สารบัญ

1. ขอบเขตของนโยบายและหลักเกณฑ์ปฏิบัติ

1.1. วัตถุประสงค์

นโยบายด้านการบริหารระบบเทคโนโลยีสารสนเทศจัดทำขึ้น เพื่อกำหนดขอบเขต บทบาท อำนาจ หน้าที่ และความรับผิดชอบของการบริหารจัดการ การใช้งาน การให้บริการ การจัดหา การบำรุงรักษา และการรักษาความมั่นคงปลอดภัย ระบบเทคโนโลยีสารสนเทศ เพื่อใช้เป็นระเบียบมาตรฐานหรือหลักเกณฑ์ ในการปฏิบัติงานให้เป็นมาตรฐานเดียวกันภายในองค์กร

1.2. ขอบเขตของนโยบาย

นโยบายฉบับนี้มีผลบังคับใช้กับพนักงานทุกคน และกับระบบเทคโนโลยีสารสนเทศทุกระบบ รวมถึงข้อมูล เครื่องมือ และอุปกรณ์ต่อพ่วงทุกชนิดที่เป็นทรัพย์สิน ทั้งที่จับต้องได้ และจับต้องไม่ได้ ซึ่งอยู่ในความควบคุมดูแลของบริษัท ทั้งที่ติดตั้งใช้งานอยู่ภายในและภายนอกบริษัท รวมถึง ลูกค้า คู่ค้า และปัจจัยแวดล้อมอื่นๆ ที่มีส่วนเกี่ยวข้องทั้งทางตรงและทางอ้อมต่อระบบเทคโนโลยีสารสนเทศของบริษัทฯ ทุกกรณี โดยรายละเอียดมีดังนี้

1.2.1. ภายใน

- บริษัทฯ หมายถึง บริษัท สุรพลฟู้ดส์ จำกัด (มหาชน) สำนักงานสาขา และบริษัทในเครือทั้งหมด ที่อยู่ภายใต้การบริหารงานโดยสำนักงานใหญ่
- พนักงาน หมายถึง บุคลากรทุกระดับที่มีส่วนได้ส่วนเสียกับบริษัทฯ
- ระบบเทคโนโลยีสารสนเทศ หมายถึง เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงทุกชนิด โปรแกรมหรือซอฟท์แวร์ทุกประเภท รวมถึงสายส่งข้อมูลในรูปแบบต่างๆ (ทั้งแบบมีสาย และไร้สาย) ที่นำมารวมกันแล้วสามารถใช้ทำธุรกรรมอย่างใดอย่างหนึ่งได้
- ข้อมูล หมายถึง เนื้อหาสาระหรือข้อความที่ประกอบด้วย ตัวหนังสือ ตัวเลข และอักขระพิเศษต่างๆ ที่มีความหมายอย่างใดอย่างหนึ่ง ซึ่งจัดเก็บอยู่ในรูปของสื่ออิเล็กทรอนิกส์

1.2.2. ภายนอก

- ลูกค้าหรือคู่ค้า หมายถึง บุคคล หน่วยงาน หรือบริษัทห้างร้านใดๆ ที่มีการติดต่อกับบริษัทฯ เพื่อทำธุรกรรมอย่างใดอย่างหนึ่งร่วมกัน
- ปัจจัยแวดล้อม หมายถึง สิ่งของ สถานที่ รวมถึงเหตุการณ์ต่างๆ ที่มีความเสี่ยงอันจะส่งผลให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศของบริษัทฯ
- หนังสือสัญญา เงื่อนไขทางการค้า หรือกฎหมายที่เกี่ยวข้องกับการทำธุรกรรมด้วยเทคโนโลยีสารสนเทศ
- ภัยคุกคามต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ประกอบด้วย
  - ภัยคุกคามจากตัวบุคคลเป็นผู้กระทำ หรือเรียกอีกอย่างว่า “Hacker”
  - ภัยคุกคามจากโปรแกรมไม่พึงประสงค์ ซึ่งมีอยู่ด้วยกันหลายประเภทหลายชนิด อาทิ ไวรัสคอมพิวเตอร์ สแปมเมลล์ สไปแวร์ เป็นต้น

1.3. อำนาจหน้าที่ และขอบเขตความรับผิดชอบ (Role & Responsibility)

1.3.1. ประธานเจ้าหน้าที่บริหาร อนุมัติประกาศใช้นโยบายด้านระบบเทคโนโลยีสารสนเทศ (IT Policy) เพื่อสนับสนุนการบริหารจัดการระบบเทคโนโลยีสารสนเทศทั้งหมดให้มีประสิทธิภาพและมีความมั่นคงปลอดภัย

1.3.2. ผู้บริหารระดับสูง จะต้องสนับสนุน และผลักดันให้พนักงานทุกคนปฏิบัติตามกฎที่สร้างขึ้นมาในเอกสารนี้

1.3.3. ผู้จัดการฝ่าย และแผนก จะต้องจัดให้บุคคลที่เกี่ยวข้อง ได้เข้าใจถึงระเบียบของนโยบาย และทำตามอย่างเคร่งครัด

1.3.4. ผู้จัดการฝ่ายสารสนเทศ วางแผน และกำหนดกลยุทธ์ให้ครอบคลุมนโยบายการบริหารระบบเทคโนโลยีสารสนเทศ กำกับการดำเนินงาน การเฝ้าระวัง การทบทวน การบำรุงรักษา และปรับปรุงพัฒนา ตลอดจนการสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยให้สอดคล้อง และเพียงพอกับนโยบายธุรกิจ การดำเนินธุรกิจและการปฏิบัติงานของพนักงาน อีกทั้งอนุมัติให้ความเห็นชอบ เพื่อนำเสนอ คณะกรรมการผู้จัดการอาวุโส กลุ่มการเงินและบริการองค์กร ตามความเหมาะสมต่อไป

ในกรณีที่ไม่สามารถจัดการได้เพียงพอจะต้องรายงานต่อ คณะกรรมการผู้จัดการอาวุโส กลุ่มการเงินและบริการองค์กรได้รับทราบโดยเร่งด่วนเพื่อกำหนดแนวทางแก้ไข พร้อมนำเสนอแนวทางออกที่เหมาะสม เช่น การจัดหาระบบทางเลือก การจัดหาโดยวิธีการเช่าใช้ หรือการใช้บริการจากผู้ให้บริการภายนอก (IT Outsource) เป็นต้น

1.3.5. พนักงานทุกคน จะต้องเข้าใจ และตระหนักถึงความสำคัญ และปฏิบัติตามนโยบายนี้

1.4. การละเมิดสิทธิ์หรือทำผิดกฎข้อบังคับ และบทลงโทษ

การละเมิดสิทธิ์หรือทำผิดกฎข้อบังคับในหนังสือนโยบายฉบับนี้ สามารถเป็นเหตุให้ถูกลงโทษถึงขั้นการสั่งพักงานหรือยุติการว่าจ้าง ทั้งนี้ขึ้นอยู่กับความรุนแรงของความผิด ตามที่บริษัทฯพิจารณา ทางบริษัทฯ มีสิทธิ์ดำเนินการตามกฎหมายที่ระบุไว้สูงสุดทั้งทางแพ่งและทางอาญา

2. การบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

2.1. วัตถุประสงค์

เพื่อกำหนดโครงสร้างการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศภายในองค์กรที่ชัดเจน และกำหนดขั้นตอนและหลักปฏิบัติทางด้านการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

2.2. รายละเอียดหลักเกณฑ์ปฏิบัติ

2.2.1. โครงสร้างการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นไปตามอำนาจหน้าที่ และขอบเขตความรับผิดชอบ ตามข้อที่ 1 ของนโยบายฉบับนี้

2.2.2. ฝ่ายสารสนเทศมีหน้าที่เผยแพร่และประชาสัมพันธ์ นโยบายด้านการบริหารระบบเทคโนโลยีสารสนเทศ พร้อมทั้งเอกสารประกอบนโยบายที่เกี่ยวข้องทั้งหมด ให้กับพนักงานของบริษัทฯ และบุคคลภายนอกที่มีความเกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของบริษัทฯ เพื่อสร้างความเข้าใจอันดีต่อกัน และปฏิบัติตามนโยบายได้อย่างถูกต้อง

2.2.3. พนักงานทุกคน ต้องรับผิดชอบต่อสิทธิ์ และหน้าที่ที่ได้รับทุกกรณี ความเสียหายที่เกิดจากการละเมิดฝ่าฝืนกฎระเบียบ และข้อบังคับใดๆ ของนโยบายนี้ ให้ผู้นั้นต้องได้รับโทษตามระเบียบข้อบังคับของบริษัทฯ และกฎหมายที่เกี่ยวข้อง ซึ่งพนักงานทุกคนต้องใช้สิทธิ์ที่ได้รับอย่างระมัดระวัง และหากพบเจอความผิดปรกติใดๆ ต้องรายงานให้ฝ่ายสารสนเทศรับทราบทันที

2.3. การบริหารจัดการความมั่นคงปลอดภัยแบ่งเป็น 4 ด้านดังนี้

2.3.1. <u>ความมั่นคงปลอดภัยทางด้านกายภาพ และสิ่งแวดล้อม **(Physical and Environment Security)**</u>

- ระบบเทคโนโลยีสารสนเทศจะต้องถูกออกแบบ ติดตั้ง และวางเอาไว้ในสถานที่ที่เหมาะสมโดยพิจารณาถึงอาคารสถานที่ ห้อง ผนัง รั้ว หลังคา กันสาด ประตู พนักงานรักษาความปลอดภัย เป็นต้น มีความมั่นคงแข็งแรง ปลอดภัยจากปัจจัยแวดล้อมทางกายภาพทั่วไปที่มีความเสี่ยง เช่น ลม ฝน แสงแดด ฝุ่น ความร้อน ความชื้น และบุคคลภายนอก เป็นต้น
- ระบบและอุปกรณ์เทคโนโลยีสารสนเทศจะได้รับการจัดหาสาธารณูปโภคพื้นฐานที่เพียงพอ เหมาะสม เช่น ระบบไฟฟ้า ระบบปรับอากาศ เป็นต้น และในจุดที่มีความสำคัญจะต้องจัดให้มีระบบสำรองฉุกเฉิน และระบบตรวจสอบด้วย เช่น ระบบสำรองพลังงานไฟฟ้า ระบบป้องกันกระแสไฟฟ้าขัดข้อง ระบบกล้องวงจรปิด ระบบกับเพลิง และป้องกันอัคคีภัย เป็นต้น
- ฝ่ายสารสนเทศมีหน้าที่ควบคุมบริเวณสำหรับจุดติดตั้ง และให้บริการระบบเทคโนโลยีสารสนเทศแม่ข่ายทุกจุด (ห้องติดตั้ง server ซึ่งต่อไปนี้จะเรียกว่า “ จุดควบคุม ”)
- ฝ่ายสารสนเทศกำหนดมาตรการป้องกัน และการควบคุมความเสี่ยงอันมีเหตุจากปัจจัยแวดล้อม รวมถึงจัดทำและปรับปรุงแผนป้องกันภัยพิบัติทางธรรมชาติ หรือเหตุการณ์ไม่ปกติ ให้มีความทันสมัย และเหมาะสมต่อสภาพการณ์ของปัจจัยเสี่ยง

- ฝ่ายสารสนเทศเป็นผู้ให้คำแนะนำในการกำหนดพื้นที่ผู้ใช้บริการระบบเทคโนโลยีสารสนเทศให้มีความเหมาะสม และจัดทำแผนผังแสดงตำแหน่งการติดตั้งระบบ อุปกรณ์ในพื้นที่ใช้งาน
- พนักงาน หรือบุคคลภายนอกที่นำอุปกรณ์ หรือเครื่องคอมพิวเตอร์ภายนอก มาใช้เชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัทฯ จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งาน และได้รับการอนุมัติจากผู้บริหารหน่วยงานหรือผู้มีอำนาจสูงสุดของหน่วยงาน

2.3.2. <u>ความมั่นคงปลอดภัยทางด้านข้อมูล และระบบโปรแกรม **(Data and Software Security)**</u>

- สิทธิ และหน้าที่ในการควบคุมการเข้าถึง และการใช้งานข้อมูลของพนักงาน เป็นของผู้บริหารหน่วยงาน หรือผู้มีอำนาจสูงสุดของหน่วยงาน
- ฝ่ายสารสนเทศมีอำนาจหน้าที่ในการเข้าถึง และตรวจสอบข้อมูลต่างๆในระบบ เพื่อให้เป็นไปตามข้อกำหนด และระเบียบปฏิบัติแห่งนโยบายนี้ โดยผู้จัดการฝ่ายสารสนเทศต้องกำหนดผู้รับผิดชอบ และหลักปฏิบัติไว้อย่างชัดเจน
- ฝ่ายสารสนเทศต้องจัดให้มีระเบียบหรือวิธีการบริหารจัดการการเข้าถึงข้อมูลในระบบของหน่วยงาน และพนักงานอย่างเป็นเอกเทศ หรือเข้าถึงการใช้งานได้เฉพาะผู้ที่มีสิทธิ์
- หากฝ่ายสารสนเทศ พบเจอข้อมูลที่ไม่เป็นไปตามข้อกำหนด หรือผิดกฎหมาย หรือมีความเสี่ยงที่จะเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ให้ทำการระงับทันที และแจ้งต่อผู้จัดการฝ่ายสารสนเทศ เพื่อพิจารณาทำการลบออกจากระบบต่อไป
- พนักงานไม่มีสิทธิ์ทำการติดตั้ง หรือถอดถอนการติดตั้งโปรแกรม หรือซอฟท์แวร์ออกจากเครื่องคอมพิวเตอร์ ซึ่งจะต้องดำเนินการโดยฝ่ายสารสนเทศเท่านั้น
- พนักงานจะได้รับสิทธิ์การใช้งานระบบสารสนเทศขั้นพื้นฐานตามที่บริษัทฯ กำหนดไว้ตามความเหมาะสม และสามารถที่จะขอสิทธิ์เพิ่มเติมในภายหลังได้โดยผ่านการพิจารณาอนุมัติจากผู้บริหารหน่วยงาน หรือผู้มีอำนาจสูงสุดของหน่วยงาน
- พนักงานจะต้องทำการบันทึกข้อมูลการทำงานลงเอาไว้ในสื่อบันทึกที่บริษัทฯจัดเอาไว้ให้เท่านั้น เช่น อุปกรณ์คอมพิวเตอร์ แฟ้มข้อมูลส่วนกลาง (Drive T) และฐานข้อมูลของโปรแกรมต่างๆ กรณีที่ พนักงานต้องการใช้งานข้อมูลร่วมกับหน่วยงานอื่น จะต้องได้รับการอนุมัติจากผู้บริหารหน่วยงานที่เป็นเจ้าของข้อมูลนั้น
- พนักงานจะต้องเข้าใช้งานระบบสารสนเทศของบริษัทฯ ผ่านช่องทางที่บริษัทฯกำหนด และอนุญาตเท่านั้น เช่น Email, Internet, FTP, Web และ VPN เป็นต้น
- พนักงานไม่มีสิทธิ์ใช้งานสื่อบันทึกข้อมูลแบบต่อพ่วงทุกชนิด เช่น Flash drive, DVD Rom รวมถึงบริการหรือโปรแกรมที่ให้บริการแบบสาธารณะผ่าน Internet เช่น โปรแกรม Facebook, LINE, Instagram ยกเว้นบางตำแหน่งงานที่ได้รับอนุญาตตามสิทธิ์พื้นฐานเพื่อใช้ในการทำงาน หากภายหลังพนักงานมีความจำเป็นต้องใช้งานให้ทำการขอสิทธิ์เพิ่มเติม โดยจัดทำเป็นหนังสือให้คำมั่นสัญญา และรับรองในการเก็บรักษาความลับสารสนเทศนำเสนอต่อผู้บริหารหน่วยงาน
- ฝ่ายสารสนเทศมีหน้าที่จัดเก็บ ป้องกันความเสียหาย และทำการกู้คืน ข้อมูลใดๆของบริษัทฯ โดยต้องแน่ใจว่าข้อมูลที่จัดเก็บเอาไว้ มีความมั่นคงปลอดภัยต่อการลักลอบ ถูกโจรกรรม หรือถูกทำลายจากปัจจัยแวดล้อมต่างๆ และพร้อมนำกลับมาใช้งานเมื่อต้องการกู้คืนข้อมูล

- พนักงานจะต้องทำการ Log off ออกจากระบบสารสนเทศใดๆ ทันทีหลังจากเลิกใช้งาน

2.3.3. ความมั่นคงปลอดภัยทางด้านตัวบุคคล **(Human Security)**

- *ฝ่ายสารสนเทศมีหน้าที่กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบเทคโนโลยีสารสนเทศ เพื่อดูแลรักษาความมั่นคงปลอดภัย โดยที่พนักงานหรือบุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารหน่วยงานหรือผู้มีอำนาจสูงสุดของหน่วยงาน และผู้จัดการฝ่ายสารสนเทศให้ความเห็นชอบ เฉพาะสำหรับระบบ ERP จะต้องได้รับความเห็นชอบจากกรรมการผู้จัดการกลุ่มการเงิน และบริการองค์กร*
- *พนักงานต้องได้รับทราบนโยบาย และหนังสือรักษาความลับของบริษัทฯ โดยให้ทำความเข้าใจในรายละเอียดเป็นอย่างดี พร้อมทั้งลงนาม และเก็บสำเนาไว้เป็นหลักฐาน 1 ชุด*
- *ฝ่ายสารสนเทศ มีหน้าที่จัดเก็บข้อมูลสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศของพนักงานไว้อย่างเป็นระบบให้สามารถตรวจสอบ และสืบค้นได้อย่างมีประสิทธิภาพ*
- *ฝ่ายสารสนเทศมีหน้าที่ในการบริหารจัดการบัญชีผู้ใช้งานระบบเทคโนโลยีสารสนเทศให้เหมาะสม และตามความจำเป็น ดังนี้*
  - *สร้าง และจัดทำบัญชีผู้ใช้งาน (User Account) ของระบบคอมพิวเตอร์*
  - *ระงับ หรือตรวจสอบความผิดปกติของบัญชีผู้ใช้*
  - *เปลี่ยนรหัสผ่าน (Reset Password) ของบัญชีผู้ใช้ตามการร้องขอ โดยใช้รหัสผ่านชั่วคราว และต้องแจ้งให้ผู้ใช้เปลี่ยนรหัสผ่านอีกครั้งโดยทันที*
- *ฝ่ายสารสนเทศจัดทำทะเบียนบัญชีผู้ใช้อย่างชัดเจน และจัดทำแผนการสอบทาน และทบทวนสิทธิ์ของบัญชีผู้ใช้งานระบบทั้งหมดอย่างน้อยปีละ 2 ครั้ง หรือทุก 6 เดือน โดยดำเนินการร่วมกับหน่วยงานต้นสังกัด*
- *การพ้นสภาพของพนักงานไม่ว่าด้วยเหตุใด*
  - *ฝ่ายสารสนเทศจะระงับสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศของพนักงานทันทีที่ได้รับแจ้งจากฝ่ายทรัพยากรบุคคล หรือผู้บริหารที่มีอำนาจสูงสุดของหน่วยงาน*
  - *ฝ่ายสารสนเทศมีสิทธิ์ และอำนาจหน้าที่ในการที่จะถอดถอนสิทธิ์ใดๆ และลบข้อมูลในระบบเทคโนโลยีสารสนเทศของพนักงานที่สิ้นสุดสภาพการเป็นลูกจ้างของบริษัทฯไปแล้วเป็นเวลา 30 วัน โดยทำการยืนยันและประสานงานกับหน่วยงานก่อน หากในกรณีที่หน่วยงานมีความจำเป็นต้องการใช้สิทธิ์ต่อเนื่องในการทำงาน ให้ฝ่ายสารสนเทศหาวิธีที่เหมาะสม*
  - *พนักงานที่พ้นสภาพจากการเป็นลูกจ้างของบริษัทฯ จะต้องนำทรัพย์สินทั้งหมดรวมถึงเอกสาร และข้อมูลต่างๆทุกชนิด ส่งคืนแก่บริษัทฯโดยทันที*
- *พนักงานมีหน้าที่ บริหารจัดการรหัสผู้ใช้งาน (User Account) และรหัสผ่าน (Password) ของตัวเอง ดังนี้*
  - *ต้องมีรหัสผู้ใช้งานเป็นของตัวเอง ห้ามใช้ร่วมกับบุคคลอื่น ยกเว้น รหัสกลุ่มผู้ใช้ ที่มีสิทธิ์ใช้งานร่วมกันหลายคนซึ่งจะต้องมอบหมายให้มีผู้รับผิดชอบหลัก 1 คน*

- *ห้ามเปิดเผย แจ้ง ประกาศ บอกผ่าน เขียน ส่งอีเมล์ แอบบอก บอกใบ้ หรือในการสื่อความรูปแบบอื่นที่เป็นเหตุให้ผู้อื่นรับรู้รหัสผ่านของตัวเอง*
- *เปลี่ยนรหัสผ่านตามวงรอบที่กำหนด ดังนี้ ระบบ ERP ปีละ 2 ครั้ง และระบบคอมพิวเตอร์ 45 วัน*

2.3.4. ความมั่นคงปลอดภัยด้านเครือข่าย **(Network Security)**

- ฝ่ายสารสนเทศมีอำนาจ และหน้าที่ในการควบคุม และป้องกันการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯทุกรูปแบบให้เป็นไปตามข้อกำหนดทางธุรกิจอย่างปลอดภัย
- อุปกรณ์ที่เชื่อมต่อเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ ที่มิใช่ทรัพย์สินของบริษัทฯ ต้องได้รับการอนุมัติจากผู้บริหารหน่วยงาน หรือผู้มีอำนาจสูงสุดของหน่วยงาน และผู้จัดการฝ่ายสารสนเทศเห็นชอบ
- การใช้งานแบบระยะไกล (Remote Access) หรือ VPN หรือการใช้ระบบคอมพิวเตอร์จากภายนอก จะต้องพิจารณาความจำเป็นในการใช้งานเป็นกรณี และต้องได้รับอนุญาตจากผู้บริหารหน่วยงานหรือผู้มีอำนาจสูงสุดของหน่วยงาน โดยพนักงานหรือผู้ที่ทำการเชื่อมต่อจะต้องปฏิบัติ ดังนี้
  - ต้องเชื่อมต่อมาจากเครื่องที่ปลอดภัย และติดตั้ง Software ถูกต้องตามกฎหมายลิขสิทธิ์เท่านั้น
  - ต้องไม่เชื่อมต่อทิ้งไว้ ขณะที่ไม่สามารถปฏิบัติงานหน้าเครื่องคอมพิวเตอร์ได้
  - บริษัทฯ จะพิจารณายกเลิกการใช้งานทันที หากพบว่ามีความเสี่ยง และไม่ปลอดภัยในการเชื่อมต่อเพื่อทำงานจากภายนอกบริษัทฯ
- ฝ่ายสารสนเทศมีสิทธิ์ และหน้าที่ในการควบคุม และตรวจสอบการเข้าถึงเครือข่าย Internet ของบัญชีผู้ใช้ที่ได้รับสิทธิ์ตามนโยบายในทุกกรณี
- ฝ่ายสารสนเทศต้องจัดให้มีอุปกรณ์จัดเก็บข้อมูลจราจรสารสนเทศ (Transaction Log) ให้เป็นไปตามที่กฎหมายกำหนด
- บัญชีผู้ใช้ใดต้องการเข้าถึงเครือข่าย Internet ต้องได้รับการอนุมัติจากผู้บริหารหรือผู้มีอำนาจสูงสุดของหน่วยงานและผู้จัดการฝ่ายสารสนเทศเห็นชอบ
- การใช้งาน Internet ต้องใช้เพื่อวัตถุประสงค์เกี่ยวกับธุรกิจของบริษัทฯเท่านั้น และไม่อนุญาตการใช้เพื่อวัตถุประสงค์ที่ไม่เกี่ยวข้อง ดังตัวอย่างข้างล่างนี้
  - การเข้าไปอัพโหลด ดาวน์โหลด หรือส่งต่อเกี่ยวกับเรื่องลามกอนาจาร หรือเรื่องทางเพศ
  - ทำให้เสื่อมเสีย หรือเกี่ยวกับการเมือง
  - ทำลายทรัพย์สินของผู้อื่น หรือขององค์กร
  - รุกรานความเป็นส่วนตัว หรือดูหมิ่นผู้อื่น
  - ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา
  - ใช้เพื่อผลประโยชน์ทางการเงิน หรือธุรกิจอื่นๆ
  - ทำให้ประสิทธิภาพของระบบเครือข่ายลดลง หรือทำการรบกวนระบบ
- พนักงานแต่ละคนจะต้องรับผิดชอบการใช้งานจาก Internet account ที่ได้รับมอบไป และต้องใช้งาน Internet อย่างระมัดระวังจากภัยคุกคามต่างๆ และต้องไม่ละเมิดต่อระเบียบข้อบังคับ และกฎหมายที่เกี่ยวข้อง

- พนักงานทุกคนจะต้องไม่ดาวน์โหลด (Download) หรืออัพโหลด (Upload) โปรแกรมหรือข้อมูลจาก Internet นอกเหนือจากได้รับอนุญาตจากฝ่ายสารสนเทศ และจะต้องไม่เป็นข้อมูลที่ผิดระเบียบและกฎหมาย
- ผู้ใช้งาน Internet พึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย
- หลังจากใช้งานระบบ Internet เสร็จแล้ว ให้ปิดเว็บเบราเซอร์ที่ใช้งาน และออกจากเครือข่าย Internet ด้วยการ Logout และผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น
- ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานผ่านระบบ Internet

3. การบริหารจัดการทรัพยากร และทรัพย์สินด้านเทคโนโลยีสารสนเทศ

3.1. วัตถุประสงค์

3.3.1. เพื่อกำหนดแนวทางการจัดสรร และการบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ ให้เพียงพอ เหมาะสม และสอดคล้องกับ รูปแบบของธุรกิจ แผนการดำเนินธุรกิจ แผนกลยุทธ์ ความเร่งด่วน และงบประมาณ

3.3.2. เพื่อจำแนกแจกแจงประเภท และชนิดของทรัพย์สินทางด้านเทคโนโลยีสารสนเทศให้มีความชัดเจนเพื่อให้สามารถบริหารจัดการได้อย่างถูกต้อง และมีประสิทธิภาพ

3.3.3. เพื่อกำหนดหลักเกณฑ์ในการพิจารณาคุณสมบัติของทรัพย์สินทางด้านเทคโนโลยีสารสนเทศแต่ละประเภท และขั้นตอนการบำรุงรักษาให้มีความสอดคล้องกับสภาวะการณ์ที่เหมาะสม และทันสมัย

3.3.4. เพื่ออธิบายถึงสิทธิ์ และหน้าที่ในความเป็นเจ้าของทรัพย์สินที่แท้จริงกับอำนาจการควบคุมบริหารจัดการทรัพย์สินทางด้านเทคโนโลยีสารสนเทศ

3.3.5. เพื่อกำหนดหลักเกณฑ์ของการได้มา โอนย้าย จำหน่าย และทำลาย ซึ่งทรัพย์สินทางด้านเทคโนโลยีสารสนเทศ

คำนิยามศัพท์

ทรัพย์สินด้านเทคโนโลยีสารสนเทศ หมายความถึง เครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงทุกชนิดทั้งที่จับต้องได้ และจับต้องไม่ได้ซึ่งบริษัทฯเป็นเจ้าของ หรือถือครองกรรมสิทธิ์อยู่ สามารถจำแนกออกได้ดังนี้

- อุปกรณ์เครื่องใช้สำนักงานด้านไอที (Hardware)
- ซอฟท์แวร์ หรือโปรแกรม (Software)
- หนังสือสัญญา และหรือเอกสารใดๆ ที่แสดงถึงความเป็นเจ้าของ หรือมีกรรมสิทธิ์ในเทคโนโลยีสารสนเทศนั้นๆ

และให้ใช้คำว่า " ทรัพย์สิน " มีความหมายเท่ากับ " ทรัพย์สินด้านเทคโนโลยีสารสนเทศ " ในหมวดนี้ด้วย

เจ้าของทรัพย์สิน หมายความถึง บุคคล หรือหน่วยงานภายในบริษัทฯที่เป็นผู้ถือครอง และใช้งานทรัพย์สินนั้นๆ

ทะเบียนทรัพย์สิน หมายความถึง ระบบจัดการข้อมูลรายละเอียดต่างๆ ของทรัพย์สินด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นคนละระบบกับทะเบียนทรัพย์สินของแผนกบัญชี

3.2. รายละเอียดหลักเกณฑ์ปฏิบัติ

3.2.1 จัดทำแผนงานด้านเทคโนโลยีสารสนเทศ และจัดลำดับความสำคัญให้สอดคล้องโดยพิจารณาจากแผนกลยุทธ ผลกระทบต่อการดำเนินธุรกิจ ความเร่งด่วนในการใช้งาน งบประมาณ ทรัพยากร และรูปแบบธุรกิจ

3.2.2. ทรัพย์สินทางด้านเทคโนโลยีสารสนเทศใดๆ ให้ตกอยู่ภายใต้การควบคุม และบริหารจัดการของฝ่ายสารสนเทศ และฝ่ายสารสนเทศ มีอำนาจหน้าที่ในการให้คำแนะนำ สั่งระงับ ยกเลิก และสับเปลี่ยน ทรัพย์สินของหน่วยงานต่างๆ ภายในบริษัทฯเพื่อให้เกิดความเหมาะสม และสอดคล้องกับนโยบาย

3.2.3. เจ้าของทรัพย์สิน มีหน้าที่ดูแลรักษาทรัพย์สินของตนให้อยู่ในสภาพปกติเรียบร้อย ปลอดภัย และต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นกับทรัพย์สินทุกกรณี รวมถึงการสูญหาย และจะต้องมีการนำไปใช้อย่างถูกวิธีตามหลักจรรยา และกฎหมาย

3.2.4. การจัดซื้อทรัพย์สินใหม่ หรือการซ่อมแซมกรณีที่มีการเปลี่ยนอะไหล่ การกำหนดคุณสมบัติของทรัพย์สินหรืออะไหล่ให้เป็นหน้าที่ของฝ่ายสารสนเทศ การจัดซื้อทรัพย์สินใหม่ต้องได้รับการพิจารณา และเห็นชอบจากฝ่ายสารสนเทศกลางก่อนการอนุมัติสั่งซื้อทุกครั้ง ส่วนการจัดซื้อให้ปฏิบัติตามระเบียบบริษัทฯด้านจัดซื้อจัดจ้าง และด้านบัญชีการเงิน เรื่อง การเบิกค่าใช้จ่าย และเรื่อง หลักเกณฑ์การมอบอำนาจ และกระทำแทนบริษัทฯ

3.2.5. การจัดทำทะเบียนทรัพย์สิน ฝ่ายสารสนเทศมีหน้าที่จัดทำทะเบียนประวัติทรัพย์สินทั้งหมดของบริษัทฯ ฝ่ายสารสนเทศมีอำนาจหน้าที่ในการเรียกคืน ตรวจสอบ และไล่สวน เพื่อให้ได้ข้อมูลทรัพย์สินที่ถูกต้องจากทุกหน่วยงาน

3.2.6. การเคลื่อนย้ายทรัพย์สิน หรือการโอนย้ายทรัพย์สินไปยังสถานที่ตั้งแห่งใหม่ หรือหน่วยงานอื่น และการจำหน่ายและการทำลายทรัพย์สิน ให้ปฏิบัติตามระเบียบบริษัทฯด้านบัญชี - การเงิน

3.2.7. ทรัพย์สินอันเป็นอุปกรณ์จัดเก็บข้อมูลทุกชนิด ก่อนการจำหน่าย และการทำลายต้องแน่ใจว่าได้ดำเนินการสำรองข้อมูลที่สำคัญไว้อย่างครบถ้วน และได้ทำลายข้อมูลในทรัพย์สินนั้นทิ้งเป็นที่เรียบร้อยแล้ว

3.2.8. ห้ามพนักงานรื้อ ถอด หรือสับเปลี่ยนอะไหล่ของทรัพย์สิน โดยเด็ดขาด ยกเว้น เจ้าหน้าที่สารสนเทศ

3.2.9. ห้ามนำทรัพย์สินใดๆออกภายนอกบริเวณบริษัทฯ โดยเด็ดขาด ยกเว้น ได้รับอนุมัติจากผู้จัดการฝ่าย หรือผู้มีอำนาจสูงสุดของหน่วยงานนั้น ร่วมกับผู้จัดการฝ่ายสารสนเทศ หากเป็นอุปกรณ์พกพา อาทิ โน้ตบุ๊ก สมาร์ทโฟน ผู้นำออกต้องเป็นเจ้าของทรัพย์สิน และจะต้องดูแลรักษาทรัพย์สินของตนให้ปลอดภัย และต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นกับทรัพย์สินทุกกรณี รวมถึงการสูญหาย

3.2.10. การชดใช้ค่าเสียหาย ในกรณีที่เกิดความเสียหาย หรือสูญหายของทรัพย์สิน พนักงานจะต้องชดใช้ค่าเสียหายตามราคาในท้องตลาด

4. ระเบียบปฏิบัติด้านระบบเทคโนโลยีสารสนเทศ

4.1. วัตถุประสงค์

4.1.1. เพื่อกำหนดหลักเกณฑ์ หรือระเบียบปฏิบัติที่ชัดเจนในแต่ละด้านของฝ่ายสารสนเทศ

4.1.2. เพื่อกำหนดขอบเขต และหน้าที่ความรับผิดชอบให้กับเจ้าหน้าที่สารสนเทศ

4.1.3. เพื่อกำหนดมาตรการรักษาความปลอดภัยเกี่ยวกับผู้ให้บริการด้านเทคโนโลยีสารสนเทศจากภายนอกองค์กร

4.1.4. เพื่อกำหนดมาตฐานด้านการให้บริการระบบเทคโนโลยีสารสนเทศภายในองค์กร

4.2. รายละเอียดหลักเกณฑ์ปฏิบัติ

4.2.1. ฝ่ายสารสนเทศ จะต้องระบุเจ้าหน้าที่สารสนเทศผู้รับผิดชอบในแต่ละส่วนงานให้ชัดเจน และระบุขอบเขตรับผิดชอบของบริการแต่ละรายการ เพื่อให้ผู้ใช้มีความคาดหวัง (Expectation) จากบริการที่ตรงกัน ซึ่งจะต้องประกอบด้วยข้อมูลอย่างน้อย ดังนี้

- สื่อในการรับแจ้งเหตุ เช่น โทรศัพท์ อีเมล์ เซ็นเตอร์(e Center) เป็นต้น
- วัน และเวลาการให้บริการ
- ชื่อบุคคล หน่วยงาน หรือกลุ่มเจ้าหน้าที่ที่รับผิดชอบการรับแจ้งเหตุ

4.2.2. ฝ่ายสารสนเทศจะต้องจัดให้มีศูนย์บริการสนับสนุน (Help Desk) ซึ่งจะต้องมีเจ้าหน้าที่สารสนเทศขั้นพื้นฐานหรือวิศวกรขั้นต้น ทำหน้าที่รับแจ้งเหตุการณ์ และแก้ปัญหาทั้งทางสื่อรับแจ้งเหตุ หรือสถานที่เกิดเหตุ และผู้เชี่ยวชาญจากภายนอก เพื่อทำหน้าที่แก้ไขปัญหาเฉพาะด้านหรือเฉพาะกิจ โดยหน้าที่รับผิดชอบของศูนย์บริการมีดังนี้

- รับแจ้งเหตุจากผู้ใช้ทุกกรณี หากอยู่นอกเหนือความรับผิดชอบให้ประสานงานต่อเพื่ออำนวยความสะดวก
- กำหนดระดับบริการ และระดับความรุนแรงของปัญหาโดยใช้แนวทางที่ระบุไว้ในนโยบายฉบับนี้ และแจ้งระยะเวลาตอบรับ และระยะเวลาแก้ไขปัญหาตามระเบียบของนโยบายฉบับนี้ให้ผู้ใช้ทราบ
- พยายามแก้ปัญหาให้สิ้นสุดโดยเร็วที่สุด และต้นทุนต่ำที่สุด ด้วยวิธีการที่เหมาะสม เกิดผลกระทบน้อย
- ในกรณีที่ไม่สามารถแก้ไขปัญหาได้ จะต้องทำการปรับระดับเหตุการณ์ขึ้น (Escalate) เพื่อให้ผู้ชำนาญระดับถัดไปเข้าร่วมแก้ไขทันที
- ในกรณีที่ฝ่ายสารสนเทศไม่สามารถแก้ไขได้ จะต้องประสานให้ผู้ชำนาญภายนอกเข้ามาแก้ไขให้เร็วที่สุด และสมบูรณ์ที่สุดภายในเวลาที่จำกัดไว้ในนโยบายฉบับนี้

4.2.3. ฝ่ายสารสนเทศกำหนด**ระดับการให้บริการ (Service Level)** ประเภทความรุนแรงของปัญหา (Severity) ระยะเวลาการตอบรับ (Response Time) และระยะเวลาที่จะต้องแก้ไข (Resolution Time) ซึ่งระดับการให้บริการ (Service Level) คือ ระดับการให้บริการสนับสนุนที่ศูนย์บริการเป็นผู้กำหนดให้กับเหตุการณ์ หรือปัญหาที่รับแจ้ง ให้เหมาะสมสอดคล้องกับความต้องการสนับสนุนขององค์กร ดังนี้

- ระดับที่ 1 หรือ ระดับแนวหน้า (Level 1 Front Line) เจ้าหน้าที่บริการด้าน IT มีหน้าที่รับแจ้งเหตุทุกกรณีจากผู้ใช้ แก้ไขปัญหาเบื้องต้น และให้คำแนะนำ หรือชี้แนะแนวทางแก้ไขให้กับผู้ใช้ ผ่านทางสื่อรับแจ้งทุกรูปแบบ เพื่อให้สถานการณ์ยุติ หรือเบาบางลงให้เร็ว และมากที่สุด ในกรณีที่ไม่สามารถแก้ไขได้ จะต้องยกระดับปัญหา (Escalate) ขึ้นเป็นระดับ 2 เพื่อให้หัวหน้างาน หรือวิศวกรผู้ดูแลระบบฯแก้ไขต่อไป
- ระดับที่ 2 หรือ ระดับกลาง (Level 2 ***Specialist Support***) จะมีหน้าที่รับเหตุการณ์จากระดับ 1 เพื่อทำการแก้ไขปัญหา โดยมีการร่วมดำเนินการของวิศวกรผู้ดูแลระบบฯ และผู้จัดการแผนกสารสนเทศ ในกรณีที่ไม่สามารถแก้ไขได้ จะต้องยกระดับปัญหา (Escalate) ขึ้นเป็นระดับ 3 เพื่อให้ผู้ชำนาญการแก้ไขต่อไป
- ระดับที่ 3 หรือ ระดับสูง (Level 3 ***Professional Support***) มีหน้าที่รับเหตุการณ์จากระดับ 2 เพื่อทำการแก้ไข หรือประสานการแก้ไขกับผู้ชำนาญการจากบริษัทภายนอกที่ให้บริการนั้นๆ และจะต้องรายงานให้ผู้จัดการฝ่ายสารสนเทศรับทราบถึงความคืบหน้าอย่างใกล้ชิด จนกว่าปัญหาจะถูกแก้เสร็จสมบูรณ์

4.2.4. **ประเภทความรุนแรงของปัญหา (Severity)** คือ ประเภทของผลกระทบที่มีต่อธุรกิจของบริษัทฯโดยรวม ซึ่งจัดไว้มี 4 ระดับดังนี้

- ระดับความรุนแรง A (Severity A) คือระดับกระทบงานถึงขั้นกระทบธุรกิจ หรือสถานการณ์เงินของบริษัทฯโดยรวม ผู้ใช้ไม่สามารถใช้งานคอมพิวเตอร์ทั้งหมด ไม่สามารถแก้ให้ใช้งานอื่นก่อนชั่วคราว และไม่สามารถปฏิบัติงานต่อได้
- ระดับความรุนแรง B (Severity B) คือ ระดับกระทบงานถึงขั้นเป็นเหตุให้งานของหลายหน่วยงาน ชะงักงัน ผู้ใช้ไม่สามารถใช้งานคอมพิวเตอร์ทั้งหมด ไม่สามารถแก้ให้ใช้งานอื่นก่อนชั่วคราว แต่พอยอมรับได้
- ระดับความรุนแรง C (Severity C) คือ ระดับกระทบงานถึงขั้นทำให้เครื่องลูกข่าย หรือ Client หยุดทำงาน ผู้ใช้ไม่สามารถใช้งานคอมพิวเตอร์บางอย่างได้ แต่พอจะใช้งานไปก่อนชั่วคราวได้
- ระดับความรุนแรง D (Severity D) คือ ระดับกระทบงานพอสมควรแต่สามารถหาทางแก้ปัญหาเฉพาะหน้าเพื่อให้ทำงานต่อได้ ผู้ใช้ไม่สามารถใช้งานคอมพิวเตอร์บางอย่างได้ แต่สามารถแก้เพื่อให้ใช้งานไปก่อนชั่วคราวได้ และไม่กระทบการทำงานแต่อย่างใด

4.2.5. **ระยะเวลาการตอบรับ (Response Time)** คือ ระยะเวลาที่จำกัดให้ศูนย์บริการจะต้องสื่อความ หรือประสานให้ทุกฝ่ายรับทราบถึงความคืบหน้าของเหตุการณ์หรือปัญหา

- ในกรณีที่ระดับความรุนแรง A ศูนย์บริการจะต้องแจ้งความคืบหน้าทุกๆ หนึ่ง (1) ชั่วโมงหลังจากการยืนยันรับแจ้งในครั้งแรก จนกว่าเหตุการณ์จะยุติ หรือเสร็จสิ้น หรือจนกว่าเหตุการณ์จะถูกเปลี่ยนระดับความรุนแรงต่ำลง
- ในกรณีปกติหรือไม่ใช่ระดับ A ศูนย์บริการจะต้องแจ้งความคืบหน้าทุกๆ สี่ (4) ชั่วโมงหลังจากการยืนยันรับแจ้งในครั้งแรก จนกว่าเหตุการณ์จะยุติหรือเสร็จสิ้น หรือจนกว่าเหตุการณ์จะถูกเปลี่ยนระดับความรุนแรงต่ำลง
- ในกรณีที่เป็นปัญหาระดับความรุนแรง A และ B แต่เป็นที่ตกลงกันว่าจะต้องใช้ระยะเวลาการแก้ไข (Resolution Time) นานเกินสาม (3) วันทำการ ศูนย์บริการไม่ต้องทำการแจ้งความคืบหน้าตามระเบียบที่กว่ามา แต่จะต้องแจ้งความคืบหน้าทันทีเมื่อมีการเปลี่ยนแปลง หรือตามความเหมาะสม เพื่อให้ผู้ใช้ได้รับการบริการที่ดีที่สุด

4.2.6. **ระยะเวลาที่จะต้องแก้ไข (Resolution Time)** คือ ระยะเวลาที่จำกัดฝ่ายสารสนเทศจะต้องแก้ไขปัญหาให้แล้วเสร็จ ซึ่งประกอบด้วยแนวทางพิจารณา ดังนี้

- ในกรณีที่ระดับความรุนแรง A ฝ่ายสารสนเทศจะต้องแจ้งแก้ไขปัญหาให้แล้วเสร็จภายใน **ยี่สิบสี่ (24)** ชั่วโมง หลังจากการยืนยันรับแจ้งในครั้งแรก ยกเว้นแต่ เหตุการณ์ได้บรรเทาลง หรือถูกเปลี่ยนระดับความรุนแรงต่ำลง
- ในกรณีที่ระดับความรุนแรง B ฝ่ายสารสนเทศจะต้องแจ้งแก้ไขปัญหาให้แล้วเสร็จภายใน **สาม (3)** วันทำการ หลังจากการยืนยันรับแจ้งในครั้งแรก ยกเว้นแต่ เหตุการณ์ได้บรรเทาลง หรือถูกเปลี่ยนระดับความรุนแรงต่ำลง
- ในกรณีที่ระดับความรุนแรง C ฝ่ายสารสนเทศจะต้องแจ้งแก้ไขปัญหาให้แล้วเสร็จภายใน **เจ็ด (7)** วันทำการ หลังจากการยืนยันรับแจ้งในครั้งแรก ยกเว้นแต่ เหตุการณ์ได้บรรเทาลง หรือถูกเปลี่ยนระดับความรุนแรงต่ำลง
- ในกรณีที่ระดับความรุนแรง D ฝ่ายสารสนเทศจะต้องแจ้งแก้ไขปัญหาให้แล้วเสร็จภายใน **สิบห้า (15)** วันทำการหลังจากการยืนยันรับแจ้งในครั้งแรก ยกเว้นแต่ เหตุการณ์ได้บรรเทาลง หรือถูกเปลี่ยนระดับความรุนแรงต่ำลง
- ในกรณีที่เป็นที่ตกลงกันว่าการแก้ไขปัญหาจะต้องใช้ระยะเวลาการนานเกินที่จำกัดไว้ ฝ่ายสารสนเทศจะต้องประเมินยะยะเวลาแก้ไขปัญหาใหม่ให้ผู้ใช้เห็นด้วย และดำเนินการตามขั้นตอนของนโยบายฉบับนี้ให้บรรลุเป้าหมายตามที่ตกลงไว้ และให้ผู้ใช้ได้รับการบริการที่ดีที่สุด

4.2.7. เจ้าหน้าที่ศูนย์บริการจะต้องให้บริการผู้ใช้ทุกระดับในองค์กร โดยที่จะต้องมีคุณสมบัติการให้บริการดังนี้

- มีความกระตือรือร้น และไวต่อการตอบรับ (Responsiveness)
- มีท่าทีต่อผู้ใช้ที่อบอุ่น และเห็นอกเห็นใจ (Caring Attitude)

- มีทักษะ และความชำนาญที่เหมาะสม (Skillful)

4.2.8. การปฐมนิเทศเรื่องสารสนเทศแก่พนักงานใหม่ ฝ่ายสารสนเทศจะต้องจัดทำหนังสือ หรือคู่มือการใช้งานระบบสารสนเทศขั้นต้น เฉพาะของบริษัทฯเพื่อแจกให้พนักงานทั้งหมด รวมถึงพนักงานที่เข้าใหม่ ซึ่งจะต้องรวมถึง

- หมายเลขติดต่อ และช่องทางการติดต่อ รวมถึงเจ้าหน้าที่หลักในการให้บริการ
- ขั้นตอนการใช้งาน และการเข้าออกระบบเครือข่ายสารสนเทศของบริษัทโดยสังเขป
- วิธีแก้ปัญหาขั้นต้นด้วยตนเอง และหมายเลขศูนย์บริการสนับสนุน (Help Desk) ในกรณีมีคำถามหรือไม่สามารถแก้ปัญหาได้

4.2.9. การจัดการสารสนเทศเมื่อพนักงานถูกโอนย้ายไปรับผิดชอบในหน่วยงานอื่น ทางฝ่ายบุคคลจะต้องแจ้งทางฝ่ายสารสนเทศเพื่อดำเนินการ

- เปลี่ยนชื่อผู้ใช้ และรหัสผ่านของพนักงานถ้าจำเป็น หรือตามที่หน่วยงานกำหนด
- เรียกคืนอุปกรณ์ที่อยู่ในความครอบครองคืน หรือทำการเปลี่ยนอุปกรณ์ที่เหมาะสมให้ใช้งานต่อไป

4.2.10. การให้บริการ และการบำรุงรักษาระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก

- จัดทำข้อตกลงหรือเงื่อนไขของการให้บริการระหว่างบริษัทฯกับหน่วยงานภายนอกเป็นลายลักษณ์อักษร พร้อมทั้งให้ผู้มีอำนาจของทั้งสองฝ่ายลงนาม และเก็บไว้คนละ 1 ชุด
- ฝ่ายสารสนเทศต้องทบทวน และตรวจสอบความถูกต้องของเอกสาร พร้อมทั้งปรับปรุงแก้ไขให้ถูกต้องทันสมัย
- ฝ่ายสารสนเทศต้องควบคุม และตรวจสอบการปฏิบัติงานของผู้ให้บริการให้เป็นไปตามข้อตกลงหรือเงื่อนไข
- ฝ่ายสารสนเทศต้องกำหนดมาตรการป้องกันความปลอดภัยที่สอดคล้องกับข้อกำหนดทางธุรกิจของบริษัทฯ และมาตรฐานความปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ พร้อมทั้งแจ้งให้กับผู้ให้บริการรับทราบ และปฏิบัติตามอย่างเคร่งครัด

4.2.11. การพัฒนาระบบเทคโนโลยีสารสนเทศ ครอบคลุมงานทุกด้านทั้งฮาร์ดแวร์ และซอฟท์แวร์ ให้จัดทำเป็นโครงการพัฒนาระบบ โดยผู้ร้องขอ หรือหน่วยงานต้นสังกัด ต้องจัดทำใบนำเสนอโครงการเพื่อผ่านการพิจารณาจากผู้บริหารหน่วยงาน และผู้จัดการฝ่ายสารสนเทศ มีหน้าที่ให้ความเห็นชอบ ร่วมวิเคราะห์ ประเมินความเสี่ยง พิจารณา และตัดสินใจในด้านเทคนิค กำกับควบคุมผลการพัฒนาให้เป็นไปตามความต้องการ ข้อกำหนดทางธุรกิจ สถาปัตยกรรมด้านเทคโนโลยีสารสนเทศที่เหมาะสม และกฎหมายข้อบังคับที่เกี่ยวข้อง

5. การบริหารจัดการระบบเทคโนโลยีสารสนเทศในสถานการณ์ฉุกเฉิน

5.1. วัตถุประสงค์

เพื่อกำหนดหลักปฏิบัติในการป้องกัน และกู้คืนระบบเทคโนโลยีสารสนเทศให้สามารถทำงานได้ในสถานการณ์ฉุกเฉิน ภายในระยะเวลาที่เหมาะสม ตลอดจนสร้างความเชื่อมั่น และหลักประกันด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ

5.2. รายละเอียดหลักเกณฑ์ปฏิบัติ

5.2.1. การเตรียมพร้อมกรณีฉุกเฉิน

- ฝ่ายสารสนเทศจะต้องจัดทำแผนป้องกัน และกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Plan)
- ดำเนินการจัดการทดสอบปฏิบัติตามแผนอย่างน้อยปีละ 1 ครั้ง
- ดำเนินการปรับปรุงแก้ไขแผนปฏิบัติ ให้มีความทันสมัย
- ฝ่ายสารสนเทศต้องแจ้งให้กับหน่วยงานที่เกี่ยวข้องกับแผนปฏิบัติทุกหน่วยงาน พร้อมทั้งชี้แจง และอธิบายถึงขั้นตอนการปฏิบัติให้กับพนักงานผู้รับผิดชอบในแต่ละขั้นตอนอย่างชัดเจน

5.2.2. การสำรองข้อมูลและระบบคอมพิวเตอร์

- จัดทำสำเนาข้อมูล และซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความสำคัญของระบบ สอดคล้อง และเพียงพอกับความต้องการ หรือการยอมรับได้ขององค์กรในการกู้คืนข้อมูล สำหรับระบบ ERP บริษัทฯ ยอมรับความสูญหายของข้อมูล ณ วันที่เกิดความเสียหาย ย้อนหลังไปสูงสุด 1 วัน หลังการกู้คืน
- มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง และเพียงพอทั้งระบบซอฟต์แวร์ และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบเทคโนโลยีสารสนเทศแต่ละระบบ
- จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการติดชื่อ หรือรหัสบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงวันที่ เวลาที่สำรองข้อมูลไว้อย่างชัดเจน เพื่อให้สะดวก และป้องกันข้อผิดพลาดในเมื่อต้องการใช้กู้คืนข้อมูล
- ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

6. การบริหารการใช้บริการจากผู้ให้บริการภายนอก (Outsourcing Management)

วัตถุประสงค์

เพื่อให้การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอกเป็นไปอย่างมีประสิทธิภาพ น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือก และควบคุมการปฏิบัติงานของผู้ให้บริการ

รายละเอียดหลักเกณฑ์ปฏิบัติ

ผู้ที่ต้องทำงานร่วมกับผู้ให้บริการจากภายนอก ต้องควบคุมการปฏิบัติงาน ดังนี้

1. ***ผู้ให้บริการภายนอกจะต้องปฏิบัติงานโดยตระหนัก และรับผิดชอบต่อความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศของบริษัทฯ***
2. ต้องมีการประเมินความพร้อมในการบริหารความเสี่ยงด้านความปลอดภัยของผู้ให้บริการจากภายนอกทั้งระบบ และขั้นตอนการดำเนินงานของผู้ให้บริการว่าอยู่ในเกณฑ์ที่ปลอดภัยเพียงพอ
3. ผู้ให้บริการจากภายนอกจะต้องมีการลงนามในข้อตกลงเพื่อป้องกันการเปิดเผยข้อมูล รวมทั้งข้อตกลงในเงื่อนไขการให้บริการ (Service Level Agreement) ที่มีการระบุมาตรการการรักษาความปลอดภัยอย่างชัดเจน เพื่อให้ทราบถึงขอบเขตความรับผิดชอบระหว่างผู้ให้บริการภายนอก และบริษัทฯ
4. อนุญาตผู้ให้บริการจากภายนอกสามารถเข้าถึงทรัพยากรต่างๆ ในบริษัทฯได้ตามที่ระบุไว้ในข้อตกลง หรือสัญญาระหว่างสองฝ่ายเท่านั้น รวมถึงจะต้องปฏิบัติงานอยู่ในสถานที่ซึ่งบริษัทฯจัดเตรียมให้เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานอื่น ก็ต้องมีการควบคุม หรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด
5. ในกรณีที่มีความจำเป็นเร่งด่วนในการทำงานของผู้ให้บริการด้วยการเชื่อมต่อระบบจากภายนอกเข้าสู่ระบบซึ่งติดตั้งอยู่ภายในบริษัทฯ จะมีการพิจารณาเป็นกรณีพิเศษโดยต้องได้รับการอนุมัติจากผู้จัดการฝ่ายสารสนเทศก่อนเสมอ โดยให้เจ้าหน้าที่บริษัทฯตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียด และปิดการเชื่อมต่อทันทีที่การให้บริการเสร็จสิ้น
6. หากผู้ให้บริการจากภายนอกมีความต้องการนำอุปกรณ์ เครื่องคอมพิวเตอร์ หรือระบบใดๆ เพื่อเข้ามาช่วยในการทำงานจะต้องได้รับการเห็นชอบ และประเมินผลต่อความปลอดภัยของบริษัทฯก่อนใช้งานทุกครั้ง ***โดยผู้บริหารหน่วยงานและผู้จัดการฝ่ายสารสนเทศ***
7. ***ผู้ให้บริการควรจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องเพื่อใช้เป็นแนวทางในการปฏิบัติงานต่อไป***

7. การตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy: IDS/IPS Policy)

วัตถุประสงค์

IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากรระบบเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่ายภายในบริษัทฯ ให้มีความมั่นคงปลอดภัย

แนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย

แนวทางการปฏิบัติและบทบาทหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการตรวจสอบการบุกรุกเครือข่าย เป็นดังนี้

7.1. IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของบริษัทฯ และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทางทุกเส้นทาง

7.2. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ต หรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

7.3. ระบบทั้งหมดใน Demilitarized zone (DMZ) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้ง และเปิดให้บริการ

7.4. โฮสต์ และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

7.5. มีการตรวจสอบ และ Update Patch/Signature ของ IDS/IPS เป็นประจำ

7.6. มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

7.7. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบเทคโนโลยีสารสนเทศตามปกติ

7.8. เครื่องแม่ข่ายที่มีการติดตั้ง Host based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

7.9. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จ และไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

7.10. พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบภายใน 1 ชั่วโมงที่ตรวจพบ

7.11. มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

7.12. บริษัทฯมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

7.13. ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของบริษัทฯ การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบเทคโนโลยีสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของบริษัทฯ จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

8. การพัฒนา และบริการจัดการความเปลี่ยนแปลงระบบสารสนเทศ (IS Development and Change Management)

8.1. หน่วยงานที่มีความต้องการพัฒนาระบบสารสนเทศ หรือเขียนโปรแกรมต่างๆ มีหน้าที่รวบรวมความต้องการ ปัญหาที่ประสบเทคโนโลยี การเชื่อมต่อ และรายงานที่เกี่ยวข้อง แจ้งต่อฝ่ายสารสนเทศให้ทำการพัฒนา

8.2. ฝ่ายสารสนเทศมีหน้าที่รับแจ้งความต้องการพัฒนาระบบ หรือเขียนโปรแกรมจากหน่วยงานต่างๆเพื่อนำมาศึกษา วิเคราะห์ออกแบบ นำเสนอระบบ ทางเลือก งบประมาณ ทำการพัฒนา (เขียนโปรแกรม) หรือจัดหามาโดยการจัดซื้อจัดจ้างเพื่อให้ได้มาซึ่งระบบตามความต้องการ ร่วมทดสอบระบบ แนะนำให้ความรู้กับผู้ใช้งาน และจัดทำ หรือรวบรวมเอกสารที่เกี่ยวข้องในการพัฒนา

8.3. หน่วยงานที่มีความต้องการปรับปรุง แก้ไข เปลี่ยนแปลงระบบสารสนเทศที่ใช้งานอยู่ สำหรับในประเด็นที่มีนัยสำคัญ หรืออาจก่อให้เกิดผลกระทบ หรือมีความเสี่ยงสูงขึ้นไป จะต้องดำเนินการตามขั้นตอน และกระบวนที่ฝ่ายสารสนเทศกำหนดในการบริหารจัดการควบคุมการเปลี่ยนแปลงระบบสารสนเทศ

8.4. ฝ่ายสารสนเทศต้องกำหนดระเบียบขั้นตอนการปฏิบัติเพื่อควบคุมการเปลี่ยนแปลงที่จะเกิดขึ้นกับระบบงานจริง (Production Environment) ซึ่งการเปลี่ยนแปลงทั้งหลายนั้น รวมตั้งแต่ขั้นตอน และกระบวนการที่ใช้ในการปฏิบัติงาน และค่า parameter ต่างๆเพื่อให้มั่นใจได้ว่าสามารถลดความเสี่ยงด้านความมั่นคง (Stability) ของระบบ และความถูกต้อง (Integrity) ของข้อมูล

9. การปฏิบัติตามข้อกำหนดทางกฎหมาย และข้อบังคับอื่นๆ

9.1. พนักงานทุกคนมีหน้าที่ตระหนัก และปฏิบัติตามกฎหมายตลอดจนข้อบังคับที่เกี่ยวข้อง

9.2. ฝ่ายสารสนเทศมีหน้าที่ติดตามข่าวสารกฎหมาย และข้อบังคับที่เกี่ยวข้องกับการดำเนินธุรกิจ เพื่อวิเคราะห์ความสอดคล้อง กำหนดวิธีการดำเนินการให้สอดคล้อง และทันสมัย

9.3. ฝ่ายสารสนเทศมีหน้าที่สื่อสารประชาสัมพันธ์ให้พนักงานผู้ใช้งานระบบเทคโนโลยีสารสนเทศมีความรู้ความเข้าใจ ปฏิบัติได้อย่างสอดคล้องถูกต้องตามกฎหมายตลอดจนข้อบังคับที่เกี่ยวข้อง

9.4. ฝ่ายสารสนเทศมีหน้าที่การกำหนดกฎระเบียบ ขั้นตอน และควบคุมการปฏิบัติด้านระบบเทคโนโลยีสารสนเทศ ให้สอดคล้องถูกต้องตามกฎหมายตลอดจนข้อบังคับที่เกี่ยวข้อง