านสำหรับบัญชีรายชื่อ ซึ่งใช้ในการบริหารจัดการอุปกรณ์ให้มีความแข็งแกร่ง เปิด Service Port เฉพาะที่จำเป็นต้องใช้งานเท่านั้น เป็นต้น รวมทั้ง กำหนด Access Control List ของอุปกรณ์สื่อสารเพื่อลดช่องโหว่ต่าง ๆ อย่างเหมาะสม

ง) กำหนดให้มีวิธีปฏิบัติในการเก็บบันทึก Log และตรวจสอบสิ่งผิดปกติต่าง ๆ ภายในระบบเครือข่าย

จ) การใช้งานเครื่องมือต่าง ๆ (Tools) เพื่อตรวจสอบระบบเครือข่ายต้องกระทำโดยผู้ดูแลระบบเครือข่ายหรืออยู่ภายใต้การควบคุมดูแลของผู้ดูแลระบบเครือข่ายเท่านั้น และต้องได้รับการอนุมัติจากผู้จัดการฝ่ายและ

สำนักที่เกี่ยวข้องก่อนทุกครั้ง โดยจะจำกัดการใช้งานเฉพาะเท่าที่จำเป็นเท่านั้น

ฉ) การใช้งานระบบไฟร์วอล์ (Firewall) และระบบตรวจจับและป้องกันการบุกรุก(IDS/IPS) ต้องดำเนินการ ดังต่อไปนี้

- มีการระบุขอบเขต (Trust Zones) ของเครือข่าย เช่น เครือข่าย Internet, Web Servers, โซนการเชื่อมต่อภายนอก เครือข่ายภายในองค์กร และโซน Remote Access และออกแบบการควบคุมการจราจรด้วยระบบ Firewall ในแต่ละโซน
- มีการระบุการควบคุมระบบ Firewall ในรูปแบบของเอกสาร เพื่อใช้ในกรณีที่มีการเปลี่ยนแปลงหรือเคลื่อนย้ายระบบ
- มีการจัดเก็บ Log File และการจราจรของเครือข่ายเป็นประจำและสม่ำเสมอ
- มีการตรวจจับเหตุการณ์ต่าง ๆ ที่เกิดขึ้นใน Host หรือเครือข่ายข้อมูล

ช) การใช้งานเครือข่าย (Internet Security Policy)

- มีการตรวจสอบสิทธิการใช้งานคอมพิวเตอร์หรือเครือข่าย เช่น หมายเลขเครื่องคอมพิวเตอร์
- มีการบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบพร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย
- มีการจัดเก็บบันทึกเหตุการณ์การเข้าถึงของระบบ
- จัดทำกำหนดการการตรวจสอบระบบ พร้อมทั้งผู้รับผิดชอบเมื่อมีการให้บริการระบบเครือข่าย

4.5.4.2.3 การควบคุมการเข้าถึงระบบเครือข่าย

ก) ผู้ใช้งานทุกคนจะได้รับสิทธิในการเข้าใช้งานระบบต่าง ๆ ต้องดำเนินการขออนุมัติต่อผู้จัดการฝ่ายต้นสังกัดที่เกี่ยวข้องอย่างเหมาะสมทุกครั้ง ทั้งนี้การพิจารณาให้สิทธิในการเข้าถึงระบบจะต้องสอดคล้องตามนโยบายการควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ

ข) ผู้ดูแลระบบเครือข่ายต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียง บริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

ค) การเชื่อมต่อเข้าสู่ระบบเครือข่ายของสำนักงานผ่านระบบเครือข่ายไร้สายต้องได้รับการเข้ารหัสอย่างเหมาะสม

ง) การทบทวนสิทธิการเข้าถึง (Review Access Right) ต้องมีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย หรือสิ้นสุดการจ้าง

จ) สิทธิการเข้าถึงของหน่วยงานภายนอกหรือผู้ให้บริการภายนอก (Third Party) ต้องได้รับการถอดถอนเมื่อสิ้นสุดการดำเนินงาน หมดสัญญา หรือสิ้นสุดข้อตกลงทันที และต้องมีการปรับปรุงให้เป็นปัจจุบัน

4.5.4.2.4 ผู้ใช้งาน VPN ที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) จะต้องมีกระบวนการในการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่าย ของหน่วยงานได้ ดังนี้

ก) ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ทุกครั้ง

ข) การอนุญาตให้ใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ในการเข้าใช้งานต้องขึ้นอยู่กับความจำเป็นของการดำเนินงานและด้านเทคนิค รวมทั้งต้องได้รับความเห็นชอบจากผู้บังคับบัญชา

ค) หากหน่วยงานหรือผู้ปฏิบัติงานที่มีความประสงค์ขอใช้ชื่อผู้ใช้งาน จะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาและฝ่ายบริหารเทคโนโลยีดิจิทัลก่อน โดยจะต้องรับผิดชอบหากเกิดข้อผิดพลาดที่เกิดขึ้นทั้งสิ้น

4.5.4.2.5 การระบุอุปกรณ์บนเครือข่าย (Equipments Identification in Networks) ต้องมีวิธีการ ที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้วิธีการระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

ก) การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของหน่วยงานต้องได้รับอนุญาตจากฝ่ายบริหารเทคโนโลยีดิจิทัล ก่อนจึงจะสามารถดำเนินการได้

ข) ผู้ดูแลระบบเครือข่ายมีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาตและให้สิทธิในการเชื่อมต่อตามที่ฝ่ายบริหารเทคโนโลยีดิจิทัลกำหนดและสามารถระงับสัญญาณการเชื่อมต่อได้เมื่อสิ้นสุดการอนุญาต

ค) จะต้องมีการจำกัดสิทธิการเข้าใช้อุปกรณ์ได้ โดยให้มีการกำหนดวิธีการพิสูจน์ ตัวตนในการเข้าใช้งานอุปกรณ์โดยใช้ Username Password หมายเลข MAC Address เพื่อความปลอดภัยและเหมาะสมในการเข้าถึง

4.5.4.2.6 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

ก) ผู้ดูแลระบบต้องกำหนดการเปิด-ปิดพอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ

ข) ผู้ดูแลระบบต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและการตั้งค่าระบบทั้งทางกายภาพและโดยมีการล๊อกอินเข้ามาใช้งาน

ค) ผู้ให้บริการภายนอกที่เข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่าย หรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

ง) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุมัติจากผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

จ) ติดตั้งอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่า Configuration ไว้ในห้องคอมพิวเตอร์แม่ข่ายที่มีระบบควบคุมการเข้าออก เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

ฉ) ผู้ดูแลระบบต้องบริหารจัดการพอร์ต (Port) ของระบบหรืออุปกรณ์ตามความจำเป็นในการใช้งานอย่างสม่ำเสมอ อย่างน้อยเดือนละ 1 ครั้ง

ช) กำหนดวิธีการป้องกันช่องทางที่ใช้ในการบำรุงรักษาระบบผ่านเครือข่ายและการตรวจสอบและปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

4.5.4.2.7 ทำการแบ่งแยกเครือข่าย (Segregation in Networks) สำหรับกลุ่มผู้ใช้งาน

ก) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งานให้มีความเหมาะสมตามความต้องการควบคุมความปลอดภัย เพื่อควบคุมการเข้าถึงระบบและเครือข่ายสำคัญ ให้มีความมั่นคงปลอดภัยในการติดต่อสื่อสารหรือการส่งผ่านข้อมูล โดยแบ่งออกเป็น 2 เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

ข) กำหนดให้มีการแยกสภาพแวดล้อมสำหรับระบบสำคัญ (Sensitive System Isolation) โดยทำการแยกออกจากระบบอื่น (Segregation in Networks)

ค) กำหนดให้มีการแบ่งแยก และควบคุมเครือข่ายไร้สายกับเครือข่าย LAN ด้วยอุปกรณ์ Firewall เพื่อควบคุมการเข้าถึงที่เหมาะสม

4.5.4.2.8 มีการควบคุมการเชื่อมโยงเครือข่าย (Network Connection Control) ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกัน หรือเชื่อมโยงระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติอย่างน้อย ดังนี้

ก) การจำกัดสิทธิ ความสามารถของผู้ใช้งานในการเชื่อมต่อเข้าสู่เครือข่ายตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตน

ข) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย ผู้ใช้งานห้ามนำอุปกรณ์เครือข่ายมาติดตั้งก่อนได้รับอนุญาต

ค) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต โดยจัดให้มีการใช้งาน Firewall เพื่อควบคุมการเข้าใช้งานข้อมูล แอปพลิเคชัน และ service ต่าง ๆ บนระบบเครือข่ายให้เป็นไปตามที่สำนักงานได้กำหนดไว้เท่านั้น และเพื่อป้องกันการเชื่อมต่อ (Connections) ต่าง ๆ ที่ไม่พึงประสงค์จากภายนอก โดยผู้ดูแลระบบ Firewall มีหน้าที่ในการตรวจสอบ, ดูแล และติดตั้ง Firewall ให้เป็นไปตาม Firewall Rule ที่กำหนดไว้ Firewall Rule ถือเป็นข้อมูลสำคัญซึ่งต้องได้รับการดูแลรักษาอย่างเหมาะสม ทั้งนี้ การดำเนินการเปลี่ยนแปลงใดๆ ต่อ Firewall Rule จะต้องปฏิบัติตามนโยบายการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ

ง) การเข้าใช้งานเชื่อมต่อเครือข่ายต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครือข่ายทุกครั้ง

จ) ควบคุมไม่ให้เปิดเผยข้อมูลระบบเครือข่ายที่สำคัญในการเชื่อมต่อเข้าสู่ระบบ ได้แก่ หมายเลข IP Address Username และ Password เป็นต้น

4.5.4.2.9 มีการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ที่ใช้ในการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลไม่ถูกเปิดเผย ดังนี้

ก) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

ข) ต้องมีการแปลงหมายเลขเครือข่ายเพื่อแยกเครือข่ายย่อย

2.5.4.2.10 การควบคุมการเข้าใช้งานจากระบบภายนอก (Remote Access)

ก) การเข้าสู่ระบบจากภายนอก (Remote Access) สู่ระบบสารสนเทศและเครือข่ายของสำนักงานต้องมีการกำหนดมาตรการรักษาความปลอดภัย

ข) การเข้าสู่ระบบจากภายนอก (Remote Access) ต้องมีการตรวจสอบข้อมูล และพิสูจน์ตัวตนของผู้ใช้งาน โดยรหัสผ่าน หรือวิธีการเข้ารหัส

ค) วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากระยะไกลต้องได้รับการอนุมัติจากผู้จัดการฝ่ายต้นสังกัดและผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล และมีการควบคุมอย่างเข้มงวดก่อนเข้าใช้โดยปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

ง) มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

4.5.4.3 ผู้รับผิดชอบ

4.5.4.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.5.4.3.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

4.5.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operation System Access Control)

4.5.5.1 แนวนโยบาย

เพื่อรักษาความมั่นคงปลอดภัยและป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

4.5.5.2 แนวทางปฏิบัติ

4.5.5.2.1 การควบคุมการเข้าถึงระบบปฏิบัติการของสำนักงาน

ก) ผู้ดูแลระบบ (System Administrator) ต้องจัดการให้เครื่องคอมพิวเตอร์ของผู้ใช้งานทั่วไปทุกเครื่องของสำนักงาน ทำงานร่วมกับระบบ Active Directory (AD) และบริหารจัดการให้ระบบ AD สามารถควบคุมเครื่องคอมพิวเตอร์ของผู้ใช้งานทั่วไปทุกเครื่องของสำนักงานและกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงาน

ข) เพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่เหมาะสม และมีการจำกัดสิทธิการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line โดยพิจารณาตามความเหมาะสมของกลุ่มผู้ใช้งาน

ค) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึง ระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ดังต่อไปนี้

- ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์
- ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง
- จำกัดการป้อนรหัสผ่านในกรณีป้อนรหัสผ่านผิดพลาดได้ไม่เกิน 5 ครั้ง
- จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

ง) การบริหารจัดการรหัสผ่าน (Password Management System) ต้องแสดงผลการทำงานของการจัดการรหัสผ่านในลักษณะเชิงโต้ตอบ (Interactive) หรือต้องทำงานใน ลักษณะอัตโนมัติ เพื่อเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกบัญชีชื่อผู้ใช้งานหรือรหัสผ่านที่ได้ถูกกำหนดไว้ตอนเริ่มต้นที่มาพร้อม กับการติดตั้งระบบโดยทันที

4.5.5.2.2 การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)ผู้ใช้งานต้องมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้

ก) การสร้างบัญชีผู้ใช้ใหม่ การแก้ไข หรือยกเลิกบัญชีผู้ใช้ ต้องแจ้งให้ผู้ดูแลระบบดำเนินการ โดยได้รับความเห็นชอบจากผู้บังคับบัญชาของผู้ใช้งาน และผู้บังคับบัญชาที่กำกับดูแลระบบ

ข) การขอเพิ่ม/เปลี่ยนแปลง/เพิกถอนบัญชีรายชื่อและสิทธิให้มีหลักฐานการร้องขอที่เป็นลายลักษณ์อักษร

ค) ผู้ใช้งานทุกคนต้องมี User ID ของตนและไม่ซ้ำกับผู้ใช้งานคนอื่น ๆ โดย User ID ที่ออกให้นั้น ต้องสามารถตรวจสอบและยืนยันกลับไปยังตัวผู้ใช้งานได้

ง) ผู้ใช้งานต้องระบุชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงาน

4.5.5.2.3 การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) จำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการดังนี้

ก) ห้ามมิให้ลงโปรแกรมอรรถประโยชน์ก่อนได้รับการอนุมัติหรืออนุญาต และยังไม่ผ่านการตรวจสอบ

ข) ไม่อนุญาตให้มีการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์ หรือละเมิดกฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเองและต่อหน่วยงาน

ค) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

ง) กรณีไม่จำเป็นต้องใช้งานโปรแกรมอรรถประโยชน์แล้ว ต้องแจ้งขอถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

4.5.5.2.4 การกำหนดเวลาในการใช้งานระบบ

เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out) ตามความเหมาะสมของระบบสารสนเทศนั้นๆ

4.5.5.3 ผู้รับผิดชอบ

4.5.5.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.5.5.3.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

4.5.6 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

4.5.6.1 แนวนโยบาย

เพื่อกำหนดกฎเกณฑ์ควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศของสำนักงานจากผู้ที่ไม่ได้รับอนุญาต

4.5.6.2 แนวทางปฏิบัติ

4.5.6.2.1 การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องดำเนินการ ดังนี้

ก) การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศของสำนักงานโดยผู้ให้บริการจากภายนอกต้องดำเนินการตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Third Party Relationship Policy)

ข) ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งานพร้อมทั้งกำหนดสิทธิตามอำนาจ หน้าที่ที่ควรได้รับจะต้องมีการทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย หรือสิ้นสุดการจ้าง

ค) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศตามที่กำหนด

ง) การเข้าถึงสารสนเทศจากหน่วยงานภายนอกรวมถึงผู้รับจ้างที่ได้รับมอบหมายเพื่อ ดำเนินการใด ๆ จะต้องได้รับสิทธิและอนุญาตในการเข้าดำเนินการ และจะต้องรายงานให้ทราบหลังจากเสร็จสิ้นแล้ว ผู้ดูแลระบบจะต้องยกเลิกสิทธิที่ให้กับหน่วยงานนั้น ๆ ซึ่งหากหน่วยงานภายนอกดำเนินการใด ๆ ที่มีผลกระทบต่อระบบ จะต้องเป็นผู้รับผิดชอบ

4.5.6.2.2 ระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน

ก) ต้องแยกระบบสารสนเทศที่มีความสำคัญสูงและจำเป็นต้องได้รับการดูแลเป็นพิเศษ ฝ่ายบริหารเทคโนโลยีดิจิทัลต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ ให้ทำงานอยู่บนเครื่องเซิร์ฟเวอร์ หรือคอมพิวเตอร์ไม่ใช้ปะปนกับระบบอื่น เพื่อป้องกันความผิดพลาดอันอาจจะเกิดจากระบบอื่นซึ่งทำงานอยู่บนเครื่องเดียวกัน

ข) ให้มีการควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ห้อง Data Center ระบบไฟฟ้า ระบบสำรองไฟฟ้า ระบบควบคุมการเข้า-ออกห้อง เครื่องเซิร์ฟเวอร์ และอื่น ๆ เป็นต้น เพื่อป้องกันการหยุดชะงักการทำงานของระบบ

ค) ควบคุมการเข้ามาใช้งานจากเครือข่ายภายในและเครือข่ายภายนอก กำหนดสิทธิการเข้าใช้งานโดยกำหนดค่าที่ Firewall

ง) มีการควบคุมหรือป้องกันอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

4.5.6.2.3 การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking)

ก) ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอก รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัย

ข) ผู้ปฏิบัติงานจากระยะไกลต้องรักษาความลับของสำนักงาน ไม่อนุญาตให้ครอบครัวหรือบุคคลอื่นใด เข้าถึงระบบเทคโนโลยีสารสนเทศและข้อมูลของสำนักงาน

ค) การขออนุมัติหรือยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน ต้องปฏิบัติตามการควบคุมการเข้าถึงเครือข่าย

4.5.6.3 ผู้รับผิดชอบ

4.5.6.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.5.6.3.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

4.5.7 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

4.5.7.1 แนวนโยบาย

สำนักงานต้องมีการกำหนดมาตรการในการควบคุมและป้องกันการรักษาความปลอดภัยการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) และหลักเกณฑ์การนำอุปกรณ์สื่อสารเคลื่อนที่เข้ามาใช้งานในระบบเครือข่ายไร้สาย เพื่อป้องกันและรักษาความปลอดภัยของข้อมูลสารสนเทศของสำนักงาน

4.5.7.2 แนวปฏิบัติ

4.5.7.2.1 การใช้งานเครือข่ายไร้สาย (Wireless Policy) ต้องดำเนินการ ดังต่อไปนี้

ก) ไม่อนุญาตให้ผู้ใช้งานเปิด Ad-hoc หรือ Peer-to-Peer Network

ข) การเข้าใช้ Wireless จะต้องเข้าใช้ผ่าน username และ password ที่สำนักงานกำหนด

ค) เจ้าหน้าที่มีสิทธิตรวจสอบเครื่องที่เชื่อมต่อผ่านระบบเครือข่ายไร้สายได้

ง) ห้ามมิให้ผู้ใดนำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้เองไม่ว่าจะเป็นอุปกรณ์กระจายสัญญาณ (Access Point), Wireless USB Client, Wireless Routers ภายในหน่วยงาน ยกเว้นจะได้รับอนุญาตจากผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล หรือผู้รับผิดชอบของหน่วยงานที่ได้รับมอบหมาย

จ) การเข้าถึงระบบเครือข่ายไร้สาย (Wireless Lan) จะต้องได้รับอนุญาตจากผู้ดูแลระบบ และมีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์นั้น ๆ ก่อนเข้าใช้งานเครือข่ายของสำนักงาน

4.5.7.2.2 การเชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่าง ๆ กับระบบเครือข่าย

ผู้ที่นำคอมพิวเตอร์แบบพกพาของตนเองมาต่อเข้าระบบเครือข่ายหลักของสำนักงานต้องดำเนินการลงทะเบียนอุปกรณ์และได้รับอนุญาตจากผู้จัดการฝ่ายต้นสังกัด เป็นลายลักษณ์อักษรก่อนทำการเชื่อมต่อเครือข่าย หรือเชื่อมต่อยังเครือข่ายที่ได้ถูกจัดสรรไว้แยกต่างหากจากระบบงานภายในของสำนักงาน

4.5.7.2.3 ผู้ดูแลระบบ (System Administrator) ต้องดำเนินการดังต่อไปนี้

ก) ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

ข) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

ค) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

4.5.7.3 ผู้รับผิดชอบ

4.5.7.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.5.7.3.2 ผู้ดูแลระบบ

4.5.8 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Outsource Access Control)

4.5.8.1 แนวนโยบาย

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน ให้เป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการควบคุมการปฏิบัติงานของหน่วยงานภายนอก โดยหน่วยงานภายนอกที่ทำงานให้กับสำนักงาน ไม่ว่าจะทำงานอยู่ภายในสำนักงานหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญา หรือข้อตกลงการไม่เปิดเผยข้อมูลของสำนักงาน โดยสัญญาหรือข้อตกลงต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ สำหรับงานลักษณะโครงการ ผู้ดูแลระบบหรือเจ้าของโครงการ

ต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอก ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของสำนักงาน ให้มีความมั่นคงปลอดภัย ทั้ง 3 ด้านคือการรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability) ทั้งนี้ ผู้ให้บริการหน่วยงานภายนอกต้องจัดทำแผนการดำเนินงานคู่มือการปฏิบัติงานและ เอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุม หรือตรวจสอบ การให้บริการของผู้ให้บริการได้อย่างเข้มงวด และให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

4.5.8.2 แนวปฏิบัติ

4.5.8.2.1 บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน ต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งาน ระบบเทคโนโลยีสารสนเทศเพื่อขออนุมัติจากผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.5.8.2.2 ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศหรือ อุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงาน

4.5.8.2.3 หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน จะต้อง ทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล โดยทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งต้องมีรายละเอียด ดังนี้

ก) เหตุผลในการขอใช้

ข) ระยะเวลาในการใช้

ค) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

ง) การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

จ) กำหนดข้อตกลงการใช้งานข้อมูล เพื่อเป็นการป้องกันการเปิดเผยข้อมูล

4.5.8.2.4 หน่วยงานภายนอกซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนาม ในสัญญาไม่เปิดเผยข้อมูล

4.5.8.2.5 สำนักงานมีสิทธิในการตรวจสอบตามสัญญา หรือข้อตกลงการใช้งานระบบเทคโนโลยี สารสนเทศเพื่อให้มั่นใจได้ว่าสำนักงานสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

4.5.8.2.6 ต้องกำหนดให้หน่วยงานภายนอกหรือผู้ให้บริการ จัดทำแผนการดำเนินงานคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของหน่วยงานภายนอกหรือผู้ให้บริการ เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดหรือตกลงไว้

4.5.8.3 ผู้รับผิดชอบ

4.5.8.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.5.8.3.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

4.5.9 นโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

4.5.9.1 แนวนโยบาย

เพื่อให้ผู้ใช้งานได้มีแนวทางปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการใช้รหัสผ่าน

4.5.9.2 แนวทางปฏิบัติ

4.5.9.2.1 การบริหารรหัสผ่าน

ก) ไม่อนุญาตให้เจ้าหน้าที่หรือผู้ใช้งานระบบใช้รหัสผ่านร่วมกัน ชื่อผู้ใช้งานและ/หรือรหัสผ่าน ต้องไม่ถูกใช้งานร่วมกันหรือแบ่งปันกันใช้งาน

ข) ผู้ดูแลระบบและ/หรือเจ้าของระบบต้องจัดทำขั้นตอนการปฏิบัติสำหรับการตั้งหรือการเปลี่ยนรหัสผ่านให้ผู้ใช้งานทราบ

ค) ผู้ดูแลระบบและ/หรือเจ้าของระบบต้องมีกระบวนการที่มั่นคงปลอดภัยในการจัดส่งรหัสผ่าน (System Generated Password) ให้แก่ผู้ใช้งาน

ง) รหัสผ่านเบื้องต้น ข้อปฏิบัติ รหัสผ่านมาตรฐาน (Standard Password) และรหัสผ่านปริยาย (Default Password) ของระบบเทคโนโลยีสารสนเทศต้องถูกเปลี่ยนโดยผู้ดูแลระบบ และ/หรือเจ้าของระบบ ให้เป็นรหัสผ่านที่มั่นคงในทันทีที่การติดตั้งระบบเสร็จสิ้น

จ) การส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งาน ต้องหลีกเลี่ยงการใช้บุคคลอื่นในการส่งมอบรหัสผ่าน

ฉ) ผู้ดูแลระบบและ/หรือเจ้าของระบบของแต่ละระบบงานมีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่านอย่างน้อย 90 วัน หรือตามความเหมาะสม

4.5.9.2.2 การกำหนดคุณภาพรหัสผ่าน

ก) กำหนดรหัสผ่านที่เดาสุ่มได้ยาก ความยาวอย่างน้อย 8 ตัวอักษร (โดยมีการผสมผสาน ตัวอักษร 3 เงื่อนไข เช่น ตัวอักษรพิมพ์เล็ก ตัวอักษรพิมพ์ใหญ่ ตัวเลข หรือสัญลักษณ์เข้าด้วยกัน)

ข) ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ สกุล เบอร์โทรศัพท์ ของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

ค) การตั้งรหัสผ่านชั่วคราวต้องยากต่อการเดาและต้องมีความแตกต่างกัน

4.5.9.2.3 การใช้งานรหัสผ่าน

ก) ห้ามใช้งานบัญชีผู้ใช้งานหรือรหัสผ่านของผู้อื่น

ข) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

ค) เปลี่ยนรหัสผ่านของตนเองที่ได้รับมาจากผู้ดูแลระบบ ไม่ว่าระบบจะบังคับให้มีการเปลี่ยนรหัสผ่านหรือไม่ก็ตาม และไม่ตั้งรหัสผ่านซ้ำกับรหัสผ่านเดิมที่ได้รับมา และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

ง) ผู้ใช้งานต้องรายงานเหตุการณ์ที่สงสัยว่ามีการเปิดเผยรหัสผ่านไปยังผู้ดูแลระบบ และให้ดำเนินการเปลี่ยนรหัสผ่านทันที

จ) ถ้าผู้ใช้งานไม่สามารถเข้าใช้งานระบบด้วยชื่อผู้ใช้และรหัสผ่านของตนเองได้ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบ

4.5.9.3 ผู้รับผิดชอบ

4.5.9.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.5.9.3.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

4.6 การเข้ารหัสลับข้อมูล (Cryptography)

วัตถุประสงค์

เพื่อกำหนดแนวทางการใช้งานการเข้ารหัสลับข้อมูลและทำให้ระบบสารสนเทศรักษาไว้ซึ่งความลับของข้อมูล การพิสูจน์ตัวตนของผู้ใช้งานระบบสารสนเทศ และ/หรือป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาตอย่างมีประสิทธิภาพและความเหมาะสม

แนวนโยบายและแนวทางปฏิบัติ

4.6.1 มาตรการการเข้ารหัสลับข้อมูล (Cryptographic Controls)

ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องกำหนดมาตรการควบคุมการเข้ารหัสลับข้อมูล และแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยกำหนดกลุ่มผู้ใช้งานอย่างเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้และมีความครอบคลุมข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่กรณีที่ไม่สามารถเข้ารหัสได้ ต้องควบคุมการเข้าถึงอย่างเหมาะสมตามหน้าที่และความรับผิดชอบ

4.6.2 การบริหารจัดการกุญแจเข้ารหัสลับข้อมูล (Key Management)

ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องกำหนดวิธีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัสลับข้อมูลซึ่งประกอบไปด้วย

4.6.2.1 การพิจารณาประเภทกลุ่มข้อมูลที่นำมาใช้เข้ารหัสว่าสอดคล้องกับการจัดระดับชั้นความลับของข้อมูล และแนวทางการดำเนินการกำกับข้อมูล

4.6.2.2 มีการพิจารณาวิธีการเข้ารหัสแต่ละรูปแบบ รวมทั้งใช้อัลกอริทึมที่เหมาะสม การเลือกใช้การเข้ารหัสข้อมูลให้สามารถดำเนินการได้ 2 แบบ ดังนี้

4.6.2.2.1 แบบสมมาตร Symmetric คือการเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสเดียวกัน (Secret Key)

4.6.2.2.2 แบบอสมมาตร Asymmetric คือการเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสคู่ (Public/Private Key)

4.6.2.3 ดำเนินการสร้างกุญแจรหัสจากโปรแกรมที่น่าเชื่อถือ โดยแนวทางการสร้างกุญแจรหัส และการบริหารจัดการกุญแจรหัส (Key Management)

4.6.2.4 ดำเนินการนำข้อมูลผ่านกระบวนการเข้ารหัส เพื่อนำข้อมูลที่เข้ารหัสไปใช้ตามจุดประสงค์ต่อไป

4.6.2.5 มีการกำหนดอายุการใช้งานของกุญแจ

4.6.2.6 มีการกำหนดมาตรการในการเก็บกุญแจ (Key)

4.6.2.7 มีการจัดทำและปฏิบัติตามตลอดวงจรชีวิตของกุญแจ

4.6.3 ผู้รับผิดชอบ

4.6.3.1 ฝ่ายบริหารเทคโนโลยีดิจิทัล

4.6.3.2 ผู้ใช้งาน

4.7 ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน และเป็นมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ

แนวนโยบายและแนวทางปฏิบัติ

4.7.1 มาตรฐานในการกำหนดบริเวณที่ต้องมีความมั่นคงปลอดภัยด้านสารสนเทศ (Secure Area)

4.7.1.1 ข้อกำหนดทั่วไป

4.7.1.1.1 สำนักงานต้องมีการจำแนกและกำหนดบริเวณพื้นที่ใช้งานระบบสารสนเทศตามที่ได้นิยามไว้ รวมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศ เพื่อการเฝ้าระวัง ควบคุมและรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ และประกาศให้รับทราบทั่วกัน

4.7.1.1.2 สำนักงานต้องดำเนินการติดตั้งอุปกรณ์ในการรักษาความปลอดภัย ประกอบด้วย กล้องวงจรปิด ระบบ Access Control หรืออุปกรณ์ที่สามารถป้องกันภัยคุกคามจากผู้บุกรุก เป็นต้น ในพื้นที่ใช้งานระบบสารสนเทศของสำนักงานได้แก่ ห้อง Data Center เพื่อให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัย

4.7.1.2 การควบคุมการเข้าออก (Secure Area)

หน่วยงานที่เป็นเจ้าของระบบงาน กำหนดมาตรการการควบคุมการเข้าออกในบริเวณพื้นที่ใช้งานระบบสารสนเทศ โดยให้ผ่านเข้าออกได้เฉพาะผู้ใช้งานที่มีสิทธิเท่านั้น ซึ่งมีแนวทางปฏิบัติดังนี้

4.7.1.2.1 มีการกำหนดสิทธิการเข้าถึงพื้นที่ และมีการทบทวนสิทธิตามรอบ โดยการกำหนดสิทธิต้องระบุเป็นลายลักษณ์อักษร

4.7.1.2.2 ผู้ใช้งานจะได้รับสิทธิให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณที่ถูกกำหนดเท่านั้น

4.7.1.2.3 ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยผู้ให้บริการภายนอกหรือหน่วยงานภายนอกเพื่อป้องกันการเข้าถึงสินทรัพย์ของสำนักงานโดยไม่ได้รับอนุญาต และจัดเป็นบริเวณแยกออกมาต่างหาก

4.7.1.2.4 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งาน ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า ให้ปฏิบัติตามหลักเกณฑ์การเข้าออกพื้นที่ห้อง Data Center

4.7.2 ความมั่นคงปลอดภัยด้านสารสนเทศสำหรับสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ (Securing Offices, Rooms and Facilities)

4.7.2.1 การปฏิบัติงานในพื้นที่สำนักงาน

4.7.2.1.1 กองบริหารกลางต้องร่วมกับฝ่ายบริหารเทคโนโลยีดิจิทัล กำหนดมาตรการความมั่นคงปลอดภัยด้านสารสนเทศให้กับสำนักงาน ห้องทำงานและเครื่องมือต่าง ๆ ได้แก่ เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูง ต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก ประตูหน้าต่างของสำนักงานต้องปิดล็อคโดยวิธีการที่ปลอดภัย ล็อคประตูที่ใช้ดอกกุญแจ หรือมีระบบ Access Control และปรับปรุงให้มีความเหมาะสมทางสภาวะแวดล้อม ได้แก่ ติดตั้งระบบปรับอากาศ การควบคุมความชื้น เป็นต้น

4.7.2.1.2 สำนักงานต้องมีการควบคุมการเข้าออกพื้นที่สำหรับผู้ติดต่อโดยจำกัดเฉพาะพื้นที่ที่จัดเตรียมไว้ให้เท่านั้น

4.7.2.1.3 สำนักงานต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยผู้ให้บริการภายนอก (Third Party) หรือหน่วยงานภายนอกเพื่อป้องกันการเข้าถึงสินทรัพย์ของสำนักงานโดยไม่ได้รับอนุญาต และจัดเป็นบริเวณแยกออกมาต่างหาก และพนักงานของสำนักงานที่ได้รับมอบหมายจะต้องคอยกำกับดูแลบุคคลภายนอกที่ได้รับอนุญาตเข้าพื้นที่ต่าง ๆ ของสำนักงาน

4.7.2.1.4 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้มาติดต่อ หรือผู้ขอเข้าใช้พื้นที่ หรือมิได้เกี่ยวข้องอันใดกับกิจการของสำนักงาน หรือมิได้แจ้งการขอเข้าพื้นที่เป็นการล่วงหน้า หน่วยงานที่เกี่ยวข้องจะต้องตรวจสอบเหตุผลและความจำเป็นก่อนการอนุญาตหรือไม่อนุญาตเข้าพื้นที่

4.7.2.2 การปฏิบัติงานในพื้นที่ความมั่นคงปลอดภัย (Secure Area)

สำนักงานต้องกำหนดแนวปฏิบัติสำหรับการปฏิบัติงานในพื้นที่ความมั่นคงปลอดภัย (Secure Area) ได้แก่ห้อง Data Center และพื้นที่ปฏิบัติงานของผู้ดูแลระบบ และกำหนดให้ฝ่ายบริหารเทคโนโลยีดิจิทัล มีการนำแนวปฏิบัติไปใช้งานอย่างเคร่งครัด

4.7.2.3 ข้อปฏิบัติสำหรับผู้ติดต่อจากหน่วยงานภายนอก

4.7.2.3.1 ต้องทำการแลกบัตรที่ใช้ระบุตัวตน ได้แก่ บัตรประชาชน หรือใบอนุญาตขับขี่ หรือบัตรประจำตัวอื่นใดที่หน่วยงานของรัฐออกให้กับเจ้าหน้าที่เพื่อรับบัตรผู้ติดต่อ (Visitor)

4.7.2.3.2 ต้องติดบัตรผู้ติดต่อที่บริเวณสามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในสำนักงาน

4.7.2.3.3 ต้องอยู่ในพื้นที่บริเวณที่จัดไว้ให้ และมีพนักงานของสำนักงานดูแล

4.7.2.3.4 ต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่ และเจ้าหน้าที่ต้องตรวจสอบการคืนบัตร

4.7.2.3.5 กรณีมีการย้ายสำนักงานให้กำหนดแนวปฏิบัติตามความเหมาะสม โดยคำนึงถึงความมั่นคงปลอดภัยเป็นสำคัญ

4.7.2.3.6 กรณีเข้าพื้นที่ความมั่นคงปลอดภัย (Secure Area) ผู้มาติดต่อที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร จะต้องลงบันทึกรายการอุปกรณ์ตามขั้นตอนการปฏิบัติงานในห้อง Data Center

4.7.2.4 พื้นที่สำหรับรับส่งสิ่งของ (Delivery and loading areas)

ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องกำหนดให้มีการควบคุมบริเวณที่ผู้ไม่มีสิทธิเข้าถึงอาจสามารถเข้าถึงได้ เป็นพื้นที่การส่งมอบสินค้า พื้นที่การเตรียม หรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าห้อง Data Center ทั้งนี้ให้แยกเป็นสัดส่วนที่ชัดเจน เพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศ และข้อมูลสารสนเทศโดยผู้ที่ไม่ได้รับอนุญาต

4.7.2.5 ความปลอดภัยของอุปกรณ์ (Equipment Security)

4.7.2.5.1 ผู้ใช้งานต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัยรวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

4.7.2.5.2 เจ้าของระบบงานต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ ได้แก่ จัดให้มีการซ่อมบำรุงตามรอบที่กำหนดโดยเฉพาะระบบที่มีความสำคัญ เป็นต้น เพื่อให้สามารถใช้งานได้อย่างต่อเนื่องและมีความพร้อมใช้อยู่เสมอ

4.7.2.5.3 ต้องกำหนดให้มีการป้องกันสินทรัพย์และอุปกรณ์ของสำนักงานเมื่อถูกนำไปใช้งานนอกสำนักงาน

4.7.2.5.4 ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์อย่างเหมาะสมตามระดับชั้นความลับของข้อมูลที่ถูกจัดเก็บในอุปกรณ์นั้น

4.7.2.6 ความปลอดภัยของระบบกระแสไฟฟ้าสำรอง (Power Supplies) และระบบป้องกันภัย

4.7.2.6.1 ต้องมีระบบไฟฟ้าสำรองอัตโนมัติ เพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง และต้องมีการตรวจสอบระบบไฟฟ้าสำรองและบำรุงรักษาอย่างน้อยปีละ 1 ครั้ง

4.7.2.6.2 ต้องจัดให้มีระบบเตือนภัย/ป้องกันภัย ได้แก่ ระบบดับเพลิง ระบบแจ้งเตือนอัคคีภัย

4.7.2.6.3 ต้องมีการวางแผนและซักซ้อมการปฏิบัติเพื่อรับมือกับเหตุการณ์ฉุกเฉินต่าง ๆ อย่างน้อยปีละ 1 ครั้ง

4.7.2.6.4 ระบบที่สำคัญของสำนักงานจะต้องมีการปฏิบัติตามนโยบายแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ เพื่อลดผลกระทบที่จะเกิดขึ้นกับการดำเนินงานของสำนักงาน

4.7.2.7 ความปลอดภัยของการเดินสายไฟฟ้าหลัก (Main Power Cable) และสายเคเบิลหลัก (Backbone Cable)

4.7.2.7.1 การเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสำนักงานที่ผ่านเข้ามาผ่านช่องพิเศษที่จัดไว้ เป็นบริเวณที่บุคคลทั่วไปไม่สามารถเข้าถึงได้ง่าย การติดตั้งตู้พักสายต้องล็อคไว้ตลอดเวลาและจำกัดการเข้าใช้งานได้เฉพาะเจ้าหน้าที่หรือบุคคลที่มีสิทธิเท่านั้น

4.7.2.8 ความปลอดภัยของโต๊ะทำงานและการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk Clear Screen)

4.7.2.8.1 ต้องควบคุมสินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล อุปกรณ์คอมพิวเตอร์ ฯลฯ ให้ปลอดภัยจากการเข้าถึงโดยผู้ไม่มีสิทธิ

4.7.2.8.2 จัดเก็บเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับของข้อมูล

4.7.2.8.3 การทำลายเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับของข้อมูลและจัดทำบันทึกการทำลายอย่างเหมาะสม

4.7.2.8.4 ข้อมูลที่มีความสำคัญมากรวมถึงข้อมูลในคอมพิวเตอร์ ต้องเคลื่อนย้ายโดยผู้เป็นเจ้าของข้อมูลเท่านั้น ไม่เคลื่อนย้ายโดยบุคคลที่ไม่ใช่เจ้าของข้อมูล เว้นเสียแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล

4.7.2.8.5 ข้อมูลที่มีความสำคัญ มีการรักษาความลับต้องมีการเข้ารหัสเมื่อถูกจัดเก็บ

4.7.2.8.6 ทุกครั้งที่ออกจากหน้าจอคอมพิวเตอร์ต้องปิดหน้าจอ หรือ log off ออกจากระบบ

4.7.2.8.7 ผู้ใช้งานต้องออกจากระบบเมื่อว่างเว้นจากการใช้งาน

4.7.2.9 การควบคุมทั่วไป (General Control)

4.7.2.9.1 ผู้จัดการฝ่ายต้องตรวจสอบความพร้อมใช้งานของพื้นที่และสินทรัพย์ ซึ่งการย้ายสถานที่ทำงานเป็นช่วงเวลาที่ต้องระวังเรื่องการรักษาความปลอดภัยที่อาจมีการมองข้ามได้ โดยเฉพาะช่วงเวลาที่ต้องเร่งจัดการย้ายให้เสร็จสิ้น จึงต้องให้ความระมัดระวัง

4.7.2.9.2 ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่าง ๆ เมื่อมีการเปลี่ยนแปลงหรือเคลื่อนย้ายเพื่อใช้เป็นข้อมูลในการควบคุมสินทรัพย์ของสำนักงาน

4.7.3 ผู้รับผิดชอบ

4.7.3.1 หัวหน้ากองบริหารกลาง

4.7.3.2 ผู้ดูแลระบบฝ่ายบริหารเทคโนโลยีดิจิทัล

4.7.3.3 ผู้ให้บริการภายนอก

4.7.3.4 ผู้ใช้งาน

4.8 การบริหารจัดการด้านการดำเนินงาน (Operations Management)

วัตถุประสงค์

เพื่อให้การบริหารจัดการด้านการปฏิบัติการด้านสารสนเทศเป็นไปอย่างถูกต้องและรักษาไว้ซึ่งความมั่นคงปลอดภัยด้านสารสนเทศ

แนวนโยบายและแนวทางปฏิบัติ

4.8.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติงาน (Operational Procedures and Responsibilities)

4.8.1.1 แนวนโยบาย

เพื่อให้การปฏิบัติงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัยจึงสมควรให้มีการกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติงาน ดังนั้นจำเป็นต้องมีการจัดทำคู่มือปฏิบัติงาน (Documented Operating Procedures) มีความพร้อมใช้สำหรับผู้ที่ต้องการนำไปใช้ต่อ และการแบ่งหน้าที่ความรับผิดชอบ (Segregation of Duties) ให้ชัดเจนและเหมาะสม เพื่อลดความเสียหายที่อาจเกิดกับทรัพย์สินสารสนเทศของสำนักงาน

4.8.1.2 แนวทางปฏิบัติ

ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องจัดให้มีคู่มือปฏิบัติงาน (Documented Operating Procedures) โดยมีการดำเนินการอย่างน้อยดังต่อไปนี้

4.8.1.2.1 จัดทำและปรับปรุงคู่มือการปฏิบัติงาน เพื่อใช้เป็นแนวทางในการปฏิบัติงาน ทั้งนี้ คู่มือดังกล่าวสามารถจัดทำในรูปแบบสิ่งพิมพ์หรืออิเล็กทรอนิกส์

4.8.1.2.2 ฝึกอบรมแก่เจ้าหน้าที่ฝ่ายบริหารเทคโนโลยีดิจิทัล เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง

4.8.1.2.3 ทดสอบการปฏิบัติงานตามคู่มือที่จัดทำขึ้น

4.8.1.2.4 คู่มือการปฏิบัติงานต้องได้รับอนุมัติจากผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัลเป็นอย่างน้อย

4.8.1.2.5 ต้องมีการกำหนดให้มีการควบคุมการเข้าถึงคู่มือการปฏิบัติงาน เพื่อป้องกันการเข้าถึงและเปิดเผยคู่มือการปฏิบัติงานโดยมิได้รับอนุญาต

4.8.1.2.6 ต้องมีการจัดทำทะเบียนคู่มือการปฏิบัติงาน และต้องมีการทบทวนทะเบียนคู่มืออย่างน้อยปีละ 1 ครั้ง เพื่อให้เกิดความมั่นใจและง่ายต่อการค้นหาคู่มือและเจ้าของคู่มือปฏิบัติงาน

4.8.1.2.7 ผู้เป็นเจ้าของทรัพย์สินสารสนเทศ ต้องควบคุมให้มีการแบ่งหน้าที่ความรับผิดชอบ (Segregation of Duties) อย่างเหมาะสมเพื่อลดความเสี่ยงในการใช้ทรัพย์สินสารสนเทศของสำนักงาน ในทางที่ไม่เหมาะสมทั้งโดยเจตนาและไม่เจตนา โดยต้องกำหนดให้มีการแบ่งแยกหน้าที่รับผิดชอบในแต่ละกระบวนการ และมีการตรวจสอบการทำงานซึ่งกันและกัน ตัวอย่างเช่น ผู้พัฒนาระบบสารสนเทศ ต้องไม่มีสิทธิในการเข้าถึงระบบที่ให้บริการจริง และต้องไม่มีสิทธิในการติดตั้งซอฟต์แวร์และแอพพลิเคชันในระบบที่ให้บริการจริง เป็นต้น ในกรณีที่ไม่สามารถดำเนินการได้ ต้องมีการพิจารณาการควบคุมในด้านอื่น ๆ เช่น การเฝ้าระวังการปฏิบัติงาน และการสอบทานหลักฐานการตรวจสอบ (Audit Trail) โดยหัวหน้างานหรือพนักงานและลูกจ้างอื่น ซึ่งไม่มีความเกี่ยวข้องโดยตรงกับการปฏิบัติงานนั้น ๆ เป็นต้น

4.8.1.3 ผู้รับผิดชอบ

4.8.1.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.8.1.3.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

4.8.2 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Security Monitoring)

ให้มีการเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Security Monitoring) ซึ่งประกอบไปด้วยเรื่องต่อไปนี้

4.8.2.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งาน (Audit Logging)

4.8.2.1.1 แนวนโยบาย

เพื่อให้มีการบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการใช้งาน รวมทั้งเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนด

4.8.2.1.2 แนวทางปฏิบัติ

ผู้ดูแลระบบต้องมีแนวทางบันทึกเหตุการณ์ต่าง ๆ โดยพิจารณาถึงประเด็นความต้องการทางธุรกิจ และข้อกำหนดที่มีผลทางกฎหมาย โดยมีรายละเอียดครอบคลุมอย่างน้อยดังต่อไปนี้

ก) รหัสผู้ใช้งาน
ข) วันที่ เวลา รายละเอียดของเหตุการณ์ เช่น การ Log on และ การ Log off เป็นต้น
ค) ข้อมูลที่ระบุถึงเครื่องต้นทางและปลายทาง เช่น ชื่อเครื่อง, IP Address, Subnet Mask, Protocol หรือ Port ที่ใช้งาน และ MAC Address เป็นต้น
ง) ความสำเร็จและล้มเหลวในการพยายามเข้าถึงระบบ
จ) ความสำเร็จและล้มเหลวในการพยายามเข้าถึงข้อมูลและทรัพยากรอื่น ๆ
ฉ) การเปลี่ยนแปลงการกำหนดค่าในระบบ (Configuration)
ช) กิจกรรมที่เกิดจากการใช่สิทธิการใช้งาน (Activities of Privilege Usage)
ซ) การเข้าถึง File และประเภทของการเข้าถึง
ฌ) ข้อความแจ้งเตือนจากระบบการควบคุมการเข้าถึง (Alarm raised by Access Control System)
ญ) การเปิดการใช้งาน (Activation) และการระงับการใช้งาน (De-Activation) ของระบบป้องกัน เช่น ระบบป้องกันไวรัส และระบบตรวจจับการบุกรุก (Intrusion Detection System)
ฎ) ควรมีการเก็บบันทึกเหตุการณ์ย้อนหลังอย่างน้อย 90 วัน

4.8.2.1.3 ผู้รับผิดชอบ

ก) ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล
ข) ผู้ดูแลระบบเครือข่าย
ค) ผู้ดูแลระบบ

4.8.2.2 การเฝ้าระวังการใช้งาน (Monitoring System Use)

4.8.2.2.1 แนวนโยบาย

เพื่อให้มีการเฝ้าระวังการใช้งานอุปกรณ์ประมวลผลสารสนเทศ และมีการสอบทานผลการเฝ้าระวังอย่างสม่ำเสมอ ตรวจจับกิจกรรมการใช้งานที่มิได้รับอนุญาตและหาทางแก้ไขอย่างทันท่วงที

4.8.2.2.2 แนวทางปฏิบัติ

ก) หน่วยงานผู้ดูแลระบบ ต้องกำหนดหลักเกณฑ์ในการเฝ้าระวังการใช้งานอุปกรณ์ประมวลผลสารสนเทศของสำนักงาน ซึ่งประกอบไปด้วยเหตุการณ์ที่ต้องการเฝ้าระวัง ช่วงเวลาของการเฝ้าระวังและความถี่ของการเฝ้าระวัง และมีการสอบทานผลการเฝ้าระวังอย่างสม่ำเสมอ โดยพิจารณาถึงประเด็นต่าง ๆ อย่างน้อยดังต่อไปนี้

- ความต้องการทางธุรกิจ
- ข้อกำหนดที่มีผลทางกฎหมาย
- ระดับความสำคัญ (Criticality) ของแอพพลิเคชัน
- ระดับความลับ (sensitivity) ระดับความสำคัญ (Criticality) ของสารสนเทศ
- เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Event) และเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Incident) ที่เกิดขึ้นในอดีต
- ขอบเขตการเชื่อมต่อ เช่น มีการเชื่อมต่อเฉพาะภายในสำนักงาน หรือมีการเชื่อมต่อกับเครือข่ายสาธารณะ
- บันทึกเหตุการณ์ (Log) ของระบบซึ่งถูกระงับการใช้งาน (De-Activation)

ข) เหตุการณ์ที่ควรเฝ้าระวัง ประกอบไปด้วยเรื่องต่าง ๆ อย่างน้อยดังต่อไปนี้

- การเฝ้าระวังการเข้าถึงที่ได้รับอนุญาต เช่น ช่วงวันและเวลา การเข้าถึง File ต่างๆ
- การเฝ้าระวังปฏิบัติงานที่มีการใช้สิทธิพิเศษ เช่น การเริ่มต้นหรือการหยุดระบบการเชื่อมต่ออุปกรณ์
- การเฝ้าระวังการพยายามเข้าถึงที่มิได้รับอนุญาต เช่น การกระทำที่ผิดพลาดหรือการถูกปฏิเสธ การละเมิดการเข้าถึงผ่านการเชื่อมต่อเครือข่าย การแจ้งเตือนตรวจจับการบุกรุก
- การเฝ้าระวังการแจ้งเตือนหรือข้อผิดพลาดจากระบบ เช่น การแจ้งเตือนจาก Console การบันทึกเหตุการณ์การยกเว้นในระบบ การแจ้งเตือนจากการบริหารจัดการเครือข่าย
- การเฝ้าระวังการเปลี่ยนแปลง หรือความพยายามที่จะเปลี่ยนแปลงการควบคุมและค่าการติดตั้งด้านความมั่นคงปลอดภัยของระบบ

4.8.2.2.3 ผู้รับผิดชอบ

ก) ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

ข) ผู้ดูแลระบบ

4.8.2.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of Log Information)

4.8.2.3.1 แนวนโยบาย

เพื่อป้องกันข้อมูลบันทึกเหตุการณ์ (Log Information) ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานอุปกรณ์ประมวลผลสารสนเทศ จากการเปลี่ยนแปลงแก้ไข หรือเข้าถึงได้โดยมิได้รับอนุญาต

4.8.2.3.2 แนวทางปฏิบัติ

หน่วยงานผู้ดูแลระบบ ต้องจัดให้มีการป้องกันข้อมูลบันทึกเหตุการณ์ (Log Information) ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานอุปกรณ์ประมวลผลสารสนเทศจากการเปลี่ยนแปลงแก้ไข หรือเข้าถึงได้โดยมิได้รับอนุญาต ทั้งนี้กระบวนการในการป้องกันต้องพิจารณาในเรื่องอย่างน้อยต่อไปนี้

ก) ความต้องการทางธุรกิจ

ข) ข้อกำหนดที่มีผลทางกฎหมาย

4.8.2.3.3 ผู้รับผิดชอบ

ก) ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

ข) ผู้ดูแลระบบ

4.8.2.4 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and Operator Logs)

4.8.2.4.1 แนวนโยบาย

เพื่อให้มีการบันทึกกิจกรรมการดำเนินงานทั้งหมดของผู้ดูแลระบบหรือเจ้าหน้าที่ผู้ปฏิบัติการที่เกี่ยวข้องอื่น ๆ กับระบบ

4.8.2.4.2 แนวทางปฏิบัติ

หน่วยงานผู้ดูแลระบบต้องกำหนดให้มีการบันทึก เฝ้าระวัง และป้องกันข้อมูลกิจกรรมการดำเนินงานของผู้ดูแลระบบอย่างเหมาะสม โดยให้พิจารณาตามหลักเกณฑ์ในข้อ 4.8.2.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งาน (Audit Logging) 4.8.2.2 การเฝ้าระวังการใช้งาน (Monitoring System Use) 4.8.2.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of Log Information)

4.8.2.4.3 ผู้รับผิดชอบ

ก) ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

ข) ผู้ดูแลระบบ

4.8.2.5 การบันทึกเหตุการณ์ข้อผิดพลาด (Fault Logging)

4.8.2.5.1 แนวนโยบาย

เพื่อให้มีการบันทึก วิเคราะห์ และดำเนินการแก้ไขเหตุการณ์ข้อผิดพลาดต่าง ๆ ที่เกี่ยวข้องกับการใช้งานอุปกรณ์ประมวลผลสารสนเทศ

4.8.2.5.2 แนวทางปฏิบัติ

หน่วยงานผู้ดูแลระบบ ต้องกำหนดให้มีการบันทึก เฝ้าระวัง และป้องกันข้อมูลบันทึกเหตุการณ์ข้อผิดพลาดอันเกิดจากระบบหรือได้รับแจ้งจากผู้ใช้งานอย่างเหมาะสม (อ้างอิง 8.2.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) 8.2.2 การเฝ้าระวังการใช้งานระบบ (Monitoring System Use) และ 8.2.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of Log Information)) โดยต้องมีแนวทางในการจัดการข้อผิดพลาดที่ได้รับรายงานอย่างน้อยดังต่อไปนี้

ก) การสอบทานบันทึกเหตุการณ์ข้อผิดพลาด เพื่อให้มั่นใจว่าข้อผิดพลาดได้รับการแก้ไขอย่างเหมาะสม

ข) การสอบทานวิธีการในการแก้ไข เพื่อให้มั่นใจว่าไม่ได้มีการละเมิดการควบคุมที่มีอยู่

4.8.2.5.3 ผู้รับผิดชอบ

ก) ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

ข) ผู้ดูแลระบบ

4.8.2.6 การบริหารจัดการช่องโหว่ทางเทคนิคของสำนักงาน (Technical Vulnerability Management)

4.8.2.6.1 แนวนโยบาย

เพื่อลดความเสี่ยงจากการใช้ประโยชน์จากช่องโหว่ทางเทคนิคโดยอาศัยจุดอ่อนต่อช่องโหว่และช่องโหว่ทางเทคนิคที่มีการเปิดเผยสู่สาธารณะ และเพื่อควบคุมช่องโหว่ในระบบปฏิบัติการและแอพพลิเคชัน

4.8.2.6.2 แนวทางปฏิบัติ

หน่วยงานผู้ดูแลระบบ ต้องจัดให้มีการจัดการช่องโหว่ทางเทคนิคที่เหมาะสมและทันท่วงที โดยพิจารณาดำเนินการในเรื่องอย่างน้อยดังต่อไปนี้

ก) เฝ้าระวังและติดตามข่าวสารเกี่ยวกับช้องโหว่ทางเทคนิคอย่างสม่ำเสมอ

ข) หากพบช่องโหว่ทางเทคนิค ต้องหาแนวทางการแก้ไข เพื่อให้สามารถป้องกันความเสียหายได้อย่างทันท่วงที

ค) ก่อนดำเนินการแก้ไขช่องโหว่ทางเทคนิค ต้องทดสอบเพื่อให้มั่นใจว่าแนวทางดังกล่าวไม่ส่งผลเสียหายต่อการดำเนินงานของระบบปฏิบัติงานจริง

ง) จัดให้มีขั้นตอนปฏิบัติการควบคุมการเปลี่ยนแปลงอย่างเหมาะสมเพื่อดำเนินการแก้ไขช่องโหว่ทางเทคนิค

จ) จัดให้มีการประเมินช่องโหว่ทางเทคนิคอย่างสม่ำเสมอ เพื่อเป็นการตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคด้านความมั่นคงปลอดภัย

4.8.2.6.3 ผู้รับผิดชอบ

ก) ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

ข) ผู้ดูแลระบบ

ค) ผู้พัฒนาระบบ

4.8.2.7 การบริการจัดการปรับปรุงระบบปฏิบัติการ (Patch Management)

4.8.2.7.1 แนวนโยบาย

เพื่อให้เป็นการปรับปรุง แก้ไขเพิ่มเติมและติดตั้งซอฟต์แวร์ที่ใช้แก้ไขของระบบที่ใช้งานจริงให้ดีขึ้นและเป็นปัจจุบันที่สุด และเพื่อปิดช่องโหว่ให้น้อยที่สุดเพื่อลดความเสี่ยงที่จะถูกโจมตีจากผู้ไม่ประสงค์ดี

4.8.2.7.2 แนวทางปฏิบัติ

หน่วยงานผู้ดูแลระบบ ต้องจัดให้มีการจัดการบริหาร Patch ที่เหมาะสมและทันท่วงที โดยพิจารณาดำเนินการในเรื่องอย่างน้อยดังต่อไปนี้

ก) มีการเก็บรวบรวมข้อมูลอุปกรณ์ทั้งหมดที่มีอยู่ในระบบ เช่น switch, router, firewall, server เป็นต้น โดยจะต้องมีรายละเอียดของอุปกรณ์นั้นใน physical เช่น serial number, รุ่นของอุปกรณ์ หรือ logical เช่น software version, windows version เป็นต้น

ข) วิเคราะห์ วางแผน การทำ Patch Management เพื่อปิดช่องโหว่โดยให้มีผลกระทบต่อการใช้งานจริงน้อยที่สุดและเป็นปัจจุบันที่สุด ซึ่งควรมีระดับความเสี่ยง ความสมควร และผลกระทบ เป็นปัจจัยขั้นต่ำในการวิเคราะห์

ค) ก่อนทำในระบบใช้งานจริง ต้องมีการทำการทดสอบการทำ Patch ในระบบทดสอบที่มีความคล้ายระบบใช้งานจริงที่สุด

ง) ต้องมีการทำ Backup อุปกรณ์ต่าง ๆ ก่อนเริ่มทำในระบบใช้งานจริง หากระบบใช้งานจริงมีความเปลี่ยนแปลงตลอดเวลา การ Backup ควรมีระยะเวลาห่างจากการทำ Patch ให้น้อยที่สุด

จ) ก่อนทำในระบบใช้งานจริง ต้องมีการแจ้งกำหนดการและระยะเวลาในการตรวจทานการใช้งานระบบใช้งานจริงและยืนยันการใช้งานกลับมายังผู้ดูแลระบบ เพื่อเป็นหลักฐานในด้านผลกระทบจากการทำ Patch ก่อนและหลังทุกครั้ง

ฉ) ต้องมีระบบการบริหารจัดการ Patch ที่เหมาะสม สามารถแจ้งเตือน รายงานสถานะปัจจุบัน ของทุกระบบที่มีอยู่ได้แม่นยำและถูกต้อง

ช) ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาหากมีการทำ Patch ในกรณีฉุกเฉิน และจะต้องมีการทำรายงานผลให้ผู้บังคับบัญชาทราบทันที

4.8.2.7.3 ผู้รับผิดชอบ

ก) ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

ข) ผู้ดูแลระบบ

4.8.2.8 การตั้งเวลาของอุปกรณ์ให้ตรงกัน (Clock Synchronization)

4.8.2.8.1 แนวนโยบาย

เพื่อตั้งเวลาของอุปกรณ์ประมวลผลสารสนเทศให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่กำหนดและเพื่อช่วยในการตรวจสอบหากอุปกรณ์ประมวลผลสารสนเทศของสำนักงานถูกบุกรุก

4.8.2.8.2 แนวทางปฏิบัติ

ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องร่วมกันกำหนดแหล่งเวลาอ้างอิงเดียวกัน เช่น ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ กรมอุทกศาสตร์กองทัพเรือ หรือสถาบันมาตรวิทยาแห่งชาติ เป็นต้น

4.8.2.8.3 ผู้รับผิดชอบ

ก) ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

ข) ผู้ดูแลระบบ

4.8.3 การป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ (Corporate Antivirus for Computer)

4.8.3.1 แนวนโยบาย

เพื่อป้องกันความเสียหายต่อซอฟต์แวร์และสารสนเทศของสำนักงานจากโปรแกรมที่ไม่ประสงค์ดี โดยจัดให้มีการตรวจจับและการป้องกันโปรแกรมที่ไม่ประสงค์ดี รวมถึงการกู้กลับคืนเมื่อได้รับความเสียหาย

4.8.3.2 แนวทางปฏิบัติ

ฝ่ายบริหารเทคโนโลยีดิจิทัล มีหน้าที่ในการบริหารจัดการ ควบคุม และวางแผนในการป้องกันความเสียหายต่อซอฟต์แวร์และสารสนเทศอันอาจเกิดจากโปรแกรมที่ไม่ประสงค์ดีโดยต้องดำเนินการอย่างน้อยต่อไปนี้

4.8.3.2.1 ติดตั้งซอฟต์แวร์หรืออุปกรณ์สำหรับตรวจจับและกำจัดโปรแกรมที่ไม่ประสงค์ดีเพื่อป้องกันซอฟต์แวร์สารสนเทศของสำนักงาน และมีการปรับปรุงซอฟต์แวร์หรืออุปกรณ์สำหรับตรวจจับและกำจัดโปรแกรมที่ไม่ประสงค์ดีให้ทันสมัยอยู่เสมอ ทั้งนี้ในการตรวจจับต้องครอบคลุมเรื่องอย่างน้อยดังต่อไปนี้

ก) ตรวจสอบไฟล์ที่อยู่ในอุปกรณ์ประมวลผลสารสนเทศ

ข) ตรวจสอบไฟล์ก่อนเปิดใช้งาน

ค) ตรวจสอบไฟล์ที่ส่งมากับข้อความอิเล็กทรอนิกส์ก่อนเปิดใช้งาน

ง) ตรวจสอบ Web Page ก่อนที่เข้าถึง

จ) ตรวจสอบสื่อบันทึกข้อมูลแบบพกพาก่อนใช้งาน

4.8.3.2.2 ควบคุมไม่ให้มีการติดตั้ง ปรับเปลี่ยนค่าการติดตั้ง และถอดถอนซอฟต์แวร์ในอุปกรณ์ประมวลผลสารสนเทศของสำนักงานโดยมิได้รับอนุญาตจากฝ่ายบริหารเทคโนโลยีดิจิทัล

4.8.3.2.3 จัดทำข้อแนะนำเพื่อให้ผู้ใช้งานดำเนินการเพื่อป้องกันโปรแกรมที่ไม่ประสงค์ดี

4.8.3.2.4 จัดทำกระบวนการเพื่อให้ผู้ใช้งานปฏิบัติตาม สำหรับผู้ใช้งานเมื่อตรวจพบโปรแกรมที่ไม่ประสงค์ดี ซึ่งรวมถึงการรายงาน และการแก้ปัญหาในเบื้องต้นจากการถูกโจมตีจากโปรแกรมที่ไม่ประสงค์ดี

4.8.3.2.5 จัดทำกระบวนการ และแผนความต่อเนื่องทางธุรกิจ เพื่อรับมือกับการถูกโจมตีโดยโปรแกรมที่ไม่ประสงค์ดี ทั้งนี้รวมถึงการเตรียมการต่าง ๆ ที่จำเป็นสำหรับการสำรองและกู้คืนซอฟต์แวร์และสารสนเทศ

4.8.3.2.6 ตรวจสอบการทำงานของซอฟต์แวร์หรืออุปกรณ์สำหรับตรวจจับและกำจัดโปรแกรมที่ไม่ประสงค์ดี เพื่อให้มั่นใจว่าการแจ้งเตือนและการให้ข้อมูลนั้นถูกต้อง

4.8.3.2.7 จัดทำข้อตกลงหรือสัญญาการให้บริการหลังการขายกับบริษัทคู่ค้าหรือเจ้าของผลิตภัณฑ์เพื่อปรับปรุงให้ซอฟต์แวร์หรืออุปกรณ์สำหรับตรวจจับและกำจัดโปรแกรมที่ไม่ประสงค์ดีมีความทันสมัยอยู่เสมอ

4.8.3.3 ผู้รับผิดชอบ

4.8.3.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.8.3.3.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

4.8.4 การสำรองข้อมูล (Back up)

4.8.4.1 แนวนโยบาย

เพื่อรักษาความถูกต้องครบถ้วนของสารสนเทศ และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ จึงควรให้มีการสำรองและกู้คืนข้อมูล (Information Backup and Recovery)

4.8.4.2 แนวทางปฏิบัติ

4.8.4.2.1 ผู้ดูแลระบบ ต้องกำหนดให้มีกระบวนการในการสำรองข้อมูล การทดสอบ และการกู้คืนข้อมูลที่เก็บไว้ ให้สอดคล้องกับความต้องการทางธุรกิจของสำนักงานและตามข้อกำหนดที่มีผลทางกฎหมายในเรื่องดังต่อไปนี้

ก) พิจารณาคัดเลือกและทบทวนระบบสารสนเทศที่มีความเหมาะสม กำหนดประเภทของข้อมูลและกำหนดความถี่ที่เหมาะสมอย่างน้อยปีละ 1 ครั้ง

ข) ประเภทของข้อมูลที่ควรสำรอง เช่น ระบบปฏิบัติการ บันทึกเหตุการณ์ของระบบปฏิบัติการ (Log) ระบบฐานข้อมูล ค่าการติดตั้งของอุปกรณ์ประมวลผลสารสนเทศ เป็นต้น

ค) ควรมีตารางการสำรองข้อมูล (ความถี่และช่วงเวลาในการสำรองข้อมูล) และระยะเวลาในการจัดเก็บ

ง) วิธีการสำรองข้อมูล เช่น การสำรองข้อมูลทั้งหมด การสำรองข้อมูลส่วนเพิ่ม และการสำรองข้อมูลที่แตกต่าง เป็นต้น

จ) ควรมีการสำรองข้อมูลแยกจากแหล่งข้อมูลเดิมโดยสิ้นเชิง

ฉ) การจัดเก็บสื่อบันทึกข้อมูลสำรองนอกพื้นที่ โดยพิจารณาตามระดับความมั่นคงปลอดภัยของสารสนเทศ เช่น ข้อมูลมีความมั่นคงปลอดภัยระดับสูง ควรมีระยะทางระหว่างสถานที่ตั้งของระบบที่ให้บริการจริงและสถานที่จัดเก็บสื่อบันทึกข้อมูลสำรองไม่น้อยกว่า 5 กิโลเมตร เป็นต้น

ช) การจัดเก็บสื่อบันทึกข้อมูลสำรองในสถานที่มีระดับการป้องกันด้านกายภาพ (Physical) สภาพแวดล้อมที่เหมาะสม โดยพิจารณาตามระดับความมั่นคงปลอดภัยของสารสนเทศ ทั้งนี้ให้มีการควบคุมเทียบเท่ากับสถานที่ตั้งของระบบที่ให้บริการจริง

ซ) ต้องจัดทำแผนและระบบสำรองสำหรับสารสนเทศ เพื่อเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน

ฌ) ต้องจัดทำแผนเตรียมความพร้อมกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

ญ) ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง

ฎ) การเข้ารหัสสื่อบันทึกข้อมูลสำรอง โดยพิจารณาตามระดับความมั่นคงปลอดภัยของสารสนเทศ

4.8.4.2.2 หน่วยงานผู้ดูแลระบบต้องทำการสำรองซอฟต์แวร์และค่าการติดตั้งก่อนที่จะมีการเปลี่ยนแปลงแก้ไข เพื่อให้มั่นใจว่าระบบสามารถกู้กลับคืนได้ในกรณีที่เกิดปัญหากับระบบหลังจากที่มีการเปลี่ยนแปลงแก้ไข ทั้งนี้ต้องจัดเก็บไว้อย่างน้อย 1 เวอร์ชั่นก่อนหน้า

4.8.4.2.3 ผู้ดูแลระบบต้องบันทึกกิจกรรมและผลการสำรองข้อมูล เช่น Backup Log Sheet เป็นต้น เพื่อให้มั่นใจว่ามีการปฏิบัติตามกระบวนการสำรองข้อมูลที่กำหนดไว้

4.8.4.2.4 ต้องปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ 1 ครั้ง

4.8.4.2.5 ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่าย จนเป็นเหตุต้องมีการดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบดำเนินการแก้ไข และรายงานปัญหาดังกล่าวต่อผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล หรือผู้ที่ได้รับหมอบหมายจากผู้จัดการฝ่ายทราบโดยด่วน

4.8.4.2.6 กรณีความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้รีบแจ้งผู้ใช้งานหรือผู้ดูแลระบบทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบ เมื่อการดำเนินการกู้คืนระบบเสร็จสิ้นสมบูรณ์

4.8.4.3 ผู้รับผิดชอบ

4.8.4.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.8.4.3.2 ผู้ดูแลระบบ

4.8.4.3.3 ผู้เป็นเจ้าของทรัพย์สินสารสนเทศ

4.8.5 การจัดการการเปลี่ยนแปลง (Change Management)

4.8.5.1 แนวนโยบาย

เพื่อควบคุมการเปลี่ยนแปลงระบบสารสนเทศ และบริการของสำนักงานให้มั่นใจว่าการเปลี่ยนแปลง ปรับปรุง แก้ไขระบบสารสนเทศ และบริการได้รับการควบคุมตลอดระยะเวลาที่มีการเปลี่ยนแปลง รวมถึงลดความเสี่ยงที่อาจเกิดความเสียหายจากการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบสารสนเทศและบริการ และเพื่อให้มีการแยกระบบให้บริการจริงออกจากระบบสำหรับพัฒนาและการทดสอบ เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบที่ให้บริการจริงโดยมิได้รับอนุญาต

4.8.5.2 แนวทางปฏิบัติ

4.8.5.2.1 ในการขอเปลี่ยนแปลงอุปกรณ์ประมวลผลสารสนเทศในระบบที่ให้บริการจริง ผู้ดูแลระบบต้องควบคุมให้มีการแจ้งความประสงค์และขออนุมัติการเปลี่ยนแปลง โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

ก) วัตถุประสงค์ในการเปลี่ยนแปลง

ข) รายละเอียดการเปลี่ยนแปลง

ค) วันที่ต้องการใช้งาน (Required Date)

ง) ประเมินผลกระทบที่อาจจะเกิดขึ้น รวมทั้งผลกระทบความมั่นคงปลอดภัยของการเปลี่ยนแปลงนั้น ๆ

จ) ผลการทดสอบ

ฉ) การอนุมัติการเปลี่ยนแปลง

ช) การสื่อสารการเปลี่ยนแปลงให้ผู้ที่เกี่ยวข้องรับทราบ

ซ) ขั้นตอนในการถอยกลับ (Fallback Process) รวมทั้งหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการกู้คืนระบบในกรณีที่การเปลี่ยนแปลงไม่เป็นไปตามแผน

4.8.5.2.2 ผู้ดูแลระบบ ต้องจัดให้มีการกำหนดหลักเกณฑ์และวิธีปฏิบัติสำหรับการขอและอนุมัติการเปลี่ยนแปลงกรณีฉุกเฉิน (Emergency Change) ซึ่งไม่สามารถรอการดำเนินงานตามขั้นตอนปกติได้

4.8.5.2.3 ผู้ดูแลระบบ ต้องจัดให้มีกระบวนการในการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log) เมื่ออุปกรณ์ประมวลผลสารสนเทศมีการเปลี่ยนแปลงเพื่อใช้ในการตรวจสอบ

4.8.5.2.4 หลังจากการเปลี่ยนแปลงเสร็จสิ้น ผู้อนุมัติการเปลี่ยนแปลง (Change Approver) ต้องจัดให้มีการประเมินผลหลังการเปลี่ยนแปลง (Post-Implementation Review) เพื่อให้มั่นใจว่าการเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ และนำผลของการประเมินมาใช้ในการปรับปรุงกระบวนการเปลี่ยนแปลงในอนาคต

4.8.5.2.5 จะต้องมีการปรับปรุงคู่มือในการใช้งาน หรือคู่มือในการอบรมผู้ใช้งาน เมื่อการขอเปลี่ยนแปลงนั้น ๆ มีผลต่อคู่มือฉบับเดิม

4.8.5.2.6 ฝ่ายบริหารเทคโนโลยีดิจิทัลต้องจัดให้มีการแยกระบบที่ให้บริการจริงออกจากระบบสำหรับการพัฒนาและการทดสอบ เพื่อป้องกันปัญหาที่อาจมีผลกระทบกับข้อมูล หรือการประมวลผลของระบบที่ให้บริการจริง โดยต้องจัดให้มีการควบคุมอย่างน้อยดังต่อไปนี้

ก) ให้มีการแยกระบบออกจากกันแบบกายภาพ (Physical) เช่น การแยกเครื่องคอมพิวเตอร์แม่ข่ายระบบสำหรับการพัฒนาหรือระบบสำหรับการทดสอบออกจากเครื่องคอมพิวเตอร์แม่ข่ายระบบที่ให้บริการจริง เป็นต้น ทั้งนี้ในกรณีที่ไม่สามารถทำได้ ต้องทำการแยกการทำงานแบบตรรกะ (Logical) เช่น แยก Directories หรือ Logical Partition ออกจากกัน เป็นต้น

ข) การเปลี่ยนแปลงแก้ไข Source Code ต้องดำเนินการบนระบบทดสอบโดยแยกจากระบบที่ใช้งานจริงเท่านั้น

ค) Source Code ที่พร้อมใช้งาน หรือ Source Code ที่ได้รับจากระบบเครือข่ายภายนอกที่ไม่น่าเชื่อถือต้องผ่านการตรวจสอบจากหน่วยงานที่รับผิดชอบ ถึงจะสามารถโอนย้ายไปยังส่วนที่ใช้งานจริงโดยผู้ที่ได้รับอนุญาตเท่านั้น

ง) การเปลี่ยนแปลง Source Code ที่ใช้งานจริงต้องมีการจัดเก็บอย่างเป็นระบบตามขั้นตอนการจัดระดับชั้นความลับของข้อมูลและมีการควบคุมเวอร์ชั่น

จ) จัดทำขั้นตอนปฏิบัติและการอนุมัติในการนำโปรแกรมคอมพิวเตอร์จากระบบสำหรับพัฒนาหรือระบบสำหรับทดสอบไปยังระบบที่ให้บริการจริง

ฉ) ระบบสำหรับทดสอบ ต้องจำลองมาจากระบบที่ให้บริการจริง โดยต้องให้มีความคล้ายคลึงกันมากที่สุด

ช) ในการเข้าระบบสำหรับการทดสอบ ต้องใช้บัญชีผู้ใช้งานที่แตกต่างระบบจริง หรือต้องมีข้อความหรือสัญลักษณ์ที่แสดงประเภทของระบบอย่างชัดเจน เพื่อลดความเสี่ยงจากการผิดพลาดในการเข้าถึงระบบ

ซ) ต้องมีการควบคุมข้อมูลในระบบทดสอบให้เป็นไปตามชั้นความลับ และการคุ้มครองข้อมูลส่วนบุคคล

4.8.5.2.7 การเปลี่ยนแปลงอุปกรณ์หรือสื่อที่ใช้ในการจัดเก็บข้อมูล ต้องทำการลบข้อมูลอย่างเหมาะสมตามระดับชั้นความลับของข้อมูลและตามความคุ้มครองข้อมูลส่วนบุคคลการดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจ จำต้องขออนุญาตเจ้าของลิขสิทธิ์เพื่อเปลี่ยนแปลงแก้ไข หรือมอบให้ผู้แทนดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจให้

4.8.5.2.8 ซอฟต์แวร์แพ็กเกจที่แก้ไขจะต้องได้รับการทดสอบและตรวจสอบถึงผลกระทบและความเสี่ยงที่อาจเกิดขึ้นก่อนการนำมาใช้งาน

4.8.5.3 ผู้รับผิดชอบ

4.8.5.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.8.5.3.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

4.8.5.3.3 ผู้ร้องขอการเปลี่ยนแปลง

4.8.6 การจัดการการให้บริการของหน่วยงานภายนอก (Third Party Service Delivery Management)

4.8.6.1 แนวนโยบาย

เพื่อบริหารจัดการการให้บริการของหน่วยงานภายนอกให้มีระดับความมั่นคงปลอดภัยและระดับการบริการเป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างสำนักงานกับหน่วยงานภายนอก

4.8.6.2 แนวทางปฏิบัติ

การบริหารจัดการการให้บริการของหน่วยงานภายนอกประกอบไปด้วยเรื่องดังต่อไปนี้

4.8.6.2.1 การให้บริการโดยหน่วยงานภายนอก (Service Delivery)

ก) ผู้ว่าจ้างต้องกำกับดูแลให้หน่วยงานภายนอกปฏิบัติตามนโยบายและมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ตลอดจนคำสั่งหรือระเบียบสำนักงานที่เกี่ยวข้องรวมถึงการควบคุมระดับและรายละเอียดของการบริการให้เป็นไปตามข้อตกลงหรือสัญญาการให้บริการ

ข) ผู้ว่าจ้างต้องประเมินการให้บริการของหน่วยงานภายนอกอย่างสม่ำเสมอหรือก่อนต่ออายุข้อตกลงหรือสัญญาการให้บริการ

ค) หน่วยงานภายนอกต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุม หรือสอบทานการให้บริการของหน่วยงานภายนอกได้อย่างเข้มงวด และมั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

4.8.6.2.2 การเฝ้าระวังและสอบทานการให้บริการโดยหน่วยงานภายนอก (Monitoring and Review of Third Party Services)

ก) ผู้ว่าจ้างมีหน้าที่รับผิดชอบในการบริหารจัดการความสัมพันธ์กับหน่วยงานภายนอกและกำหนดให้หน่วยงานภายนอกมีการสอบทานการปฏิบัติงานให้เป็นไปตามข้อตกลง หรือสัญญาการให้บริการ

ข) ผู้ว่าจ้างต้องเฝ้าระวังและสอบทานการให้บริการของหน่วยงานภายนอก เช่น การบริการกับข้อตกลงที่ได้จัดทำไว้ รายงานการให้บริการของหน่วยงานภายนอก

เพื่อสรุปการดำเนินงานตามเงื่อนไข การบันทึกเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดจากข้อตกลง เป็นต้น

4.8.6.2.3 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ (Managing Changes to Third Party Services)

ผู้ว่าจ้างต้องทำการทบทวนหรือแก้ไขข้อตกลง หรือสัญญาการให้บริการกับหน่วยงานภายนอกเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก โดยประเมินจากผลกระทบที่เกิดขึ้นเมื่อมีการเปลี่ยนแปลงโดยสำนักงาน เช่น การแก้ไขนโยบาย มาตรการและขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เป็นต้น หรือมีการเปลี่ยนแปลงโดยหน่วยงานภายนอก เช่น การใช้เทคโนโลยีใหม่ การเปลี่ยนคู่ค้า หรือคู่สัญญาใหม่ เป็นต้น

4.8.6.3 ผู้รับผิดชอบ

4.8.6.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.8.6.3.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

4.8.6.3.3 หน่วยงานภายนอก

4.8.7 การจัดการทรัพยากรระบบ (Capacity Management)

4.8.7.1 แนวนโยบาย

เพื่อให้มีการบริหารจัดการขีดความสามารถของอุปกรณ์ประมวลผลสารสนเทศให้เพียงพอต่อการใช้งานและมีประสิทธิภาพทั้งในปัจจุบันและอนาคต

4.8.7.2 แนวทางปฏิบัติ

4.8.7.2.1 ผู้ดูแลระบบและฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องจัดให้มีการประมาณการ หรือสำรวจความต้องการใช้งานอุปกรณ์ประมวลผลสารสนเทศในอนาคต เพื่อให้รองรับความต้องการด้านธุรกิจของสำนักงานและงบประมาณที่เหมาะสม

4.8.7.2.2 ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องรวบรวมความต้องการสำหรับการใช้งานอุปกรณ์ประมวลผลสารสนเทศ พร้อมทั้งสำรวจความสามารถในการให้บริการในปัจจุบัน เพื่อจัดเตรียมโครงสร้างพื้นฐานด้านสารสนเทศในส่วนที่รับผิดชอบให้เพียงพอต่อความต้องการ โดยพิจารณาในเรื่องอย่างน้อยต่อไปนี้

ก) ความสามารถในการประมวลผล (Processing Power)

ข) ความต้องการหน่วยความจำ (Memory Requirement)

ค) ปริมาณการใช้งานและความจุของหน่วยเก็บข้อมูล (Disk Usage and Size)

ง) ปริมาณข้อมูลในระบบเครือข่ายที่สามารถรองรับได้ (Network Traffic Load)

จ) จำนวนและประเภทของสิทธิการใช้ซอฟต์แวร์ (Software License)

ฉ) การตั้งค่าการติดตั้งของระบบ (System Configuration)

4.8.7.2.3 ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องจัดให้มีการเฝ้าระวังการใช้งานของอุปกรณ์ประมวลผลสารสนเทศ (Utilization) และทำการปรับแต่ง เพื่อให้อุปกรณ์ประมวลผลสารสนเทศสามารถทำงานได้อย่างมีประสิทธิภาพ

4.8.7.2.4 ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องจัดทำรายงานการใช้งานอุปกรณ์ประมวลผลสารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อรองรับการประมาณการในอนาคตได้อย่างเหมาะสม

4.8.7.3 ผู้รับผิดชอบ

4.8.7.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.8.7.3.2 ผู้ดูแลระบบ

4.9 การบริหารจัดการด้านการสื่อสาร (Communication Management)

วัตถุประสงค์

เพื่อให้การบริหารจัดการด้านการสื่อสารด้านสารสนเทศเป็นไปอย่างถูกต้องและรักษาไว้ซึ่งความมั่นคงปลอดภัยด้านสารสนเทศ

แนวนโยบายและแนวปฏิบัติ

4.9.1 การใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

4.9.1.1 แนวนโยบาย

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใด ๆ ที่สร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์เป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

4.9.1.2 แนวทางปฏิบัติ

หน่วยงานผู้ดูแลระบบ ต้องจัดให้มีการควบคุมการรับส่งข้อความทางจดหมายอิเล็กทรอนิกส์ให้มั่นคงปลอดภัย โดยดำเนินการอย่างน้อยดังต่อไปนี้

4.9.1.2.1 ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของสำนักงานให้เหมาะสมกับการใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

4.9.1.2.2 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของสำนักงาน

4.9.1.2.3 ผู้ดูแลระบบ ต้องจัดให้มีการเข้ารหัสเพื่อรักษาความลับของข้อมูลตามระดับความมั่นคงปลอดภัยของสารสนเทศ

4.9.1.2.4 ผู้ดูแลระบบ ต้องจัดให้มีการยืนยันและพิสูจน์แหล่งที่มาของข้อความ มีกระบวนการเพื่อให้มั่นใจว่าผู้รับได้รับข้อความ และมีการพิสูจน์ความถูกต้องครบถ้วนของข้อความตามระดับความมั่นคงปลอดภัยของสารสนเทศ

4.9.1.2.5 สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) สำหรับการเข้าระบบจดหมายอิเล็กทรอนิกส์ และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที หรือผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านครั้งแรก

4.9.1.2.6 การกำหนดรหัสผ่านที่ดี (Good Password) ควรปฏิบัติตามนโยบายบริหารจัดการรหัสผ่านของสำนักงาน

4.9.1.2.7 ผู้ดูแลระบบ ควรจำกัดการป้อนรหัสผ่านในกรณีป้อนรหัสผ่านผิดพลาดได้ไม่เกิน 5 ครั้ง

4.9.1.2.8 ผู้ใช้งาน ควรออกจากระบบทุกครั้งเมื่อการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น เพื่อป้องกันบุคคลอื่นแอบอ้างและเข้าใช้งาน

4.9.1.2.9 ผู้ใช้งาน ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

4.9.1.2.10 ผู้ดูแลระบบ ควรมีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่านอย่างน้อย 90 วัน หรือตามความเหมาะสม

4.9.1.2.11 ผู้ใช้งาน ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อองค์กรหรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์

4.9.1.2.12 ผู้ใช้งาน ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของบัญชี และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

4.9.1.2.13 ผู้ใช้งาน ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe เป็นต้น

4.9.1.2.14 ผู้ใช้งาน หากได้รับจดหมายอิเล็กทรอนิกส์จากผู้ส่งที่ไม่แน่ใจหรือไม่คุ้นเคย หรือเป็นที่น่าสงสัย จะต้องแจ้งผู้ดูแลระบบโดยทันที และไม่ทำการเปิดดูข้อความภายในหรือส่งต่อจดหมายอิเล็กทรอนิกส์

4.9.1.2.15 ผู้ใช้งาน ไม่ควรทำการส่งข้อมูลที่เป็นความลับผ่านช่องทางจดหมายอิเล็กทรอนิกส์ หากมีความจำเป็นผู้ใช้งานจะต้องทำการกำหนดและใส่รหัสผ่านเพื่อป้องกันการโจรกรรมข้อมูลผ่านช่องทางจดหมายอิเล็กทรอนิกส์ และจะต้องไม่ใส่หรือระบุข้อความลับใด ๆ ลงในจดหมายอิเล็กทรอนิกส์ และต้องแจ้งรหัสผ่านในการเปิดดูข้อมูลโดยช่องทาง การสื่อสารอื่น ๆ หรือผ่านช่องทางจดหมายอิเล็กทรอนิกส์ฉบับแยกจากฉบับที่มีข้อมูล

4.9.1.2.16 มีการบริหารจัดการการเข้าถึงของผู้ใช้งานอย่างเหมาะสม เพื่อควบคุมการเข้าถึงระบบเฉพาะผู้ที่ได้รับอนุญาต

4.9.1.2.17 ผู้ดูแลระบบ จัดทำเงื่อนไขการใช้งานข้อความจดหมายอิเล็กทรอนิกส์และสื่อสารให้ผู้ใช้งานรับทราบ

4.9.1.2.18 มีการบันทึกเหตุการณ์ที่เกี่ยวข้องการใช้งาน (Audit Log) และมีการตรวจสอบการใช้งานระบบอย่างสม่ำเสมอ

4.9.1.2.19 มีการปฏิบัติที่มีผลตามข้อกำหนดทางกฎหมาย

4.9.1.3 ผู้รับผิดชอบ

4.9.1.2.20 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.9.1.2.21 ผู้ดูแลระบบ

4.9.1.2.22 ผู้ใช้งานจดหมายอิเล็กทรอนิกส์

4.9.2 การใช้งานอินเทอร์เน็ต (Internet)

4.9.2.1 แนวนโยบาย

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

4.9.2.2 แนวทางปฏิบัติ

4.9.2.2.1 ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่ออินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่สำนักงานจัดสรรไว้เท่านั้น

4.9.2.2.2 เครื่องคอมพิวเตอร์ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการปิดช่องโหว่ของระบบปฏิบัติการ Web Browser สม่ำเสมอ

4.9.2.2.3 ในการรับข้อมูลทางอินเทอร์เน็ตจะต้องมีการตรวจสอบไวรัส โดยโปรแกรมป้องกันไวรัสก่อนการใช้งานทุกครั้ง

4.9.2.2.4 ห้ามใช้และห้ามเผยแพร่ข้อมูลในเครือข่ายของสำนักงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเพื่อการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม หรือข้อมูลที่ละเมิดสิทธิ์ของบุคคลอื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับสำนักงาน

4.9.2.2.5 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด หรือภายที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

4.9.2.2.6 ห้ามผู้ใช้งาน เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสำนักงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

4.9.2.2.7 ห้ามกระทำการติดตั้ง Download/Upload ซอฟต์แวร์หรือโปรแกรม ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ที่ละเมิดทรัพย์สินทางปัญญาผ่านช่องทางอินเทอร์เน็ตของสำนักงาน

4.9.2.2.8 ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยของข้อมูลของสำนักงาน

4.9.2.2.9 ผู้ใช้งานมีหน้าที่ต้องตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้

4.9.2.2.10 ในกรณีที่ผู้ใช้งานพบเว็บไซต์ที่ไม่เหมาะสม เป็นภัยต่อความมั่นคงปลอดภัย ขัดต่อศีลธรรม ขัดต่อชาติ ศาสนา พระมหากษัตริย์ เป็นภัยต่อสังคม หรือกระทบต่อความปลอดภัยของสำนักงาน ผู้ใช้งานต้องยกเลิกการติดต่อกับเว็บไซต์ดังกล่าว และแจ้งฝ่ายบริหารเทคโนโลยีดิจิทัล ทราบทันที

4.9.2.2.11 ในการใช้งาน Social Media หรือ Web board ของผู้ใช้งานเพื่อแลกเปลี่ยนข้อมูลในการปฏิบัติงานสามารถกระทำได้โดยจะต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของสำนักงาน โดยความคิดเห็นนั้นให้ถือว่าเป็นความคิดเห็นส่วนบุคคลของผู้ใช้งานไม่ใช่ความคิดเห็นจากสำนักงาน

4.9.2.2.12 ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสีย ต่อชื่อเสียงของสำนักงาน การทำลายความสัมพันธ์กับลูกค้า พันธมิตรธุรกิจ และเจ้าหน้าที่ของหน่วยงานอื่น ๆ

4.9.2.2.13 หลังใช้งานอินเทอร์เน็ตแล้ว ให้ออกจากระบบ และปิด Web Browser เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

4.9.2.2.14 ฝ่ายบริหารเทคโนโลยีดิจิทัล สงวนสิทธิ์ในการเข้าตรวจสอบ เก็บหลักฐาน และดำเนินการอันสมควร หากพบว่ามีการละเมิดนโยบายการใช้งานอินเทอร์เน็ต

4.9.2.3 ผู้รับผิดชอบ

4.9.2.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.9.2.3.2 ผู้ดูแลระบบ

4.9.2.3.3 ผู้ใช้งานอินเทอร์เน็ต

4.9.3 การใช้สื่อสังคมออนไลน์ (social media)

4.9.3.1 แนวนโยบาย

เพื่อให้เกิดความเข้าใจและใช้งานสื่อสังคมออนไลน์ (Social Media) ได้อย่างถูกต้องและเป็นไปตามระเบียบของสำนักงาน เพื่อหลีกเลี่ยงผลกระทบและความเสียหายที่อาจเกิดขึ้นได้แก่สำนักงาน และผู้ใช้งาน

4.9.3.2 แนวทางปฏิบัติ

4.9.3.2.1 ผู้ใช้งาน ต้องพึงตระหนักถึง ข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง ข้อมูล ต่าง ๆ หรือความคิดเห็นที่เผยแพร่บนสื่อสังคมออนไลน์ เป็นสื่อที่สามารถเข้าถึงได้โดยสาธารณะ ผู้เผยแพร่ต้องรับผิดชอบทั้งทางด้านสังคม และด้านกฎหมาย

4.9.3.2.2 ผู้ใช้งาน ต้องไม่ใช้สื่อสังคมออนไลน์ในการเผยแพร่ความคิดเห็นที่อาจกระตุ้นหรือนำไปสู่การยั่วยุ การโต้แย้งที่รุนแรง หรือขัดต่อจริยธรรม เช่น เรื่องเกี่ยวกับการเมือง ศาสนา ความมั่นคงแห่งชาติ และชนชั้นในชาติ เป็นต้น หรือเผยแพร่

เนื้อหาที่ขัดต่อกฎหมาย ศีลธรรม กระทบกระเทือนหรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม

4.9.3.2.3 ผู้ใช้งาน ต้องระมัดระวังการใช้งานที่ผิดรูปแบบหรือจุดประสงค์โดยละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และพระราชบัญญัติความคุ้มครองข้อมูลส่วนบุคคล

4.9.3.2.4 ผู้ใช้งาน ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อความของตน ควรให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน และหากมีความจำเป็นต้องใช้งานอันมีลิขสิทธิ์เพื่อประกอบในการทำสื่อสังคมออนไลน์ จะต้องได้รับอนุญาตจากเจ้าของลิขสิทธิ์ก่อนการเผยแพร่

4.9.3.2.5 ผู้ใช้งาน หากประสงค์ใช้สื่อสังคมออนไลน์เพื่อเผยแพร่ข้อมูลเกี่ยวกับสำนักงาน ควรแยกบัญชีผู้ใช้งานระหว่างการใช้เพื่อเรื่องส่วนตัว และเรื่องหน้าที่ในงานออกจากกัน และหากประสงค์ใช้งานสื่อสังคมออนไลน์ที่แสดงสังกัดหน่วยงานภายในของสำนักงาน ต้องแจ้งให้ผู้บังคับบัญชาทราบก่อนทุกครั้ง และผู้เผยแพร่ต้องแสดงชื่อ ตำแหน่ง และสังกัด ให้ชัดเจน เพื่อความน่าเชื่อถือและเพื่อให้ผู้ติดตามสามารถใช้ดุลพินิจในการติดตามได้

4.9.3.2.6 ผู้ใช้งาน ต้องพึงระวังการใช้ถ้อยคำ การใช้ภาษาที่อาจก่อให้เกิดความเข้าใจคลาดเคลื่อน เข้าข่ายการดูหมิ่น หมิ่นประมาทบุคคลอื่น หรือละเมิดสิทธิส่วนบุคคล และควรใช้ภาษาให้ถูกต้อง สุภาพ และสร้างสรรค์

4.9.3.2.7 งดการใช้สื่อสังคมออนไลน์เปิดเผย วิพากษ์ วิจารณ์ ตลอดจนแสดงความคิดเห็นในเรื่องที่เป็นข้อมูลภายใน ข้อมูลที่มีความสำคัญหรือเป็นความลับของสำนักงาน ซึ่งอาจส่งผลกระทบต่อสำนักงานได้

4.9.3.2.8 ต้องไม่ใช้งานสื่อสังคมออนไลน์ไม่ว่าด้วยช่องทางใด ๆ ณ เวลาใด ณ สถานที่ใด เพื่อด่าทอให้ร้าย ดูหมิ่น หมิ่นประมาท รวมถึงการสื่อสารเพื่อวิจารณ์การบังคับบัญชา การบริหารกิจการของสำนักงาน ผู้บริหารและผู้บังคับบัญชาทุกระดับชั้น ตลอดจนผู้ใต้บังคับบัญชา ผู้ร่วมงาน ผู้ใช้บริการ ผู้ให้บริการ โดยการกระทำเช่นว่านั้นอาจหรือก่อให้เกิดความเสียหายทั้งด้านชื่อเสียง ภาพลักษณ์ การยอมรับนับถือไม่ว่าทางตรงหรือทางอ้อมแก่สำนักงาน หรือบุคคลอื่นดังกล่าวข้างต้น

4.9.3.2.9 การแสดงความคิดเห็นใด ๆ (Comment) ที่มีการเผยแพร่บนสื่อสังคมออนไลน์อาจกระทำได้แต่ต้องเป็นการกระทำโดยสุจริตและไม่ละเมิดสิทธิของผู้อื่น โดยผู้แสดงความคิดเห็นจะต้องรับผิดชอบในการแสดงความคิดเห็น และการเผยแพร่บนสื่อสังคมออนไลน์ทุกกรณี

4.9.3.2.10 หากพบว่ามีข้อความบนสื่อสังคมออนไลน์ที่มีการบิดเบือนข้อเท็จจริง ประเด็นขัดแย้ง หรือ ข้อความอื่นใดซึ่งอาจทำให้เกิดความเสื่อมเสียชื่อเสียงของสำนักงาน ให้พนักงานผู้ดูแลการใช้งานแจ้งต่อผู้บังคับบัญชาของตน

หรือฝ่าย/สำนัก ที่เกี่ยวข้องกับเรื่องนั้น ๆ ทราบ และทั้งนี้ขอให้หน่วยงานที่รับผิดชอบมอบหมายให้มีผู้เฝ้าระวังและตรวจตราข่าวสารในทุกช่องทางที่อาจส่งผลกระทบต่อชื่อเสียงของสำนักงานได้

4.9.3.2.11 ป้องกันการถูกละเมิดความเป็นส่วนตัวโดยศึกษาการใช้ “การตั้งค่าความเป็นส่วนตัว” หรือ “Privacy Setting” ให้เข้าใจเป็นอย่างดี และปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมกับบริบท การถูกละเมิดความเป็นส่วนตัวโดยไม่เหมาะสม นอกเหนือจากส่งผลกระทบต่อตนเองแล้ว อาจส่งผลต่อสำนักงานได้ด้วย

4.9.3.2.12 ไม่เผยแพร่ข้อความที่เป็นข่าวลือ ข่าวไม่ปรากฏที่มา หรือข้อมูลที่เป็นเพียงการคาดเดาเป็นเท็จ หรือข้อมูลที่ก่อให้เกิดความเข้าใจผิด หรือการยั่วยุให้เกิดความขัดแย้งขึ้นภายในสำนักงาน

4.9.3.2.13 การนำเสนอหรือเผยแพร่ข้อมูลต่าง ๆ ผ่านสื่อสังคมออนไลน์ หากเกิดความผิดพลาด ซึ่งอาจก่อให้เกิดผลกระทบต่อสำนักงานหรือบุคคลอื่นได้ ต้องแสดงความรับผิดชอบและดำเนินการแก้ไขในทันที

4.9.3.3 ผู้รับผิดชอบ

4.9.3.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.9.3.3.2 ผู้ดูแลระบบ

4.9.3.3.3 ผู้ใช้งานสื่อสังคมออนไลน์

4.9.4 การรับส่งข้อมูลสารสนเทศ (Information Transfer)

เพื่อรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในสำนักงานและระหว่าง ระบบเครือข่ายภายในสำนักงานกับระบบเครือข่ายภายนอก โดยประกอบไปด้วยเรื่องดังต่อไปนี้

4.9.4.1 การควบคุมการรับส่งข้อมูลสารสนเทศ (Information Transfer Control)

4.9.4.1.1 แนวนโยบาย

เพื่อให้มีการควบคุมเพื่อป้องกันปัญหาของการรับส่งข้อมูลสารสนเทศภายในสำนักงาน และระหว่างสำนักงานกับหน่วยงานภายนอก โดยผ่านช่องทางการสื่อสารทุกชนิด

4.9.4.1.2 แนวทางปฏิบัติ

ก) ต้องจัดให้มีการควบคุมการรับส่งข้อมูลสารสนเทศให้สอดคล้องกับระดับความมั่นคงปลอดภัยของสารสนเทศ

ข) ต้องจัดให้มีการป้องกันการดักจับข้อมูลที่รับส่ง การทำสำเนา การเปลี่ยนแปลงแก้ไข การส่งผิดเส้นทาง (Mis-Routing) และการถูกทำลาย

ค) ต้องมีการตรวจจับและป้องกันโปรแกรมที่ไม่ประสงค์ดี

ง) ต้องมีการป้องกันข้อมูลที่สำคัญในรูปสื่ออิเล็กทรอนิกส์ที่ส่งผ่านในรูปแบบของเอกสารแนบ และการควบคุมการส่งต่อ เช่น การส่งต่อจดหมาย

อิเล็กทรอนิกส์ภายในสำนักงานไปจดหมายอิเล็กทรอนิกส์ภายนอกโดยอัตโนมัติ

จ) ต้องมีการควบคุมในช่องทางการสื่อสารแบบไร้สาย โดยจะต้องคำนึงถึงความเสี่ยงเฉพาะด้านที่เกี่ยวข้อง

ฉ) ต้องมีการกำกับดูแลหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของพนักงาน ลูกจ้าง หน่วยงานภายนอก บุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานให้สำนักงานและนักศึกษาฝึกงาน

ช) ต้องมีการควบคุมการใช้เทคนิคการเข้ารหัส เช่น เพื่อป้องกันสารสนเทศที่เป็นความลับ เพื่อให้สารสนเทศมีความถูกต้องและระบุตัวตนได้

ซ) ต้องมีการเก็บรักษาและทำลายเอกสารเพื่อให้เป็นไปตามข้อกำหนดที่มีผลทางกฎหมาย

ฌ) ต้องมีการป้องกันอุปกรณ์ประมาลผลสารสนเทศที่ไม่มีผู้ดูแล

4.9.4.1.3 ผู้รับผิดชอบ

ก) ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

ข) ผู้ดูแลระบบ

ค) ผู้เป็นเจ้าของทรัพย์สินสารสนเทศ

4.9.4.2 ข้อตกลงในการรับส่งข้อมูลสารสนเทศ (Transfer Agreement)

4.9.4.2.1 แนวนโยบาย

เพื่อจัดทำข้อตกลงในการรับส่งข้อมูลสารสนเทศและซอฟต์แวร์ระหว่างสำนักงานกับหน่วยงานภายนอกอย่างเป็นลายลักษณ์อักษร

4.9.4.2.2 แนวทางปฏิบัติ

ก) ในการรับส่งข้อมูลสารสนเทศและซอฟต์แวร์ของสำนักงานกับหน่วยงานภายนอก ต้องได้รับการอนุมัติจากหัวหน้าหน่วยงาน

ข) หัวหน้าหน่วยงาน ต้องจัดให้มีการทำข้อตกลงหรือสัญญากับหน่วยงานภายนอก กรณีมีการรับส่งข้อมูลสารสนเทศและซอฟต์แวร์ โดยต้องพิจารณาข้อกำหนดหรือเงื่อนไขอย่างเหมาะสมและอย่างน้อยดังต่อไปนี้

- การรักษาความลับของสารสนเทศและซอฟต์แวร์
- ข้อตกลงในการฝากข้อมูลหรือ Source Code ไว้ที่หน่วยงานภายนอก ซึ่งไม่ใช่คู่สัญญาเพื่อให้สำนักงานสามารถเข้าถึงข้อมูลดังกล่าวได้ในกรณีที่หน่วยงานคู่สัญญาหรือหน่วยงานที่ได้รับการว่าจ้างให้พัฒนาซอฟต์แวร์ไม่สามารถให้บริการได้ (Escrow Agreement)
- หน้าที่ความรับผิดชอบของสำนักงาน และคู่สัญญาในการควบคุมสารสนเทศและซอฟแวร์ระหว่างการส่งผ่าน (Transmission) การกระจายต่อ (Dispatch) และการได้รับ (Receipt) สารสนเทศ

- ความรับผิดชอบ และการใช้ เมื่อสารสนเทศสูญหาย ถูกแก้ไข หรือถูกเปิดเผยโดยมิชอบ
- กรรมสิทธิ์ การป้องกันสิทธิและทรัพย์สินทางปัญญาของสารสนเทศและซอฟต์แวร์
- กำหนดข้อตกลงร่วมกันในการจัดทำป้ายชื่อ ตามระดับความมั่นคงปลอดภัยของสารสนเทศ เพื่อให้มีความเข้าใจตรงกันและสามารถดำเนินการป้องกันได้อย่างเหมาะสม
- มาตรฐานทางเทคนิคอื่น ๆ สำหรับ รูปแบบของข้อมูล การจัดเก็บ การประมวลผล และการส่งสารสนเทศที่มีการรับส่งข้อมูล
- ขั้นตอนปฏิบัติงานสำหรับการรับส่งข้อมูลสารสนเทศ
- กระบวนการติดตาม (Traceability) และป้องกันการปฏิเสธความรับผิด (Non-Repudiation)

4.9.4.2.3 ผู้รับผิดชอบ

ก) ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล
ข) ผู้ดูแลระบบ
ค) ผู้เป็นเจ้าของทรัพย์สินสารสนเทศ
ง) หัวหน้าหน่วยงาน

2.9.4.3 การรับส่งสื่อบันทึกข้อมูล (Physical Media in Transit)

4.9.4.3.1 แนวนโยบาย

เพื่อป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยมิได้รับอนุญาต การใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเกิดความเสียหาย

4.9.4.3.2 แนวทางปฏิบัติ

ก) ต้องมีการใช้บริการผู้จัดส่งที่มีความน่าเชื่อถือซึ่งได้รับอนุญาตเท่านั้น
ข) กำหนดให้มีกระบวนการในการระบุตัวตนเพื่อให้สามารถติดตามเจ้าหน้าที่ผู้จัดส่งได้
ค) มีการบรรจุหีบห่ออย่างเหมาะสมและเป็นไปตามคำแนะนำของผู้ผลิต เพื่อป้องกันความเสียหายทางกายภาพ ที่อาจเกิดขึ้นในช่วงขนส่ง เช่น การถูกความร้อน ความชื้น หรือคลื่นแม่เหล็กไฟฟ้า เป็นต้น
ง) มีการป้องกันการเปิดเผยหรือดัดแปลงสารสนเทศอย่างเหมาะสม เช่น การเปิดผนึกและลงนามกำกับ การใช้บรรจุภัณฑ์ที่สามารถล็อคได้ และการส่งมอบด้วยตนเอง เป็นต้น
จ) หัวหน้าหน่วยงาน ต้องจัดให้มีกระบวนการรับส่งที่เหมาะสมเพื่อให้มั่นใจว่า ผู้รับได้รับของถูกต้องครบถ้วน โดยพิจารณาตามระดับความมั่นคงปลอดภัยของสารสนเทศ

4.9.4.3.3 ผู้รับผิดชอบ

ก) ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล
ข) ผู้ดูแลระบบ

ค) ผู้เป็นเจ้าของทรัพย์สินสารสนเทศ

ง) หัวหน้าหน่วยงาน

4.9.4.4 ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information System)

4.9.4.4.1 แนวนโยบาย

เพื่อป้องกันสารสนเทศที่มีการรับส่งข้อมูลระหว่างแอพพลิเคชันทางธุรกิจ

4.9.4.4.2 แนวทางปฏิบัติ

ก) จัดให้มีการควบคุมทางกายภาพ เพื่อป้องกันการเข้าถึงอุปกรณ์ที่ให้บริการข้อความทางอิเล็กทรอนิกส์โดยได้รับอนุญาต

ข) จัดให้มีการบริหารจัดการการเข้าถึงของผู้ใช้อย่างเหมาะสม เพื่อควบคุมการเข้าถึงระบบเฉพาะผู้ที่ได้รับอนุญาต

ค) จัดทำหลักเกณฑ์การใช้งานแอพพลิเคชันทางธุรกิจและทำการสื่อสารให้ผู้ใช้งานทราบเรื่องการรับส่งข้อมูลสารสนเทศระหว่างแอพพลิเคชัน

ง) จัดให้มีการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งาน และมีการตรวจสอบการใช้งานระบบอย่างสม่ำเสมอ

จ) จัดให้มีการปฏิบัติตามข้อกำหนดที่มีผลทางกฎหมาย เช่น การสำรองข้อมูล การควบคุมการเปลี่ยนแปลง และการบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ เป็นต้น

ฉ) ต้องมีการเข้ารหัสเพื่อรักษาความลับของข้อมูล ตามระดับความมั่นคงปลอดภัยของสารสนเทศ

ช) ต้องจัดให้มีการยืนยันและพิสูจน์ตัวตนของแหล่งที่มาของสารสนเทศและพิสูจน์ความถูกต้องครบถ้วนของสารสนเทศที่ส่งระหว่างแอพพลิเคชัน ตามระดับความมั่นคงปลอดภัยของสารสนเทศ

ซ) กำหนดให้ผู้ดูแลระบบตั้งค่าความมั่นคงปลอดภัย สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายของบริการที่สำคัญของสำนักงาน ตามมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security baseline configuration standards) ก่อนที่จะมีการเชื่อมต่อ การเปลี่ยนแปลง หรือปรับปรุงระบบสารสนเทศ และกำหนดรอบการตรวจสอบการตั้งค่าความมั่นคงปลอดภัยอย่างน้อยปีละ 1 ครั้ง

4.9.4.4.3 ผู้รับผิดชอบ

ก) ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

ข) ผู้ดูแลระบบ

4.10 การจัดหา การพัฒนา และการบำรุงรักษา ระบบสารสนเทศ (Information System Acquisition, Development and Maintenance)

วัตถุประสงค์

เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบตลอดวงจรการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่ายสาธารณะ

แนวนโยบายและแนวทางปฏิบัติ

4.10.1 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in Development and Support Processes)

4.10.1.1 กฎเกณฑ์ในการพัฒนาซอฟต์แวร์และระบบ ต้องมีการกำหนดขั้นตอนการปฏิบัติงาน เพื่อเป็นแนวปฏิบัติสำหรับการพัฒนาระบบของสำนักงาน

4.10.1.2 การเปลี่ยนแปลงระบบหรือการพัฒนาระบบ ต้องมีการควบคุมโดยปฏิบัติตามนโยบายการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ (Change Management) และขั้นตอนการปฏิบัติงานการบริหารจัดการการเปลี่ยนแปลง

4.10.1.3 เมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ ระบบที่สำคัญต้องมีการทบทวนและทดสอบเพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงาน หรือต่อความมั่นคงปลอดภัยของสำนักงาน

4.10.1.4 สำนักงานต้องพิจารณาสภาพแวดล้อมที่เหมาะสมต่อการพัฒนาระบบที่มีความมั่นคงปลอดภัย ได้แก่ พื้นที่ปฏิบัติงานไม่อยู่พื้นที่พลุกพล่าน หรือเข้าถึงได้ง่าย

4.10.1.5 ต้องจัดให้มีการแยกระบบที่ให้บริการจริงออกจากระบบสำหรับการพัฒนาและการทดสอบ เพื่อป้องกันปัญหาที่อาจมีผลกระทบกับข้อมูล หรือการประมวลผลของระบบที่ให้บริการจริง

4.10.1.6 การจ้างพัฒนาระบบจากผู้ให้บริการภายนอก ต้องมีการควบคุม เฝ้าระวัง ติดตามการดำเนินงานอย่างใกล้ชิดเพื่อให้เป็นไปตามขอบเขตการดำเนินงาน และสอดคล้องกับนโยบาย ขั้นตอนปฏิบัติของสำนักงานที่กำหนดไว้

4.10.1.7 ผู้พัฒนาระบบควรมีการจัดทำคู่มือหรือขั้นตอนการทดสอบระบบ และจะต้องมีการปรับปรุงคู่มือในการใช้งาน หรือคู่มือในการอบรมผู้ใช้งาน เมื่อการขอเปลี่ยนแปลงนั้น ๆ มีผลต่อคู่มือฉบับเดิม

4.10.1.8 ควรมีการทดสอบการใช้งานระบบ เพื่อเป็นการสอบทานคู่มือหรือขั้นตอนการทดสอบระบบ รวมถึงการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยสำหรับระบบใหม่ ระบบที่ปรับปรุง และระบบเวอร์ชั่นใหม่

4.10.1.9 ควรมีการยืนยันผลการทดสอบจากผู้ที่เกี่ยวข้อง และมีการอนุมัติจากผู้มีอำนาจก่อนการโอนย้ายระบบงานที่ได้จัดทำเรียบร้อยแล้วจากระบบทดสอบเข้าสู่ระบบงานจริงอย่างเป็นลายลักษณ์อักษร

4.10.1.10 ต้องมีการควบคุม กำหนดสิทธิการเข้าถึง Source Code อย่างเหมาะสม ให้สอดคล้องตามบทบาทหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย

4.10.1.11 ในกระบวนการพัฒนาระบบเทคโนโลยีสารสนเทศ จะต้องมีการตรวจทานความถูกต้องของข้อมูลที่ดีเพื่อลดความเสี่ยงที่อาจเกิดจากความผิดพลาดในการนำเข้าข้อมูล และความผิดพลาดของข้อมูลที่เกิดจากประมวลผลข้อมูล

4.10.1.12 ควรมีการควบคุมและตรวจสอบการทำงานของแอปพลิเคชัน เพื่อป้องกันความเสี่ยงที่อาจเกิดจากการทำงานหรือการประมวลผลข้อมูลที่ผิดพลาดอันจะส่งผลเสียต่อระบบโดยรวม

4.10.1.13 ควรจัดทำข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอปพลิเคชัน รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสม

4.10.2 การควบคุมข้อมูลในการทดสอบ (Test Data)

หน่วยงานที่รับผิดชอบ และผู้ใช้งานต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่มีอยู่บนระบบให้บริการมาใช้ในการทดสอบ ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงเพื่อใช้ในการทดสอบต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง และต้องมีการควบคุมข้อมูลในระบบทดสอบให้เป็นไปตามชั้นความลับและการคุ้มครองข้อมูลส่วนบุคคล

4.10.3 ผู้รับผิดชอบ

4.10.3.1 ผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล

4.10.3.2 ผู้ดูแลระบบ

4.10.3.3 ผู้พัฒนาระบบ

4.11 ความมั่นคงปลอดภัยระบบสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Third Party Relationship)

<u>วัตถุประสงค์</u>

การใช้บริการจากผู้ให้บริการภายนอก อาจก่อให้เกิดความเสี่ยงได้ ได้แก่ ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น จึงจำเป็นต้องมีการควบคุมผู้ให้บริการภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางการคัดเลือก ควบคุมการปฏิบัติงานของผู้ให้บริการภายนอก

<u>แนวนโยบายและแนวทางปฏิบัติ</u>

4.11.1 นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก

4.11.1.1 สำนักงานต้องกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับผู้ให้บริการภายนอก โดยผู้ที่เกี่ยวข้องต้องพิจารณา หรือประเมินความเสี่ยงที่อาจเกิดขึ้น และกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนที่จะอนุญาตให้ผู้ให้บริการภายนอก หรือบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศขององค์กร

4.11.1.2 ผู้ดูแลระบบและฝ่ายต่าง ๆ ที่รับผิดชอบในการประสานงานกับผู้ให้บริการภายนอก ต้องกำกับให้มีการดูแลให้บุคคล หรือผู้ให้บริการภายนอกแก่หน่วยงานตามที่ว่าจ้างปฏิบัติตามสัญญา หรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

4.11.2 การควบคุมการเข้าใช้งานของผู้ให้บริการภายนอก (Third Party)

4.11.2.1 ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศหรืออุปกรณ์ที่ใช้ในการประมวลผล และมีมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบได้

4.11.2.2 ผู้ให้บริการภายนอก (Third Party) ที่ต้องการสิทธิในการเข้าถึงแหล่งข้อมูลของสำนักงานจะต้องทำเรื่องขออนุมัติจากผู้จัดการฝ่ายและฝ่ายของข้อมูล ซึ่งเป็นผู้รับผิดชอบต่อการกระทำทั้งหมดของบุคคลดังกล่าวเป็นลายลักษณ์อักษร ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

4.11.2.2.1 เหตุผลในการขอใช้

4.11.2.2.2 ระยะเวลาในการใช้

4.11.2.2.3 การตรวจสอบความปลอดภัยของอุปกรณ์เชื่อมต่อเครือข่าย

4.11.2.2.4 การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

4.11.2.3 ผู้ให้บริการภายนอก (Third Party) ไม่ว่าจะปฏิบัติงานอยู่ภายในสำนักงานหรือนอกสำนักงานต้องลงนามในสัญญาการรักษาข้อมูลที่เป็นความลับของสำนักงาน

4.11.2.4 เจ้าของระบบมีหน้าที่กำหนดและทบทวนสิทธิของการเข้าใช้งานระบบสารสนเทศเฉพาะบุคคลที่จำเป็นเท่านั้น และมีการทบทวนสิทธิให้เป็นปัจจุบัน

4.11.2.5 สำนักงานต้องพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของผู้ให้บริการภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศ

4.11.2.6 สำนักงานมีสิทธิในการตรวจสอบตามสัญญาจ้างเพื่อให้มั่นใจได้ว่าสำนักงานสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

4.11.2.7 ในกรณีที่มีการเปลี่ยนแปลงการดำเนินงาน ผู้ให้บริการจากภายนอกต้องแจ้งให้สำนักงานรับทราบและอนุมัติการเปลี่ยนแปลงนั้น ก่อนการดำเนินงาน เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

4.11.2.8 เมื่อสิ้นสุดระยะเวลาการใช้งาน สำนักงานต้องดำเนินการยกเลิกสิทธิในการเข้าถึงแหล่งข้อมูลทันที

4.11.2.9 หากพบเหตุละเมิดด้านความมั่นคงปลอดภัยสารสนเทศให้แจ้งไปยังเจ้าของระบบ

4.11.2.10 ต้องดำเนินการตามนโยบายความมั่นคงปลอดภัยสารสนเทศที่สำนักงานประกาศไว้อย่างเคร่งครัด

4.11.3 การระบุนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในข้อตกลงการให้บริการกับผู้ให้บริการภายนอก

4.11.3.1 สำนักงานต้องแสดงนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้แก่ผู้ให้บริการภายนอกที่เกี่ยวกับการเข้าถึง การประมวลผล การจัดเก็บ การสื่อสาร และการให้บริการสารสนเทศของสำนักงาน

4.11.3.2 ผู้ให้บริการภายนอกต้องยอมรับนโยบาย กฎหมายที่เกี่ยวข้องและการควบคุมด้านความมั่นคงปลอดภัยของสำนักงาน

4.11.3.3 สำนักงานมีสิทธิที่จะตรวจสอบสภาพแวดล้อมการทำงานรวมทั้งการตรวจสอบการทำงานของผู้ให้บริการภายนอก

4.11.4 ผู้รับผิดชอบ

4.11.4.1 ผู้จัดการฝ่าย
4.11.4.2 เจ้าของระบบ
4.11.4.3 ผู้ดูแลระบบ
4.11.4.4 ผู้ให้บริการภายนอก
4.11.4.5 ฝ่ายบริหารเทคโนโลยีดิจิทัล

4.12 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของสำนักงาน ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และมีวิธีการที่สอดคล้องและได้ผลสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของสำนักงาน

แนวนโยบายและแนวทางปฏิบัติ

4.12.1 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุละเมิดด้านความมั่นคงปลอดภัย (Management of Information Security Incidents and Improvements)

4.12.1.1 สำนักงานต้องมีการกำหนดหน้าที่ความรับผิดชอบ และกำหนดขั้นตอนปฏิบัติเพื่อรับมือกับเหตุละเมิดด้านความมั่นคงปลอดภัยอย่างทันท่วงที

4.12.1.2 สำนักงานต้องกำหนดให้มีการจำแนกสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดออกจากเหตุการณ์ด้านการปฏิบัติงานทั่วไปเพื่อกำหนดแนวทางการแก้ไขที่ถูกต้องเหมาะสม

4.12.1.3 สำนักงานต้องกำหนดช่องทาง และเกณฑ์ในการรายงานเหตุการณ์ หรือจุดอ่อนหรือเหตุการณ์ความมั่นคงสารสนเทศ หรือสื่อสารให้บุคลากรในองค์กร และหน่วยงานภายนอกรับทราบ

4.12.1.4 กำหนดให้มีการเก็บรวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ ที่มีอยู่ในปัจจุบันหรือมีแนวโน้มที่จะเกิดขึ้น เพื่อจัดทำข้อมูลข่าวกรองภัยคุกคามเชิงลึก (Threat intelligence) และกำหนดแนวทางการป้องกันและลดผลกระทบจากภัยคุกคาม

4.12.2 การรายงานเหตุการณ์น่าสงสัย (Reporting Information Security Events)

หากผู้ใช้งานพบเหตุการณ์ที่น่าสงสัยให้ทำการรายงานต่อผู้ดูแลระบบและผู้บังคับบัญชาทันที ได้แก่ เหตุการณ์ต่อไปนี้

4.12.2.1 พบว่ารหัสผ่านไม่สามารถใช้งานได้ โดยไม่ทราบสาเหตุ

4.12.2.2 เวลาการเข้าใช้งานระบบครั้งล่าสุด (Last Logon Time) ที่ผิดปกติ

4.12.2.3 พบหลักฐานหรือสิ่งผิดสังเกตในเครื่องคอมพิวเตอร์ของตน ได้แก่ พบไฟล์ที่น่าสงสัยว่าเป็นไวรัสการเปลี่ยนแปลงของค่าต่าง ๆ

4.12.2.4 พบหรือคาดว่าระบบงานจะมีปัญหาด้านความปลอดภัยของข้อมูล

4.12.2.5 พบหรือคาดว่าข้อมูลในระบบจะถูกทำลาย แก้ไข หรือลบทิ้ง

4.12.2.6 ความพยายามที่จะเข้าใช้ระบบอย่างผิดวิธี ไม่ว่าจะสำเร็จหรือไม่

4.12.2.7 การให้บริการของระบบเกิดการหยุดชะงัก หรือไม่สามารถให้บริการ

4.12.2.8 เกิดการละเมิดสิทธิเข้าไปใช้งานระบบเพื่อประมวลผลหรือจัดเก็บข้อมูล

4.12.2.9 การแก้ไขค่าความปลอดภัยในระบบโดยไม่ได้รับอนุญาต

4.12.3 การรายงานจุดอ่อนด้านความมั่นคงปลอดภัย (Reporting Information Security Weakness)

ผู้ใช้งานต้องรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กรต่อผู้ดูแลระบบและผู้บังคับบัญชา โดยผ่านช่องทางการรายงานที่กำหนดไว้ และจะต้องดำเนินการรายงานอย่างรวดเร็วที่สุด

4.12.4 การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and Decision on Information Security Events)

ผู้ดูแลระบบต้องประเมินเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ทำการจัดแยกกลุ่มเหตุการณ์ หรือจุดอ่อนด้านความมั่นคงปลอดภัย และจัดลำดับความสำคัญตามเกณฑ์ที่กำหนดไว้ และแจ้งหน่วยงานที่เกี่ยวข้องทราบเพื่อแก้ไขในกรณีที่พบว่าเหตุการณ์ หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ที่ส่งผลกระทบด้านความมั่นคงปลอดภัยสารสนเทศ

4.12.5 การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการทำงานที่บกพร่องของระบบสารสนเทศ (Responding to Security Incidents and Malfunctions)

4.12.5.1 หากพบเห็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือการทำงานที่บกพร่อง หรือการทำงานผิดปกติ ต้องรายงานสิ่งที่เกิดขึ้นให้แก่หน่วยงานที่รับผิดชอบทราบโดยทันที

4.12.5.2 กรณีเกิดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ผู้ดูแลระบบต้องร่วมกับหน่วยงานที่รับผิดชอบ ประเมินขอบเขต (Scope) และความรุนแรง (Severity) ของปัญหา หากพบว่าเป็นปัญหาที่จะมีผลกระทบรุนแรง หรือมีผลต่อชื่อเสียงของสำนักงาน จะต้องรายงานให้คณะทำงานหรือผู้บริหารที่เกี่ยวข้อง ทราบโดยด่วน เพื่อหาแนวทางแก้ไขและป้องกันต่อไป

4.12.6 การเรียนรู้จากเหตุละเมิดด้านความมั่นคงปลอดภัย (Learning from Security Incidents)

4.12.6.1 ผู้ดูแลระบบต้องบันทึกเหตุละเมิดด้านความมั่นคงปลอดภัย จุดอ่อน ช่องโหว่ ภัยคุกคามหรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไขจากเหตุการณ์ที่เกิดขึ้นเพื่อเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

4.12.6.2 ต้องมีการทบทวนเหตุละเมิดความมั่นคงปลอดภัย เพื่อป้องกันการเกิดปัญหาเดิมซ้ำ

4.12.6.3 ต้องมีการจัดทำรายการเฝ้าระวังล่วงหน้าจากเหตุละเมิดความมั่นคง เพื่อป้องกันการเกิดปัญหาเดิมซ้ำ

4.12.6.4 ต้องมีการวิเคราะห์ความเสี่ยง และประเมินสถานการณ์การบุกรุก/ละเมิด/ระบาดที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

4.12.7 การเก็บรวบรวมหลักฐาน (Collection of Evidence)

4.12.7.1 ผู้ดูแลระบบต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่า ได้ปฏิบัติตามข้อกำหนดทางด้านกฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล ระเบียบสำนักงาน และกฎหมายที่เกี่ยวข้อง

4.12.7.2 ส่วนกฎหมายและผู้ดูแลระบบสารสนเทศที่สำคัญต้องศึกษากฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง

4.12.8 ผู้รับผิดชอบ

4.12.8.1 ผู้ใช้งาน
4.12.8.2 ผู้ดูแลระบบ
4.12.8.3 หน่วยงานที่รับผิดชอบระบบงาน

4.13 การบริหารความต่อเนื่องในการดำเนินงาน (Business Continuity Management)

วัตถุประสงค์

เพื่อเป็นแนวทางในการบริหารจัดการความต่อเนื่องในการดำเนินงานของสำนักงาน เมื่ออยู่ภายใต้สภาวะวิกฤตและเหตุฉุกเฉินต่าง ๆ ทำให้มั่นใจได้ว่า ขั้นตอนการดำเนินงานและระบบสารสนเทศต่าง ๆ ของสำนักงานที่สำคัญ มีการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan หรือ BCP) และแผนกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Plan หรือ DRP) อย่างเหมาะสม เพื่อให้การดำเนินงานของสำนักงานเป็นไปอย่างต่อเนื่อง

แนวนโยบายและแนวทางปฏิบัติ

4.13.1 ขั้นตอนเตรียมการของแผนรองรับเหตุการณ์ฉุกเฉิน

4.13.1.1 สำนักงานต้องจัดตั้งคณะทำงานรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ซึ่งประกอบไปด้วยตัวแทนจากหน่วยงานเจ้าของข้อมูล เจ้าของระบบงาน

4.13.1.2 คณะทำงานจะต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศที่เป็นลายลักษณ์อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผน อย่างน้อยปีละ 1 ครั้ง

4.13.1.3 กระบวนการหลักในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศประกอบด้วย

4.13.1.3.1 การวิเคราะห์ผลกระทบทางการดำเนินงานของสำนักงาน (Business Impact Analysis)

4.13.1.3.2 การประเมินความเสี่ยงและการควบคุม (Risk Analysis &Control)

4.13.1.3.3 แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan หรือ BCP) แผนการกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Plan หรือ DRP)

4.13.1.3.4 การประชาสัมพันธ์และการฝึกอบรม การทดสอบ ปรับปรุงแผนรองรับ

4.13.1.4 แนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

4.13.1.4.1 เพื่อป้องกันผลกระทบและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อการให้บริการของสำนักงาน

4.13.1.4.2 เพื่อกำหนดแนวทางในการจัดการต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย

4.13.1.4.3 เพื่อให้กระบวนการการดำเนินงานเป็นไปได้อย่างต่อเนื่อง ได้แก่ การสำรองข้อมูล การกู้คืนระบบ เป็นต้น

4.13.1.4.4 ต้องมีแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ

4.13.2 การตอบสนองต่อเหตุการณ์ฉุกเฉินเพื่อให้สามารถดำเนินงานได้อย่างต่อเนื่อง

คณะทำงานรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ มีหน้าที่ ดังต่อไปนี้

4.13.2.1 ระบุขั้นตอนการดำเนินการ ประเมินสถานการณ์เบื้องต้น สถานที่ สาเหตุ และขอบเขตความเสียหาย เพื่อระงับเหตุการณ์ความเสียหาย และวิธีการดำเนินงานต่าง ๆ ที่เกี่ยวข้อง ได้แก่ แนวทางการเก็บรักษาข้อมูล เอกสาร ความปลอดภัยของผู้ปฏิบัติงาน การเคลื่อนย้ายอพยพพนักงานและผู้ใช้งานและสินทรัพย์ที่จำเป็น

4.13.2.2 ระบุแผนปฏิบัติการด้านการติดต่อสื่อสาร กำหนดวิธีการสื่อสาร และประสานงานกับหน่วยงานหรือบุคคลที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อแจ้งสถานการณ์และแนวทางการดำเนินงาน หรือสถานที่ติดต่อฉุกเฉิน รวมทั้งจัดทำรายชื่อหน่วยงานหรือผู้ที่รับผิดชอบในการดำเนินการช่วยเหลือ ยุติเหตุการณ์ความเสียหายทั้งภายในและภายนอกสำนักงาน

4.13.2.3 ระบุความต้องการใช้ทรัพยากรต่าง ๆ ระบุความต้องการทรัพยากรที่มีความจำเป็น งบประมาณ จำนวนแรงงาน สถานที่ ระบบการสื่อสารโทรคมนาคม สาธารณูปโภค อุปกรณ์และเครื่องมือต่าง ๆ ให้ชัดเจน

4.13.3 การกลับคืนสู่การทำงานปกติ

ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องร่วมกับคณะทำงานรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศดำเนินการดังต่อไปนี้

4.13.3.1 ระบุขั้นตอนการปฏิบัติงานเพื่อฟื้นฟูให้เหตุการณ์กลับสู่ภาวะปกติ การควบคุมการติดตั้งการตั้งค่าและทดสอบระบบที่ถูกกู้คืนมาหรือทดแทนใหม่ การรายงานสรุปความเสียหายต่อผู้บังคับบัญชา

4.13.3.2 ระบุรายชื่อผู้ที่เกี่ยวข้องจัดทำรายชื่อของหน่วยงาน หรือผู้ที่รับผิดชอบทั้งจากภายในและภายนอก เพื่อการดำเนินการช่วยเหลือ ฟื้นฟูให้เหตุการณ์กลับสู่ภาวะปกติ

4.13.3.3 การกำหนดกระบวนการป้องกันและควบคุมความเสี่ยง เพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ความเสียหายในอนาคต

4.13.4 การประชาสัมพันธ์ และการฝึกอบรม

คณะทำงานรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศต้องระบุขั้นตอนและวิธีการประชาสัมพันธ์ให้แก่เจ้าหน้าที่ ผู้ใช้งาน ลูกค้า ผู้ใช้บริการ และจัดฝึกอบรมให้แก่ผู้มีส่วนเกี่ยวข้องให้รับทราบถึงวัตถุประสงค์ ขั้นตอนการปฏิบัติงาน การประสานงาน การติดต่อสื่อสาร ขั้นตอนการรายงาน ระบบรักษาความปลอดภัย และหน้าที่ความรับผิดชอบตามแผนอย่างชัดเจน

4.13.5 การทดสอบ ปรับปรุงและสอบทานแผนฉุกเฉิน

คณะทำงานรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ต้องดำเนินการทดสอบ ปรับปรุงและสอบทานแผนฉุกเฉิน ดังต่อไปนี้

4.13.5.1 การทดสอบ

4.13.5.1.1 กำหนดเวลาการทดสอบแผนกู้คืนที่ชัดเจน รวมถึงกำหนดระยะเวลาที่ใช้ในการทดสอบตั้งแต่เริ่มต้นจนสิ้นสุดกระบวนการทดสอบ

4.13.5.1.2 กำหนดเหตุการณ์จำลองและรายละเอียดของเหตุการณ์ที่จะใช้ทดสอบต้องระบุวัตถุประสงค์ ขอบเขตของระบบงาน หรือกระบวนการทำงานที่เกี่ยวข้องกับการทดสอบแผนทั้งหมด รวมถึงการกำหนดขั้นตอนการทดสอบแผน

4.13.5.1.3 กำหนดทรัพยากรต่าง ๆ ที่ใช้ในการทดสอบแผน กำหนดผู้รับผิดชอบที่จะทำหน้าที่ ควบคุม ประสานงาน และรับผิดชอบในการจัดการทดสอบแผน รวมถึงสถานที่ และ อุปกรณ์เครื่องมือต่าง ๆ และงบประมาณที่ต้องใช้

4.13.5.1.4 กำหนดเกณฑ์การประเมินผลและผู้รับผิดชอบในการประเมินผลเกณฑ์การประเมินผล ซึ่งอาจมีความแตกต่างกันไปตามลักษณะของระบบงาน กระบวนการทำงาน และวัตถุประสงค์ของการทดสอบในแต่ละครั้ง

4.13.6 การปรับปรุงและสอบทานแผน

4.13.6.1 กำหนดเวลา แนวทาง ระยะเวลา และปรับปรุงแผนอย่างชัดเจน เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน

4.13.6.2 กำหนดผู้รับผิดชอบในการสอบทานแผน เพื่อยืนยันความเหมาะสมของขั้นตอนต่าง ๆ ในการจัดทำแผน

4.13.7 รายละเอียดเพิ่มเติมอื่น ๆ

4.13.7.1 รายชื่อ ที่อยู่ หมายเลขโทรศัพท์ของเจ้าหน้าที่ และผู้ใช้งานที่มีหน้าที่รับผิดชอบในการปฏิบัติตามแผน

4.13.7.2 รายชื่อหน่วยงาน สถานที่ตั้ง และหมายเลขโทรศัพท์ของหน่วยงานภายนอกที่เกี่ยวข้อง

4.13.7.3 รายละเอียดการปฏิบัติตามแผน (Checklist)

4.13.7.4 รูปแบบรายงานต่าง ๆ ที่จำเป็น

4.13.8 สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

4.13.8.1 ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องควบคุมให้มีการประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งานของระบบสารสนเทศที่มีความสำคัญสูง

4.13.8.2 ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องกำกับให้มีการติดตั้งระบบสารสนเทศสำรองหรืออุปกรณ์สำรอง หรือระบบสำหรับสนับสนุนการให้บริการที่เพียงพอ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจที่เหมาะสม

4.13.9 ผู้รับผิดชอบ

4.13.9.1 ฝ่ายบริหารเทคโนโลยีดิจิทัล

4.13.9.2 คณะทำงานรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

4.14 การปฏิบัติตามข้อกำหนด (Compliance)

วัตถุประสงค์

เพื่อป้องกันการละเมิดที่เกี่ยวข้องกับการปฏิบัติงาน ระเบียบ ข้อบังคับ เงื่อนไขในสัญญา และข้อกำหนดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นแนวทางในการปฏิบัติงานของสำนักงานที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

แนวนโยบายและแนวทางปฏิบัติ

4.14.1 การนำนโยบายไปสู่การปฏิบัติ (Policy Implementation)

4.14.1.1 ฝ่ายกฎหมาย ต้องระบุแนวทางหรือมาตรการทางกฎหมาย ระเบียบปฏิบัติ และสัญญาว่าจ้าง รวมทั้งสัญญาที่ทำกับผู้ให้บริการภายนอก (Third Party) หรือบุคคลภายนอกที่เกี่ยวข้องเพื่อทำให้มีการปฏิบัติตามนโยบายฉบับนี้

4.14.1.2 ปรับปรุงแนวทางหรือมาตรการให้ทันสมัยอยู่เสมอ

4.14.2 การปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ในการใช้งานทรัพย์สินทางปัญญา (Compliance with Intellectual Property Rights (IPR))

4.14.2.1 การนำซอฟต์แวร์ของบุคคลที่สามมาใช้ในสำนักงาน ต้องเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ (Licensing Agreement) ถูกต้องตามกฎหมาย

4.14.2.2 ผู้ใช้งานซอฟต์แวร์บนระบบสารสนเทศของสำนักงาน ต้องยึดถือและปฏิบัติตามกฎหมายและข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด สิทธิ์เรื่องทรัพย์สินทางปัญญาพนักงานของสำนักงาน สิทธิ์ผู้ใช้งานจากข้อมูลสำคัญของสำนักงานต้องดำเนินการให้

4.14.2.3 ต้องควบคุมการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ โดยมีการบันทึกข้อมูลการใช้งาน เพื่อเก็บเป็นหลักฐาน และมีการตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้อง ถ้าหากพบว่ามีการละเมิดข้อตกลงจะต้องทำการยกเลิกการติดตั้งหรือลบทิ้งทันที

4.14.2.4 ซอฟต์แวร์หรือระบบงานที่พัฒนาขึ้นเพื่อสำนักงาน ถือเป็นสินทรัพย์ของสำนักงาน ทั้งนี้เพื่อเป็นการป้องกันข้อพิพาทในเรื่องกรรมสิทธิของซอฟต์แวร์ที่อาจเกิดขึ้น

4.14.2.5 ซอฟต์แวร์ที่ถูกพัฒนาโดยเจ้าหน้าที่หรือลูกจ้าง ถือเป็นสินทรัพย์ของสำนักงาน

4.14.2.6 การติดตั้งซอฟต์แวร์ใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงการปรับปรุงระบบหรือซ่อมแซมแก้ไขระบบต่าง ๆ จากผู้ให้บริการภายนอกต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

4.14.2.7 ถ้ามีการติดตั้งซอฟต์แวร์ใด ๆ ในเครื่องคอมพิวเตอร์ของสำนักงาน โดยไม่ได้รับอนุญาตแล้วเกิดข้อพิพาททางกฎหมาย หรือข้อกำหนดและเงื่อนไขของผู้ผลิตซอฟต์แวร์นั้น ๆ ทาง “สำนักงานขอสงวนสิทธิที่จะไม่รับผิดชอบในการดำเนินการดังกล่าวไม่ว่าจะกรณีใด ๆ”

4.14.2.8 ห้ามมิให้ผู้ใช้งานคัดลอก แก้ไข หรือปรับแต่ง ซอฟต์แวร์ที่เป็นสินทรัพย์ของสำนักงาน หรือนำไปให้ผู้อื่นใช้งานโดยไม่ได้รับอนุญาต

4.14.3 การป้องกันข้อมูลสำคัญของสำนักงาน (Protection of Organizational Records)

4.14.3.1 ข้อมูลสำคัญของสำนักงาน ต้องได้รับการป้องกันจากการสูญหาย การถูกทำลาย การปลอมแปลง การเข้าถึง และการเผยแพร่โดยไม่ได้รับอนุญาต

4.14.3.2 การปฏิบัติงานต้องสอดคล้องกับกฎหมาย นโยบาย ระเบียบ ข้อบังคับ ของสำนักงาน

4.14.4 การป้องกันข้อมูลส่วนบุคคลและการเข้ารหัส

4.14.4.1 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคลต้องมีการดำเนินการให้สอดคล้องกับกฎหมายและระเบียบ ข้อบังคับที่เกี่ยวข้อง

4.14.4.2 ผู้ดูแลระบบ ต้องจัดให้มีวิธีการป้องกันข้อมูลส่วนบุคคลของผู้ใช้งาน ได้แก่ ข้อมูลในจดหมายอิเล็กทรอนิกส์ ข้อมูลในระบบบริหารงานบุคคล เป็นต้น

4.14.4.3 ผู้ดูแลระบบ ต้องศึกษาและปฏิบัติตามข้อกำหนดหรือกฎหมายภายในประเทศและต่างประเทศ เกี่ยวกับการเข้ารหัสข้อมูล กรณีมีเหตุจำเป็นในการโยกย้ายข้อมูลที่เข้ารหัสไปยังอีกประเทศหนึ่ง ให้ศึกษาและปฏิบัติตามข้อกำหนด หรือกฎหมายของประเทศนั้นด้วย

4.14.5 การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of Misuse of Information Processing Facilities)

4.14.5.1 อุปกรณ์ประมวลผลสารสนเทศของสำนักงานมีไว้เพื่อใช้ในกิจการของสำนักงานเท่านั้น ยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากผู้บังคับบัญชาที่มีอำนาจ

4.14.5.2 ต้องกำหนดให้มีผู้รับผิดชอบ รวมถึงการจัดทำบัญชีรายการของอุปกรณ์ประมวลผลสารสนเทศที่ซื้อหรือเช่ามาใช้งาน

4.14.5.3 ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่าง ๆ เมื่อมีการเปลี่ยนแปลง เพื่อใช้เป็นข้อมูลในการควบคุมสินทรัพย์ของสำนักงาน

4.14.5.4 การดำเนินการใด ๆ ที่เป็นการติดตั้งซอฟต์แวร์หรืออุปกรณ์เพิ่มเติมต้องได้รับการอนุมัติจากผู้จัดการฝ่ายต้นสังกัดและผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัล เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

4.14.5.5 อุปกรณ์ประมวลผลสารสนเทศจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนเป็นอย่างน้อยก่อนการเข้าใช้งานด้วยวิธีการใส่รหัสผ่านตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

4.14.6 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)

4.14.6.1 ผู้จัดการฝ่ายต้องกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยของสำนักงาน

4.14.6.2 วิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย วัตถุประสงค์ มาตรการ นโยบาย กระบวนการ ขั้นตอนการปฏิบัติ การประเมินความเสี่ยง ต้องมีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

4.14.6.3 ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องมีการทบทวนความสอดคล้องทางเทคนิคของระบบอย่างสม่ำเสมอเพื่อพิจารณาความสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน

4.14.7 มาตรการการตรวจประเมินระบบสารสนเทศ (Information Systems Audit Controls)
ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องมีการวางแผนการตรวจประเมินระบบสารสนเทศ เพื่อให้ลดผลกระทบต่อระบบและกระบวนการดำเนินงานของสำนักงานอย่างน้อยปีละ 1 ครั้ง

4.14.8 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of Information Systems Audit Tools)
ฝ่ายบริหารเทคโนโลยีดิจิทัล ต้องมีแนวทางป้องกันเครื่องมือที่ใช้ในการตรวจประเมินระบบมิให้มีการนำเครื่องมือไปใช้ในทางที่ผิด และป้องกันการเข้าถึงข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยเครื่องมือ

4.14.9 ผู้รับผิดชอบ
4.14.9.1 ฝ่ายกฎหมาย
4.14.9.2 ผู้ดูแลระบบ
4.14.9.3 เจ้าของข้อมูล
4.14.9.4 ผู้จัดการฝ่าย
4.14.9.5 ผู้ใช้งาน

4.15 การใช้บริการคลาวด์ (Cloud Computing)

<u>วัตถุประสงค์</u>

เพื่อให้เกิดการควบคุมการใช้บริการคลาวด์จากผู้ให้บริการด้านเทคโนโลยีสารสนเทศ ในงานด้านโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ หรือระบบงานในการจัดเก็บข้อมูล หรือดำเนินการใดๆ เกี่ยวกับข้อมูล หรือระบบสารสนเทศ ซึ่งครอบคลุมการใช้บริการประเภท Cloud Infrastructure as a Service (IaaS) Platform as a Service (PaaS) และ Software as a Service (SaaS)

<u>แนวนโยบายและแนวทางปฏิบัติ</u>

4.15.1 มีการบริหารความเสี่ยงให้เหมาะสมกับรูปแบบ และลักษณะของการใช้บริการคลาวด์
4.15.1.1 มีการระบุนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในข้อตกลงการให้บริการกับผู้ให้บริการ โดยคำนึงถึงความเสี่ยงการใช้บริการคลาวด์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย และการพึ่งพิงการใช้บริการจากผู้ให้บริการภายนอกจนอาจทำให้การเปลี่ยนแปลง หรือการยกเลิกการใช้บริการทำได้ยาก (Vendor lock-in) และส่งผลกระทบต่อระบบงานที่สำคัญของสำนักงาน นอกจากนี้ ในกรณีที่ต้องมีการใช้บริการในต่างประเทศ ต้องคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นจากการขัดข้อง หรือปิดกั้นเครือข่าย หรือระบบสื่อสารระหว่างประเทศ (Information Access Risk) และความเสี่ยงด้านกฎหมายที่เกี่ยวข้องกับการปฏิบัติตามหลักเกณฑ์ของต่างประเทศ (Cross-Border Compliance)

4.15.1.2 การบริหารความเสี่ยงการใช้บริการคลาวด์ ควรสอดคล้องกับความเสี่ยงจากการใช้บริการ โดยต้องได้รับความเห็นชอบจากผู้อำนวยการ

4.15.1.3 ต้องมีการจัดทำสัญญาการใช้บริการจากผู้ให้บริการเป็นลายลักษณ์อักษร หรือจัดทำข้อตกลงการให้บริการ (Service Level Agreement) โดยระบุบทบาท หน้าที่ความรับผิดชอบ ขอบเขตงานที่ใช้บริการครอบคลุมสาระสำคัญ หรืออย่างน้อยดังนี้

- ขอบเขตการให้บริการ ประเภท และเงื่อนไขการให้บริการ
- เงื่อนไขความเป็นเจ้าของข้อมูล สิทธิการใช้ และลิขสิทธิ์ที่เกี่ยวข้อง
- ข้อกำหนดด้านการเข้าถึงข้อมูลของผู้ให้บริการ สิทธิการเข้าถึง และเงื่อนไขการเปิดเผยข้อมูล
- มาตรฐานของการปฏิบัติงานขั้นต่ำที่ต้องการจากผู้ให้บริการ
- ระบบการควบคุมภายในของผู้ให้บริการ
- การจัดทำแผนฉุกเฉินสำหรับการให้บริการของผู้ให้บริการ ควรสอดคล้องกับแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) หรือแผนสำรองฉุกเฉิน (Disaster Recovery Plan) ของระบบสารสนเทศของสำนักงาน
- การรายงานผลการปฏิบัติงานของผู้ให้บริการ
- ความรับผิดชอบของสำนักงาน และผู้ให้บริการ ภาระผูกพันในกรณีที่เกิดปัญหาในการให้บริการ เงื่อนไข หรือแนวทางในการเปลี่ยนแปลง หรือยกเลิกสัญญา
- ข้อกำหนดและเงื่อนไขการส่งมอบข้อมูลเมื่อมีการยกเลิก หรือสิ้นสุดการใช้บริการ
- ข้อกำหนดและมาตรการป้องกันการรั่วไหลของข้อมูลที่อาจเกิดขึ้นจากผู้ให้บริการ
- ข้อกำหนดด้านสิทธิในการตรวจสอบ หรือการเปิดเผยรายงานผลการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
- การบริหารความเสี่ยงที่เกี่ยวข้องกับความต่อเนื่องในการให้บริการจากการยกเลิกสัญญาการใช้บริการ และแนวทางการยกเลิก หรือสิ้นสุดการใช้บริการ โดยพิจารณาเงื่อนไขและข้อกำหนดที่ระบุในสัญญาการใช้บริการ

4.15.1.4 ต้องกำหนดกระบวนการ และหลักเกณฑ์ในการคัดเลือกผู้ให้บริการที่ชัดเจน เพื่อให้มั่นใจว่า ผู้ให้บริการจะสามารถให้บริการได้อย่างต่อเนื่อง และสามารถตอบสนองความต้องการของสำนักงาน โดยครอบคลุมเนื้อหาดังต่อไปนี้

- ผู้ให้บริการมีมาตรฐานสากลหรือผลการตรวจสอบด้านความมั่นคงปลอดภัยในขอบเขตที่ให้บริการ เช่น มาตรฐาน ISO/IEC 27001 ISO/IEC 27017 ISO/IEC 27018 มาตรฐาน CSA STAR มาตรฐาน PCI DSS เป็นต้น
- ความพร้อมด้านเทคโนโลยีของผู้ให้บริการในการให้บริการ
- ขีดความสามารถของการให้บริการ (Capacity) ทั้งในกรณีการใช้งานที่กำหนดทรัพยากรที่ตายตัว และกรณีที่เป็นการคิดค่าใช้จ่ายตามจริง
- ข้อตกลงการให้บริการ (Service Level Agreement) ของผู้ให้บริการสอดคล้องกับความต้องการทางธุรกิจของสำนักงาน
- ความพร้อมในการดำเนินงานให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และนโยบายของสำนักงาน

- บริการที่ใช้งานสามารถโอนย้ายข้อมูลได้หากมีการยกเลิกการใช้งาน

4.15.1.5 ต้องจัดให้มีแนวทางในการรับทราบการเปลี่ยนแปลงที่เกิดขึ้นกับผู้ให้บริการ รวมถึงแนวทางในการรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นจากการให้บริการ (Day-to-day incident)

4.15.2 มีการกำหนดหน้าที่ผู้ให้บริการให้เหมาะสมกับรูปแบบ และประเภทการใช้ ตามลักษณะการใช้บริการ

4.15.2.1 เลือกใช้และกำหนดรายละเอียดรูปแบบการใช้ประเภทการบริการ ที่รองรับการดำเนินธุรกิจของสำนักงาน

4.15.2.2 กำหนดมาตรฐานการรักษาความลับ ความปลอดภัยของข้อมูล

- ผู้ให้บริการต้องมีแนวทาง หรือมาตรฐานในการรักษาความปลอดภัย ความลับของระบบงานตามมาตรฐานสากล
- ต้องจัดให้มีกระบวนการ ขั้นตอน หรือระบบในการติดตาม ตรวจสอบผู้ให้บริการเพื่อให้มั่นใจว่าผู้ให้บริการสามารถดำเนินการได้ตามแนวทางที่ได้ตกลงไว้

4.15.2.3 ผู้ให้บริการต้องจัดให้มีการสำรองข้อมูล และระบบงานสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน

4.15.2.4 ผู้ให้บริการต้องจัดให้มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) หรือ แผนสำรองฉุกเฉิน (Disaster Recovery Plan) ของระบบสารสนเทศของสำนักงาน ที่ครอบคลุมถึงการใช้บริการ เพื่อให้สามารถปฏิบัติงานได้จริง รวมทั้งต้องจัดให้มีกระบวนการในการบริหารจัดการปัญหาหรือเหตุการณ์ผิดปกติ ที่เกิดจากการใช้บริการ และมีการรายงานปัญหาหรือเหตุการณ์ผิดปกติ และการจัดการปัญหาหรือเหตุการณ์ผิดปกติดังกล่าว ให้สำนักงาน รับทราบตามข้อตกลงการให้บริการ

4.15.2.5 ผู้ให้บริการต้องกำหนดให้มีวิธีการพิสูจน์ตัวตนตามแนวทางการพิสูจน์ตัวตนที่มีความปลอดภัย มีประสิทธิภาพ และเป็นที่ยอมรับตามมาตรฐานสากล

4.15.3 มาตรการรักษาความปลอดภัย

4.15.3.1 ผู้ให้บริการต้องมีการรักษาความปลอดภัยข้อมูลสารสนเทศ เช่น เข้ารหัสข้อมูล (Data Encryption) การควบคุมกุญแจที่ใช้เข้าถึงและเข้ารหัสข้อมูลบนคลาวด์ (Key Management) เป็นต้น

4.15.3.2 ผู้ให้บริการต้องมีแนวทางการป้องกันภัยคุกคาม อย่างน้อย ดังต่อไปนี้

- การโจมตีในลักษณะ DDoS (Distributed Denial of Service)
- การป้องกันภัยคุกคามในรูปแบบใหม่ (Advanced Persistent Threat)
- การป้องกันการบุกรุกจากโปรแกรมไม่ประสงค์ดี (Malware)

4.15.3.3 ผู้ให้บริการต้องมีการแบ่งแยกเครือข่าย (Segregation in Networks)

4.15.3.4 ผู้ให้บริการต้องสร้างความมั่นคงปลอดภัยให้กับระบบงานสารสนเทศ (Hardening) เช่น การปิดช่องโหว่ และป้องกันปัญหาที่เกิดขึ้นจากการทดสอบ เพื่อให้มั่นใจว่าระบบงานสารสนเทศมีความมั่นคงปลอดภัย ดังต่อไปนี้

- แก้ไขการตั้งค่าที่เป็น Default ของระบบงานสารสนเทศ เช่น User Password เป็นต้น
- ติดตั้ง Patch หรือ Hotfix ให้เป็น Version ล่าสุด

- ปิดการใช้งาน user account ไม่จำเป็นและจัดการสิทธิให้เหมาะสม
- ปิด Port หรือบริการต่างๆ ที่ไม่จำเป็น เช่น Telnet หรือ FTP เป็นต้น

4.15.4 กระบวนการตรวจสอบการให้บริการคลาวด์

ผู้ให้บริการต้องยินยอมให้มีกระบวนการตรวจสอบ กรณีสำนักงานมีการเรียกดูข้อมูลที่เกี่ยวข้อง ทั้งนี้ ในกรณีที่ไม่สามารถจัดให้มีการตรวจสอบผู้ให้บริการได้ สำนักงานมีสิทธิขอเรียกดูผลการตรวจสอบของผู้ให้บริการที่ได้รับการรับรองจากผู้ตรวจสอบภายนอกที่มีความเป็นอิสระที่มีหัวข้อและขอบเขตการตรวจสอบสอดคล้องกับขอบเขตการดำเนินงาน และภาระหน้าที่ความรับผิดชอบของผู้ให้บริการ หรือได้มาตรฐานสากลในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

4.15.5 ผู้รับผิดชอบ

4.15.5.1 ฝ่ายบริหารเทคโนโลยีดิจิทัล

4.15.5.2 ผู้ดูแลระบบ