บริษัท อินเตอร์ ฟาร์มา จำกัด (มหาชน)

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการสื่อสาร

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการเสื่อสารของบริษัทอินเตอร์ ฟาร์มา จำกัด (มหาชน) เป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารที่ไม่ถูกต้อง ตลอดจนการถูกคุมคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่สำนักงาน อันเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายอื่นที่เกี่ยวข้อง บริษัทอินเตอร์ ฟาร์มา จำกัด (มหาชน) จึงได้กำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารองค์กรขึ้น โดยมีประเด็นและวัตถุประสงค์ครอบคลุมและเป็นไปตามมาตรฐาน ISO/IEC 27001:2013 ดังนี้

ความหมายและคำจำกัดความ

“สินทรัพย์คอมพิวเตอร์” หมายความว่า สินทรัพย์ทุกอย่างที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล เป็นต้น

“ระบบเครือข่าย” หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ของบริษัทอินเตอร์ ฟาร์มา จำกัด (มหาชน) (มหาชน)

“คอมพิวเตอร์แม่ข่าย” หมายความว่า เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทาหน้าที่เป็นศูนย์กลางของการทำงาน อาทิ จัดเก็บข้อมูลหรือซอฟต์แวร์สาหรับให้บริการแก่เครื่องคอมพิวเตอร์ อื่น ๆ หรือควบคุมการทำงานในเครือข่าย

“การเข้าถึงเครือข่ายจากระยะไกล” หมายความว่า การที่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์หรือเครือข่ายอื่นผ่านอุปกรณ์สื่อสารหรือสื่อสัญญาณอื่น ๆ อาทิ Modem VPN

“การควบคุมการเข้าถึง” หมายความว่า การควบคุมการเข้าถึงหรือใช้งานสินทรัพย์คอมพิวเตอร์ให้เป็นไปตามสิทธิที่กำหนดไว้เท่านั้น

“เครื่องคอมพิวเตอร์” หมายความว่า อุปกรณ์ที่ใช้ในการประมวลผลข้อมูลที่ทางานด้วยระบบอิเล็กทรอนิกส์ โดยทำงานตามคาสั่งผ่านทางซอฟต์แวร์ให้ได้ผลตามที่ต้องการ อาทิ คอมพิวเตอร์แม่ข่าย (Server) คอมพิวเตอร์ส่วนบุคคล (Personal computer) และคอมพิวเตอร์แบบพกพาได้ (Notebook computer)

“อุปกรณ์คอมพิวเตอร์” หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์เพื่อสนับสนุนให้เครื่องคอมพิวเตอร์ปฏิบัติงานได้ตามต้องการ และให้รวมถึงเครื่องคอมพิวเตอร์

“สื่อสัญญาณ” หมายความว่า สื่อกลางใด ๆ ที่ใช้เชื่อมต่อระหว่างอุปกรณ์คอมพิวเตอร์ อาทิ สายทองแดง สายใยแก้วนำแสง เครือข่ายไร้สาย

“ฮาร์ดแวร์” หมายความว่า อุปกรณ์คอมพิวเตอร์

“ซอฟต์แวร์” หมายความว่า ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงานตามต้องการ

“ซอฟต์แวร์ระบบ” หมายความว่า ซอฟต์แวร์ที่ควบคุมการทำงานของอุปกรณ์คอมพิวเตอร์ เช่น ระบบปฏิบัติการ เป็นต้น

“ซอฟต์แวร์ประยุกต์” หมายความว่า ซอฟต์แวร์ที่พัฒนาขึ้นเพื่อใช้กับงานเฉพาะด้านตามความต้องการ อาทิ ซอฟต์แวร์สำหรับพิมพ์เอกสาร ซอฟต์แวร์สำหรับการคำนวณทางบัญชี

“ระบบเทคโนโลยีสารสนเทศ” หมายความว่า ระบบงานของหน่วยงานที่นาเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนามาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ อาทิ อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ระบบงาน และสารสนเทศ

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การสงวนไว้ซึ่งความลับ ความครบถ้วนถูกต้อง และความพร้อมใช้ของสารสนเทศของสถาบันนิติวิทยาศาสตร์

“สารสนเทศ” หมายความว่า ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของ ตัวเลข ข้อความ หรือภาพกราฟฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ ได้

ระบบงาน” หมายความว่า การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงานเพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ อาทิ ระบบจัดเก็บเอกสาร เป็นต้น

“ระบบปฏิบัติการ” (Operating system) หมายความว่า ซอฟต์แวร์ควบคุมการทำงานของเครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรระบบ ซึ่งได้แก่ การจัดการหน่วยความจำ การควบคุม การทำงานของอุปกรณ์ป้อนข้อมูล (แป้นพิมพ์ เมาส์) และอุปกรณ์แสดงผล (จอภาพ เครื่องพิมพ์)

“ระบบป้องกันการบุกรุก” (Firewall) หมายความว่า ระบบรักษาความปลอดภัยที่ประกอบด้วยกลุ่มอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ ซึ่งทำหน้าที่ป้องกันผู้ไม่ได้รับอนุญาตจากเครือข่ายภายนอกเข้าใช้ระบบ และจำกัดการใช้งานของผู้ใช้งานภายในให้เป็นไปตามนโยบายที่บริษัทอินเตอร์ ฟาร์มา จำกัด (มหาชน) (มหาชน) กำหนด

“ข้อมูล” หมายความว่า ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลได้ด้วยวิธีการทางอิเล็กทรอนิกส์บนอุปกรณ์คอมพิวเตอร์ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

“ไฟล์” (File) หมายความว่า ข้อมูลที่ถูกรวบรวมลงสื่อบันทึกและระบุเป็นหนึ่งหน่วยโดยมี ชื่อเฉพาะ เช่น ซอฟต์แวร์ใช้งาน และไฟล์เอกสารต่าง ๆ ที่สร้างขึ้นและใส่ชื่อให้แก่ไฟล์นั้นแล้วเก็บบันทึกลง สื่อบันทึก เป็นต้น

“ผู้ใช้งาน” (User) หมายความว่า เจ้าหน้าที่หรือบุคคลภายนอกที่มีสิทธิใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทอินเตอร์ ฟาร์มา จำกัด (มหาชน)

“ผู้บริหารเครือข่าย” (Network administrator) หมายความว่า บุคคลที่ทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษาเครือข่าย

“บัญชีผู้ใช้งาน” (User account) หมายความว่า บัญชีที่ผู้ใช้งานใช้ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นไปตามข้อตกลงระหว่างผู้ใช้งานกับผู้ให้บริการระบบเทคโนโลยีสารสนเทศ

“สิทธิ์ของผู้ใช้งาน” (User Authorization) หมายความว่า สิทธิ์ของเจ้าหน้าที่หรือบุคคลภายนอกในการเข้าถึง และใช้งานระบบเทคโนโลยีสารสนเทศ ที่ได้รับการอนุมัติอย่างถูกต้องจากผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ เพื่อดำเนินการตามวัตถุประสงค์และเป้าหมายของบริษัทอินเตอร์ ฟาร์มา จำกัด (มหาชน)

“ความเสี่ยง” หมายความว่า โอกาสของสินทรัพย์คอมพิวเตอร์ในการถูกละเมิดการรักษาความปลอดภัย

“เหตุการณ์การบุกรุกด้านความมั่นคงปลอดภัยสารสนเทศ” (Information Security Incident) หมายความว่า เหตุการณ์ใด ๆ ที่สามารถส่งผลกระทบที่สำคัญต่อการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศ

“ส่วนงานเจ้าของข้อมูล” หมายความว่า เจ้าหน้าที่ในส่วนงานตั้งแต่ 1 คนขึ้นไปที่ได้รับมอบหมายจากส่วนงานให้เป็นผู้รับผิดชอบข้อมูล

“โปรแกรมประสงค์ร้าย” หมายความว่า ฮาร์ดแวร์หรือซอฟต์แวร์ที่มีการตั้งใจใส่เข้าไปในระบบโดยไม่ได้รับอนุญาต เพื่อให้ทางานตามความประสงค์ของผู้ประสงค์ร้าย ซึ่งมีผลให้คอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศ หรือชุดคำสั่งอื่นได้รับความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคาสั่งที่กำหนดไว้

1. นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)

1.1. นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

วัตถุประสงค์ เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของสำนักงาน เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

รายละเอียดที่เกี่ยวข้อง:

(1) เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information Security Policy Document)

(2) การตรวจสอบและประเมินนโยบายความมั่นคงปลอดภัย (Review of the Information Security Policy)

2. โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ (Organizational of Information Security)

2.1. โครงสร้างทางด้านความมั่นคงปลอดภัยสสารสนเทศภายในสำนักงาน (Internal Organization)

วัตถุประสงค์: เพื่อให้มีการกำหนดกรอบการบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศของสำนักงาน ตั้งแต่การเริ่มต้นและควบคุมการปฏิบัติเพื่อให้มีความมั่นคงปลอดภัย

รายละเอียดที่เกี่ยวข้อง:

(1) บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

(2) การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

(3) การบริหารจัดการโครงการเพื่อให้ความมั่นคงปลอดภัย (Information Security in Project Management)

2.2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากภายนอก (Mobile Devices and Teleworking)

วัตถุประสงค์: เพื่อรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศของการปฏิบัติการระยะไกลหรือการปฏิบัติงานจากภายนอกและการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา

รายละเอียดที่เกี่ยวข้อง:

(1) นโยบายสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)

เมื่อมีการใช้งานอุปกรณ์เคลื่อนที่แบบพกพา เช่น เครื่องคอมพิวเตอร์แบบพกพาได้และอุปกรณ์สื่อสารอื่น ๆ พนักงานของบริษัท อินเตอร์ ฟาร์มา จำกัด (มหาชน) จะต้องระมัดระวังเป็นพิเศษเพื่อให้มั่นใจได้ว่า ข้อมูลที่มีความสาคัญของบริษัทฯ ที่บันทึกอยู่ในอุปกรณ์จะไม่ถูกเปิดเผย เปลี่ยนแปลง แก้ไข หรือถูกทำลาย โดยผู้ไม่หวังดี โดยต้องมีการดำเนินการต่าง ๆ เพื่อลดความเสี่ยงของการใช้งานเป็นอย่างน้อย ดังนี้

- อุปกรณ์เคลื่อนที่แบบพกพาและอุปกรณ์สื่อสารอิเล็กทรอนิกส์แบบไร้สาย ที่ต้องการใช้งานผ่านระบบเครือข่ายของบริษัทฯ จะต้องได้รับการลงทะเบียนการใช้งานตามนโยบายความปลอดภัย ก่อนได้รับการอนุมัติเพื่อให้งานในระบบ โดยการลงทะเบียนของอุปกรณ์
- ต้องมีการเข้ารหัสไฟล์ข้อมูลหรือสื่อบันทึกข้อมูล

(2) การปฏิบัติงานจากระยะไกล (Teleworking)

เมื่อมีการปฏิบัติงานนอกสถานที่ตั้งของบริษัทอินเตอร์ ฟาร์มา จำกัด (มหาชน) ต้องมีการกำหนดเงื่อนไขและข้อจำกัดในการเข้าถึงและใช้งานสารสนเทศอย่างน้อยดังนี้

- การรักษาความมั่นคงปลอดภัยของสถานที่ปฏิบัติงานนอกสถานที่ตั้ง จะต้องสอดคล้องกับนโยบายด้านการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมที่กาหนดไว้
- ต้องมีการควบคุมการเข้าถึงระบบสารสนเทศภายในองค์กร
- ต้องมีการป้องกันความเสี่ยงจากการเข้าถึงสารสนเทศโดยไม่ได้รับอนุญาต จากบุคคลภายนอกองค์กร

3. การรักษาความปลอดภัยด้านทรัพยากรมนุษย์ (Human Resource Security)

3.1 การจัดหาบุคลากรก่อนการจ้างงาน (Prior to Employment)

วัตถุประสงค์: เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทหน้าที่ ที่ได้รับพิจารณาจ้างงานสำนักงาน

รายละเอียดที่เกี่ยวข้อง:

(1) การสรรหาบุคลากร (Screening)

(2) ข้อกำหนดและเงื่อนไขการจ้างงาน (Terms and conditions of employment)

3.2 การสร้างความมั่นคงปลอดภัยขณะเป็นเจ้าหน้าที่ (During employment)

วัตถุประสงค์: เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของสำนักงาน

รายละเอียดที่เกี่ยวข้อง:

(1) หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)

(2) การสร้างความตระหนัก การให้ความรู้และการอบรมให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training)

(3) กระบวนการทางวินัย (Disciplinary Process)

3.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

วัตถุประสงค์: เพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของการเปลี่ยนหน้าที่ หรือสิ้นสุดการจ้างงาน

รายละเอียดที่เกี่ยวข้อง:

(1) การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or Change of Employment Responsibilities)

4. การบริหารจัดการสินทรัพย์ (Asset Management)

4.1. การรับผิดชอบต่อสินทรัพย์ (Responsibility for Assets)

วัตถุประสงค์: เพื่อให้สินทรัพย์ของสำนักงาน ได้รับการป้องกันและปกป้องอย่างเหมาะสม

รายละเอียดที่เกี่ยวข้อง:

(1) ทะเบียนสินทรัพย์ (Inventory of assets)

(2) ความเป็นเจ้าของสินทรัพย์ (Ownership for Assets)

(3) การอนุญาตให้ใช้สินทรัพย์ (Acceptable Use for Assets)

(4) การคืนสินทรัพย์ (Return on Assets)

4.2 การจัดหมวดหมู่ข้อมูลและสินทรัพย์สารสนเทศ (Information Classification)

วัตถุประสงค์: เพื่อทำให้แน่ใจว่าสารสนเทศของสำนักงาน ได้รับการปกป้องในระดับที่เหมาะสม

รายละเอียดที่เกี่ยวข้อง:

(1) การจัดทำป้ายชื่อ ของข้อมูล (Labeling of Information)

(2) การจัดการสินทรัพย์ (Handling of Asset)

5. การเข้ารหัสข้อมูล (Cryptography)

5.1 การกำหนดการควบคุมการเข้ารหัสข้อมูล (Cryptographic controls)

วัตถุประสงค์: เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และเพื่อป้องกันความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

รายละเอียดที่เกี่ยวข้อง:

(1) นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)

6. ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมองค์กร (Physical and Environmental Security)

6.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

วัตถุประสงค์: เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพ ที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นสินทรัพย์สำนักงาน

รายละเอียดที่เกี่ยวข้อง:

(1) การกำหนดพื้นที่มั่นคงปลอดภัย (Physical Security Perimeter)

(2) การควบคุมการเข้าออก (Physical Entry Controls)

(3) การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ (Securing Offices, Rooms and Facilities)

(4) การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อมอื่น ๆ (Protecting against External and Environmental Threats)

(5) การปฏิบัติงานในพื้นที่มั่นคงปลอดภัย (Working in Secure Areas)

(6) การกำหนดพื้นที่สำหรับบุคคลภายนอกใช้รับ-ส่งสิ่งของ (Delivery and Loading Areas)

6.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment)

วัตถุประสงค์: เพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อให้มั่นใจได้ว่าอุปกรณ์คอมพิวเตอร์ได้มีการป้องกันอย่างเพียงพอจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่น ๆ

รายละเอียดที่เกี่ยวข้อง:

(1) การจัดตั้งและป้องกันอุปกรณ์ (Equipment Setting and Protection)

(2) การดูแลอุปกรณ์ต่าง ๆ (Supporting Utilities)

(3) การเดินสายไฟและสายเคเบิล (Cabling Security)

(4) การดูแลรักษาอุปกรณ์ (Equipment Maintenance)

(5) การนำสินทรัพย์ขององค์กรออกนอกสำนักงาน (Removal of Asset)

(6) การป้องกันอุปกรณ์และสินทรัพย์สารสนเทศที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment and asset Off-Premises)

(7) การจัดการอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้ใหม่ (Secure Disposal or Re-use of Equipment)

(8) การป้องกันอุปกรณ์ของผู้ใช้งานที่ไม่มีผู้ดูแล (Unattended User Equipment)

(9) การควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศที่สำคัญไว้ในที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy)

7. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)

7.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation Procedures and Responsibilities)

วัตถุประสงค์: เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

รายละเอียดที่เกี่ยวข้อง:

(1) การกำหนดขั้นตอนการปฏิบัติงานให้เป็นลายลักษณ์อักษร (Document Operating Procedures)

(2) การจัดการการเปลี่ยนแปลง (Change Management)

(3) การจัดการขีดความสามารถ (Capacity Management)

7.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

วัตถุประสงค์: เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเป็ฯไปอย่างถูกต้อง และมั่นคงปลอดภัย

รายละเอียดที่เกี่ยวข้อง:

(1) มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware)

7.3 การสำรองข้อมูล (Backup)

วัตถุประสงค์: เพื่อเป็นแนวทางในกำหนดการสำรองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่าง ๆ เช่น ภัยธรรมชาติ ระบบเสียหาย ฯลฯ

รายละเอียดที่เกี่ยวข้อง:

(1) การสำรองข้อมูล (Information Backup)

8 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communication Security)

8.1 การจัดการระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

วัตถุประสงค์: เพื่อป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของสำนักงาน

รายละเอียดที่เกี่ยวข้อง:

(1) การควบคุมการเข้าถึงเครือข่าย (Network Control)

(2) ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Service)

(3) การจัดแบ่งเครือข่ายภายในสำนักงาน (Segregation in Network)

9 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

9.1 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

วัตถุประสงค์: เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของสำนักงาน ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

รายละเอียดที่เกี่ยวข้อง:

(1) หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

(2) การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events)

(3) การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)

(4) การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)

(5) การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

(6) การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from Information Security Incidents)

(7) การเก็บรวบรวมหลักฐาน (Collection of Evidence)

10 การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)

10.1ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

วัตถุประสงค์: เพื่อป้องกันการหยุดชะงักในการดำเนินงานของสำนักงาน ที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบ

รายละเอียดที่เกี่ยวข้อง:

(1) การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)

(2) การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implement information security continuity)

(3) การตรวจสอบ ทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)

13.2 การเตรียมอุปกรณ์ประมวลผลสำรอง (Redundancies)

วัตถุประสงค์: เพื่อจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ

รายละเอียดที่เกี่ยวข้อง:

(1) สภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)

ลงชื่อ_____

ผู้จัดทำ

ลงชื่อ_____

ผู้อนุมัติ