ประกาศที่ 036/2565

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
INFORMATION TECHNOLOGY SECURITY POLICY

TAO KAE NOI

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่งคงปลอดภัยเทคโนโลยีสารสนเทศ

<u>บทนำ</u>

บริษัท เถ้าแก่น้อย ฟู้ดแอนด์มาร์เก็ตติ้ง จำกัด (มหาชน) และบริษัทในเครือ ได้จัดทำประกาศฉบับนี้ขึ้น เพื่อเป็นนโยบายและแนวทางปฏิบัติในการรักษาความมั่งคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยตระหนักถึงความสำคัญการจัดการ เก็บรักษา และดูแลข้อมูลบนระบบเทคโนโลยีสารสนเทศโดยให้มีความสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 รวมทั้ง ประกาศที่เกี่ยวข้องของบริษัทฯ โดยประกาศฉบับนี้บังคับใช้กับบุคคลที่มีปฏิสัมพันธ์กับบริการระบบเทคโนโลยีสารสนเทศต่างๆ ของบริษัท เถ้าแก่น้อย ฟู้ดแอนด์มาร์เก็ตติ้ง จำกัด(มหาชน) และบริษัทในเครือทั้งหมด

<u>คำนิยาม</u>

1. **“บริษัทฯ”** หมายถึง บริษัท เถ้าแก่น้อย ฟู้ดแอนด์มาร์เก็ตติ้ง จำกัด (มหาชน) และบริษัทในเครือประกอบด้วย 4 บริษัท ดังนี้
   บริษัท เถ้าแก่น้อย เรสเตอรองท์ แอนด์ แฟรนไชส์ จำกัด “TKNRF”
   Taokaenoi USA Inc. “TKNUS”
   บริษัท เอ็นซีพี เทรดดิ้ง แอนด์ ซัพพลาย จำกัด “NCP”
   บริษัท เถ้าแก่น้อย แคร์ๆ จำกัด “TKNC“
2. **“โปรแกรมประยุกต์”** หมายถึง โปรแกรม หรือชุดคำสั่ง ที่ใช้บันทึกข้อมูล, ประมวนผลข้อมูลต่างๆ ในบริษัทฯ หรือควบคุมการทำงานของคอมพิวเตอร์เคลื่อนที่และอุปกรณ์ต่อพ่วงต่างๆ
3. **“VPN (Virtual Private Network)”** หมายถึง ระบบสร้างการเชื่อมต่อระหว่างเครือข่ายหนึ่งไปยังอีกระบบหนึ่งซึ่งเดิมไม่สามารถเชื่อมต่อได้ ให้เสมือนเป็นระบบเดียวกันสามารถใช้งานทรัพยากรภายใต้ข้อกำหนดและการอนุญาตให้เข้าถึงข้อมูลที่มีความปลอดภัย
4. **“Mac Address”** หมายถึง หมายเลขรหัสที่มีตัวเลขฐานสิบหก จะไม่ซ้ำกันที่ติดอยู่กับอุปกรณ์ที่เชื่อมต่อกับเน็ตเวิร์คและเครือข่าย
5. **“User ID”** หมายถึง รหัสผู้ใช้งาน ที่ใช้สำหรับเข้าใช้งานระบบ
6. **“Authentication”** หมายถึง การยืนยันตัวตนในขณะที่เรากำลังใช้งานระบบใดๆ บนระบบอินเตอร์เน็ตของบริษัทฯ ซึ่งต้องมีการยืนยันตัวตนก่อนที่จะเข้าใช้งานได้ โดยใช้ User ID และ Password
7. **“Authorization”** หมายถึง การลงชื่อเข้าสู่ระบบโดยขั้นตอนแรกต้องผ่านการ ยืนยันตัวตนเพื่อทำการพิสูจน์ตัวตนก่อน เมื่อทำการยืนยันตัวตนเรียบร้อยแล้ว จะทำการตรวจสอบว่ามีสิทธิ์ในการใช้งานในส่วนใดได้บ้างตามที่กำหนด
8. **“Disaster Recovery Site (DR Site)”** หมายถึง พื้นที่สำรองสำหรับแก้ไขปัญหาระบบสารสนเทศ ที่เกิดขึ้นจากภัยพิบัติต่างๆ ให้สามารถทำงานได้อย่างต่อเนื่อง

9. **“การสำรองข้อมูล”** หมายถึง เป็นการคัดลอกแฟ้มข้อมูลเพื่อทำสำเนา เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น หากข้อมูลเกิดการเสียหายหรือสูญหาย จะสามารถนำข้อมูลที่สำรองไว้มาใช้งานได้ทันที
10. **“MAS”** หมายถึง ระบบเว็บแอพพลิเคชั่นและแอพพลิเคชั่นของบริษัทฯ ที่ใช้ในการจัดการระบบงานภายใน หรือข้อมูลต่างๆ เป็นต้น
11. **“อุปกรณ์พิสูจน์อัตลักษณ์”** หมายถึง ข้อมูลทางชีวภาพ ไม่ว่าจะเป็นลักษณะเฉพาะทางกายภาพหรือพฤติกรรม มาใช้ในการตรวจสิทธิหรือแสดงตน เช่น ลายนิ้วมือ ฝ่ามือ เสียง ม่านตา เรตินา ใบหน้า ดีเอ็นเอ ลายลงนาม เป็นต้น
12. **“สื่อบันทึกข้อมูล”** หมายถึง สื่อบันทึกข้อมูลใดๆ ที่ใช้วิธีการทางอิเล็กทรอนิกส์
13. **“ระบบปฏิบัติการ”** หมายถึง โปรแกรมประยุกต์ระบบ (Systems software) ที่ทำหน้าที่ควบคุมการทำงานของฮาร์ดแวร์ทั้งหมด รวมทั้งการปฏิบัติงานของโปรแกรมด้วย เพื่อให้โปรแกรมและฮาร์ดแวร์ต่างๆ ทำงานประสานกันแนวทางปฏิบัติ
14. **“เครื่องเซิร์ฟเวอร์”** หมายถึง เครื่องหลักที่มีการแชร์ข้อมูลให้เครื่องอื่นๆ ที่เข้ามาใช้งานผ่านเครื่องตัวเอง เช่น การแชร์ Printer, การแชร์ไฟล์งานต่างๆ เป็นต้น
15. **“เว็บบราวเซอร์”** หมายถึง โปรแกรมคอมพิวเตอร์ที่ใช้งานเพื่อดูข้อมูลและโต้ตอบกับข้อมูลสารสนเทศที่จัดเก็บในเว็บแอพพลิเคชั่น
16. **“Database”** หมายถึง กลุ่มของข้อมูลที่ถูกเก็บรวบรวมไว้ โดยมีความสัมพันธ์ซึ่งกันและกันโดยไม่ได้บังคับว่าข้อมูลทั้งหมดนี้จะต้องเก็บไว้ในแฟ้มข้อมูลเดียวกันหรือแยกเก็บหลาย ๆ แฟ้มข้อมูล
17. **“SSL”** (Secure Socket Layer Protocols) หมายถึง เกณฑ์วิธีการส่งข้อมูล ที่ถูกใช้เป็นมาตรฐานในการเพิ่มความปลอดภัย ในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ตโดยการเข้ารหัส
18. **“เว็บเซิร์ฟเวอร์ (Web Server)”** หมายถึง เครื่องคอมพิวเตอร์ที่ให้บริการเว็บเพจ เมื่อผู้ใช้งานร้องขอเว็บเพจผ่านเว็บบราวเซอร์เรียกใช้โดยการระบุตำแหน่งของเว็บเพจ (URL) เว็บเซิร์ฟเวอร์จะส่งเว็บเพจที่ค้นหาได้กลับไปแสดงผลผ่านเว็บบราวเซอร์ของผู้ใช้งาน
19. **“กุญแจรหัส (Key)”** หมายถึง ชุดตัวอักษรที่ซับซ้อนและยากต่อการคาดเดา ใช้สำหรับเข้ารหัสและถอดรหัส
20. **“อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่”** หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่มีหน่วยประมวลผล หน่วยความจำ หรือมีหน่วยเชื่อมต่อกับอุปกรณ์อื่นๆ เช่น คอมพิวเตอร์ โน๊ตบุ๊ค แล็ปท็อป โทรศัพท์มือถือ สมาร์ทโฟน แท็บเล็ต เป็นต้น
21. **“ล็อก (Log)”** หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ แสดงถึงแหล่งกำเนิด, ต้นทาง, ปลายทาง, เส้นทาง, เวลา, วันที่, ปริมาณ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์
22. **“AD Online”** หมายถึง ฟังก์ชั่นการร้องข้อ, เพิ่มเติม และจัดการสิทธิการเข้าถึงของผู้ใช้งานบริษัทฯ ภายใต้ระบบ MAS

23. **"IP Address"** หมายถึง ป้ายตัวเลขที่กำหนดให้กับอุปกรณ์แต่ละเครื่องที่เชื่อมต่อกับเครือข่ายคอมพิวเตอร์ ที่ใช้โปรโตคอลอินเทอร์เน็ตเพื่อการติดต่อสื่อสาร IP Address ทำหน้าที่สองหน้าที่หลัก คือ เชื่อมต่อเครือข่าย และ บอกตำแหน่งที่อยู่
24. **"Job Order"** หมายถึง คำร้องขอความต้องการเพิ่มเติม เช่น ขอสิทธิ์การใช้งานระบบ MAS , ขอระบบงานใหม่ , ขอดูข้อมูลกล้องวงจรปิดย้อนหลัง เป็นต้น
25. **"บันทึกภาพ"** หมายถึง ภาพถ่าย ที่มีความสามารถในการบันทึกภาพจากสิ่งที่ส่องอยู่
26. **"PRD"** หมายถึง ระบบปฏิบัติการที่ใช้ในการดำเนินงานของระบบต่างๆ ภายในบริษัทฯ
27. **"QAS"** หมายถึง ระบบปฏิบัติการจำลองที่ใช้สำหรับทดสอบระบบ ก่อนนำขึ้นบนระบบ PRD
28. **"PR"** หมายถึง Purchase Requisition หรือ ใบขอซื้อ เป็นเอกสารภายในบริษัทฯ สำหรับการขออนุมัติการซื้อ หากได้รับการพิจารณาอนุมัติ ใบขอซื้อจะส่งให้ฝ่ายจัดซื้อเพื่อออกใบสั่งซื้อ เป็นลำดับถัดไป
29. **"Cost Center"** หมายถึง ข้อมูลใช้อ้างอิงถึงหน่วยงาน, ฝ่าย หรือแผนก เพื่อการควบคุมต้นทุนและงบประมาณค่าใช้จ่าย
30. **"อุปกรณ์สารสนเทศ"** หมายถึง เครื่องคอมพิวเตอร์ตั้งโต๊ะ (Computer PC), เครื่องคอมพิวเตอร์พกพา (Notebook), แท็บเล็ต (Tablet), เครื่องถ่ายเอกสาร, อุปกรณ์เก็บข้อมูลแบบพกพา เป็นต้น
31. **"โปรแกรมยูทิลิตี้"** หมายถึง โปรแกรมประเภทหนึ่งที่ทำงานบนระบบปฏิบัติการ คุณสมบัติการใช้งานนั้นค่อนข้างหลากหลาย ส่วนมากใช้เพื่อบำรุงรักษาและเพิ่มประสิทธิภาพการทำงานของคอมพิวเตอร์ ช่วยสนับสนุน เพิ่ม หรือขยายขีดความสามารถของโปรแกรมที่ใช้งานให้มีประสิทธิภาพมากขึ้น

คำนิยามผู้รับผิดชอบ

1. **"ผู้ใช้งาน"** หมายถึง ผู้ที่สามารถเข้าถึงระบบงาน เพื่อทำให้เกิดการดำเนินการ หรือเพื่อใช้งานให้เกิดประโยชน์ต่างๆ
2. **"ผู้ดูแลระบบ"** หมายถึง บุคคลซึ่งทำหน้าที่ออกแบบ, ติดตั้ง, ดูแลและจัดการระบบคอมพิวเตอร์ และระบบเครือข่าย ทั้ง ฮาร์ดแวร์, ระบบปฏิบัติการ และโปรแกรมประยุกต์ของบริษัทฯ
3. **"ผู้บังคับบัญชา"** หมายถึง ผู้มีอำนาจเหนือ และมีหน้าที่ควบคุมดูแลผู้ใต้บังคับบัญชาในการปฏิบัติงานในสายงานนั้นๆ
4. **"ผู้บริหารสายงานสารสนเทศ"** หมายถึง ผู้ซึ่งดำรงตำแหน่งในระดับผู้จัดการฝ่ายขึ้นไปของสายงานสารสนเทศ
5. **"หน่วยงานอื่นที่เกี่ยวข้อง"** หมายถึง สายงาน, ฝ่าย หรือแผนก ที่มีความเกี่ยวข้องและได้รับผลกระทบจากระบบงานใดระบบงานหนึ่งร่วมกัน

แนวทาง

1. จัดให้มีนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่มีนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมายหลักการมาตรฐานสากลของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
2. จัดให้ข้อมูลสารสนเทศ ระบบสารสนเทศ อุปกรณ์เทคโนโลยีสารสนเทศ สถานที่และสิ่งแวดล้อมที่เกี่ยวข้องกับสารสนเทศการพัฒนาและบำรุงรักษาระบบสารสนเทศ และสิ่งใดๆ ที่เกี่ยวข้องกับสารสนเทศ มีการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมและเพียงพอ และมีการควบคุมการเข้าถึงที่กำหนดอย่างชัดเจนตามหลักการของความต้องการในการใช้งานที่เหมาะสมและมั่นคงปลอดภัย
3. จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยมีแนวทางที่สอดคล้องกับการบริหารความเสี่ยงของบริษัทฯ
4. จัดให้มีระบบสำรองข้อมูล ระบบกู้คืนข้อมูล และระบบสำรองที่ใช้ทดแทนระบบสารสนเทศหลักในกรณีฉุกเฉิน โดยระบบสำรองต้องอยู่ในสภาพพร้อมใช้ และมีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน
5. จัดให้มีการตรวจสอบ และดำเนินการแก้ไข เมื่อมีเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยเกิดขึ้น พร้อมทั้งดำเนินการป้องกันไม่ให้เกิดซ้ำ และให้รายงานและทำบันทึกไว้อย่างชัดเจน
6. จัดให้ผู้ใช้งานได้รับความรู้เรื่องนโยบาย แนวทางปฏิบัติ มาตรฐาน และระเบียบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผู้ใช้งานจะต้องยึดถือและปฏิบัติตามอย่างเคร่งครัด

นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

<u>การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control)</u>

แนวทางปฏิบัติ

1. การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ
   1.1. ต้องกำหนดให้มีขั้นตอนสำหรับการลงทะเบียนต่างๆ เพื่อให้มีสิทธิ์และควบคุมสิทธิ์ในการเข้าถึงสารสนเทศและระบบสารสนเทศของบริษัทฯตามความจำเป็น รวมถึงขั้นตอนการยกเลิก สิทธิ์การใช้งาน เช่น เมื่อลาออกหรือเปลี่ยนแปลงตำแหน่ง เป็นต้น รวมถึงต้องมีกระบวนการ จัดการรหัสผ่านสำหรับผู้ใช้งาน เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานตามความ เหมาะสมหรือที่เกี่ยวข้องกับงานที่ได้รับมอบหมาย
   1.2. การเข้าถึงระบบสารสนเทศและสารสนเทศของบริษัทฯ จะกระทำได้เมื่อได้รับอนุมัติโดยหัวหน้าหน่วยงานและหัวหน้าส่วนงานเทคโนโลยีสารสนเทศ สามารถใช้ได้เฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น และต้องถูกจำกัดการเข้าถึง ให้เฉพาะผู้ที่ได้รับอนุญาต หรือผู้ที่มีความจำเป็นต้องใช้ข้อมูลนั้น และต้องได้รับความยินยอมจากเจ้าของข้อมูล
   1.3. การเข้าถึงระบบสารสนเทศใดๆ ต้องได้รับการพิสูจน์ตัวตนทุกครั้งเมื่อเข้าถึงระบบสารสนเทศและสารสนเทศของบริษัทฯ
   1.4. พนักงานต้องมีวิธีป้องกัน ไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์สารสนเทศที่ไม่มีพนักงาน ดูแล เช่น แจ้งหัวหน้าหน่วยงาน หรือเจ้าหน้าที่รักษาความปลอดภัยทุกครั้งที่พบเห็น รวมถึงมีนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึก ข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย หรือพบเห็นได้ง่าย
   1.5. มีกำหนดการยืนยันตัวตน ประกอบด้วย
      1.5.1. การแสดงตัวตน (Identification)
      1.5.2. การยืนยันตัวตน (Authentication)
      1.5.3. การกำหนดสิทธิ์ (Authorization)
      1.5.4. การบันทึกการใช้งาน (Accountability)
   1.6. มีกำหนดช่องทางการเข้าถึงระบบสารสนเทศ ประกอบด้วย
      1.6.1. ระบบเครือข่ายภายในองค์กร
      1.6.2. ระบบเครือข่ายภายนอกองค์กร
      1.6.3. เข้าถึงโดยผ่านระบบที่จัดไว้ให้ เช่น VPN
2. การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน การบริหารรหัสผ่าน
   2.1. กำหนด ชื่อผู้ใช้ (Username) ระบบสารสนเทศเฉพาะบุคคลไม่ซ้ำกัน
   2.2. สายงานสารสนเทศกับหน่วยงานต่างๆ ของบริษัทฯจะทบทวนสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งานอย่างน้อย ปีละ 1 ครั้ง หรือเมื่อจำเป็น

2.3. ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแลรักษาบัญชีผู้ใช้งาน และรหัสผ่านของตนให้มีความมั่นคงปลอดภัย และถือเป็นความลับ

2.4. กำหนดให้มีการเปลี่ยนแปลงรหัสผ่านทุก 90 วัน โดยสามารถปรับเปลี่ยนขยายได้เมื่อมีความจำเป็น หรือมีเหตุฉุกเฉิน

2.5. กำหนดให้รหัสผ่าน (Password) ต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยจะต้องมีการผสมกันระหว่าง ตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์พิเศษ

2.6. ในกรณีที่ลืมรหัสผ่าน หรือสงสัยว่ารหัสผ่าน (Password) ถูกผู้อื่นทราบ ให้รีบทำการเปลี่ยนแปลงรหัสผ่าน ทันที หรือแจ้งให้สายงานสารสนเทศทราบ เพื่อทำการเปลี่ยนรหัสผ่าน (Password) ทั้งหมดที่เกี่ยวข้อง

3. การควบคุมการเข้าใช้งานระบบจากภายนอก

3.1. กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่าง ๆ ทางเครือข่าย และกำหนดสิทธิ์ ผู้ใช้งานผ่านเครือข่ายโดยอนุญาตเฉพาะผู้ที่มีสิทธิ์เท่านั้น

3.2. ต้องจำกัดการเชื่อมต่อจากภายนอกเข้าสู่ระบบเครือข่ายภายใน เช่น การเข้าถึงเครือข่ายจากระยะไกลผ่านทางอินเตอร์เน็ต รวมถึงไม่ติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใดๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย โดยไม่ได้รับอนุญาต

4. การบริการจัดการการให้บริการของหน่วยงานภายนอก

4.1. ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการโดยหน่วยงานภายนอก เช่นมีการยอมรับ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯ และขอบเขต รายละเอียด ระดับการให้บริการ ต้องได้รับการตรวจสอบจากฝ่ายกฎหมายของบริษัทฯ รวมถึง สัญญาในการไม่เปิดเผยข้อมูลของบริษัทฯ เป็นต้น

4.2. หน่วยงานภายนอกหรือบุคคลภายนอกอื่นๆ ที่ได้รับอนุญาตในการเข้าถึง ระบบสารสนเทศ ของบริษัทฯต้องยอมรับและปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศของบริษัทฯ

4.3. กรณีที่บุคคลภายนอกนำอุปกรณ์ที่ใช้งานมาลงทะเบียนกับสายงานสารสนเทศ โดยจะมีการเก็บข้อมูลการขอใช้สิทธิ์ สำหรับบุคคลภายนอก ประกอบด้วย ชื่อ, นามสกุล , บัตรประจำตัวประชาชน/หนังสือเดินทางของชาวต่างชาติ และ Mac Address ของอุปกรณ์ที่จะใช้งานอินเตอร์เน็ต รวมไปถึงการเข้าใช้งานข้อมูลบนระบบเครือข่ายทางบริษัทฯ จะดำเนินการเก็บข้อมูลไว้เป็นเป็นระยะเวลาไม่ต่ำกว่า 90 วัน แต่ไม่เกิน 1 ปี เพื่อใช้สำหรับการตรวจสอบย้อนหลัง

<u>การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม</u>

แนวทางปฏิบัติ

1. การบริหารจัดการทางกายภาพ (Physical security management)
   1.1. กำหนดระดับความสำคัญของพื้นที่ปฏิบัติงานของสายงานสารสนเทศ
   1.2. มีระบบป้องกัน ให้ครอบคลุมพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน หรือบริเวณที่มีความสำคัญ
2. การควบคุมการเข้า-ออก (Physical entry Controls)
   2.1. สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติแต่ละส่วนของพื้นที่ภายในบริษัทฯ
   2.2. มีการควบคุมการเข้าถึงพื้นที่ ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่
   2.3. มีการพิสูจน์ยืนยันตัวตน เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มี ความสำคัญ
   2.4. มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ
3. การจัดวางและการป้องกันอุปกรณ์ (Equipment setting and protection)
   3.1. แยกประเภทความสำคัญของอุปกรณ์ ให้เก็บแต่ละส่วนพื้นที่ที่เหมาะสม มั่นคง
   3.2. มีการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศติดตั้งอยู่ เพื่อป้องกันความเสียหายต่ออุปกรณ์
4. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)
   4.1. มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของบริษัทฯ ที่เพียงพอต่อความต้องการใช้งาน เพื่อให้อุปกรณ์พร้อมใช้งานอยู่เสมอ โดยให้มีระบบสนับสนุนกระแสไฟฟ้า และระบบปรับอากาศ เป็นต้น
   4.2. มีการตรวจสอบหรือทดสอบระบบสนับสนุนตาม ข้อ 4.1 อย่างสม่ำเสมอ
5. การบำรุงรักษาอุปกรณ์ (Equipment maintenance)
   5.1. กำหนดให้มีการบำรุงรักษาอุปกรณ์อย่างน้อยปีละ 1 ครั้ง บันทึกกิจกรรม, ปัญหาข้อบกพร่องการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบ, ประเมิน และปรับปรุง
   5.2. ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดย ไม่ได้รับอนุญาต
   5.3. จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
6. หากนำอุปกรณ์สารสนเทศออกนอกพื้นที่บริษัทฯ จะต้องได้รับการอนุญาตจากผู้บังคับบัญชาของหน่วยงานต้นสังกัดก่อน พร้อมทั้งมีการบันทึกข้อมูล
7. มีการกำหนดมาตรการการใช้อุปกรณ์สารสนเทศนอกสถานที่ เพื่อปลอดภัยของสินทรัพย์เพื่อป้องกันความเสี่ยงจากการนำสินทรัพย์ของบริษัทฯ

8. มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในสินทรัพย์สำหรับจัดเก็บ ข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำสินทรัพย์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

นโยบายการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน

การบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน ต้องมีแผนการปรับปรุงและพัฒนา การดำเนินการให้มีประสิทธิภาพมากยิ่งขึ้น ดังนี้

1. จัดให้มีการวางแผนการล่วงหน้าในกรณีที่มีเหตุการณ์อันตรายเกิดขึ้น (Plan) จากจุดที่สำคัญของบริษัทฯ ที่กล่าวว่า ระบบสารสนเทศที่ส่งผลกระทบต่อธุรกิจ สายงานสารสนเทศต้องรักษาระบบให้สามารถให้บริการได้ตลอดเวลา พร้อมทั้งมีแผนรองรับในกรณีการเคลื่อนย้ายข้อมูลเพื่อนำไปใช้งานที่ DR Site
2. จัดให้มีการลงมือ และการควบคุมการดำเนินการตามแผนที่วางไว้ (DC) เครื่องแม่ข่ายสำรองเพื่อเตรียมพร้อมสำหรับการถ่ายโอนงานไปยัง DR Site เมื่อจำเป็น
3. จัดให้มีการตรวจสอบและทบทวน (Check) เมื่อมีการโอนย้ายข้อมูลระหว่างเครื่องแม่ข่ายเพื่อให้ทราบว่าระบบทำงานต่อเนื่อง ข้อมูลสมบูรณ์ หรือไม่สูญหาย
4. จัดให้มีการปรับปรุงแผนการอย่างต่อเนื่อง (Act) ตามความเปลี่ยนแปลงของระบบงาน หรือความต้องการที่เปลี่ยนแปลงไปของบริษัทฯ

<u>การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ (Communications and operations management)</u>

แนวทางปฏิบัติ

1. ขั้นตอนการปฏิบัติงานที่เป็นข้อมูลความรู้เพื่อการสื่อสาร
   1.1. มีการจัดทำคู่มือการปฏิบัติงานระบบเทคโนโลยีสารสนเทศ เพื่อให้มีความเข้าใจรายละเอียดการปฏิบัติงานในส่วนต่างๆ ของระบบเทคโนโลยีสารสนเทศ
   1.2. มีการแจกจ่ายและควบคุมดูแลให้มีการปฏิบัติงานตามแนวทางที่กำหนดในคู่มือการปฏิบัติงาน
   1.3. มีการทบทวนปรับปรุงคู่มือการปฏิบัติงานให้เหมาะสมอยู่เสมอ
2. ควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบเทคโนโลยีสารสนเทศ (Change management) ต้องมีการและกำหนดผู้รับผิดชอบ และผู้มีอำนาจในการควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบเทคโนโลยี สารสนเทศของบริษัทฯ
3. การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)
   3.1. มีการกำหนดแบ่งแยกหน้าที่ความรับผิดชอบในการปฏิบัติงานของแต่ละบุคคลไว้อย่างชัดเจนโดยมิให้มีการกำหนดหน้าที่ที่สำคัญไว้ที่บุคคลเพียงคนเดียว
   3.2. ให้ผู้บังคับบัญชามีการควบคุมดูแลอย่างใกล้ชิด สำหรับงานที่มีความเสี่ยงต่อการเกิดความเสียหาย
   3.3. ให้มีการจัดเก็บหลักฐานการปฏิบัติงานที่สามารถใช้ตรวจสอบได้ในภายหลัง
4. การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, test, and operational facilities)

4.1. ให้กำหนดมาตรการแยกเครื่องคอมพิวเตอร์ของระบบงาน สำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกันตามความจำเป็น เพื่อป้องกันผลกระทบจากการทำงาน

4.2. กำหนดมาตรการควบคุมการถ่ายโอนระบบงานจากเครื่องที่ใช้สำหรับการพัฒนา ไปสู่เครื่องที่ใช้สำหรับการให้บริการ

4.3. กำหนดให้มีการแยกบัญชีผู้ใช้งานออกจากกัน สำหรับระบบงานที่ใช้ในการพัฒนา ทดสอบ และใช้ระบบงานจริง

<u>การบริหารจัดการการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย</u>

แนวทางปฏิบัติ

1. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
   1.1. กำหนดให้ผู้ใช้งานเครื่องแม่ข่ายต้องมีสิทธิ์เข้าถึง แบ่งแยกออกจากผู้ใช้งานทั่วไป พร้อมทั้งมีระบบตรวจสอบสิทธิ์อย่างเคร่งครัด
   1.2. กำหนดให้มีชื่อผู้ใช้ และรหัสผ่าน ต้องปฏิบัติให้สอดคล้องกับการบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน การบริหารรหัสผ่าน
   1.3. กำหนดให้เครื่องคอมพิวเตอร์ที่เชื่อมต่อลงชื่อเข้าใช้เครื่องแม่ข่ายต้องมีระบบการล็อคหน้าจอเมื่อไม่มีการใช้งาน และเมื่อต้องการกลับเข้าใช้งานต้องลงชื่อเข้าใช้ใหม่
2. การควบคุมการติดตั้งโปรแกรมประยุกต์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่าย
   2.1. มีการควบคุมการเปลี่ยนแปลงต่อระบบงานของบริษัทฯ เพื่อป้องกันความเสียหายอาจเกิดขึ้นต่อระบบนั้นๆ
   2.2. ต้องมีการตรวจสอบและประเมินผลกระทบก่อนการติดตั้ง หรือปรับปรุงโปรแกรมประยุกต์ของระบบ
   2.3. ต้องมีการประเมินระบบความต้องการ และจุดประสงค์การดำเนินการอย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งหรือปรับปรุงบนเครื่องแม่ข่าย
   2.4. ต้องมีการประเมินและการทดสอบด้านความมั่นคงปลอดภัยของระบบอย่างครบถ้วน ก่อนดำเนินการ ติดตั้งหรือปรับปรุงบนเครื่องแม่ข่าย
3. ให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ และโปรแกรมประยุกต์
   3.1. ต้องมีการแจ้งให้ผู้ที่เกี่ยวข้องกับระบบ ได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้ดำเนินการทดสอบ และทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ และโปรแกรมประยุกต์
   3.2. ต้องมีการกำหนดแผนงานการดำเนินการเปลี่ยนแปลงระบบปฏิบัติการและโปรแกรมประยุกต์ของระบบ
4. การพัฒนาโปรแกรมประยุกต์โดยผู้รับจ้างภายนอก
   4.1. ต้องมีการกำหนดแผนงานการควบคุมโครงการพัฒนาโปรแกรมประยุกต์ โดยผู้รับจ้างให้บริการจากภายนอก

4.2. มีการกำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพ และความถูกต้องของโปรแกรมประยุกต์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

5. การเฝ้าดูและตรวจสอบ

5.1. ต้องดำเนินการเก็บ Log ของเหตุการณ์ที่เกิดขึ้นกับระบบต้องเก็บไว้เป็นเวลา 90 วัน พร้อมทั้งมีความปลอดภัยและพร้อมใช้งาน

5.2. ต้องมีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง

<u>การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer)</u>

แนวทางปฏิบัติ

1. การปฏิบัติทั่วไป

1.1. อุปกรณ์สารสนเทศที่เป็นทรัพยสินของบริษัทฯ ไม่อนุญาตให้ใช้เพื่อประโยชน์ส่วนบุคคล

1.2. โปรแกรมที่ได้ติดตั้งลงบนเครื่องคอมพิวเตอร์ของบริษัทฯ ต้องเป็นโปรแกรมที่บริษัทฯได้ซื้อลิขสิทธิมา อย่างถูกต้องตามกฎหมาย

1.3. ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ ของบริษัทฯ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

1.4. ไม่อนุญาตให้ ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม โปรแกรมยูทิลิตี้ ในเครื่อง คอมพิวเตอร์ส่วนบุคคลของบริษัทฯ เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ

1.5. ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

1.6. ปิดเครื่องคอมพิวเตอร์ส่วนบุคคล ที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น

1.7. ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของบริษัทฯ ยกเว้นจะ ได้รับการพิจารณาอนุมัติจากผู้จัดการสายงานสารสนเทศ ก่อนการใช้งาน

1.8. การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคลจะต้องกำหนดโดยผู้ดูแลระบบเท่านั้น โดยผู้ใช้งานห้ามทำการเปลี่ยนแปลง

1.9. ห้ามมิให้ผู้ใช้งานทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์จากจุดเชื่อมต่อเครือข่ายเดิมไปยังจุดเชื่อมต่อเครือข่ายใหม่ภายใน บริษัทฯ

1.10. ห้ามมิให้ผู้ใช้งานทำการนำเครื่องคอมพิวเตอร์ออกไป ซ่อมที่ศูนย์บริการภายนอก หากพบปัญหาในการใช้งานให้ดำเนินการตามข้อ “การซ่อมแซมแก้ไขอุปกรณ์สารสนเทศเมื่อชำรุด”

1.11. ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัทฯทุกเครื่อง หากพบปัญหาในการใช้งานให้ดำเนินการตามข้อ "การซ่อมแซมแก้ไขอุปกรณ์สารสนเทศเมื่อชำรุด"

1.12. เครื่องคอมพิวเตอร์ทุกเครื่องต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัสด้วยโปรแกรมป้องกันไวรัสของบริษัทฯเท่านั้น

1.13. ผู้ใช้งานไม่ควรสร้าง Short-cut หรือปุ่มกดง่าย บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของบริษัทฯ

1.14. ผู้ใช้งานมีหน้าที่ และความรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์โดยต้องปฏิบัติตามนี้

1.14.1. ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

1.14.2. ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

1.15. ห้ามผู้ใช้งานทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์ ส่วนบุคคลของบริษัทฯ ทุกเครื่อง และต้องดูแลมิให้เครื่องที่ถือครอบครองถูกแก้ไขการตั้งค่าเวลา ในกรณีที่ค่าเวลาของเครื่องคอมพิวเตอร์ส่วนบุคคลถูกแก้ไข เจ้าของเครื่องจะปฏิเสธความรับผิดชอบไม่ได้ และเมื่อรู้ว่าเครื่องมีการแก้ไข การตั้งค่าเวลาต้องแจ้งให้สายงานสารสนเทศทราบทันที

1.16. ต้องทำการล้างข้อมูลในเครื่องคอมพิวเตอร์ทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์ให้กับเจ้าของเครื่อง รายใหม่ พร้อมทั้งต้องทำการปลด Password สำหรับการเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และ ต้องทำการแจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้งานเครื่องคอมพิวเตอร์ทุกครั้ง

2. ความปลอดภัยทางด้านกายภาพ

2.1. ผู้ใช้งาน มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย โดยการล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่อง ทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

2.2. ผู้ใช้งาน ไม่ควรเก็บหรือใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ในสถานที่ที่มีความร้อน ความชื้น ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

2.3. ไม่ควรนำเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่พกพาในกระเป๋าเดินทาง ที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจเกิดจากการเคลื่อนย้ายไม่ถูกวิธีได้

2.4. ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์ และสื่อสารเคลื่อนที่ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

2.5. หลีกเลี่ยงการใช้ของแข็งกดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่อง คอมพิวเตอร์และสื่อสารเคลื่อนที่แตกเสียหายได้

2.6. ไม่วางของทับบนหน้าจอและแป้นพิมพ์

2.7. การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ด แบบหมุนวน เพราะจะทำให้หน้าที่มีรอยขีดข่วนได้

2.8. การเคลื่อนย้ายเครื่องคอมพิวเตอร์ ขณะที่เครื่องเปิดอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการ ดึงหน้าจอภาพขึ้น

2.9. ไม่เคลื่อนย้ายเครื่องในขณะที่ฮาร์ดดิสก์กำลังทำงาน

2.10. ไม่ใช้หรือวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ใกล้สิ่งที่เป็นของเหลว

2.11. ไม่ใช้หรือวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

2.12. ไม่ควรวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้

2.13. ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน

3. การเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และ รหัสผ่าน

3.1. ผู้ใช้งาน ต้องกำหนดรหัสผ่านให้มีคุณภาพดีตามที่ระบุไว้ในเอกสาร "การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน การบริหารรหัสผ่าน"

3.2. ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

3.3. ผู้ใช้งาน ต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ของตน ในการเข้าใช้ เครื่องคอมพิวเตอร์ร่วมกัน

<u>การจัดการอุปกรณ์พิสูจน์อัตลักษณ์</u>

แนวทางปฏิบัติ

1. กำหนดสิทธิ์ระดับเจ้าหน้าที่ในการเข้าถึงข้อมูลบนอุปกรณ์ พิสูจน์อัตลักษณ์เฉพาะบุคคลที่รับอนุญาตเท่านั้น
2. ห้ามมิให้เปิดเผยข้อมูลภายในอุปกรณ์พิสูจน์อัตลักษณ์ของบริษัทฯ ที่ไม่เข้าหลักเกณฑ์การเปิดเผย ประกาศอย่างเป็นทางการ
3. ห้ามมิให้เคลื่อนย้ายอุปกรณ์พิสูจน์อัตลักษณ์โดยไม่ได้รับความเห็นชอบจากผู้ดูแล
4. กำหนดให้มีผู้มีหน้าที่รับผิดชอบต่อการดูแลรักษา และตั้งค่าอุปกรณ์พิสูจน์อัตลักษณ์

<u>การใช้งานอินเทอร์เน็ต (Use of the Internet)</u>

แนวทางปฏิบัติ

1. หากต้องการใช้งานระบบอินเตอร์เน็ต ให้ดำเนินการตามที่ระบุไว้ใน การขอใช้สิทธิ์ในระบบเครือข่ายของบริษัทฯ "การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ"
   1.1. ต้องมีกำหนดเส้นทางการเชื่อมต่อระบบ เข้าใช้งานอินเทอร์เน็ตบนระบบรักษาความปลอดภัยทางคอมพิวเตอร์ เพื่อให้เกิดความปลอดภัยในการใช้งานอินเตอร์เน็ต
2. เครือข่ายอินเทอร์เน็ตของบริษัทฯ ต้องไม่ถูกใช้งานเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าเว็บไซต์ที่ไม่เหมาะสม

3. มีการกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูล ตามหน้าที่ความรับผิดชอบความปลอดภัยทางข้อมูลของบริษัทฯ โดยผ่านความเห็นชอบจากผู้มีสิทธอนุมัติของหน่วยงานต้นสังกัด
4. ห้ามมิให้เปิดเผยข้อมูลสำคัญเกี่ยวกับงานของบริษัทฯ ที่ไม่เข้าหลักเกณฑ์การเปิดเผยประกาศอย่างเป็นทางการ ผ่านทางอินเทอร์เน็ต
5. มีมาตราการการตรวจสอบความถูกต้อง และความน่าเชื่อถือของข้อมูลที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
6. ข้อมูลการเชื่อมต่ออินเตอร์เน็ต จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูล จราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

<u>การใช้งานจดหมายอิเล็กทรอนิกส์ และพื้นที่จัดเก็บข้อมูลออไลน์ (Use of Electronic Mail and Storage Online)</u>

แนวทางปฏิบัติ

1. หากต้องการใช้งานระบบจดหมายอิเล็กทรอนิกส์ ให้ดำเนินการตามที่ระบุไว้ใน "การขอใช้สิทธิ์ในระบบเครือข่ายของบริษัทฯ" "การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ"
2. ผู้ใช้งานรายใหม่จะต้องทำการเปลี่ยนรหัสผ่าน (Password) โดยทันที เมื่อได้รับรหัสผ่าน (Default Password) ในการผ่านเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรก โดยต้องกำหนดรหัสผ่านให้มีคุณภาพดี ตามที่ระบุไว้ใน "การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน"
3. ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์ หรือพื้นที่จัดเก็บข้อมูลออนไลน์ของบริษัทฯ เท่านั้น ในการติดต่อหรือรับ-ส่งข้อมูลหรือแชร์ข้อมูลกับหน่วยงานภายนอก ทั้งราชการ และเอกชน
4. การรับ-ส่งข้อมูลของบริษัทฯ ที่เป็นความลับ ห้ามรับ-ส่งผ่านทางระบบจดหมายอิเล็กทรอนิกส์ หรือการแชร์ข้อมูล
5. ผู้ใช้งานควรตรวจสอบชื่อบัญชีอีเมลของผู้รับ และผู้ส่ง ให้ละเอียดถี่ถ้วนก่อนทำการส่งอีเมลหรือแชร์ข้อมูลทุกครั้ง เพื่อป้องกันการรับ หรือให้ข้อมูลที่สำคัญของทางบริษัทฯ
6. ห้ามผู้ใช้งานตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบ จดหมายอิเล็กทรอนิกส์
7. ผู้ใช้งานควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด โดยเปลี่ยนรหัสผ่านทุก 3-6 เดือน
8. ผู้ใช้งาน ต้องไม่ใช้จดหมายอิเล็กทรอนิกส์ หรือพื้นที่จัดเก็บข้อมูลออนไลน์ที่ส่งผลให้เกิดความเสียหายต่อบริษัทฯ หรือละเมิดสิทธิสร้าง ความรำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม ส่งต่อข้อความที่กล่าวร้าย ทำให้เสื่อมเสีย ข้อความที่หยาบคาย ลามก ข่มขู่ ก่อกวน หรือสร้างความเสียหายให้กับผู้อื่น รวมถึงไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่าย ของบริษัทฯ
9. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ให้ทำการออกจากระบบ (Log out) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์พื้นที่จัดเก็บข้อมูลออนไลน์
10. ผู้ใช้งาน ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการ ตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดฟล์ที่เป็น Executable file
11. ผู้ใช้งาน ห้ามเปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ รวมถึงข้อมูลที่ถูกแชร์มาจากผู้ส่งที่ไม่มั่นใจด้านความปลอดภัยของข้อมูล
12. ผู้ใช้งาน ควรตรวจสอบพื้นที่จัดเก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูล และจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด
13. ผู้ใช้งาน ควรลบจดหมายอิเล็กทรอนิกส์ หรือข้อมูลในพื้นที่ที่จัดเก็บออนไลน์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

14. ผู้ใช้งานต้องไม่ส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็น ข้อมูลคอมพิวเตอร์ประเภทดังต่อไปนี้
    14.1. ข้อมูลคอมพิวเตอร์อันเป็นเท็จ
    14.2. ข้อมูลคอมพิวเตอร์อันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือ ก่อให้เกิดความตื่นตระหนกแก่ประชาชน
    14.3. ข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิด เกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา
    14.4. ข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกอนาจาร
15. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์หรือพื้นที่จัดเก็บข้อมูลออนไลน์ ของผู้อื่นเพื่ออ่าน รับส่ง ข้อความยกเว้น แต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งาน และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน
16. ผู้ใช้งาน ต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ หรือแชร์ข้อมูลที่ไม่เหมาะสม ข้อมูลอันอาจทำให้ เสียชื่อเสียงของบริษัทฯ ทำให้เกิดความแตกแยกระหว่างบริษัทฯ ผ่านทางจดหมายอิเล็กทรอนิกส์
17. ข้อมูลจดหมายอิเล็กทรอนิกส์ หรือข้อมูลในพื้นที่จัดเก็บที่ถูกลบ จะถูกจัดเก็บในถังขยะ (Trash) 30 วัน
18. กรณีที่ข้อมูลถูกลบออกจากถังขยะ (Trash) ทั้งลบด้วยตัวผู้ใช้งานเอง หรือเกิน 30 วัน ข้อมูลนั้นจะถูกลบถาวร โดยไม่สามารถกู้คืนได้

นโยบายการบริหารจัดการด้านข้อมูลของระบบสารสนเทศ

แนวทางปฏิบัติ

1. การสร้างและการรวบรวมข้อมูล
   1.1. ข้อมูลบนระบบ
      1.1.1. การสร้างและการรวบรวมข้อมูล ต้องมีการรักษาความมั่นคงปลอดภัย และปฏิบัติตามแนวปฏิบัติที่ชัดเจนในการการปกป้องข้อมูล และมีความมั่นคงปลอดภัย พร้อมทั้งมีการกำหนดเป็นแนวปฏิบัติเพื่อให้เกิดแบบแผน
      1.1.2. การสร้างและการรวบรวมข้อมูลที่มีแหล่งกำหนดข้อมูลจากภายนอกองค์กร ต้องมีแนวทางการขอความยินยอมจากแหละข้อมูลให้มีความชัดเจน
      1.1.3. ต้องมีการจัดให้มีคำอธิบายชุดข้อมูล บัญชีข้อมูลที่มีความถูกต้องครบถ้วนและเป็นปัจจุบัน พร้อมทั้งมีการกำหนดเป็นแนวปฏิบัติ หรือมีมาตราฐานรองรับการจัดทำ
      1.1.4. ต้องมีการจัดชั้นความลับของข้อมูล และมีการกำหนดแนวทางปฏิบัติให้เป็นมาตรฐานการจัดชั้นความลับของข้อมูล
2. การจัดเก็บ และการทำลายข้อมูล
   2.1. การจัดเก็บ และการทำลายข้อมูล ต้องดำเนินการโดยผู้ที่มีสิทธิ์เกียวกับข้อมูลนั้นๆ เท่านั้น
   2.2. การจัดเก็บ และการทำลายข้อมูล ต้องมีการรักษาความมั่นคงปลอดภัย และมีการกำหนดแนวทางการปฏิบัติให้เกิดเป็นมาตราฐานการดำเนินการที่ชัดเจน
   2.3. การจัดเก็บข้อมูล ต้องจัดเก็บลงในสื่อบันทึกข้อมูล ตามมาตรฐานสถาปัตยกรรมข้อมูล
   2.4. การจัดเก็บข้อมูล ต้องมีการจัดประเภทข้อมูลให้เหมาะสมกับ การใช้งาน กฎหมาย และช่วงเวลาการจัดเก็บ โดยแบ่งช่วงเวลการจัดเก็บออกเป็น 3 ปี, 5 ปี และ 10 ปี
   2.5. ข้อมูลที่พ้นระยะเวลาการจัดเก็บที่กำหนดไว้ในแต่ระบบ ต้องไม่สามารถอ้างอิง หรือนำข้อมูลมาใช้ในรูปแบบเดิมได้อีก
   2.6. การสำรองข้อมูล ต้องดำเนินการให้ถูกต้อง ครบถ้วน มั่นคงปลอดภัย และเป็นปัจจุบัน โดยต้องมีมาตรฐานการสำรองข้อมูล ที่ทำให้มั่นใจได้ว่าข้อมูลจะไม่สูญหาย
   2.7. การทำลายข้อมูล ต้องเป็นการดำเนินการกับข้อมูลที่ไม่ต้องการนำกลับมาใช้งานอีกต่อไป โดยให้เป็นไปตามมาตราฐาน และบทบัญญัติต่างๆ ที่เกียวข้อง
   2.8. กำหนดให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลไม่สามารถระบุตัวตนได้ เพื่อการใช้ประโยชน์ด้านอื่น เช่น การวิเคราะห์ทางสถิติ การปรับปรุงประสิทธิภาพการทำงาน หรือประโยชน์สาธารณะที่สำคัญ
3. การเข้ารหัสข้อมูล
   3.1. ประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และการเข้าถึงข้อมูลแต่ละส่วนให้เหมาะสม สำหรับข้อมูลที่จำเป็นต้องป้องกัน

3.2. กำหนดหลักการสำหรับการป้องกันข้อมูลโดยใช้การเข้ารหัสข้อมูล

3.3. จัดเก็บบัญชีผู้ใช้งานและรหัสผ่าน ของระบบสารสนเทศลงในฐานข้อมูล ต้องเข้ารหัสในส่วนของรหัสผ่านก่อนบันทึกลงในฐานข้อมูลทุกครั้ง

3.4. เชื่อมต่อผ่านโพรโทคอล SSL สำหรับระบบสารสนเทศแบบเว็บแอพพลิเคชั่น (Web Application) เพื่อเป็นการเข้ารหัสข้อมูลที่ส่งระหว่างเว็บบราวเซอร์ (Web Browser) และเว็บเซิร์ฟเวอร์ (Web Server)

4. กำหนดวิธีการในการบริหารจัดการและการใช้งานกุญแจรหัส (Key)
สำหรับการเข้ารหัสข้อมูล ดังนี้วิธีการป้องกันกุญแจรหัสที่ใช้สำหรับการเข้ารหัสข้อมูล

4.1. วิธีการกู้คืนข้อมูลที่ถูกเข้ารหัสไว้ในกรณีที่กุญแจรหัสเกิดการสูญหาย หรือถูกทำให้เสียหาย

4.2. กำหนดบทบาทและผู้มีหน้าที่รับผิดชอบที่เกี่ยวข้องกับการเข้ารหัสข้อมูล ประกอบด้วย ผู้ทำหน้าที่ควบคุมและดูแลกุญแจรหัส, ผู้สร้างกุญแจรหัส, ผู้ทำหน้าที่ทำลาย, ผู้ใช้งาน และผู้ทำหน้าที่จัดการกรณีกุญแจรหัสเกิดการสูญหาย

นโยบายการสำรองและกู้คืนข้อมูล และการจัดการภัยพิบัติที่มีผลต่อระบบสารสนเทศ

แนวทางปฏิบัติ

1. กำหนดให้ใช้แนวทางปฏิบัติในการจัดทำนโยบายการสำรอง และกู้คืนข้อมูล ดังต่อไปนี้
   - 1.1. มีการจัดทำบัญชีระบบเครือข่าย และระบบสารสนเทศ พร้อมทั้งกำหนดระบบสารสนเทศที่ต้องทำระบบสำรอง และกำหนดแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง
   - 1.2. กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่ มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น มีวิธีการเบื้องต้น ดังนี้
     - 1.2.1. มีการกำหนดประเภทของข้อมูลที่ต้องการสำรอง และความถี่ในการสำรอง ที่เหมาะสม
       - 1.2.1.1. Web และ Service servers : สำรองข้อมูลเผยแพร่บนเว็บไซต์ 1 ครั้งต่อเดือน
       - 1.2.1.2. Database servers : สำรองข้อมูลในฐานข้อมูลของระบบที่สำคัญ 1 ครั้งต่อสัปดาห์
       - 1.2.1.3. Firewall server : สำรองข้อมูล Rule ของ Firewall 1 ครั้งต่อเดือน
       - 1.2.1.4. ระบบอื่นๆ : สำรองข้อมูลบนเครื่องเซิร์ฟเวอร์อื่นๆ เช่น ระบบงานต่างๆ 1 ครั้งต่อเดือน
     - 1.2.2. กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่ทำการสำรอง
     - 1.2.3. กำหนดให้มีระบบการเก็บข้อมูล ที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ขนาดข้อมูลที่ สำรอง สำเร็จไม่สำเร็จ เป็นต้น
     - 1.2.4. จัดเก็บข้อมูลที่สำรองคลละสถานที่กับข้อมูลต้นฉบับ ต้องมีความมั่งคงปลอดภัย และพร้อมนำข้อมูลมาทดสอบใช้งานได้ทุกเวลา
     - 1.2.5. มีการจัดทำแผนและขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองระบบต่างๆ
     - 1.2.6. ตรวจสอบ และทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ
   - 1.3. กำหนดผู้รับผิดชอบในการสำรองข้อมูล
   - 1.4. กำหนดประเภทของระบบงาน ที่ความจำเป็นต้องสำรองข้อมูล อย่างน้อย ต้องประกอบด้วย ข้อมูลในระบบ ข้อมูลของระบบงาน และข้อมูลสำหรับตัวระบบ
   - 1.5. กำหนดความถี่ในการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของระบบงาน และข้อมูล
   - 1.6. กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง
   - 1.7. จัดเก็บข้อมูลที่สำรองคลละสถานที่กับข้อมูลต้นฉบับ ต้องมีความมั่งคงปลอดภัย

1.8. ต้องมีการทดสอบกู้คืนข้อมูลที่สำรอง อย่างน้อยปีละ 1 ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานสามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

1.9. จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน ให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนด

1.10. กำหนดให้มีระบบการเก็บข้อมูลที่เกี่ยวข้องการสำรองข้อมูล และการกู้ข้อมูลของทุกระบบและมีการตรวจสอบความถูกต้องสม่ำเสมอ

2. กำหนดแผนการจัดการภัยพิบัติที่มีผลต่อระบบสารสนเทศ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความ พร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

2.1. จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการได้ โดยมีรายละเอียดอย่างน้อย ดังนี้

2.1.1. กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

2.1.2. มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลด ความเสี่ยงเหล่านั้น ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว น้ำท่วม การชุมนุม ประท้วง โรคระบาด การโจมดีทางไซเบอร์ ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

2.1.3. การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

2.1.4. การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรอง

2.1.5. กำหนดช่องทางในการติดต่อกับ บุคคลภายใน หน่วยงานที่เกียวข้อง และผู้ให้บริการภายนอก เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

2.1.6. การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

2.2. กำหนดให้มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่าง เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

3. กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และจัดทำแผนการจัดการภัยพิบัติที่มีผลต่อระบบสารสนเทศ

4. กำหนดการทำ Disaster Recovery Site ตามความจำเป็น และความสำคัญของระบบงาน มีรูปแบบเบื้องต้น ดังนี้

4.1. Hot Site หมายถึง สามารถทำงานได้ทันทีโดยที่อุปกรณ์ในสถานที่หลักและสถานที่สำรอง ทำงานควบคู่กันไป เมื่อเกิดเหตุอุบัติภัยขึ้นสามารถที่จะดำเนินงานตามปกติได้ทันที

4.2. Warm Site หมายถึง สามารถทำงานได้ต่อเมื่อ เมื่อเกิดเหตุอุบัติภัยขึ้นจะต้องทำการติดตั้งอุปกรณ์ต่างๆ ก่อนจึงจะสามารถดำเนินงานได้ตามปกติ

4.3. Cold Site หมายถึง เมื่อเกิดเหตุอุบัติภัยขึ้น จึงทำการซื้อหรือเช่าอุปกรณ์ต่างๆใหม่ เช่น เครื่องเซิร์ฟเวอร์ และจะต้องทำการติดตั้งระบบสารสนเทศใหม่ทั้งหมด ใช้เวลานานพอสมควรในการขึ้นระบบสารสนเทศ

4.4. Standby site หมายถึง จัดการสรรหาสถานที่ ยังมิได้ดำเนินการใดๆ ทั้งสิ้น

4.5. Nothing หมายถึง ไม่มีการดำเนินการทำระบบสำรองใดๆ

5. พนักงานที่เกี่ยวข้องกับแผนการจัดการภัยพิบัติที่มีผลต่อระบบสารสนเทศ ต้องเข้ารับการอบรม หรือสร้างความตระหนักเพื่อให้รู้หรือทราบ วิธีปฏิบัติในกรณีที่เกิดเหตุฉุกเฉินในกรณีต่างๆ

6. กำหนดให้มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนการจัดการภัยพิบัติที่มีผลต่อระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

7. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนการจัดการภัยพิบัติที่มีผลต่อระบบสารสนเทศ ที่เพียงพอต่อสภาพ ความเสี่ยงที่ยอมรับได้ของแต่ละส่วนงาน อย่างน้อยปีละ 1 ครั้ง

นโยบายความมั่นคงปลอดภัยของ Firewall

แนวทางปฏิบัติ

1. สายงานสารสนเทศ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ (Firewall) ทั้งหมด
2. การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่าย และอินเตอร์เน็ตต้องเป็นค่า การปฏิเสธเสมอ
3. ต้องมีการยืนยันตัวตนก่อนการใช้งานระบบเครือข่าย และระบบอินเตอร์เน็ต
4. การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น
5. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูล จราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน
6. กำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อ พื้นฐานของโปรแกรมประยุกค์ ที่สายงานสารสนเทศอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อ นอกเหนือที่กำหนด จะต้องได้พิจารณาการใช้งานพอร์ตการเชื่อมต่อที่จำเป็นเท่านั้น
7. กำหนดให้มีมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์สม่ำเสมอ
8. เครื่องแม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป
9. ผู้ดูแลระบบมีสิทธิที่จะระงับหรือบล็อกการใช้งาน ของอุปกรณ์ที่มีพฤติกรรมการใช้งานที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข
10. มีการเก็บข้อมูลการเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน
11. ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานระบบสารสนเทศ

นโยบายการตรวจสอบและประเมินความเสี่ยง

แนวทางปฏิบัติ

1. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ที่อาจเกิดขึ้นกับระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศโดยมีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้
    1.1. จัดลำดับความสำคัญของความเสี่ยง
    1.2. ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง
    1.3. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง
    1.4. สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้
    1.5. มีมาตรการในการตรวจประเมินระบบสารสนเทศอย่างน้อย ดังนี้
        1.5.1. กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบโดยการให้สิทธิ์แบบอ่านได้อย่างเดียว
        1.5.2. กรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาข้อมูลนั้นๆ เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบทันทีมีการตรวจสอบเสร็จหรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี
        1.5.3. กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็น ต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
        1.5.4. กำหนดให้มีการเฝ้าระวัง การเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ
        1.5.5. ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบ ให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต
2. ความเสี่ยงที่อาจเป็นอันตรายต่อระบบสารสนเทศจากการติดตามตรวจสอบความเสี่ยงต่างๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่างๆ ดังนี้
    2.1. เกิดจากบุคคล (Human Error) เกิดจากขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์และระบบสารสนเทศเบื้องต้น เพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศมีแผนการรับมือเบื้องต้น ต้องมีการจัดหลักสูตรอบรมผู้เกียวข้องให้มีความรู้ความเข้าใจระบบสารสนเทศเบื้องต้นเพื่อลดความเสี่ยงด้าน Human error
    2.2. เกิดจาก Cybersecurity ที่สร้างความเสียหาย ให้แก่ระบบคอมพิวเตอร์ หรือระบบเครือข่าย และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่สามารถใช้งานได้

2.2.1. มีการติดตั้งอุปกรณ์ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุก

2.2.2. กำหนดให้มีการตรวจสอบไวรัส และพฤกติกรรมที่เข้ามาในระบบเครือข่ายต้องมีการตรวจสอบได้ว่าเข้ามาทำความเสียหายกับระบบสารสนเทศ

2.2.3. เมื่อเกิดความเสียหายจากการโจมตีเจ้าหน้าที่ หรือพนักงานที่ได้รับการแต่งตั้งต้องมีการติดต่อสานงานทั้งภายในและภายนอกองค์กรที่จำเป็น เพื่อสร้างความเข้าใจ, รับมือแก้ไข และปรับปรุงระบบให้มีความมั่นคงและปลอดภัยมากยิ่งขึ้น

2.2.4. กรณีความเสียหายมีผลกระทบต่อบุคคล ที่สามารถต้องมีมาตราการเยี่ยวยาให้เหมาะสมผลกระทบที่บุคคลที่สามได้รับ

2.3. เกิดจากไฟไหม้หรือระบบไฟฟ้าจัดเป็นภัยร้ายแรง ที่ทำความเสียหายให้แก่ระบบสารสนเทศได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

2.3.1. กำหนดให้มีระบบสนับสนุนระบบไฟฟ้า และระบบจุดการอุณหภูมิที่เหมาะสม กับการทำงานของอุปกรณ์ พร้อมทั้งมีการตรวจสอบระบบอย่างสม่ำเสมอ

2.3.2. ต้องมีระบบตรวจสอบสถานะต่างๆ ภายในห้องเซิฟเวอร์ เช่น ตรวจสอบอุณหภูมิ, ก๊าซ และควัน เป็นต้น เพื่อให้ทรานถึงสถานการณ์ต่างๆ ที่เกิดขึ้นภายในห้องเซิฟเวอร์

2.4. เกิดจากภัยธรรมชาติ และโรคระบาด ด้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

2.4.1. กำหนดให้มีการประเมินสถานการณ์ตามข้อมูล ข่าวสาร ซึ่งสถานการณ์แวดล้อม หรือเหตุการณ์อาจจะส่งผลกระทบต่อการใช้งานระบบสารสนเทศ พร้อมทั้งมีการวางแผนรับมือ เพื่อให้เกิดแนวทางปฏิบัติเมื่อสถานการณ์แวดล้อมหรือเหตการณ์ส่งผลกระทบ

2.4.2. กำหนดให้มีการดูแลข้อมูลระบบงาน และระบบสำรองข้อมูลต้องมีลำดับความสำคัญสำหรับการจัดเก็บ และมีการแยกเก็บข้อมูลระหว่างกันให้ปลอดภัยและมันคง

2.4.3. กำหนดให้มีการสนับสนุนการเข้าถึง และการใช้ข้อมูลระบบสารสนเทศเมือมีผลกระทบสถานการณ์แวดล้อมหรือเหตการณ์ที่เกิดขึ้นสังคม

2.4.4. กำหนดให้มีการตรวจสอบ ประเมินระบบ และแผนรับมืออย่างสม่ำเสมอ เพื่อสร้างความรู้ความเข้าใจ และปรับปรุงแผนให้เหมาะสมกับสถานการณ์ที่เปลี่ยนไป

แนวทางปฏิบัติการดำเนินการงานระบบสารสนเทศ (MIS Services Process)

1. การขอใช้สิทธิ์ในระบบเครือข่ายของบริษัทฯ แบ่งออกได้เป็น 3 ประเภท
   1.1. การขอใช้สิทธิ์ในระบบเครือข่ายสำหรับพนักงานใหม่ มีวิธีดำเนินการดังนี้
      1.1.1. ผู้ใช้งาน หรือเจ้าหน้าที่สายงานทรัพยากรบุคคล เข้าไปดำเนินการสร้างรายการขอใช้สิทธิ์ในระบบ MAS/AD Online ในส่วนของสร้างรายการขอใช้สิทธิ์ และเลือกสิทธิ์ทั่วไป โดยต้องระบุข้อมูลต่างๆ ของผู้ขอใช้สิทธิ์ ได้แก่ รหัสพนักงาน, ชื่อนามสกุล, ฝ่าย, แผนก และตำแหน่ง และจะต้องดำเนินการก่อนพนักงานใหม่จะเริ่มงาน 3 วัน
      1.1.2. ผู้บังคับบัญชาที่มีสิทธิ์อนุมัติของพนักงานใหม่ เข้าไปพิจารณารายการขอใช้สิทธิ์บนระบบ MAS/AD Online ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือไม่อนุมัติ หากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที และกรณีข้อมูลไม่ครบถ้วนสามารถส่งรายการกลับไปยังผู้ใช้งาน
      1.1.3. ผู้ดูแลระบบเข้าไปพิจารณารายการขอใช้สิทธิ์บนระบบ MAS/AD Online ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือไม่อนุมัติ หากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที และกรณีข้อมูลไม่ครบถ้วนสามารถส่งรายการกลับไปยังผู้ใช้งาน
      1.1.4. ผู้บริหารสายงานสารสนเทศ ลำดับที่ 1 เข้าไปพิจารณารายการขอใช้สิทธิ์บนระบบ MAS/AD Online ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือไม่อนุมัติ หากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที และกรณีข้อมูลไม่ครบถ้วนสามารถส่งรายการกลับไปยังผู้ใช้งาน
      1.1.5. ผู้บริหารสายงานสารสนเทศ ลำดับที่ 2 เข้าไปพิจารณารายการขอใช้สิทธิ์บนระบบ MAS/AD Online ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือไม่อนุมัติ หากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที และกรณีข้อมูลไม่ครบถ้วนสามารถส่งรายการกลับไปยังผู้ใช้งาน
      1.1.6. ผู้ดูแลระบบดำเนินการกำหนดสิทธิ์ และเพิ่มสิทธิ์ในระบบเครือข่าย โดยกำหนดสิทธิ์ตามรายการที่ถูกอนุมัติ
   1.2. การขอใช้สิทธิ์ในระบบเครือข่ายเพิ่มเติมสำหรับพนักงาน มีวิธีดำเนินการดังนี้
      1.2.1. ผู้ใช้งาน เข้าไปดำเนินการสร้างรายการขอใช้สิทธิ์เพิ่มเติมในระบบ MAS/AD Online ในส่วนของขอใช้สิทธิ์เพิ่มเติม โดยต้องระบุข้อมูลต่างๆ ของผู้ขอใช้สิทธิ์เพิ่มเติม ได้แก่ รหัสพนักงาน, ชื่อนามสกุล, ฝ่าย, แผนก และตำแหน่ง
      1.2.2. ผู้บังคับบัญชาที่มีสิทธิ์อนุมัติของผู้ใช้งานที่ดำเนินรายการ เข้าไปพิจารณารายการขอใช้สิทธิ์บนระบบ MAS/AD Online ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือไม่อนุมัติ หากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที และกรณีข้อมูลไม่ครบถ้วนสามารถส่งรายการกลับไปยังผู้ใช้งาน

1.2.3. ผู้ดูแลระบบเข้าไปพิจารณารายการขอใช้สิทธิ์บนระบบ MAS/AD Online ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือไม่อนุมัติ หากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที และกรณีข้อมูลไม่ครบถ้วนสามารถส่งรายการกลับไปยังผู้ใช้งาน

1.2.4. ผู้บริหารสายงานสารสนเทศ ลำดับที่ 1 เข้าไปพิจารณารายการขอใช้สิทธิ์บนระบบ MAS/AD Online ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือไม่อนุมัติ หากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที และกรณีข้อมูลไม่ครบถ้วนสามารถส่งรายการกลับไปยังผู้ใช้งาน

1.2.5. ผู้บริหารสายงานสารสนเทศ ลำดับที่ 2 เข้าไปพิจารณารายการขอใช้สิทธิ์บนระบบ MAS/AD Online ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือไม่อนุมัติ หากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที และกรณีข้อมูลไม่ครบถ้วนสามารถส่งรายการกลับไปยังผู้ใช้งาน

1.2.6. ผู้ดูแลระบบดำเนินการกำหนดสิทธิ์ และเพิ่มสิทธิ์ในระบบเครือข่าย โดยกำหนดสิทธิ์ตามรายการที่ถูกอนุมัติ

1.3. การขอใช้สิทธิ์ในระบบเครือข่ายสำหรับบุคคลภายนอก มีวิธีดำเนินการดังนี้

1.3.1. ผู้ใช้งานที่เชิญบุคคลภายนอกเข้ามาที่บริษัทฯ เข้าไปดำเนินการสร้างรายการขอใช้สิทธิ์ในระบบ MAS/AD Online ในส่วนของสร้างรายการขอใช้สิทธิ์ และเลือกสิทธิ์ชั่วคราว โดยต้องระบุข้อมูลต่างๆ ของผู้ขอใช้สิทธิ์ ได้แก่ ชื่อบริษัทฯ/หน่วยงาน, บัตรประจำตัวประชาชน/บัตรประจำตัวคนต่างชาติ, ชื่อนามสกุล และระยะการใช้งาน

1.3.2. ผู้บังคับบัญชาที่มีสิทธิ์อนุมัติของผู้ใช้งานที่ดำเนินรายการ เข้าไปพิจารณารายการขอใช้สิทธิ์บนระบบ MAS/AD Online ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือไม่อนุมัติ หากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที และกรณีข้อมูลไม่ครบถ้วนสามารถส่งรายการกลับไปยังผู้ใช้งาน

1.3.3. ผู้บริหารสายงานสารสนเทศ ลำดับที่ 1 เข้าไปพิจารณารายการขอใช้สิทธิ์บนระบบ MAS/AD Online ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือไม่อนุมัติ หากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที และกรณีข้อมูลไม่ครบถ้วนสามารถส่งรายการกลับไปยังผู้ใช้งาน

1.3.4. ผู้บริหารสายงานสารสนเทศ ลำดับที่ 2 เข้าไปพิจารณารายการขอใช้สิทธิ์บนระบบ MAS/AD Online ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือไม่อนุมัติ หากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที และกรณีข้อมูลไม่ครบถ้วนสามารถส่งรายการกลับไปยังผู้ใช้งาน

1.3.5. ผู้ดูแลระบบดำเนินการกำหนดสิทธิ์ และเพิ่มสิทธิ์ในระบบเครือข่าย โดยกำหนดสิทธิ์ตามรายการที่ถูกอนุมัติ

2. การซ่อมแซมแก้ไขอุปกรณ์สารสนเทศเมื่อชำรุด
   2.1. ผู้ใช้งานที่มีความต้องการขอให้ผู้ดูแลระบบ ตรวจสอบปัญหาการใช้งานต่างๆ สามารถดำเนินการได้ที่ระบบ MAS/MIS Service โดยต้องระบุข้อมูลต่างๆ เช่น ชื่อ นามสกุล, ตำแหน่งงาน, เบอร์โทรศัพท์, รายละเอียดปัญหา หรือแนบไฟล์ เป็นต้น
   2.2. ผู้ดูแลระบบดำเนินการตรวจสอบรายการแจ้งซ่อมบนระบบ MAS/MIS Service ในส่วนของระบบแจ้งซ่อมไอที ตามลำดับการแจ้งซ่อม โดยมีระยะเวลาในการดำเนินงานหลังจากรับงานให้เสร็จสิ้นภายใน 3 วันทำการ ยกเว้นบางกรณีที่อาจจะมีระยะเวลาการดำเนินงานที่มากกว่ารายการแจ้งซ่อมทั่วไป เช่น รออะไหล่, ส่งเครม, ติดต่อซัพภายนอก หรือรอผู้ใช้งานสะดวกให้ดำเนินการ เป็นต้น
   2.3. กรณีการส่งซ่อมภายนอก
      2.3.1. ผู้ดูแลระบบ จะดำเนินการตรวจสอบประกันของอุปกรณ์ก่อนทำการส่งซ่อมภายนอก กรณีที่หมดประกัน ผู้ดูแลระบบจะทำการติดต่อบริษัทฯหรือร้านภายนอกอย่างน้อย 2 ร้าน เพื่อขอใบเสนอราคาเปรียบเทียบค่าใช้จ่ายในการส่งซ่อม
      2.3.2. ผู้ดูแลระบบจะดำเนินการสรุปราคาการส่งซ่อมภายนอกให้ผู้บริหารสายงานสารสนเทศพิจารณา
      2.3.3. กรณีผู้บริหารสายงานสารสนเทศอนุมัติการส่งซ่อมภายนอก
         2.3.3.1. กรณีค่าใช้จ่ายเกิน 3,000 บาท ผู้ดูแลระบบดำเนินการเปิด PR เพื่อเบิกค่าใช้จ่ายในการส่งซ่อม โดยอ้างอิง Cost Center บนระบบ SAP แล้วให้ผู้บริหารสายงานสารสนเทศลงนามกำกับลงใน PR และส่งให้สายงานจัดซื้อดำเนินการตามขั้นตอนการดำเนินงานเรื่องการจัดซื้อ
         2.3.3.2. กรณีค่าใช้จ่ายไม่เกิน 3,000 บาท ผู้ดูแลระบบจะดำเนินการแจ้งผู้ใช้งานให้ทำเบิกเงินสดย่อย โดยค่าใช้จ่ายในการส่งซ่อมจะลง Cost Center ของสายงานที่ถือครองอุปกรณ์
         2.3.3.3. เมื่อได้รับอุปกรณ์สารสนเทศคืนจากการส่งซ่อม ผู้ดูแลระบบจะทำการตรวจสอบอุปกรณ์ เพื่อส่งคืนผู้ใช้งาน ภายใน 3 วันทำการ
      2.3.4. กรณีผู้บริหารสายงานสารสนเทศ พิจารณาไม่อนุมัติการส่งซ่อมภายนอก
         2.3.4.1. ผู้ดูแลระบบดำเนินการแจ้งผู้ใช้งานบนระบบ MAS/MIS Service ในส่วนของระบบแจ้งซ่อมไอที ที่ได้ทำการแจ้งซ่อมมา ว่าไม่ได้รับการอนุมัติ และผู้ดูแลระบบจะทำการปิดงานทันที โดยสรุปรายละเอียดของอุปกรณ์ที่ชำรุด และสาเหตุที่ไม่ได้รับการอนุมัติ
3. การร้องขอสิทธิ์เพิ่มเติมในระบบเอ็นเตอร์ไพรส์แอพพลิเคชั่น
   3.1. ผู้ใช้งานที่มีความต้องการขอสิทธิ์ หรือแก้ไขระบบเอ็นเตอร์ไพรส์แอพพลิเคชั่น ในการใช้งานเพิ่มเติม โดยต้องระบุ ชื่อนามสกุล, ตำแหน่งงาน, ฝ่าย, แผนก, และ User ID เป็นต้น เพื่อเป็นการระบุตัวตนของผู้ใช้งาน รวมทั้งระบุสิทธิ์เดิมหรือข้อมูลระบบ

เดิม และระบุสิทธิ์ใหม่หรือข้อมูลระบบใหม่ ที่ต้องการร้องขอเพิ่มเติม โดยดำเนินการร้องขอสิทธิ์ที่ระบบ MAS/Change Request โดยระบุระบบที่ต้องการร้องขอสิทธิ์

3.2. ผู้บังคับบัญชาที่มีสิทธิ์อนุมัติลำดับที่ 1 ของผู้ใช้งานระบบ ต้องพิจารณาอนุมัติสิทธิ์ที่ผู้ร้องขอดำเนินการไว้ผ่านระบบ MAS/Change Request ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือหากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที

3.3. ผู้บังคับบัญชาที่มีสิทธิ์อนุมัติลำดับที่ 2 ของผู้ใช้งานระบบ ต้องพิจารณาอนุมัติสิทธิ์ที่ผู้ร้องขอดำเนินการไว้ผ่านระบบ MAS/Change Request ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือหากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที

3.4. ผู้บังคับบัญชาที่มีสิทธิ์อนุมัติลำดับที่ 3 ของผู้ใช้งานระบบ ต้องพิจารณาอนุมัติสิทธิ์ที่ผู้ร้องขอดำเนินการไว้ผ่านระบบ MAS/Change Request ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือหากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที

3.5. ผู้ดูแลระบบพิจารณาคำร้องขอ ดังกล่าวว่ามีผลกระทบอย่างไรต่อกระบวนการทำงาน และพิจารณาคำร้องขอดังกล่าวซึ่งต้องได้รับอนุมัติจากหน่วยงานอื่นหรือไม่ในการพิจารณาคำร้องขอสิทธิ์ หากมีผลกระทบกับหน่วยงานอื่น ผู้ดูแลระบบจะระบุหน่วยงานอื่นเพื่อร่วมพิจารณาแก้ไขเปลี่ยนแปลงระบบ หรือสิทธิ์ตามที่ผู้ใช้งานร้องขอ

3.6. ในกรณีมีหน่วยงานอื่นที่เกี่ยวข้องพิจารณาอนุมัติคำร้องขอดังกล่าว บนระบบ MAS/Change Request ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือไม่อนุมัติ หากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที

3.7. ผู้บริหารตามสายงานพิจารณาคำร้องขอดังกล่าวตามความเหมาะสม โดยพิจารณาอนุมัติคำร้องขอดังกล่าวในระบบ MAS/Change Request หากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที

3.8. ผู้ดูแลระบบ ดำเนินการตามคำร้องที่ได้รับการอนุมัติ บนระบบปฏิบัติการจำลอง QAS และบันทึกข้อมูลในระบบ MAS/Change Request เมื่อดำเนินการเสร็จสิ้น

3.9. ผู้บริหารสายงานสารสนเทศที่ได้รับมอบหมายพิจารณาตรวจสอบคำร้องขอ บนระบบปฏิบัติการจำลอง QAS และพิจารณารายการบนระบบ MAS/Change Request

3.10. ผู้ใช้งานดำเนินการตรวจสอบบนระบบปฏิบัติการจำลอง QAS และบันทึกผลการทดสอบบนระบบ MAS/Change Request หากทดสอบตามคำร้องขอดังกล่าวแล้วไม่เป็นตามคำร้องขอ ผู้ใช้งานต้องส่งเรื่องกลับไปยังผู้ดูแลระบบต่อไป

3.11. ผู้ดูแลระบบจะทำการเตรียมข้อมูลตามคำร้องในระบบ เพื่อขึ้นระบบที่ใช้งานจริง (Production Environment) และทำการบันทึกผลบนระบบ MAS/Change Request

3.12. ผู้บริหารสายงานสารสนเทศที่ได้รับมอบหมาย พิจารณาตรวจสอบความถูกต้องของผู้ดูแลระบบตามคำร้องดังกล่าว และดำเนินการในระบบ PRD ร่วมทั้งทำการบันทึกผลบนระบบ MAS/Change Request

3.13. ผู้ใช้งานดำเนินการตรวจสอบบนระบบที่ใช้งานจริง PRD และบันทึกผลการทดสอบบนระบบ MAS/Change Request หากทดสอบตามคำร้องขอดังกล่าวแล้วไม่เป็นตามคำร้องขอ ผู้ใช้งานต้องส่งเรื่องกลับไปยังผู้ดูแลระบบต่อไป

3.14. รายการคำร้องขอที่เกิดขึ้นบนระบบ MAS/Change Request มีการเก็บข้อมูล 3 ปี

4. การควบคุม และการจัดการอุปกรณ์กล้องวงจรปิด

4.1. ติดตั้งป้ายแจ้งให้รับทราบว่ามีการบันทึกภาพบริเวณที่มีติดตั้งอุปกรณ์กล้องวงจรปิด

4.2. ผู้ใช้งานต้องกรอกชื่อผู้ใช้งาน และรหัสผ่าน ก่อนเข้าถึงข้อมูลกล้องวงจรปิดที่มีการบันทึกไว้ทุกครั้ง

4.3. ผู้ดูแลระบบต้องจัดให้มีระบบความปลอดภัยเพื่อจำกัดการเข้าถึงข้อมูลกล้องวงจรปิดเฉพาะผู้ที่มีสิทธิ์เท่านั้น

4.4. จัดให้มีการแบ่งประเภทสิทธิ์การเข้าใช้งานอุปกรณ์กล้องวงจรปิด 3 ประเภท ดังนี้

4.4.1. สิทธิ์การจัดการอุปกรณ์กล้องวงจรปิด

4.4.2. สิทธิ์การเข้าดูภาพกล้องวงจรปิด เฉพาะ ณ เวลานั้น

4.4.3. สิทธิ์การเข้าดูข้อมูลกล้องวงจรปิดย้อนหลัง และนำข้อมูลออกจากอุปกรณ์เครื่องบันทึกกล้องวงจรปิด

4.5. การเปิดเผยข้อมูลต่อบุคคลที่สาม โดยบริษัทฯ อาจเปิดเผยข้อมูลส่วนบุคคลของผู้ที่ถูกบันทึกข้อมูลต่อบุคคลที่สาม ในกรณีที่มีความจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลนั้นเพื่อวัตถุประสงค์ตามที่ระบุข้างต้น

4.6. กรณีสนับสนุนการร้องขอข้อมูลจากหน่วยงานบังคับใช้กฎหมาย ต้องมีเอกสารบันทึกประจำวันหรือเอกสารที่เกี่ยวข้องกับคดี เพื่อขอเข้าถึงหรือคัดลอกข้อมูลกล้องวงจรปิด

4.7. จัดเก็บอุปกรณ์เครื่องบันทึกกล้องวงจรปิดให้มีความเหมาะสม และมีการจำกัดการเข้าถึงตัวอุปกรณ์เครื่องบันทึกกล้องวงจรปิด

4.8. การเก็บรักษาข้อมูลส่วนบุคคลของอุปกรณ์เครื่องบันทึกกล้องวงจรปิด แบ่งการเก็บออกเป็น 2 รูปแบบ ดังนี้

4.8.1. บริษัท เถ้าแก่น้อย ฟู้ดแอนด์มาร์เก็ตติ้ง จำกัด(มหาชน) บันทึกข้อมูลเป็นระยะเวลาอย่างน้อย 90 วัน แต่ไม่เกิน 120 วัน

4.8.2. บริษัทในเครือ บันทึกข้อมูลเป็นระยะเวลา 14 วัน แต่ไม่เกิน 30 วัน

4.8.3. ผู้ใช้งานที่ต้องการดูบันทึกย้อนหลังหรือต้องการไฟล์วีดีโอ ต้องทำ Job Order ส่งให้ผู้ดูแลระบบ

5. การร้องขอสิทธิ์เพิ่มเติมในระบบ Job order

5.1. ผู้ใช้งานที่มีความต้องการขอสิทธิ์ หรือขอความต้องการเพิ่มเติม เช่น ขอสิทธิ์การใช้งานระบบ MAS , ขอระบบงานใหม่ , ขอดูข้อมูลกล้องวงจรปิดย้อนหลัง ผู้บังคับบัญชาที่มีสิทธิ์อนุมัติตามหน่วยงาน ของผู้ใช้งาน ต้องพิจารณาอนุมัติสิทธิ์ที่ผู้ร้องขอดำเนินการไว้ผ่านระบบ Job order ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือหากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที

5.2. ผู้ดูแลระบบพิจารณาคำร้องขอดังกล่าวว่ามีผลกระทบอย่างไร และพิจารณาคำร้องขอดังกล่าวซึ่งต้องได้รับอนุมัติจากหน่วยงานอื่นที่เกี่ยวข้อง ผู้ดูแลระบบจะระบุหน่วยงานอื่นเพื่อร่วมพิจารณาแก้ไขเปลี่ยนแปลงระบบหรือสิทธิ์ตามที่ผู้ใช้งานร้องขอ

5.3. ในกรณีมีหน่วยงานอื่นที่เกี่ยวข้องพิจารณาอนุมัติคำร้องขอดังกล่าวบนระบบระบบ Job order ซึ่งต้องระบุเหตุผลในการอนุมัติ หรือไม่อนุมัติ หากไม่อนุมัติเอกสารจะถือเป็นการจบการดำเนินการทันที

5.4. ผู้ดูแลระบบ ดำเนินการตามคำร้องที่ได้รับการอนุมัติและบันทึกข้อมูลในระบบ Job order เมื่อดำเนินการเสร็จสิ้น

5.5. ผู้ใช้งานดำเนินการตรวจสอบบนระบบที่ใช้งาน PRD และบันทึกผลการทดสอบบนระบบ Job order หากทดสอบตามคำร้องขอดังกล่าวแล้วไม่เป็นตามคำร้องขอ ผู้ใช้งานต้องส่งเรื่องกลับไปยังผู้ดูแลระบบต่อไป

<u>บทลงโทษ</u>

ผู้ใช้งานคนใดฝ่าฝืนนโยบายและแนวปฏิบัติฉบับนี้ บริษัทฯจะพิจารณาลงโทษทางวินัยตามระเบียบ บริหารงานบุคคล รวมทั้งอาจมีความรับผิดทั้งทางแพ่ง และทางอาญา

<u>การทบทวนนโยบาย</u>

ผู้บริหารสายงานสารสนเทศ ต้องดำเนินการทบทวนนโยบายฉบับนี้เป็นประจำ อย่างน้อยปีละ 1 ครั้ง และต้องเสนอให้ คณะอนุกรรมการบริหารความเสี่ยง และคณะกรรมการบริหารอนุมัติหากมีการเปลี่ยนแปลง

ให้ประกาศฯ ฉบับนี้มีผลใช้บังคับตั้งแต่วันที่ 21 เมษายน 2565

ลงชื่อ

(นายณัชชัชพงศ์ พีระเดชาพันธ์)
กรรมการผู้จัดการ (สนับสนุนธุรกิจ)