SKIN
LABORATORY

นโยบายความปลอดภัยสารสนเทศ

บริษัท สกิน ลาบอราทอรี่ จำกัด

เพื่อให้ระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย และคอมพิวเตอร์ของบริษัท สกิน ลาบอราทอรี่ จำกัด (มหาชน) ("**บริษัท**") เป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัยและสามารถสนับสนุนการดำเนินงานของบริษัทได้อย่างต่อเนื่อง มีการใช้งานระบบในลักษณะที่ถูกต้องสอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่บริษัทบริษัทจึงกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

1. วัตถุประสงค์

1.1 เพื่อให้ข้อมูลของบริษัทมีความปลอดภัย ถูกต้อง พร้อมใช้งาน และไม่ถูกเปิดเผย หรือเปลี่ยนแปลงโดยผู้ไม่มีสิทธิเข้าถึง

1.2 เพื่อกำหนดหน้าที่ สิทธิในการเข้าถึงข้อมูล ของพนักงานในบริษัทได้อย่างชัดเจน

1.3 เพื่อกำหนดระยะเวลาในการทบทวนเพื่อความเหมาะสมในการปฏิบัติงาน

1.4 เพื่อกำหนดระยะเวลาในการดำเนินการ การจัดเก็บ และวิธีการทำลาย

1.5 เพื่อให้การใช้งานของระบบ, Application ของพนักงานมีความพร้อมใช้งานและทำงานได้อย่างมีประสิทธิภาพ

2. ขอบเขต

2.1 นโยบายนี้มีผลบังคับใช้กับทุกหน่วยงานโดยครอบคลุมข้อมูลประเภทต่าง ๆ รวมทั้ง ข้อมูลอิเล็กทรอนิกส์ของบริษัท

เอกสารอ้างอิง

แบบฟอร์มการแจ้งปัญหา (IT Request)"

3. คำจำกัดความ

"**พระราชบัญญัติ**" หมายความว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

"**ระบบคอมพิวเตอร์ของบริษัท**" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ ที่เชื่อการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ ทั้งที่เป็นทรัพย์สินของบริษัทและที่บริษัท
เป็นผู้จัดให้ใช้งาน

"**ข้อมูลคอมพิวเตอร์**" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"**ข้อมูลจราจรทางคอมพิวเตอร์**" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"**แผนกเทคโนโลยีสารสนเทศ**" หมายถึง แผนกที่ดูแล ติดตั้ง และควบคุมการให้บริการระบบเครือข่ายแก่แผนกต่าง ๆ ในบริษัท

"**ผู้ถือครองคอมพิวเตอร์**" หมายถึง พนักงาน หัวหน้างาน ผู้จัดการ หรือผู้ที่ทางบริษัทอนุญาตให้ถือครองเครื่องคอมพิวเตอร์ กรณีไม่มีผู้ถือครองโดยตรงให้เป็นความรับผิดชอบของหัวหน้าหน่วยงานซึ่งได้ถือครองอุปกรณ์คอมพิวเตอร์ดังกล่าว

"**หน่วยงาน**" หมายถึง แผนก และหน่วยงานต่างๆ ภายในบริษัท

"**ผู้ใช้งาน**" หมายถึง พนักงาน หัวหน้างาน ผู้จัดการ หรือผู้ที่ทางบริษัทอนุญาตให้ใช้ระบบคอมพิวเตอร์

"**โปรแกรมคอมพิวเตอร์**" หมายถึง ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์อื่นๆ ที่ทางบริษัทอนุญาตให้ทำการติดตั้ง

"**บริษัท**" หมายถึง บริษัท สกิน ลาบอราทอรี่ จำกัด (มหาชน) รวมถึงบริษัทในเครือที่อยู่ในความดูแลของหน่วยงาน/แผนกเทคโนโลยีสารสนเทศ

"**นโยบาย**" หมายถึง นโยบายการใช้ระบบคอมพิวเตอร์ของบริษัท

4. ผู้รับผิดชอบ พร้อมขอบเขตความรับผิดชอบ

4.1 แผนกเทคโนโลยีสารสนเทศ มีหน้าที่กำกับการปฏิบัติงานของผู้ใต้บังคับบัญชา ให้เป็นไปตามนโยบายความปลอดภัยสารสนเทศ

4.2 แผนกเทคโนโลยีสารสนเทศทำหน้าที่วางแผน และให้ความช่วยเหลือ แจ้งเตือน กรณีที่พนักงานในองค์กรไม่ปฏิบัติตามนโยบายความปลอดภัยสารสนเทศ

4.3 ผู้จัดการแผนก / หัวหน้างาน ต้องแจ้งให้ผู้ใต้บังคับบัญชาที่รับเข้าทำงานใหม่ รับทราบและลงชื่อก่อนเข้าปฏิบัติงานถึงระเบียบข้อบังคับการใช้งาน โดย

- 4.3.1 ไม่นำข้อมูลของบริษัทและลูกค้าไปเปิดเผย หรือหาผลประโยชน์จากผู้อื่น
- 4.3.2 ไม่นำทรัพย์สินของบริษัทเช่น Notebook, คอมพิวเตอร์, Server, อุปกรณ์คอมพิวเตอร์, ระบบอินเตอร์เน็ต, ข้อมูล, โปรแกรมต่าง ๆ ไปใช้งานเพื่อประโยชน์ส่วนตัว ทรัพย์สิน
- 4.3.3 ปฏิบัติตามข้อบังคับ กฎระเบียบของบริษัทอย่างเคร่งครัด รายละเอียดขอบเขต หน้าที่การงานที่ต้องปฏิบัติงาน

4.4 พนักงานแต่ละตำแหน่งมีสิทธิในการจัดการกับข้อมูลระดับต่างๆ ตามหน้าที่ที่กำหนดใน Job Description หรือและตามสิทธิที่กำหนดตามนโยบายฉบับนี้

5. นโยบาย (Policy)

บริษัทกำหนดระดับความปลอดภัย ประเภทข้อมูล สิทธิในการเข้าถึงข้อมูล ผู้รับผิดชอบ และเจ้าหน้าที่ทุกคนต้องปฏิบัติตามนโยบายนี้

เนื่องจากในบริษัทได้นำเอาระบบคอมพิวเตอร์มาใช้ส่วนสำคัญของการดำเนินธุรกิจและการปฏิบัติงานในทุกหน่วยงาน หากเครื่องมือในการให้บริการไม่มีความพร้อมใช้งาน หรือใช้งานอย่างไม่มีประสิทธิภาพก็จะส่งผลให้การให้บริการหยุดชะงัก เป็นผลให้เกิดความไม่พึงพอใจต่อผู้ใช้งาน

แนวทางในการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ โดยแบ่งเนื้อหาครอบคลุมต่างๆ ดังนี้

5.1 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

<u>วัตถุประสงค์</u>

เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ แก้ไขเปลี่ยนแปลง หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ และเพื่อป้องกันมิให้ข้อมูล และระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้าออกห้องคอมพิวเตอร์ และระบบป้องกันความเสียหายต่าง ๆ

แนวทางปฏิบัติ

5.1.1 กำหนดพื้นที่ใช้งานระบบสารสนเทศให้ชัดเจน และจัดทำแผนผังโดยการกำหนดพื้นที่ให้เป็นสัดส่วน เช่น แบ่งส่วนระบบเครือข่าย (Network zone) ส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server zone) ส่วนปฏิบัติงาน เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากยิ่งขึ้น

5.1.2 กำหนดสิทธิในการเข้าถึง และมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานแต่ละส่วนให้ชัดเจน

5.1.3 จัดให้มีระบบบันทึกรายละเอียดการผ่านเข้า-ออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

5.1.4 ในพื้นที่ใช้งานระบบสารสนเทศต้องมีระบบป้องกันความเสียหายต่างๆ

(1) ระบบป้องกันไฟไหม้ อย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

(2) ระบบป้องกันไฟฟ้าขัดข้อง ต้องมีระบบป้องกันไม่ให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟ, ต้องมีระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์สำคัญเพื่อให้การดำเนินงานมีความต่อเนื่อง

(3) ระบบควบคุมอุณหภูมิ โดยควรตั้งอุณหภูมิเครื่องปรับอากาศให้เหมาะสมกับคุณลักษณะของอุปกรณ์คอมพิวเตอร์ เนื่องจากอุปกรณ์คอมพิวเตอร์อาจทำงานผิดปกติภายใต้อุณหภูมิไม่เหมาะสม

5.2 การรักษาความปลอดภัยด้านการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

วัตถุประสงค์

เป็นการควบคุมการใช้ระบบคอมพิวเตอร์และระบบเครือข่ายเพื่อให้มีการใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ โดยให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

แนวทางปฏิบัติ

5.2.1 ผู้ใช้งานจะต้องไม่ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายโดยมีวัตถุประสงค์เพื่อนำเข้า เผยแพร่ หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะดังต่อไปนี้

(1) ข้อมูลคอมพิวเตอร์ใด ๆ ที่อาจกระทบกระเทือนต่อความมั่นคงของบริษัทหรือก่อให้เกิดความตื่นตระหนกแก่พนักงาน

(2) ข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของพนักงาน ซึ่งบุคคลทั่วไปอาจเข้าถึงข้อมูลนั้น ๆ ได้

(3) ข้อมูลคอมพิวเตอร์อันเป็นเท็จ หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน อันน่าจะเกิดความเสียหายแก่ผู้อื่น

5.2.2 ผู้ใช้งานจะต้องไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตามข้อ 6.2.1 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

5.2.3 การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์

(1) มีการกำหนดสิทธิการใช้ข้อมูลระบบคอมพิวเตอร์และระบบเครือข่าย โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร

5.2.4 การติดตามการทำงานของระบบคอมพิวเตอร์ (Monitoring)

(1) การบำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ให้อยู่ในสภาพที่ดีและพร้อมใช้งานอยู่เสมอ

5.2.5 การจัดการปัญหาต่าง ๆ

(1) มีกำหนดหน้าที่และความรับผิดชอบในดูแลระบบอย่างชัดเจนตาม (Organization Chart) โดยกำหนดผู้รับผิดชอบในการแก้ไขปัญหาเกี่ยวกับ ฮาร์ดแวร์ ซอฟท์แวร์ และระบบเครือข่ายอย่างชัดเจน

5.3 การรักษาความปลอดภัยด้านข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย

วัตถุประสงค์

การรักษาความปลอดภัยด้านข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่ายมีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (Access Risk) หรือแก้ไขเปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่ ส่วนการป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส รวมทั้ง Malware ต่าง ๆ มิให้เข้าถึง หรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย

แนวทางปฏิบัติ

5.3.1 การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege)

(1) ต้องกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ สิทธิการใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

(2) ในกรณีมีความจำเป็นต้องใช้ user ที่มีสิทธิพิเศษ ต้องมีการควบคุมการใช้งานอย่างรัดกุม โดยใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณา

- ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ก็ควรเปลี่ยนรหัสบ่อยๆ

(3) ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิและหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (log out ใน 900 วินาที) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์

(4) ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ share files เป็นต้น จะต้องเป็นการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว และเจ้าของข้อมูลต้องมีหลักฐาน

5.3.2 การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account)

(1) ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นจำนวน 7 Characters เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี user account เป็นของตนเอง และจะต้องทำการเปลี่ยนรหัสผ่านทุก 90 วัน

(2) ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญ อย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิใช้งานระบบแล้ว เช่น บัญชีรายชื่อของพนักงานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น disable ลบออกจากระบบ หรือเปลี่ยน password เป็นต้น

5.3.3 การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)

(1) ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

(2) ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติม

(3) ต้องดำเนิน Update ระบบงานสำคัญเพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) เช่น ระบบปฏิบัติการ และ Web Server เป็น อย่างสม่ำเสมอ

(4) ควรทดสอบ system software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา

(5) ควรกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของโปรแกรมระบบอย่างชัดเจน

5.3.4 การบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network)

(1) ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

(2) ระบบเครือข่ายทั้งหมดของบริษัทที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ นอกบริษัทต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก เช่น ไฟร์วอล (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

(3) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของบริษัทในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

5.3.5 การวางแผนการรองรับประสิทธิภาพของระบบคอมพิวเตอร์ (Capacity Planning)

5.3.6 การป้องกันไวรัส และ Malicious Code

5.3.7 บันทึกเพื่อการตรวจสอบ (Audit Logs)

5.4 การรักษาความปลอดภัยด้านการพัฒนา หรือปรับปรุงระบบงานคอมพิวเตอร์

วัตถุประสงค์

การคุมการพัฒนา หรือปรับปรุงระบบงานคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

แนวทางปฏิบัติ

5.4.1 การกำหนดขั้นตอนการปฏิบัติงาน

(1) ควรมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไข เปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน

(2) ควรมีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (Emergency Change) และควรมีการบันทึกเหตุผลความจำเป็น และขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง

(3) ควรสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม

5.4.2 การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน

(1) การร้องขอ

- การร้องขอให้มีการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร (อาจเป็น Electronic Transaction เช่น E-Mail หรือแบบฟอร์มในการร้องขอ เป็นต้น) และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ และ หัวหน้าแผนกเทคโนโลยีสารสนเทศ เป็นต้น
- ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง
- ควรสอบทานกฎเกณฑ์ของบริษัทที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของบริษัท

(2) การพัฒนาระบบงาน

- ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment : Database Test) ออกจากส่วนที่ใช้งานจริง (Production Environment : Database Live) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนตามที่กล่าว อาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้
- ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้องควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ
- ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนาหรือการแก้ไขเปลี่ยนแปลง

(3) การทดสอบ

- ผู้ที่ร้องขอและแผนกเทคโนโลยีสารสนเทศ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้อง และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง
- ในระบบงานสำคัญควรมีหน่วยงานหรือทีมงานอิสระ เข้าตรวจสอบว่ามีการปฏิบัติตามขั้นตอนการพัฒนาและการทดสอบระบบ ก่อนที่จะโอนย้ายไปใช้งานจริง

(4) การโอนย้ายระบบงานเพื่อใช้งานจริง ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ

(5) การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน และจัดเก็บ Version ของระบบงานที่ได้รับการพัฒนา

- ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงที่ผ่านมา
- ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และ Program Specification เป็นต้น และต้องจัดเก็บเอกสารตามที่กล่าวในที่ปลอดภัย และสะดวกต่อการใช้งาน
- ต้องจัดเก็บโปรแกรม Version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

(6) การทดสอบหลังการใช้งาน (Post-implementation Test) ควรกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

(7) การสื่อสารการเปลี่ยนแปลง ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

5.5 การรักษาความปลอดภัยด้านการสำรองข้อมูล และระบบคอมพิวเตอร์

<u>วัตถุประสงค์</u>

การสำรองข้อมูลและระบบคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และพร้อมใช้งานในเวลาที่ต้องการ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา

<u>แนวทางปฏิบัติ</u>

5.5.1 การสำรอง

(1) มีการสำรองข้อมูลสำคัญที่ใช้ในการปฏิบัติงาน รวมถึงโปรแกรมระบบปฏิบัติการ โปรแกรมระบบงานคอมพิวเตอร์ และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

(2) ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง

(3) จำนวนที่ต้องสำรอง (copy) ไม่น้อยกว่า 1 ชุด

(4) สถานที่รักษาสื่อบันทึก ต้องมีใช่ที่เดียว

(5) ควรมีการบันทึกการปฏิบัติงาน เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

5.5.2 การทดสอบ

(1) ควรมีขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน

5.5.3 การเก็บรักษา

(1) ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยมีหลายชุดการสำรองข้อมูล

(2) ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึกถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น ถ้าจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการเก็บอุปกรณ์และซอฟท์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นๆ ไว้ด้วยเช่นกัน

(3) ควรระบุชื่อชุดการสำรองข้อมูลที่ชัดเจนบนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็ว และเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

(4) การขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจหน้าที่ และควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง

5.6 การรักษาความปลอดภัยด้านการเตรียมพร้อมกรณีฉุกเฉิน

<u>วัตถุประสงค์</u>

การเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์เพื่อให้มีการจัดทำและการทดสอบแผนฉุกเฉิน เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และพร้อมใช้งานในกรณีเกิดเหตุการณ์ฉุกเฉิน

<u>แนวทางปฏิบัติ</u>

5.6.1 ต้องมีแผนฉุกเฉินเพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็วเพื่อให้เกิดความเสียหายน้อยที่สุด โดยแผนฉุกเฉินต้องมีรายละเอียดดังนี้

(1) ต้องจัดลำดับความสำคัญของระบบงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงาน

(2) ต้องกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา

(3) ต้องมีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

(4) ต้องกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ

(5) รวมทั้งต้องมีรายชื่อและหมายเลขโทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด

(6) ต้องปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ

5.6.2 ควรสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องได้รับทราบเฉพาะเท่าที่จำเป็น

5.6.3 ในกรณีเกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหาไว้ด้วย

5.7 การรักษาความปลอดภัยด้านการใช้บริการจากผู้ให้บริการรายอื่น

วัตถุประสงค์

การใช้บริการด้านงานสารสนเทศจากผู้ให้บริการรายอื่นอาจก่อให้เกิดความเสี่ยงต่อบริษัทในรูปแบบต่าง ๆ เช่น ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล ความเสี่ยงเกี่ยวกับความถูกต้องครบถ้วนของข้อมูลและการประมวลผลของระบบงาน ที่อาจเพิ่มขึ้นจากการดำเนินงานของผู้ให้บริการ เป็นต้น เพื่อให้บริษัทใช้บริการงานด้านสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ จึงจำเป็นต้องกำหนดแนวปฏิบัติโดยมีเนื้อหาครอบคลุมเกี่ยวกับการคัดเลือก และควบคุมการปฏิบัติงานของผู้ให้บริการ

แนวทางปฏิบัติ

5.7.1 การคัดเลือกผู้ให้บริการ

(1) ควรมีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุม และเป็นที่น่าเชื่อถือ

(2) ควรมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data Confidentiality) ขอบเขตงาน และเงื่อนไขในการให้บริการอย่างชัดเจน

5.7.2 การควบคุมผู้ให้บริการ

(1) ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ เช่น ให้เจ้าหน้าที่ผู้รับผิดชอบ ควบคุมดูแลการทำงานของผู้ให้บริการอย่างละเอียด และใกล้ชิด ทั้งในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ในพื้นที่ของบริษัท(Onsite Service) และในกรณีที่เป็นการให้บริการโดยเข้าถึงคอมพิวเตอร์หรือเครือข่ายจากระยะทางไกล (Remote Access) และต้องปิดการสื่อสาร ทันทีที่การให้บริการเสร็จสิ้น

(2) ควรดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

(3) ควรกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่าง ๆ และแนวทางแก้ไข

(4) ควรมีขั้นตอนในการตรวจรับงานของผู้ให้บริการ ให้เป็นไปตามกฎระเบียบและวิธีปฏิบัติของบริษัทอย่างเคร่งครัด

5.8 การรักษาความปลอดภัยด้านการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

วัตถุประสงค์

เพื่อกำหนดมาตรการในการใช้งานระบบจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัทซึ่งผู้ใช้ จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูและระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูและระบบเครือข่ายนั้นอย่างเคร่งครัด ซึ่งจะส่งผลให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัย และมีประสิทธิภาพ

<u>แนวทางปฏิบัติ</u>

5.8.1 สำหรับผู้ใช้งาน

(1) ผู้ใช้งานที่ต้องการใช้ระบบจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัท ต้องทำการกรอกข้อมูลคำขอเข้าใช้งาน เพื่อดำเนินการกำหนดสิทธิชื่อผู้ใช้งาน (User Name)

(2) ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของบริษัทเพื่อการทำงานของบริษัทเท่านั้น

(3) ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

(4) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

(5) ควรตรวจสอบและลบจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันเพื่อลดปริมาณการใช้พื้นที่ของระบบให้เหลือจำนวนน้อยที่สุด

(6) ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้งาน เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

5.8.2 สำหรับผู้ดูแลระบบ

(1) ต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของบริษัทให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ และหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้ง มีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก การโอนย้าย เป็นต้น

(2) ต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่ และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท

(3) ต้องกำหนดการใส่รหัสผ่านจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น เช่น ในการพิมพ์แต่ละตัวอักษร

(4) การตัดการใช้งานของผู้ใช้เมื่อไม่มีผู้ใช้ พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น disable ลบออกจากระบบ หรือเปลี่ยน password เป็นต้น

6.9 การรักษาความปลอดภัยด้านการใช้งานระบบอินเทอร์เน็ต (Internet)

<u>วัตถุประสงค์</u>

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และ เป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่นการส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบ คอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของบริษัทหรือบริษัทย่อยถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

แนวทางปฏิบัติ

5.9.1 สำหรับผู้ใช้งาน

(1) ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของบริษัทเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

(2) ต้องถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพ ของเครือข่ายและความปลอดภัยทางข้อมูลของบริษัท

(3) ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับบริษัท

(4) ห้ามผู้ใช้ เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัทที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

(5) ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จอันเป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูล คอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

(6) ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของบริษัทรวมถึง การทำลายความสัมพันธ์กับพนักงานของแผนกอื่น ๆ

(7) หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดโปรแกรมเว็บบราวเซอร์ (Web Browser) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

5.9.2 สำหรับผู้ดูแลระบบ

(1) ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น firewall เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและได้รับการอนุมัติจากผู้ดูแลระบบที่ได้รับมอบหมายแล้วเท่านั้น

(2) เครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์แบบพกพาจะต้องมีการติดตั้งโปรแกรมป้องกันไวรัส เพื่อเพิ่มความปลอดภัยในเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บบราวเซอร์

5.10 การรักษาความปลอดภัยด้านของไฟร์วอลล์ (Firewall Policy)

วัตถุประสงค์

เพื่อเป็นการสร้างความปลอดภัยให้กับเครือข่ายของบริษัท ทั้งในด้านของการจำกัดการเชื่อมต่อ และการจำกัดการใช้งาน ไฟร์วอลล์จะทำหน้าที่กำหนดขอบเขตที่ควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ข้อมูลที่ผ่านเข้า – ออกไฟร์วอลล์ จะเป็นข้อมูลที่ตรงตามที่นโยบายของบริษัทกำหนดเท่านั้น นโยบายการใช้งานไฟร์วอลล์มีไว้เพื่อใช้เป็นแนวทางปฏิบัติในการบริหาร และดูแลรักษาความปลอดภัยของระบบสารสนเทศของบริษัท

แนวทางปฏิบัติ

5.10.1 บริษัทมีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

5.10.2 การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

5.10.3 ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

5.10.4 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

5.10.5 การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

5.10.6 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

5.10.7 การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางบริษัทอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนดจะต้องได้รับความยินยอมจากบริษัทก่อน

5.10.8 การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

5.10.9 จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกเดือน หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

5.10.10 บริษัทมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มี ความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

5.10.11 ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

5.11 การทำลายอุปกรณ์บันทึกข้อมูล (การทำลายข้อมูลแบบกายภาพ)

วัตถุประสงค์

เพื่อทำลายข้อมูลสารสนเทศของบริษัท ที่มีความสำคัญซึ่งไม่สามารถเปิดเผยได้ ซึ่งข้อมูลดังกล่าวต้องได้รับการปกป้องไม่ให้ถูกเปิดเผยอย่างไม่เหมาะสม หรือถูกเข้าถึงโดยบุคคลที่ไม่มีสิทธิ์ในการเข้าถึงจากการเลิกใช้งานของสื่อบันทึกสารสนเทศต่าง ๆ จึงจัดให้มีข้อกำหนดในการทำลายอุปกรณ์บันทึกข้อมูล และสื่อบันทึกข้อมูลสารสนเทศของบริษัทขึ้น โดยให้ดำเนินการตามประเภทของสื่อบันทึกข้อมูล โดยกำหนดให้มีการทำลายสื่อบันทึกข้อมูลสารสนเทศ ปีละ 1 ครั้ง

นิยาม

“การชำระล้างข้อมูล และทำลายสื่อบันทึกข้อมูลอิเล็กทรอนิกส์” หมายถึง รูปแบบในการลบข้อมูล การล้างข้อมูล การทำลายสื่อบันทึกข้อมูลด้วยวิธีการที่ทำให้ไม่สามารถกู้กลับคืนมาใช้ได้อีก แม้ใช้วิธีการในห้องปฏิบัติการ

หมายเหตุ : Data Center and Network Equipment: แยกชิ้นส่วน HDD ออกจากเครื่อง, Factory reset ก่อนทำการขายซาก

Computer and Peripherals: แยกชิ้นส่วน HDD ออกจากเครื่อง, Factory reset แล้วทำการขายซาก

Storage Media : ดำเนินการทำลายข้อมูลทางกายภาพแล้วทำการขายซาก

<u>แนวทางปฏิบัติ</u>

5.11.1 ประเภท Optical Media เช่น CD, DVD ทำลายทางกายภาพ จนไม่สามารถนำข้อมูลกลับมาใช้ใหม่ได้ เช่น ขูดพื้นผิวด้านที่ใช้บันทึกข้อมูล, ตัดเป็นชิ้นเล็ก ๆ ก่อนกำจัดออกนอกบริษัท

5.11.2 สื่อแม่เหล็ก เช่น Floppy Disk, Magnetic Disk, Magnetic Tape เป็นต้น ทำลายทางกายภาพจนไม่สามารถนำข้อมูลกลับมาใช้ใหม่ได้ เช่น การใช้เครื่อง Hydraulic Press ในการกดทำลายสื่อ, ใช้วัตถุที่มีความแข็งแรงทุบทำลายสื่อ หรือจ้างบริษัทกำจัดสื่อบันทึกข้อมูลที่มีมาตรฐานสากล ก่อนกำจัดออกนอกบริษัท

5.11.3 Flash Memory-Based Storage Devices เช่น ATA Solid State Drive, SCSI SSD, NVM Express SSD เป็นต้น ทำลายทางกายภาพ จนไม่สามารถนำข้อมูลกลับมาใช้ใหม่ได้ เช่น การใช้เครื่อง Hydraulic Press ในการกดทำลายสื่อ ใช้วัตถุที่มีความแข็งแรงทุบทำลายสื่อ หรือจ้างบริษัทกำจัดสื่อบันทึกข้อมูลที่มีมาตรฐานสากล ก่อนกำจัดออกนอกบริษัท

5.11.4 Flash Memory-Based Storage Devices ที่เป็น USB Removable Media ทำลายทางกายภาพ จนไม่สามารถนำข้อมูลกลับมาใช้ใหม่ได้ เช่น ใช้วัตถุที่มีความแข็งแรงทุบทำลายสื่อ หรือหักทำลายชิ้นส่วน ก่อนกำจัดออกนอกบริษัท

5.11.5 RAM and ROM-Based Storage Devices เช่น DRAM ทำลายทางกายภาพ จนไม่สามารถนำข้อมูลกลับมาใช้ใหม่ได้ เช่น ใช้วัตถุที่มีความแข็งแรงทุบทำลายสื่อ หรือหักทำลายชิ้นส่วน ก่อนกำจัดออกนอกบริษัท

6. การทบทวนนโยบาย

กำหนดให้มีการทบทวนนโยบายความปลอดภัยสารสนเทศอย่างน้อยปีละ 1 ครั้งหรือทุกครั้งที่มีการเปลี่ยนแปลงนโยบาย

นโยบายฉบับนี้มีผลบังคับใช้ตั้งแต่วันที่ 26 กุมภาพันธ์ 2569 เป็นต้นไป
หมายเหตุ : เอกสารฉบับนี้ได้รับการทบทวนประจำปี 2569 โดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 1/2569

ลงชื่อ.....

(นายชาญวิทย์ เขียวนาวาวงศ์ษา)
ประธานเจ้าหน้าที่บริหาร
บริษัท สกิน ลาบอราทอรี่ จำกัด (มหาชน)