นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

บริษัท ไบโอซายน์ แอนิมัล เฮลธ์ จำกัด (มหาชน)

นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

1. คำนำ (Preamble)

บริษัท ไบโอซายน์ แอนิมัล เฮลธ์ จำกัด (มหาชน) และบริษัทย่อย (รวมเรียกว่า "**กลุ่มบริษัท**") ได้จัดทำนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อใช้เป็นแนวทางในการปฏิบัติงาน ควบคุมและดูแลการใช้งานเทคโนโลยีสารสนเทศ และใช้เป็นเครื่องมือในการประกอบธุรกิจได้อย่างเหมาะสม มีประสิทธิภาพ (Efficiency) และประสิทธิผล (Effectiveness) สามารถใช้งานบริการด้านเทคโนโลยีสารสนเทศ ด้วยความต่อเนื่อง (Availability) มีความถูกต้องครบถ้วนและมีความน่าเชื่อถือของข้อมูลและการทำงานของระบบคอมพิวเตอร์ (Confidentiality & Integrity) โดยมีการบริหารจัดการเรื่องการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์ในลักษณะที่ไม่ถูกต้อง (Privacy) ป้องกันความเสี่ยงเกี่ยวกับการใช้เทคโนโลยีสารสนเทศในการดำเนินงานของกลุ่มบริษัท (IT Risk Management) อันอาจจะก่อให้เกิดผลกระทบต่อการดำเนินงาน หรือก่อให้เกิดความเสียหายต่อกลุ่มบริษัทและลูกค้า ช่วยเสริมสร้างความมั่นใจในการใช้งานและการบริการด้านเทคโนโลยีสารสนเทศ รวมทั้งเสริมสร้างภาพลักษณ์ของกลุ่มบริษัทในการดำเนินกิจการต่าง ๆ ทั้งนี้ กลุ่มบริษัทจะต้องได้รับความร่วมมือจาก Authorized Users ทุกคนที่จะมี Awareness ในส่วนความรับผิดชอบด้านการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้กระบวนการจัดการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีประสิทธิผลตามนโยบายที่จัดทำขึ้น

2. วัตถุประสงค์ (Objectives)

นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศนี้ จะนำไปสู่การบรรลุเป้าหมายหรือวัตถุประสงค์หลักด้านการรักษาความปลอดภัย ดังนี้

(1) **การรักษาความลับของข้อมูล** (Confidentiality) คือ สามารถสร้างความมั่นใจได้ว่าข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับไม่ได้ถูกเปิดเผย และสามารถเข้าถึงได้เฉพาะบุคคลที่มีอำนาจหน้าที่ที่เกี่ยวข้องเท่านั้น ซึ่งเป็นการลดความเสี่ยงด้าน Access Risk

(2) **ความถูกต้อง ครบถ้วนสมบูรณ์ของข้อมูลและระบบสารสนเทศ** (Integrity & Reliability) คือ สามารถสร้างความมั่นใจในการใช้ข้อมูลและระบบงาน ซึ่งจะไม่สามารถแก้ไขด้วยวิธีการใด ๆ ที่ไม่ได้รับอนุญาต ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk

(3) **ความพร้อมใช้** (Availability) คือ สามารถสร้างความมั่นใจในการใช้ข้อมูลและระบบสารสนเทศที่มีอยู่ได้อย่างต่อเนื่อง หรือในทุกเวลาเมื่อต้องการ ซึ่งจะเป็นการลดความเสี่ยงด้าน Availability Risk

(4) **ประสิทธิภาพ และ ประสิทธิผล** (Efficiency & Effectiveness) คือ สามารถสร้างความมั่นใจในการบริหารจัดการและการวางแผนระบบเทคโนโลยีสารสนเทศ รวมทั้งการบริหารจัดการบุคลากรด้านนี้ ให้เพียงพอแก่การสนับสนุนการประกอบธุรกิจ อันจะเป็นการลดความเสี่ยงด้าน Infrastructure Risk

3. **ขอบเขตของนโยบาย** (Policy Scope)

นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ มีเนื้อหาครอบคลุมสาระสำคัญดังต่อไปนี้

(1) การจัดการด้านบุคลากร การกำหนดหน้าที่ปฏิบัติ โดยคำนึงถึงการควบคุมในระดับต่าง ๆ (Job Description and Segregation of Duties)

(2) การจัดการระบบรักษาความปลอดภัยทางกายภาพ (Physical Security)

(3) การจัดการระบบรักษาความปลอดภัยด้านข้อมูล (Information Security)

(4) การจัดการระบบรักษาความปลอดภัยด้านระบบงานคอมพิวเตอร์ ระบบปฏิบัติการ และระบบเครือข่าย (Application, Operating System and Network Security)

(5) การจัดการ การควบคุม การพัฒนา และการปรับปรุงระบบงานคอมพิวเตอร์ (Change Management)

(6) การจัดการระบบสำรองข้อมูล และการเตรียมพร้อมกรณีเกิดเหตุฉุกเฉิน (Backup System and IT Contingency Plan)

(7) การจัดการ การควบคุมการปฏิบัติงานประจำ และระเบียบวิธีการควบคุมการปฏิบัติงาน (Computer Operation Control)

(8) การจัดการ การควบคุม และตรวจสอบผู้ให้บริการ (IT Outsourcing)

ทั้งนี้ จะมีการทบทวนและปรับปรุงนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นประจำทุกปี โดยมีการประเมินความเสี่ยงจากผู้ตรวจสอบจากหน่วยงานอื่น หรือหน่วยงานภายนอก อย่างน้อยปีละ 1 ครั้ง

4. **คำจำกัดความ**

(1) กลุ่มบริษัท หมายถึง "บริษัท ไบโอซายน์ แอนิมัล เฮลธ์ จำกัด และบริษัทย่อย"

(2) กรรมการ หมายถึง ผู้ที่ได้รับการแต่งตั้งให้ทำหน้าที่กำหนดทิศทาง กลยุทธ์ และการดำเนินงานของกลุ่มบริษัท

(3) ประธานเจ้าหน้าที่บริหาร หมายถึง "Chief Executive Officer (CEO)" ซึ่งเป็นผู้มีสิทธิ์สูงสุด มีหน้าที่ในการสั่งการ มอบหมายงาน กำกับ หรือควบคุมการปฏิบัติงาน

(4) เจ้าหน้าที่สารสนเทศ หมายถึง เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ

(5) พนักงาน หมายถึง บุคคลที่ตกลงทำงานให้แก่กลุ่มบริษัท เพื่อรับค่าตอบแทนภายหลัง ซึ่งในที่นี้หมายความรวมถึง พนักงานที่ได้ผ่านพ้นกำหนดระยะทดลองงาน พนักงานทดลองงาน ลูกจ้างชั่วคราว พนักงานที่มีสัญญาจ้างพิเศษ พนักงานรายเดือน และพนักงานรายวัน

(6) บุคคลภายนอก หมายถึง บุคคลหรือหน่วยงาน ซึ่งไม่ได้รับค่าตอบแทนจากกลุ่มบริษัทโดยตรง ที่ได้รับอนุญาตให้เข้าถึงข้อมูลสารสนเทศ

(7) ข้อมูลสารสนเทศ ซึ่งต่อไปนี้เรียกว่า "ข้อมูล" หมายถึง ข่าวสาร ข้อเท็จจริง ข้อมูลในรูปแบบใด ๆ หรือข้อมูลที่มีการประมวลผลใด ๆ ทั้งในเหตุการณ์หรือกิจกรรมต่าง ๆ

หมวดที่ 1: การจัดการด้านบุคลากร การกำหนดหน้าที่ปฏิบัติ โดยคำนึงถึงการควบคุมในระดับต่าง ๆ (Job Description and Segregation of Duties)

1. **วัตถุประสงค์** (Objective)

เพื่อให้มีความชัดเจน เรื่องขอบเขตความรับผิดชอบและการปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย และทำให้เกิดดุลยภาพในการควบคุมและอำนาจในการจัดการดูแลระบบต่าง ๆ ในกลุ่มบริษัท ซึ่งเป็นการลดความเสี่ยงด้าน Infrastructure Risk

2. **ขอบเขต** (Scope)

(1) จะต้องกำหนด IT Organization ให้มีสายงานการบังคับบัญชาแยกกันระหว่างสายงาน Programming / Application สายงานการดูแล Operating System และ Network & Communication เพื่อให้การควบคุมด้าน Access ข้อมูลสำคัญต่าง ๆ มีความรัดกุม ทั้งนี้ จะต้องมีเจ้าหน้าที่สารสนเทศรับผิดชอบมากกว่า 1 หน่วยงาน ในการเข้าถึงข้อมูล ซึ่งจะเป็นการลดความเสี่ยงด้าน Access Risk

(2) กำหนด Job Description ของเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ ซึ่งจะระบุหน้าที่และขอบเขตการทำงาน รวมถึงความรับผิดชอบอย่างชัดเจน โดยรายละเอียดดังกล่าว จะแสดงไว้ในเอกสาร Job Description ตามแต่ละบุคคลในแผนก นอกจากนี้ เจ้าหน้าที่สารสนเทศทุกคนจะต้องได้รับทราบ Job Description ของตนเอง

(3) มีการกำหนดเจ้าหน้าที่สารสนเทศ อย่างน้อย 1 คน ในหน้าที่ความรับผิดชอบแต่ละงาน

หมวดที่ 2: การจัดการระบบรักษาความปลอดภัยทางกายภาพ (Physical Security)

1. **วัตถุประสงค์** (Objective)

การรักษาความปลอดภัยทางกายภาพ จะเน้นการดูแลห้อง Server ทั้งในลักษณะการควบคุมการเข้า - ออกของบุคลากรต่าง ๆ ทั้งในและนอกกลุ่มบริษัท เพื่อป้องกันการล่วงรู้ และ/หรือ การแก้ไขเปลี่ยนแปลงข้อมูล โดยผู้ที่ไม่มีอำนาจหน้าที่ รวมทั้งการจัดการระบบป้องกันความเสียหายต่าง ๆ ที่อาจจะเกิดขึ้นภายในศูนย์คอมพิวเตอร์ ทั้งจากสภาวะแวดล้อมและภัยพิบัติต่าง ๆ เพื่อป้องกันความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ อันจะนำความเสียหายต่อธุรกิจของกลุ่มบริษัท ซึ่งจะเป็นการลดความเสี่ยงด้าน Access Risk, Integrity Risk และ Availability Risk

2. **ขอบเขต** (Scope)

(1) การควบคุมการเข้า - ออกห้อง Server ของบุคลากรทั้งในและนอกกลุ่มบริษัท จะต้องได้รับสิทธิ์หรือได้รับอนุญาตก่อนเสมอ โดยเจ้าหน้าที่สารสนเทศจะมี Authorization ในการเข้า - ออกตลอด 24 ชั่วโมง อย่างไรก็ดี สำหรับบุคลากรที่นอกเหนือจากนี้ จะต้องได้รับอนุญาตจากประธานเจ้าหน้าที่บริหารก่อน จึงจะสามารถเข้าห้อง Server ได้ ทั้งนี้ ห้อง Server เป็นที่จัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญที่ได้มีการใช้งานในปัจจุบัน เช่น Server, Network & Communication Equipment เป็นต้น ซึ่งจะเป็นห้องแยกต่างหากจากพื้นที่ส่วนกลาง โดยมีการควบคุมการเข้า - ออกพื้นที่ส่วนนี้เพิ่มเติมจากพื้นที่ส่วนกลางและต้องมีการควบคุมการเข้า – ออกอย่างเข้มงวด โดยจะต้องมีการกำหนดในเรื่องดังต่อไปนี้

1) กำหนดสิทธิ์ของผู้ที่จะเข้า - ออกห้อง Server

2) ผู้ที่มาติดต่อหรือผู้ให้บริการด้านต่าง ๆ ที่เกี่ยวข้องกับอุปกรณ์ที่ใช้งานในห้อง Server จะต้องมีการลงลายมือชื่อและเวลาเข้า - ออก โดยจะมีเจ้าหน้าที่สารสนเทศเป็นผู้รับผิดชอบและควบคุมการเข้า - ออกห้อง Server ลงชื่อกำกับทุกครั้ง

3) ผู้รับผิดชอบส่วนงานทั้งด้านระบบปฏิบัติการและเครือข่าย จะต้องดูแลรับผิดชอบดูแลรักษาความสะอาด และจัดอุปกรณ์ต่าง ๆ ในห้อง Server ให้ทำงานอย่างถูกต้องและเรียบร้อย

4) ผู้รับผิดชอบส่วนงานทางด้าน Administration จะต้องตรวจสอบและควบคุมให้มีการบันทึกลงนามบุคคลต่าง ๆ ที่ไม่มีหน้าที่รับผิดชอบโดยตรงกับห้อง Server และเวลาการเข้า - ออกห้อง Server ทุกครั้ง และให้เจ้าหน้าที่สารสนเทศลงนามรับทราบในทะเบียนด้วยทุกครั้งที่มีการเข้า - ออก นอกจากนี้ จะต้องมีเจ้าหน้าที่สารสนเทศควบคุมดูแลการทำงานตลอดเวลา

5) ห้ามสูบบุหรี่ หรือนำอาหาร-เครื่องดื่มเข้าห้อง Server

(2) มาตรฐานพื้นที่บริเวณห้อง Server

1) มีการกั้นผนังแบ่งพื้นที่เป็นห้องอย่างเป็นสัดส่วน โดยมีการควบคุมเรื่องการเข้า – ออกห้อง Server ด้วยประตูที่มีระบบ Scan นิ้ว และกุญแจล็อคพื้นที่ภายในห้อง Server

2) พื้นที่ภายในห้อง Server ต้องมีการจัดสรรพื้นที่ โดยจัดตั้งและวางอุปกรณ์เป็นสัดส่วน สามารถควบคุมดูแลได้อย่างสะดวก และมีความสะอาดเรียบร้อย

3) พื้นที่ภายในห้อง Server ต้องมีสภาพแสงที่เหมาะสม ผนังหรือกระจกของห้องต้องสามารถป้องกันแสงแดดและรังสีจากภายนอกได้

4) พื้นที่ภายในห้อง Server รวมถึงฝ้า ต้องมีการปิดสนิทมิดชิด เพื่อป้องกันสัตว์ เช่น หนู และแมลงต่าง ๆ เป็นต้น รวมทั้ง เพื่อควบคุมความชื้นและหยดน้ำต่าง ๆ ที่อาจเป็นภัยต่อระบบได้

5) พื้นที่ภายในห้อง Server ต้องมีการควบคุมอุณหภูมิให้คงที่ด้วยระบบความเย็นตลอด 24 ชั่วโมง และตรวจเช็คทำความสะอาดแอร์ ทุก ๆ 6 เดือน

6) พื้นที่ภายในห้อง Server ต้องมีเครื่องสำรองไฟ เพื่อป้องกันไฟตกหรือไฟกระชาก ที่อาจทำให้ Hardware เสียหาย นอกจากนี้ ควรมีการตรวจสอบเครื่องสำรองไฟในห้อง Server ทุก ๆ 6 เดือน

7) พื้นที่ภายในห้อง Server อย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

หมวดที่ 3: การจัดการระบบรักษาความปลอดภัยด้านข้อมูล (Information Security)

1. **วัตถุประสงค์** (Objective)

การรักษาความปลอดภัยของข้อมูล เป็นสิ่งที่สำคัญอย่างยิ่ง เพื่อควบคุมการเข้าถึงข้อมูลของบุคคลที่ไม่มีอำนาจหรือหน้าที่เกี่ยวข้อง เช่น การแก้ไขหรือเปลี่ยนแปลงข้อมูลโดยที่ไม่มี Authorization เป็นต้น และเพื่อให้การใช้งานระบบคอมพิวเตอร์เป็นไปอย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk และ Access Risk

2. **ขอบเขต** (Scope)

(1) การบริหารจัดการข้อมูล (Data Management)

1) มีการกำหนดระดับของข้อมูล หรือประเภทของข้อมูล เพื่อควบคุมการเข้าถึงข้อมูลของเจ้าหน้าที่สารสนเทศและผู้ปฏิบัติงาน ให้เป็นไปอย่างถูกต้อง ตรงกับหน้าที่และความรับผิดชอบของแต่ละบุคคล

2) มีการกำหนดวิธีการเข้าถึงข้อมูลตามลักษณะการปฏิบัติงานของเจ้าหน้าที่สารสนเทศ ซึ่งสามารถแบ่งได้ดังนี้

ก. การเข้าถึงข้อมูลโดยตรง ผู้ที่เข้าถึงข้อมูลได้แก่เจ้าหน้าที่ผู้ดูแลรักษาระบบนั้น ๆ เพื่อประโยชน์ในงานบริการ ซึ่งได้แก่ การตรวจสอบ ความถูกต้องของข้อมูล หรือการตรวจสอบแก้ไขระบบงาน เป็นต้น

ข. การเข้าถึงข้อมูลผ่านระบบ ได้แก่ ผู้ใช้งานระบบที่มีอำนาจหน้าที่และความรับผิดชอบตามที่ได้รับมอบหมายจากประธานเจ้าหน้าที่บริหาร รวมทั้งเจ้าหน้าที่ปฏิบัติการหรืองาน Administration ด้านเทคโนโลยีสารสนเทศ

ค. การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL การใช้ VPN เป็นต้น

ง. การรับส่งข้อมูลที่เป็นข้อมูลสำคัญ ต้องมีการรับส่งผ่าน E-Mail ของกลุ่มบริษัท (@bis-group.com) เท่านั้น ทั้งนี้ การรับส่งข้อมูลที่เป็นข้อมูลสำคัญต้องไม่ใช้ E-Mail ส่วนตัวในการรับส่งข้อมูล

3) การถ่ายโอนข้อมูลที่เป็นข้อมูลสำคัญ หรือ ความลับ ผ่านการใช้สื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ เช่น Thumb-Drive, CD-ROM, External Hard disk เป็นต้น ต้องได้รับอนุญาตจากประธานเจ้าหน้าที่บริหาร และต้องให้เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศเป็นผู้ดำเนินการให้

4) มีมาตรการการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ ตั้งแต่การนำข้อมูลเข้าประมวลผล การประมวลผล การแสดงผล รวมทั้ง การจัดการด้าน Storage

5) การนำอุปกรณ์คอมพิวเตอร์ออกนอกพื้นที่ของกลุ่มบริษัท เช่น การส่งซ่อม การขายทรัพย์สิน เป็นต้น โดยเฉพาะอุปกรณ์ที่มีการจัดเก็บข้อมูลสำคัญต่าง ๆ ควรพิจารณาหาวิธีการที่เหมาะสมในการควบคุมดูแลรักษาข้อมูล หากไม่สามารถควบคุมดูแลรักษาข้อมูลได้ ควรทำลายข้อมูลที่มีการจัดเก็บอยู่ในสื่อบันทึกข้อมูลก่อน เพื่อป้องกันการแพร่กระจายของข้อมูลออกไปนอกกลุ่มบริษัท

6) การนำอุปกรณ์คอมพิวเตอร์ส่วนบุคคลเข้ามาใช้ในกลุ่มบริษัท จะต้องไม่เชื่อมต่อกับเครือข่ายภายในกลุ่มบริษัท หากต้องการเชื่อมต่อกับเครือข่ายภายในกลุ่มบริษัทต้องดำเนินการขออนุญาตจากประธานเจ้าหน้าที่บริหาร และต้องได้รับการตรวจสอบจากเจ้าหน้าที่สารสนเทศก่อนเสมอ

7) มีมาตรการจัดการและควบคุมดูแลด้านฐานข้อมูลต่าง ๆ ภายในองค์กร เช่น การจัดการข้อมูลในเครื่องคอมพิวเตอร์ของพนักงานในส่วนที่ไม่จำเป็น เป็นต้น เพื่อป้องกันข้อมูลที่มากเกินกว่าหน่วยความจำที่รับได้ในแต่ละอุปกรณ์

(2) การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Permission)

1) จะต้องมีการกำหนดสิทธิ์ในการใช้งานข้อมูลและระบบงานคอมพิวเตอร์

2) การใช้งาน User ที่มีสิทธิ์พิเศษสูงสุดของแต่ละระบบงาน เช่น User Admin, User System เป็นต้น จะต้องมีการควบคุมการใช้งานดังนี้

ก. การใช้งานจะต้องได้รับอนุญาตจากประธานเจ้าหน้าที่บริหาร

ข. การเก็บ Password ของ User เหล่านี้ ไว้ในซองปิดผนึก ในกรณีที่พิจารณาแล้วว่าเป็นกรณีที่สำคัญและจำเป็นต้องใช้งาน และไม่เปิดเผยให้กับบุคคลที่ไม่ได้รับอนุญาต

ค. มีการกำหนดระยะเวลาการใช้งาน และเมื่อใช้งานเสร็จสิ้นแล้ว ควรมีการเปลี่ยนรหัสผ่านใหม่ทุกครั้ง

ง. กำหนดให้มีการเปลี่ยนรหัสผ่านในทุก 180 วันหรือทุกครั้งที่ได้รับการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

3) การใช้งาน User ที่มีสิทธิพิเศษสูงสุดของแต่ละระบบ ผู้ใช้งานจะต้องมีความระมัดระวังอย่างสูง ในกรณีที่ไม่ใช้งาน User แล้ว ผู้ใช้งานจะต้อง Logout ออกจากระบบทันที ทั้งนี้ ผู้ใช้งานจะต้องไม่ทิ้งหน้าจอให้ Login ค้างอยู่ โดยที่ไม่มีเจ้าหน้าที่ควบคุมการทำงานอยู่ในบริเวณนั้นโดยเด็ดขาด

4) การให้สิทธิการใช้งาน User ที่มีสิทธิพิเศษสูงสุดของแต่ละระบบแก่บุคคลอื่น ในกรณีฉุกเฉิน หรือชั่วคราว จะต้องมีการขออนุมัติจากผู้บังคับบัญชาสูงสุดด้านเทคโนโลยีสารสนเทศ และควรจะระบุถึงเหตุผลและความจำเป็นในการใช้งาน โดยจะต้องมีการกำหนดเวลาใช้งาน รวมทั้งจะต้องมีการควบคุมและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาที่กำหนดไว้

5) การกำหนดสิทธิสำหรับผู้ใช้งานอื่นใดที่นอกเหนือจากเจ้าของข้อมูลสำคัญ จะต้องมีการควบคุมการกำหนดสิทธิให้เฉพาะราย หรือเฉพาะกลุ่มที่ได้มีการพิจารณาเห็นชอบจากผู้บังคับบัญชาหน่วยงานนั้น ๆ หรือผู้มีอำนาจหน้าที่ทุกครั้งว่ามีความจำเป็นในการใช้งานจริง และควรมีการกำหนดระยะเวลาใช้งาน หรือการควบคุมการใช้งานให้เป็นไปตามที่กำหนด และระงับการใช้งานทันทีที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไป

6) ในกรณีที่มีความจำเป็นที่ผู้ใช้งาน ซึ่งเป็นเจ้าของข้อมูลสำคัญ มีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ Share files เป็นต้น จะต้องเป็นการให้สิทธิเฉพาะราย หรือเฉพาะกลุ่มเท่านั้น และต้องดำเนินการยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว

(3) การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User ID) และ รหัสผ่าน (Password)

1) จัดให้มีระบบการตรวจสอบตัวตนในการเข้าใช้งานระบบงานต่าง ๆ ของกลุ่มบริษัท (Identification and Authentication) เช่น การสร้าง User Account หรือ User ID สำหรับการใช้งานระบบงานต่าง ๆ โดยกำหนดให้ผู้ใช้งานแต่ละรายมี User ID เป็นของตัวเอง

2) การสร้าง User ID ให้แก่ผู้ใช้งาน เพื่อควบคุมการใช้ระบบงานคอมพิวเตอร์ที่มีการเก็บข้อมูลสำคัญของกลุ่มบริษัท โดยจะต้องมีการพิจารณาถึงความเหมาะสม และอำนาจหน้าที่ที่มีความจำเป็นในการใช้งานระบบต่าง ๆ ของผู้ใช้งาน ซึ่งการสร้างและการปรับปรุงแก้ไข เช่น การเพิ่มและลดบัญชีรายชื่อผู้ใช้งาน เป็นต้น จะต้องได้รับการพิจารณาเห็นชอบจากผู้บังคับบัญชาหน่วยงานนั้น ๆ หรือผู้มีอำนาจหน้าที่ทุกครั้งเป็นลายลักษณ์อักษร ว่ามีความจำเป็นในการขอใช้ระบบงานนั้นจริง

3) จะต้องมีการกำหนดเกณฑ์การสร้าง Password หรือแก้ไข Password อย่างน้อย ดังต่อไปนี้

ก. กำหนดให้ Password มีความยาวอย่างน้อย 8 ตัวอักษร

ข. จะต้องมีการกำหนดให้มีการเปลี่ยน Password ตามช่วงเวลา ดังนี้

- กรณีที่เป็น User ที่มีสิทธิพิเศษของแต่ละระบบ จะต้องมีการเปลี่ยน Password อย่างน้อยทุก 90 วัน
- กรณีที่เป็น User ทั่วไป จะต้องเปลี่ยนรหัสผ่านในทุก 180 วันหรือทุกครั้งที่ได้รับการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ค. ผู้ใช้งานจะต้องเก็บ Password ไว้เป็นความลับ อย่างไรก็ดี ในกรณีที่มีการล่วงรู้ Password โดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที ทั้งนี้ หลักการกำหนดรหัสผ่านมีดังต่อไปนี้

- ไม่กำหนด Password อย่างเป็นแบบแผน เช่น "123456" หรือ "ABCDEF" เป็นต้น
- ไม่กำหนด Password ที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน-เดือน-ปี เกิด ที่อยู่ เป็นต้น
- ไม่กำหนด Password เป็นคำศัพท์ที่อยู่ในพจนานุกรม

ง. สำหรับระบบงานที่มีข้อมูลสำคัญควรมีการกำหนดวิธีการต่าง ๆ เพิ่มเติมดังนี้

- ควรมีการกำหนดให้ใช้ตัวอักษรเล็กสลับกับตัวอักษรใหญ่ หรืออักขระพิเศษประกอบอยู่ใน Password
- จัดให้มีการจัดส่ง Password ให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย

4) เจ้าหน้าที่สารสนเทศจะทำการตรวจสอบจำนวนรายชื่อผู้ใช้งาน (User ID) และ รหัสผ่าน (Password) ทุกเดือน เพื่อให้สอดคล้องกับจำนวนของผู้ใช้งานที่มีอยู่จริง ร่วมกับฝ่ายงานที่เกี่ยวข้อง

5)

6) ในกรณีที่มีพนักงานลาออก เจ้าหน้าที่สารสนเทศต้องดำเนินการเปลี่ยนรหัส หรือ ยกเลิกรายชื่อผู้ใช้งาน (User ID) และ รหัสผ่าน (Password) ทันที

หมวดที่ 4: การจัดการระบบรักษาความปลอดภัยด้านระบบงานคอมพิวเตอร์ ระบบปฏิบัติการและระบบเครือข่าย (Application, Operating System and Network Security)

1. วัตถุประสงค์ (Objective)

เพื่อเป็นการรักษาความปลอดภัยของข้อมูลและระบบงานคอมพิวเตอร์ที่สำคัญของกลุ่มบริษัท จะต้องสามารถควบคุมการเข้าถึงข้อมูลและระบบงานต่าง ๆ ได้ โดยป้องกันไม่ให้บุคคลที่ไม่มีอำนาจ บุคคลที่ไม่มีหน้าที่เกี่ยวข้องหรือบุคคลภายนอก สามารถเข้าถึงข้อมูลหรือระบบงาน การจัดการระบบรักษาความปลอดภัยจะต้องสามารถป้องกันการ

แก้ไขหรือเปลี่ยนแปลงข้อมูลโดยที่ไม่มี Authorization ตรวจสอบ ดูแลและป้องกันการถูกบุกรุกระบบผ่านเครือข่าย ทั้งการ Access เข้ามาโดยตรง หรือผ่าน Virus, Malicious Code ต่าง ๆ ทั้งนี้ เพื่อให้การใช้งานระบบคอมพิวเตอร์เป็นไปอย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk, Access Risk และ Availability Risk

2. **ขอบเขต** (Scope)

(1) การบริหารจัดการและรักษาความปลอดภัยระบบเครือข่าย (Firewall)

1) กำหนดกฎของ Firewall ให้เปิดใช้บริการที่จำเป็นต้องใช้ ทั้งนี้ นอกเหนือจากกฎที่กำหนด ให้มีการปฏิเสธการใช้งานระบบทั้งหมด และปฏิเสธการสแกนตรวจสอบด้วยโปรแกรมประเภท Network Scanning Tools ต่าง ๆ เช่น Nmap เป็นต้น

2) จำกัด User ที่ใช้บริหารจัดการและผู้ใช้ที่มีบน Firewall ให้น้อยที่สุด

3) เปลี่ยน User Name ที่ผู้ขายได้ให้มาเช่น Root หรือ Administrator และเปลี่ยน Password ให้ยากต่อการคาดเดา

4) ในการเพิ่มกฎของ Firewall เข้าไปใหม่ จะต้องไม่ขัดแย้งกับกฎเดิมที่มีอยู่แล้ว และกฎที่เพิ่มเข้าไปจะต้องทำงานได้มีประสิทธิภาพดีกว่าเดิม

5) จะต้องมีการ Backup กฎของ Firewall เดิมทุกครั้ง มีการแก้ไขกฎ เพื่อที่จะป้องกันในกรณีที่กฎที่เพิ่มเข้าไปมีปัญหาจะได้นำกลับมาติดตั้งและใช้งานได้อย่างรวดเร็ว

6) ควรตอบสอบกฎของ Firewall อย่างน้อยปีละ 1 ครั้ง

7) ไม่อนุญาตการเข้าถึง Firewall ในระยะไกล เช่น Telnet Ssh เป็นต้น

8) เมื่อมีการแก้ไขหรือเพิ่มกฎทุกครั้ง ต้องมีการบันทึกการแก้ไขไว้เป็นหลักฐาน ซึ่งต้องสามารถนำมาตรวจสอบได้ในกรณีที่ Firewall มีปัญหา และต้องได้รับอนุญาตจากผู้ดูแลระดับสูง หรือ หัวหน้าระดับสูงก่อนเข้าไปเพิ่มหรือแก้ไขข้อมูลใน Firewall ทุกครั้ง

9) สำรองข้อมูลของ Firewall ไว้ในสื่อที่บันทึกทับไม่ได้ เช่น CD-R เพื่อใช้อ้างอิงหรือดำเนินคดีทางกฎหมาย

10) สำรองข้อมูลของ Firewall เดือนละ 1 ครั้งและจะต้องนำไปรักษาที่ปลอดภัยเก็บนอกกลุ่มบริษัท

11) ผู้ที่ดูแลระบบ Firewall จะต้องมีความรู้ความสามารถในการบริหารจัดการ และได้รับการอบรมจากผู้ขายในด้าน Firewall ที่ใช้งานอยู่และการสร้างความปลอดภัย

12) จัดทำคู่มือการบริหารและการจัดการ Firewall โดยในกรณีที่ผู้ดูแลระบบลาออกจะต้องสามารถนำมาใช้อ้างอิงการทำงานในภายหลังได้

13) มีการตรวจเช็คความถูกต้องในการเพิ่มกฎข้อมูล ทุก ๆ 1 เดือน ในกรณี เพิ่ม/แก้ไข ข้อมูล Firewall เพื่อป้องกันการสร้างกฎที่เป็นภัยกับองค์กร

14) มีการเก็บ Logging Firewall ย้อนหลังเพื่อไว้ตรวจสอบ Log การใช้งานต่าง ๆ ของ User หากในกรณีที่เกิดปัญหาต่าง ๆ ขึ้น

(2) การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server Security) จัดให้มีการเปิดบริการ (Service) เท่าที่จำเป็นบนแต่ละ Server

1) ในกรณีที่มีความจำเป็นต้องเปิด Service เพิ่มเติม จะต้องมีการพิจารณาเป็นรายกรณีไป และจะต้องมีการตรวจสอบ เพื่อความมั่นใจว่ามีความเสี่ยงต่อระบบรักษาความปลอดภัยมากน้อยเพียงใด ทั้งนี้ อาจจะต้องมีการกำหนดมาตรการ รวมทั้ง มีการติดตั้งอุปกรณ์ หรือ Software อื่นใดเพิ่มเติม เพื่อเพิ่มการป้องกันและรักษาความปลอดภัยของระบบ

2) ในกรณีที่มีการทดสอบระบบงานใหม่ หรือปรับปรุงระบบงานเพิ่มเติม ซึ่งจำเป็นจะต้องมีการเปิด Service เพิ่มเติม ควรจะต้องมีการจัดทำตามข้อ 1) และจะต้องมีการกำหนดช่วงเวลาการทดสอบนอกจากนี้ หากมีการยกเลิกการทดสอบดังกล่าวแล้ว จะต้องทำการปิด Service เหล่านั้นโดยทันที

3) จะต้องมีการตรวจสอบค่า Parameter ของ Server อย่างสม่ำเสมอ ในกรณีที่พบว่ามีการใช้งานหรือมีการเปลี่ยนแปลงค่า Parameter เหล่านั้น ในลักษณะที่ผิดปกติ อันอาจจะก่อให้เกิดปัญหาในการควบคุมความปลอดภัยของระบบ จะต้องดำเนินการแก้ไข รวมทั้ง จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันที

(3) การบริหารจัดการและตรวจสอบระบบเครือข่าย (Network Security)

1) จะต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งจะต้องครอบคลุมรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก รวมถึงอุปกรณ์ต่าง ๆ ที่ใช้ในระบบเครือข่าย ทั้งนี้ จะต้องมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอและจะต้องเก็บรักษาข้อมูลในส่วนที่เป็นข้อมูลสำคัญให้อยู่ในที่ปลอดภัย

2) ต้องมีการแยกระบบเครือข่ายเป็นสัดส่วนตามการใช้งาน โดยอย่างน้อยจะต้องมีการแยกเครือข่ายระหว่างเครือข่ายภายในบกลุ่มบริษัทและเครือข่ายนอกกลุ่มบริษัทออกจากกัน

3) จัดให้มีระบบป้องกันการบุกรุกจากเครือข่ายภายนอกในการเข้ามาในระบบเครือข่ายภายในนอกจากนี้ ควรมีการพิจารณาการป้องกันการถูกบุกรุกหรือการใช้งานในลักษณะผิดปกติจากผู้ใช้งานในระบบเครือข่ายภายในอย่างสม่ำเสมอ โดยมีการตรวจสอบในเรื่องดังต่อไปนี้

ก. ความพยายามในการบุกรุกผ่านระบบเครือข่าย

ข. การใช้งานในลักษณะผิดปกติ

ค. การใช้งานและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง ทั้งนี้ การตรวจสอบโดยเฉพาะการจัดทำ Network Scanning จะต้องจัดทำโดยเจ้าหน้าที่สารสนเทศที่มีหน้าที่รับผิดชอบเรื่องนี้โดยตรง พนักงานของกลุ่มบริษัท คนอื่น ๆ ไม่ว่าจะเป็นเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศที่ไม่เกี่ยวข้อง หรือฝ่ายอื่นก็ตาม จะต้องไม่กระทำการจัดทำ Network Scanning โดยเด็ดขาด

4) การเพิ่มเติมหรือปรับปรุงการต่อเชื่อมระบบเครือข่ายระหว่างภายในและภายนอกเพิ่มเติม จะต้องมีการพิจารณาและตรวจสอบระบบการรักษาความปลอดภัยของอุปกรณ์คอมพิวเตอร์เหล่านั้น ไม่ว่าจะเป็นการกำหนดค่า Parameter ต่าง ๆ ที่เกี่ยวข้องกับระบบรักษาความปลอดภัยหรือการตรวจสอบไวรัส

5) ในกรณีที่มีการติดตั้งอุปกรณ์เครือข่ายเพิ่มเติม เพื่อการทดสอบระบบงานใหม่หรือทดสอบการต่อเชื่อมเครือข่ายใด ๆ ควรมีการกำหนดช่วงเวลาการทดสอบ ทั้งนี้ หากได้มีการยกเลิกการทดสอบนั้นแล้ว จะต้องทำการตัดการเชื่อมต่อเข้าเครื่องคอมพิวเตอร์และยกเลิกจุดเชื่อมต่อทั้งหมดโดยทันที นอกจากนี้ ต้องมีการตรวจสอบการกำหนดค่า Parameter ของอุปกรณ์เครือข่ายที่เกี่ยวข้องกับอุปกรณ์ดังกล่าว เพื่อความมั่นใจในการดูแลและจัดการระบบรักษาความปลอดภัยเครือข่าย

6) การใช้ระบบเครือข่ายในลักษณะ Remote Access หรือการเชื่อมต่อเครือข่ายภายนอก

ก. กรณีที่ 1 การเชื่อมต่อโดยเจ้าหน้าที่สารสนเทศ เพื่อใช้งานโดยรวมของกลุ่มบริษัท จะต้องมีการควบคุมการใช้งานอย่างเข้มงวด ได้แก่ การตรวจสอบตัวตนจริงและสิทธิของผู้ใช้งาน การบันทึกรายละเอียดการใช้งาน และการตัดการเชื่อมต่อหลังจากเลิกการใช้งานแล้วในทันที

ข. กรณีที่ 2 การเชื่อมต่อโดยบุคคลอื่น ๆ นอกเหนือจากเจ้าหน้าที่สารสนเทศต้องได้รับการอนุมัติจากประธานเจ้าหน้าที่บริหาร และต้องมีการควบคุมการเชื่อมต่ออย่างเข้มงวด

7) การรับส่งข้อมูลผ่านเครือข่ายสาธารณะต้องได้รับการเข้ารหัสที่เป็นมาตรฐานสากล

(4) การบริหารจัดการการเปลี่ยนแปลงระบบคอมพิวเตอร์ (Configuration Management)

1) การปรับปรุงระบบ หรือการเปลี่ยนแปลงอุปกรณ์ต่าง ๆ นั้น ควรมีการทดสอบและประเมินผลกระทบที่อาจจะเกิดขึ้น รวมทั้งควรมีการแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบถึงการเปลี่ยนแปลงนั้น ๆ

2) การติดตั้ง Software ต่าง ๆ ควรมีการพิจารณาถึงความเหมาะสมและความจำเป็นในการใช้งานของผู้ใช้งาน ไม่ควรติดตั้ง Software อื่นใดที่ไม่เกี่ยวข้องกับงานที่อยู่ในความรับผิดชอบของผู้ใช้งาน ดังนั้น ควรมีการควบคุม Software ที่ติดตั้งตามเครื่องคอมพิวเตอร์ต่าง ๆ และมีการตรวจสอบอย่างสม่ำเสมอ เพื่อป้องกันการเกิดปัญหาในการใช้ระบบงานคอมพิวเตอร์

3) เพิ่มการควบคุมการติดตั้ง Software อื่นใดที่นอกเหนือจากงานที่อยู่ในความรับผิดชอบของผู้ใช้งาน โดยการกำหนดและควบคุมสิทธ์การใช้งานคอมพิวเตอร์ให้เป็น User ทั่วไป เพื่อทำให้ผู้ใช้งานไม่สามารถทำการติดตั้ง Software ลงเครื่องคอมพิวเตอร์ด้วยตนเองได้

(5) การวางแผนการรองรับประสิทธิภาพของระบบคอมพิวเตอร์ (Capacity Planning)

1) มีการประเมินการใช้งานระบบคอมพิวเตอร์ที่สำคัญไว้ล่วงหน้า เพื่อรองรับการขยายงานในอนาคต

2) ควรมีการตรวจสอบ Resource และ Capacity ของระบบคอมพิวเตอร์ที่สำคัญเป็นประจำ เพื่อความมั่นใจในการใช้ระบบงาน

(6) การป้องกันไวรัส และ Malicious Code

1) เครื่อง Server และเครื่องคอมพิวเตอร์ของผู้ใช้งานที่ใช้เชื่อมต่อกับระบบเครือข่ายทุกเครื่องจะต้องติดตั้ง Software ที่มีประสิทธิภาพ และจะต้องมีการปรับปรุงข้อมูลให้เป็นปัจจุบันอยู่เสมอ

2) เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศควรมีการจัดหาวิธีควบคุม มิให้ผู้ใช้งานระงับการใช้งาน (Disable) Software การป้องกันไวรัสที่ได้มีการติดตั้งไว้

3) ถ้ามีการตรวจพบไวรัส เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศจะต้องจัดการ Clear ไวรัสบนแครื่องที่พบนั้นทันที ทั้งนี้ หากกรณีที่มีความจำเป็นอาจจะต้องมีการ Disconnect ออกจากระบบเครือข่ายเพื่อความปลอดภัยของระบบเครือข่ายของกลุ่มบริษัท

4) เจ้าหน้าที่สารสนเทศควรจะมีการให้ความรู้เกี่ยวกับการป้องกันการติดไวรัส รวมทั้งควรมีการแจ้งข้อมูลเกี่ยวกับไวรัสชนิดใหม่ ๆ อย่างสม่ำเสมอ เพื่อเพิ่ม Awareness ให้แก่พนักงาน

5) ควรมีการ Scan ไวรัสในเครื่องคอมพิวเตอร์ของ User ที่ใช้งาน อย่างน้อยสัปดาห์ละ 3 ครั้ง

6) ก่อนเชื่อมต่ออุปกรณ์สำรองข้อมูล เช่น Flash Disk , External Hard disk เป็นต้น ต้องทำการ Scan ไวรัส เพื่อตรวจสอบและป้องกันก่อนการถ่ายโอนข้อมูลทุกครั้ง

7) เจ้าหน้าที่สารสนเทศ ควรจะมีการติดตาม ศึกษา และทดสอบระบบป้องกันไวรัส และ Malicious Code ใหม่ ๆ เพื่อสามารถป้องกันระบบงานจากการถูกบุกรุก ที่มีวิวัฒนาการหรือการเปลี่ยนแปลงอย่างรวดเร็ว

8) เจ้าหน้าที่สารสนเทศ จะทำการตรวจสอบการคุกคามของไวรัสจาก Server อย่างน้อยสัปดาห์ละ 1 ครั้ง เมื่อตรวจพบไวรัสหรือการทำงานในลักษณะที่ผิดปกติจากเครื่องที่อยู่นอกเหนือการควบคุมสิทธ์การใช้งาน จะมีการดำเนินการเร่งตรวจสอบความผิดปกติของเครื่องนั้น แล้วทำการจัดการ Clear ไวรัสและ Software ที่ไม่พึงประสงค์ ซึ่งอาจก่อให้เกิดปัญหาในการใช้งานกับเครื่องคอมพิวเตอร์นั้น ๆ

(7) การบันทึกเพื่อการตรวจสอบ (Audit Logs)

1) จัดให้มีการบันทึกการทำงานของระบบเครือข่าย และ Server ต่าง ๆ (Firewall Logs) เพื่อใช้ตรวจสอบการถูกบุกรุกหรือใช้งานในลักษณะผิดปกติ โดยจะต้องเก็บบันทึกข้อมูลดังกล่าวไว้อย่างน้อย 3 เดือน

2) สำหรับระบบงานที่สำคัญ ต้องจัดให้มีการบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) การเข้า - ออกระบบงาน (Login - Logout Logs) และบันทึกการพยายามเข้าสู่ระบบ (Login Attempts) เพื่อประโยชน์ในการตรวจสอบ โดยจะต้องเก็บบันทึกข้อมูลดังกล่าวไว้อย่างน้อย 3 เดือน

3) เจ้าหน้าที่สารสนเทศผู้ดูแลรักษาระบบจะต้องไม่ทำการปรับปรุง แก้ไข เปลี่ยนแปลงบันทึกต่าง ๆ และจะต้องดูแลไม่ให้บุคคลภายนอกหรือบุคคลอื่นใดที่ไม่มีหน้าที่เกี่ยวข้อง เข้าถึงบันทึกข้อมูลเหล่านี้โดยเด็ดขาด

(8) การกำหนดหน้าที่ความรับผิดชอบและข้อปฏิบัติสำหรับการควบคุมดูแลของผู้ดูแลเครือข่ายคอมพิวเตอร์

1) เจ้าหน้าที่สารสนเทศจะต้องดูแลรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งจะต้องสอดส่องดูแลการใช้เครือข่ายคอมพิวเตอร์ ทั้งนี้ หากเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศพบพนักงานผู้ใดมีพฤติการณ์ส่อไปในทางที่จะทำให้การใช้งานเครือข่ายคอมพิวเตอร์เกิดปัญหา เจ้าหน้าที่สารสนเทศจะต้องรายงานให้ประธานเจ้าหน้าที่บริหารทราบโดยเร็วที่สุด นอกจากนี้ หากกรณีที่จำเป็นต้องมีการป้องกันความเสียหายที่อาจจะเกิดขึ้นแก่กลุ่มบริษัท เจ้าหน้าที่สารสนเทศมีอำนาจในการระงับการใช้งานเครือข่ายคอมพิวเตอร์ของพนักงานดังกล่าวได้ทันที

2) เจ้าหน้าที่สารสนเทศควรจะเสนอความเห็นและข้อสังเกตต่อประธานเจ้าหน้าที่บริหาร เพื่อพิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพและการบริหารเครือข่ายคอมพิวเตอร์

3) เจ้าหน้าที่สารสนเทศมีหน้าที่ในการติดตั้งอุปกรณ์ ซอฟต์แวร์ ระบบการเข้ารหัสข้อมูลอัตโนมัติ หรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ

4) เจ้าหน้าที่สารสนเทศจะต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และจะต้องไม่เปิดเผยข้อมูลที่ตนได้รับมาจากหรือเนื่องจากการปฏิบัติหน้าที่ผู้ดูแลเครือข่ายคอมพิวเตอร์ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้บุคคลใดทราบ

5) เจ้าหน้าที่สารสนเทศจะต้องคืนทรัพย์สินอันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นของกลุ่มบริษัท เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า - ออก เป็นต้น ให้แก่

ตัวแทนของกลุ่มบริษัท ได้แก่ ผู้บังคับบัญชา ในทันทีที่พ้นหน้าที่และให้ผู้บังคับบัญชาดำเนินการตรวจสอบการคืนทรัพย์สินของเจ้าหน้าที่สารสนเทศที่พ้นจากหน้าที่โดยละเอียด เพื่อความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์

(9) การจัดอบรมให้พนักงานทราบเกี่ยวกับการปฏิบัติตามนโยบาย

1) มีการประกาศใช้และสื่อสารนโยบายให้แก่พนักงานระดับ หรือ ฝ่ายต่างๆ ที่เกี่ยวข้องอย่างทั่วถึง เพื่อให้สามารถปฏิบัติตามได้ เช่น

ก. จัดอบรมให้ความรู้แก่พนักงานฝ่ายต่าง ๆ เกี่ยวกับนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศ

ข. พนักงานใหม่ทุกคนต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและระเบียบปฏิบัติที่เกี่ยวข้องกับหน่วยงานก่อนหรืออย่างน้อยภายใน 30 วันนับจากเข้าทำงานในหน่วยงาน โดยการอบรมดังกล่าวควรเป็นส่วนหนึ่งของการปฐมนิเทศ

2) จัดให้มีการติดตามการปฏิบัติงานของเจ้าหน้าที่สารสนเทศให้เป็นไปตามนโยบาย

3) จัดให้มีการตรวจสอบ รวมทั้งประเมินความเพียงพอของนโยบายและระบบควบคุมภายในด้านเทคโนโลยีสารสนเทศโดยหน่วยงานที่เป็นอิสระอย่างน้อยปีละ 1 ครั้ง ซึ่งอาจเป็นหน่วยงานตรวจสอบภายในของกลุ่มบริษัทหรือผู้ตรวจสอบภายนอก

หมวดที่ 5: การจัดการและการควบคุมการพัฒนา และการปรับปรุงระบบงานคอมพิวเตอร์ (Change Management)

1. **วัตถุประสงค์** (Objective)

เพื่อให้การพัฒนา และการปรับปรุงแก้ไขระบบงานคอมพิวเตอร์ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk รวมทั้ง การจัดทำมาตรการการควบคุมการพัฒนา และการปรับปรุงแก้ไขระบบงาน ให้มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน รวมทั้งจัดให้มีการสื่อสารการเปลี่ยนแปลง ให้ผู้ที่เกี่ยวข้องได้รับทราบโดยทั่วกัน

2. **ขอบเขต** (Scope)

(1) การกำหนดขั้นตอนการปฏิบัติงาน

1) จัดให้มีแบบฟอร์มมาตรฐานในการขอปรับปรุงแก้ไขระบบงาน โดยในแบบฟอร์มควรจะมีการระบุที่มา สาเหตุ หรือรายละเอียดในการขอปรับปรุงระบบงาน

2) มีการกำหนดขั้นตอนและวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร ตั้งแต่การยื่นแบบฟอร์มและเอกสารประกอบ ขั้นตอนการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนการทดสอบ ตลอดจนการ Implement ระบบ

3) มีการจัดเก็บเอกสารอย่างเรียบร้อย และจัดให้มีการตรวจสอบแบบคำขอที่ยังคงค้างอยู่อย่างสม่ำเสมอ

4) มีการประกาศขั้นตอนการขอปรับปรุงแก้ไขระบบงาน และแบบฟอร์มที่ใช้ให้ผู้ใช้งานได้รับทราบอย่างทั่วถึง รวมทั้งการแจ้งพนักงานใหม่ให้รับทราบ เพื่อให้สามารถใช้งานได้อย่างถูกต้อง

(2) การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน

1) การขอปรับปรุงแก้ไขระบบงานจะต้องจัดทำอย่างเป็นลายลักษณ์อักษร เพื่อใช้ในการควบคุมการพัฒนาหรือเปลี่ยนแปลงแก้ไขระบบงาน

2) การปรับปรุงใด ๆ จะต้องได้รับความเห็นชอบหัวหน้าส่วนงานที่ร้องขอ และเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ

3) การปรับปรุงระบบที่เกี่ยวข้องกับกฎเกณฑ์ หรือข้อปฏิบัติที่ทางการกำหนด ทั้งนี้ เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศจะดำเนินการตรวจสอบกับหน่วยงานที่เกี่ยวข้องภายในกลุ่มบริษัท หรืออาจขอคำปรึกษากับที่ปรึกษาภายนอกก่อนที่จะมีการปรับปรุงระบบงาน

4) การพัฒนาหรือปรับปรุงแต่ละระบบงาน จะต้องมีการแยกส่วนการพัฒนา (Development Environment) ออกจากส่วนที่ใช้งานจริง (Go Live Environment) ซึ่งอาจมีการใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือมีการแบ่ง โดยจัดสรรเนื้อที่คนละส่วนในเครื่องคอมพิวเตอร์เครื่องเดียวกัน ทั้งนี้ ให้มีการพิจารณาถึงความเหมาะสมในการใช้งาน

5) จะต้องมีการทดสอบโดยผู้ใช้งาน และได้รับความเห็นชอบว่าระบบได้ถูกพัฒนาได้ถูกต้องครบถ้วนตรงความต้องการของผู้ใช้งาน ก่อนมีการดำเนินการโอนย้ายไปใช้งานบน Go Live Environment

6) เจ้าหน้าที่สารสนเทศจะต้องจัดทำตามขั้นตอนที่กำหนดไว้จนเสร็จสิ้นขบวนการ และมีการลงนามชื่อกำกับ ทั้งผู้ใช้งานและเจ้าหน้าที่สารสนเทศในแบบฟอร์มทุกครั้ง

7) การโอนย้ายไปใช้งานใน Go Live Environment จะต้องมีการตรวจสอบระบบงานให้ถูกต้องครบถ้วนก่อนที่ผู้ใช้งานจะเริ่มใช้งานจริง และต้องมีการ Backup Version ก่อนหน้าที่จะมีการ Implement ใหม่

8) มีการจัดเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้งานอยู่ในปัจจุบัน

9) มีการควบคุมการจัดเก็บเอกสารประกอบระบบงาน และการ Update ข้อมูลเอกสารต่าง ๆ หรือคู่มือให้ Up-to-date รวมทั้ง การจัดเก็บเอกสารให้อยู่ในที่ปลอดภัยและสะดวกต่อการใช้งาน

10) ต้องสื่อสารการเปลี่ยนแปลงและคู่มือการใช้งานให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบ เพื่อให้สามารถใช้งานได้อย่างถูกต้อง และลดข้อผิดพลาดของการทำงานเมื่อขึ้นระบบใหม่

หมวดที่ 6: การจัดการระบบสำรองข้อมูล และการเตรียมพร้อมกรณีเกิดเหตุฉุกเฉิน (Backup System and IT Contingency Plan)

1. **วัตถุประสงค์** (Objective)

เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และสามารถใช้ได้ในเวลาที่ต้องการได้ โดยกลุ่มบริษัทจะต้องจัดเตรียมระบบการสำรอง / แผนฉุกเฉิน รวมถึง การทดสอบระบบสำรอง / แผนฉุกเฉิน ที่ได้กำหนดไว้ เพื่อให้เกิดความมั่นใจในความถูกต้องและครบถ้วนในการใช้งานระบบคอมพิวเตอร์ ทำให้การใช้งานเป็นไปอย่างถูกต้อง มีประสิทธิภาพ และมีความต่อเนื่องหรือพร้อมใช้งานในเวลาที่ต้องการ ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk และ Availability Risk

2. **ขอบเขต** (Scope)

(1) การสำรองข้อมูลและระบบคอมพิวเตอร์ (Backup System)

1) จัดให้มีการสำรองข้อมูลสำคัญ รวมทั้ง โปรแกรมระบบงานต่าง ๆ ได้แก่ Operating System, Application Software, Database หรือชุดคำสั่งต่าง ๆ ที่ใช้ในการทำงาน โดยจัดให้อยู่ในสภาพที่พร้อมจะนำกลับมาใช้งานได้อย่างต่อเนื่อง

2) จัดให้มีระเบียบปฏิบัติหรือขั้นตอนในการจัดทำการสำรองข้อมูล โดยจะต้องกำหนดรายละเอียดดังนี้

ก. จัดประเภทหรือหมวดหมู่ของข้อมูลที่จะทำการสำรองข้อมูล

ข. ความถี่ในการจัดทำการสำรองข้อมูล

ค. วิธีการหรือขั้นตอนการทำการสำรองข้อมูล

ง. ประเภทสื่อบันทึก (Media)

จ. จำนวนที่ต้องสำรอง (Copy)

ฉ. สถานที่การจัดเก็บรักษาสื่อบันทึก

ช. ระยะเวลาการเก็บสื่อบันทึก แต่ละประเภทข้อมูล

ซ. การจัดเก็บอุปกรณ์และ Software ที่ใช้ในการอ่านสื่อบันทึกประเภทนั้น

ฌ. การควบคุมการจัดเก็บสื่อบันทึก จะต้องมี Label กำกับทุกสื่อ โดยจะต้องระบุรายละเอียดอย่างชัดเจนไว้บนสื่อ เช่น ประเภทของข้อมูล วันเดือนปีของข้อมูลที่บันทึก cycle no. เป็นต้น

ญ. ขั้นตอนการปฏิบัติการจัดเก็บสื่อบันทึก

ฎ. การเบิกสื่อบันทึก ซึ่งจะต้องกำหนดผู้มีอำนาจอนุมัติการเบิก

ฏ. การควบคุมอายุการใช้งานของสื่อบันทึก จะต้องมีการกำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว

3) จัดให้มีการบันทึกการจัดเก็บสื่อบันทึกนอกสถานที่ (Logging) เพื่อให้เกิดความมั่นใจในเรื่องการควบคุมการจัดเก็บสื่อบันทึก และเพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยจะต้องพิจารณาเลือกสถานที่ที่มีระบบควบคุมการเข้าออก และระบบป้องกันความเสียหายของข้อมูลตามมาตรฐานสากล

4) ในการเคลื่อนย้ายอุปกรณ์ประเภทสื่อบันทึก (Media) ที่เก็บข้อมูล Backup ไว้ ควรบรรจุหีบห่อกันกระแทกก่อนเคลื่อนย้ายทุกครั้ง เพื่อไม่ให้อุปกรณ์ประเภทสื่อบันทึก (Media) เสียหาย หรือ ชำรุดระหว่างเคลื่อนย้าย

5) จัดให้มีการทดสอบข้อมูลสำรองที่สำคัญอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่าง ๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วน และใช้งานได้

6) จัดให้มีมาตรการในการทำลายอุปกรณ์หรือสื่อบันทึกข้อมูลที่เสื่อมสภาพ ไม่ได้ใช้งาน เพื่อป้องกันการรั่วไหลของข้อมูล

(2) การเตรียมพร้อมกรณีฉุกเฉิน (IT Contingency Plan)

1) จัดทำแผนฉุกเฉิน โดยเฉพาะระบบงานที่สำคัญ เพื่อให้สามารถกู้ระบบคอมพิวเตอร์ หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็วและให้เกิดความเสียหายน้อยที่สุด โดยจะต้องระบุรายละเอียดต่าง ๆ ดังนี้

ก. กำหนดลักษณะของระบบงานหลักและระบบงานสำรอง

ข. กำหนดสถานการณ์ หรือความรุนแรงของปัญหา เพื่อนำมาใช้ประกอบการตัดสินใจ ในการกู้ระบบคอมพิวเตอร์

ค. กำหนดขั้นตอนการแก้ไขปัญหาในแต่ละสถานการณ์

ง. กำหนดเจ้าหน้าที่รับผิดชอบและผู้มีอำนาจตัดสินใจในการกู้ระบบคอมพิวเตอร์ ในแต่ละสถานการณ์ หรือระดับความรุนแรงของปัญหา

จ. มีข้อมูลรายชื่อ และหมายเลขติดต่อของบุคคลที่มีหน้าที่เกี่ยวข้องทั้งหมด

2) จัดให้มีการทดสอบการปฏิบัติตามแผนฉุกเฉินเป็นประจำ อย่างน้อยปีละ 1 ครั้ง โดยจัดทำการทดสอบให้มีการจำลองสถานการณ์จริง เพื่อให้เกิดความมั่นใจในการนำไปใช้งานในทางปฏิบัติ รวมทั้ง จะต้องมีการบันทึกผล การทดสอบ และวิเคราะห์ผลการทดสอบว่า บรรลุผลตามแผนฉุกเฉินหรือไม่ อย่างไร

3) กรณีเกิดเหตุฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ เพื่อนำมาวิเคราะห์สาเหตุของปัญหาและวิธีการแก้ไข โดยกลุ่มบริษัทจะนำมาเปรียบเทียบและปรับปรุงแผนฉุกเฉิน ให้มีความครอบคลุมในทุกปัญหา และแนวทางแก้ไข

หมวดที่ 7: การจัดการและการควบคุมการปฏิบัติงานประจำ และ ระเบียบวิธีการควบคุมการปฏิบัติงาน (Computer Operation Control)

1. วัตถุประสงค์ (Objective)

เพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk, Availability Risk และเพื่อให้เกิดความมั่นใจในเรื่องต่าง ๆ ดังนี้

(1) การใช้ระบบงานเป็นไปตามวัตถุประสงค์ที่ได้รับอนุมัติเท่านั้น

(2) การจำกัดการเข้าถึงการปฏิบัติงานคอมพิวเตอร์เฉพาะผู้ที่ได้รับอนุมัติเท่านั้น

(3) สามารถใช้โปรแกรมคำสั่งงานที่ได้รับอนุมัติแล้วเท่านั้น

(4) การตรวจสอบและการแก้ไขข้อผิดพลาดในการประมวลผล

2. ขอบเขต (Scope)

จะต้องจัดให้มีมาตรการที่เพียงพอในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ โดยมีรายละเอียดดังนี้

(1) การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ โดยจะต้องมีการกำหนดรายละเอียดดังนี้

1) กำหนดเวลาเริ่มต้น – สิ้นสุดของเวลาปฏิบัติงาน และกำหนดจำนวนเจ้าหน้าที่สารสนเทศ

2) มีเอกสารที่เป็นลายลักษณ์อักษร ซึ่งแสดงรายละเอียดขั้นตอนการเปิด - ปิดระบบงานประจำวัน ประกอบการปฏิบัติงาน (Daily Operation Log) ซึ่งเจ้าหน้าที่สารสนเทศจะต้องกรอกรายละเอียดของเวลาการปฏิบัติงาน และลงชื่อผู้ปฏิบัติงาน

3) กรณีที่เกิดปัญหาในการปฏิบัติงาน จะต้องมีการบันทึกปัญหาที่เกิดขึ้นด้วย และแจ้งให้ประธานเจ้าหน้าที่บริหารทราบเร็วที่สุดเท่าที่จะทำได้

4) มีการกำหนดรายชื่อ วิธีการและหมายเลขติดต่อของผู้รับผิดชอบระบบงานและเจ้าหน้าที่สารสนเทศ เพื่อให้การแก้ไขปัญหาสามารถทำได้อย่างรวดเร็วและทันเหตุการณ์

5) ดูแลรับผิดชอบการเข้า - ออกห้อง Server โดยเฉพาะนอกเวลาทำการ

6) ดูแลรับผิดชอบการเข้า - ออกห้อง Server รวมถึง ดูแลรักษาความสะอาดภายในห้องไปจนถึงการใช้งานของบุคลากรจากแผนกอื่น ๆ หรือบุคลากรจากบริษัทอื่นที่ให้บริการด้านคอมพิวเตอร์ ระบบไฟ และระบบโทรศัพท์

7) การขอใช้เครื่องคอมพิวเตอร์ Server นอกเวลาทำการปกติ จะต้องมีการแจ้งวันและเวลาการใช้งานให้ประธานเจ้าหน้าที่บริหารรับทราบ และอนุมัติเป็นรายครั้ง โดยจะต้องมีการจัดเจ้าหน้าที่สารสนเทศสำหรับให้บริการในช่วงเวลาทำงานดังกล่าว

(2) การควบคุมการเปิด - ปิดอุปกรณ์ที่เกี่ยวกับเทคโนโลยีสารสนเทศ จะต้องมีการกำหนดหน้าที่ความรับผิดชอบ และการดูแลควบคุมการเปิด - ปิดอุปกรณ์ต่าง ๆ และภายในห้อง Server

(3) การควบคุมการซ่อมบำรุงรักษาอุปกรณ์คอมพิวเตอร์ จะต้องมีการพิจารณาและตรวจสอบอุปกรณ์ที่สำคัญ เพื่อจัดทำสัญญา Maintenance โดยจะต้องดูแลความต่อเนื่องของสัญญา ปรับปรุงสัญญาให้เหมาะสมกับอุปกรณ์ต่าง ๆ รวมทั้ง ดูแลการซ่อมบำรุงอุปกรณ์ตามที่ระบุในสัญญา

(4) การควบคุมรายงานที่เกี่ยวกับด้านเทคโนโลยีสารสนเทศ จะต้องมีการกำหนดรายละเอียดดังนี้

1) กำหนดเจ้าหน้าที่ในการควบคุม ดูแล และรับผิดชอบการจัดพิมพ์รายงาน

2) กำหนดขั้นตอน วิธีการจัดส่งรายงาน และการแยกหมวดหมู่ของรายงานให้ถูกต้องตามหน่วยงานผู้ใช้งาน

3) การพิมพ์รายงานใด ๆ เพิ่มเป็นพิเศษ หรือการเพิ่ม แก้ไข ยกเลิกรายงานใด ๆ จะต้องมีหนังสือแจ้งให้ผู้บังคับบัญชาที่ดูแลด้านเทคโนโลยีสารสนเทศรับทราบทุกครั้ง

(5) การควบคุมการใช้สื่อในการบันทึกข้อมูล จะต้องมีการกำหนดรายละเอียดดังนี้

1) จัดเตรียมสื่อบันทึกให้มีความเหมาะสมกับข้อมูลของระบบงานต่าง ๆ และจัดให้มี Label กำกับสื่อทุกชิ้น รวมทั้ง แสดงรายละเอียดของข้อมูลได้อย่างครบถ้วนและสามารถนำกลับมาใช้งานได้อย่างถูกต้อง

2) จัดให้มีการแบ่งประเภทการจัดเก็บข้อมูลตาม Cycle ให้เหมาะสมกับข้อมูลของระบบงานต่าง ๆ

3) จัดเตรียมสถานที่เก็บข้อมูลให้เหมาะสม ทั้งในสถานที่ทำการและนอกสถานที่ทำการ รวมทั้งกำหนดหมวดหมู่ของการเก็บสื่อบันทึกข้อมูลให้ชัดเจน

4) กำหนดขั้นตอนการจัดเก็บสื่อ การบันทึกการดำเนินการจัดเก็บสื่อ โดยเฉพาะการนำสื่อไปจัดเก็บนอกสถานที่ทำการ

5) การนำสื่อบันทึกข้อมูลกลับมาใช้งานในกรณีฉุกเฉินหรือกรณีที่ต้องการข้อมูลจากสื่อบันทึกเป็นพิเศษ จะต้องมีการขออนุมัติตามขั้นตอน

6) จะต้องจัดให้มีขบวนการนำสื่อมาทดสอบการใช้งานจริง โดยจัดให้มีการปฏิบัติเป็นประจำ และบันทึกผลการทดสอบให้เป็นลายลักษณ์อักษร

(6) การติดตามการทำงานของระบบคอมพิวเตอร์ (Monitoring) ทางเจ้าหน้าที่สารสนเทศจะต้องมีการศึกษาระบบงานต่าง ๆ อย่างต่อเนื่อง เพื่อให้มีการพัฒนาและเพิ่มประสิทธิภาพของการทำงานและระบบการตรวจสอบความพร้อมของระบบในการทำงาน อีกทั้ง เพื่อประเมิน Capacity ของ Resource ที่ใช้ในระบบงานต่าง ๆ ที่จำเป็น เช่น การใช้งาน Hard Disk, การใช้งาน CPU และ Memory เป็นต้น

(7) ควรมีการบำรุงรักษา ทำความสะอาดอุปกรณ์คอมพิวเตอร์และระบบคอมพิวเตอร์ ให้อยู่ในสภาพที่ดีและพร้อมใช้งานเสมอ

(8) เจ้าหน้าที่ผู้ดูแลส่วนระบบงานต่าง ๆ จะต้องมีการรายงานปัญหาที่เกิดขึ้นให้ประธานเจ้าหน้าที่บริหารทราบเป็นลายลักษณ์อักษร โดยเฉพาะปัญหาที่ก่อให้เกิดผลกระทบในวงกว้าง รวมทั้ง จะต้องรายงานวิธีการแก้ไขปัญหาที่เกิดขึ้นเพื่อทำการรวบรวมและตรวจสอบสาเหตุของปัญหาที่เกิดขึ้น เพื่อหาทางแก้ไขและป้องกันปัญหาได้อย่างถูกต้อง

หมวดที่ 8: การจัดการ การควบคุม และการตรวจสอบผู้ให้บริการ (IT Outsourcing)

1. **วัตถุประสงค์** (Objective)

เพื่อให้สามารถใช้งานบริการด้านงานเทคโนโลยีสารสนเทศจากผู้บริการรายอื่น ๆ ได้อย่างมีประสิทธิภาพน่าเชื่อถือ และสามารถควบคุมความเสี่ยงอันเกิดจากการใช้บริการของผู้ให้บริการจากภายนอกกลุ่มบริษัท ได้แก่ การควบคุมเกี่ยวกับการเข้าถึงข้อมูล (Access Risk) การประมวลผลของระบบงาน (Integrity Risk) รวมทั้ง ความต่อเนื่องในการใช้งานระบบคอมพิวเตอร์ (Availability Risk) ดังนั้น จึงจะต้องมีการกำหนดแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการ

2. **ขอบเขต** (Scope)

(1) การคัดเลือกผู้ให้บริการควรมีการพิจารณาคัดเลือกผู้ให้บริการในด้านต่าง ๆ ดังนี้

1) ข้อมูลทางด้านโครงสร้างกลุ่มบริษัท ผู้ถือหุ้นของกลุ่มบริษัท

2) ธุรกิจหลักของผู้ประกอบการ

3) ผลประกอบการทางการเงินที่ผ่านมา

4) การกำหนดกลยุทธ์ในการดำเนินงานทางธุรกิจ

5) ความสามารถในการบริหารจัดการ

6) ผังการดำเนินงานและขั้นตอนต่าง ๆ ของระบบที่จะจัดทำ

7) ความสามารถในการบริการในลักษณะ One-Stop Service

8) ลูกค้ารายสำคัญที่ผู้ให้บริการดูแลอยู่ (Reference Site)

(2) การจัดทำสัญญา โดยสัญญาที่จัดทำขึ้น ควรมีข้อความครอบคลุมในเรื่องต่าง ๆ ดังนี้

1) การรักษาความลับของข้อมูล (Data Confidentiality)

2) ขอบเขตงาน (Work Flow, Flow Chart or Diagram)

3) เงื่อนไขการให้บริการ (Service Level Agreement)

(3) การจัดทำคู่มือประกอบการปฏิบัติงาน

1) ผู้ให้บริการจะต้องจัดทำคู่มือการปฏิบัติงาน เพื่อเป็นเอกสารประกอบการใช้งานทุกระบบงาน

2) ผู้ให้บริการควรปรับปรุงคู่มือการให้บริการให้เป็นปัจจุบันอยู่เสมอ

(4) การควบคุมผู้ให้บริการ

1) ผู้ให้บริการจะต้องมีหลักเกณฑ์ หรือนโยบายในงานให้บริการอย่างชัดเจน

2) ผู้ให้บริการจะต้องมีการควบคุมการปฏิบัติงานให้เป็นไปตามนโยบายที่กำหนดไว้

3) จะต้องมีการตรวจสอบและควบคุมการเข้าถึงข้อมูลสำคัญ หรือข้อมูลที่เป็น Go Live ของผู้ให้บริการอย่างเข้มงวด

ก. กรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่กลุ่มบริษัท (Onsite Service) กลุ่มบริษัทจะต้องมีการจัดเจ้าหน้าที่ควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิด

ข. กรณีที่ผู้ให้บริการได้ให้บริการผ่านระบบเครือข่าย (Network Communication) กลุ่มบริษัทจะต้องจัดระบบให้สามารถควบคุมการเข้า-ออกของผู้ให้บริการจากเครือข่ายของกลุ่มบริษัทได้ เช่น การเข้าสู่เครือข่ายกลุ่มบริษัทในลักษณะ Remote Access จะต้องมีการควบคุมการเชื่อมต่ออย่างเข้มงวด รวมทั้ง ควรมีการจดบันทึกการเข้าถึงของข้อมูลและกำหนดระยะเวลาการเข้าใช้งานทุกครั้ง

ค. เมื่อผู้ให้บริการดำเนินการแก้ไขหรือปรับปรุงระบบด้วยวิธีการเข้าสู่เครือข่ายกลุ่มบริษัทในลักษณะ Remote Access เรียบร้อยแล้ว กลุ่มบริษัทควรปิดหรือระงับการเข้าถึงระบบทันที จนกว่าจะมีการร้องขอจากผู้ให้บริการในการเข้ามาแก้ไขหรือปรับปรุงระบบ โดยกลุ่มบริษัทจะพิจารณาเป็นรายครั้ง

4) ในกรณีที่เกิดปัญหา กลุ่มบริษัทควรดำเนินการติดตามผู้ให้บริการ โดยการให้ผู้ให้บริการรายงานสาเหตุของปัญหาและแนวทางการแก้ไข

5) การปรับปรุงระบบงานในแต่ละครั้ง จะต้องมีเอกสารประกอบ รวมทั้ง มีการทดสอบและขั้นตอนการตรวจรับงานของผู้ให้บริการทุกครั้ง

นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศนี้ให้มีผลใช้บังคับตั้งแต่วันที่ 13 เดือน สิงหาคม พ.ศ. 2564 เป็นต้นไป

(นายวันชัย ศรีหิรัญรัศมี)
ประธานกรรมการบริษัท
บริษัท ไบโอซายน์ แอนิมัล เฮลธ์ จำกัด (มหาชน)