PRUKSA HOLDING	นโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ		
	เรื่อง: นโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)		
	เลขเอกสาร: PO-Q-PSH-IT-001 Rev.00	วันที่มีผลบังคับใช้ : 24 พฤษภาคม 2567	Revision: 0
	SBU/BU: Information Technology	Group: CDO Group Digital & Innovation	

สารบัญ

1. บทนำ (Introduction)

บทสรุปผู้บริหาร

บริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน) และบริษัทย่อย คำนึงถึงความสำคัญของการนำเทคโนโลยีสารสนเทศ มาใช้ในการเพิ่มศักยภาพการดำเนินงาน และความมั่นคงปลอดภัยสารสนเทศ ซึ่งเป็นปัจจัยสำคัญที่ช่วยสนับสนุนการพัฒนาธุรกิจอย่างยั่งยืนไปกับสิ่งแวดล้อม และสังคมขององค์กร โดยตอบสนองต่อความคาดหวัง และความต้องการของผู้มีส่วนได้ส่วนเสีย จึงดำเนินการแต่งตั้งคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ และมอบหมายการจัดทำนโยบาย และแนวปฏิบัติให้สอดคล้องกับกลยุทธ์ วิสัยทัศน์ กฎหมาย ข้อบังคับ และมาตราฐานสากล ต่างๆ ที่เกี่ยวข้อง โดยมีเป้าหมายให้องค์กรได้รับประโยชน์ดังต่อไปนี้

1. เพื่อปกป้อง และรักษาเอกภาพของข้อมูลในระบบสารสนเทศ รวมถึงปกป้องข้อมูลส่วนบุคคลจากการควบคุมความเสี่ยงต่อภัยคุกคาม ให้อยู่ในระดับที่ยอมรับได้จากองค์กร
2. เพื่อให้ผู้ใช้งานระบบสารสนเทศ และผู้มีส่วนเกี่ยวข้องสามารถปฏิบัติงานตาม แนวทางที่ถูกต้อง หลักกฎหมาย มาตราฐานสากล และมีความร่วมในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร
3. เพื่อดำเนินงานทางธุรกิจบนระบบสารสนเทศได้อย่างต่อเนื่อง และสร้างความเชื่อมั่นต่อการให้บริการระบบสารสนเทศขององค์กรแก่ผู้มีส่วนได้เสีย
4. เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศรักษาว่าซึ่ง ความลับ ความถูกต้อง และ การพร้อมใช้งานอย่างมีประสิทธิ์ภาพ

หลักการและเหตุผล

เพื่อให้องค์กรได้มีกรอบและทางแนวปฏิบัติที่ชัดเจนแก่ผู้บริหาร บุคลากร และบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กร ซึ่งจะนำไปสู่การประสานงาน และการทำงานที่มีประสิทธิ์ภาพยิ่งขึ้น

มาตราฐาน กฎหมาย และพระราชบัญญัติที่เกี่ยวข้อง

1. พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (27 พฤษภาคม 2562)
3. ISO/IEC 27001:2022

บทบังคับใช้และบทลงโทษ

1. นโยบายรักษาความมั่นคงปลอดภัยสารสนเทศฉบับนี้ (IS Policy) ให้มีผลบังคับใช้ ณ วันที่ประกาศแก่ บริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน) และบริษัทย่อย ทั้งหมด โดยไม่มีการยกเว้น ผู้ฝ่าฝืนจะมีความผิดและต้องได้รับโทษทางวินัยตามระเบียบที่องค์กรกำหนดไว้
2. การปฏิบัติงานใดๆ ที่ไม่เป็นไปตามข้อกำหนดในนโยบายฯ ฉบับนี้ ต้องได้รับอนุมัติจากคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ

การเผยแพร่นโยบาย

คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ(ISMC) รับผิดชอบในการเผยแพร่นโยบายไปยังผู้ใช้งานระบบสารสนเทศ เพื่อให้เกิดความเข้าใจในบทบาทหน้าที่ของตนเอง และให้ความร่วมมือต่อการรักษาความมั่นคงปลอดภัยสารสนเทศ

การทบทวนนโยบาย

นโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ (IS Policy) ต้องได้รับการทบทวนปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง หรือเปลี่ยนแปลงที่มีนัยสำคัญ เช่น สภาพธุรกิจ กฎหมาย และเทคโนโลยี เป็นต้น โดยเป็นหน้าที่ของคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ เป็นผู้ควบคุมดูแลให้เกิดการทบทวนและปรับปรุงตามที่ได้กำหนดไว้

คำจำกัดความ

ความมั่นคงปลอดภัยสารสนเทศ

1.1 ความมั่นคงปลอดภัยสารสนเทศ Information Security (IS)

การป้องกันข้อมูลสารสนเทศ และระบบสารสนเทศ เพื่อรักษาความลับ ความครบถ้วน และความพร้อมใช้งานของข้อมูล นอกจากนี้ ยังรวมถึงการป้องกันจากการเข้าถึง การใช้งาน หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

1.2 นโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ (IS Policy)

เอกสารที่ผ่านการพิจารณา และลงนามจากคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ โดยเอกสารมีเนื้อหาเกี่ยวข้องกับ ข้อกำหนดในนโยบาย แนวปฏิบัติ มาตราการ และความรับผิดชอบของบุคคลที่เกี่ยวข้อง ที่จำเป็นในการรักษาความมั่นคงปลอดภัยสารสนเทศ ทั้งระบบและข้อมูลขององค์กร

1.3 คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMC)

คณะกรรมการที่ประกอบด้วยผู้เชี่ยวชาญ และผู้ที่เกี่ยวข้องในการบริหารและดูแลเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศภายในองค์กร ถูกแต่งตั้งจากคณะกรรมการบริหาร บริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน) หรือ Excom เพื่อบริหารจัดการข้อมูลสารสนเทศ และระบบสารสนเทศ ได้แก่ ข้อมูลลูกค้า ข้อมูลทางการเงิน และข้อมูลความลับขององค์กร เป้าหมายหลักของคณะกรรมการนี้ คือการกำหนดนโยบาย แนวปฏิบัติงานให้มีมาตราฐานสากล เพื่อให้มั่นใจว่าระบบสารสนเทศได้รับการป้องกันอย่างเหมาะสมและมีความมั่นคงปลอดภัยทั่วทั้งองค์กร

1.4 คณะบริหารความมั่นคงปลอดภัยสารสนเทศ (Management Team in ISMC)

กลุ่มผู้บริหารที่ได้รับการแต่งตั้งจากคณะกรรมการบริหาร บริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน) หรือ Excom เพื่อรับผิดชอบในการบริหารและกำหนดนโยบายและแผนงานเพื่อรักษาความมั่นคงปลอดภัยสารสนเทศภายในองค์กร

1.5 คณะปฏิบัติงานความมั่นคงปลอดภัยสารสนเทศ (Operational team in ISMC)

กลุ่มผู้ปฏิบัติงานที่ได้รับการแต่งตั้งจากคณะบริหารความมั่นคงปลอดภัยสารสนเทศ เพื่อรับผิดชอบต่อการร่างนโยบายเสนอแก่ฝ่ายบริหาร ผ่านการประเมิน ธุรกิจ เทคโนโลยี ข้อกฎหมาย มาตรฐาน และผลตอบกลับจากการนำนโยบายไปใช้งาน รวมถึงการทำงานร่วมกับหน่วยงานภายใน/ภายนอกองค์กร เพื่อกำกับดูแลให้องค์กรสามารถดำเนินตามนโยบายได้อย่างถูกต้องครบถ้วน

1.6 ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS)

ระบบบริหารงาน (Management System) หมายถึงการบริหารระบบต่างในองค์กร โดยใช้กรอบการอ้างอิง IS Policy ซึ่งระบบดังกล่าวจะนำนโยบาย แนวทางปฏิบัติ และเกณฑ์กับกำหนดการควบคุม มาปรับใช้ ส่งผลให้องค์กรมีการพัฒนา IT Security System และพัฒนาการบริหารบุคลากรในองค์กร ให้มีความมั่นคงปลอดภัยสารสนเทศตามนโยบาย

องค์กร หรือบริษัท

1.1 องค์กร

บริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน) และบริษัทย่อย

1.2 พนักงานบริษัท

ผู้บริหาร พนักงาน และที่ปรึกษาของ บริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน) และบริษัทย่อย

1.3 ฝ่าย IT

หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารเทคโนโลยีสารสนเทศขององค์กร

1.4 ผู้ดูแลระบบ

บุคคลที่เป็นพนักงานบริษัท และได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์ และสามารถเข้าถึงโปรแกรมคอมพิวเตอร์ หรือข้อมูลอื่นเพื่อจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

1.5 ผู้ใช้งานระบบสารสนเทศ

บุคคลที่ได้รับอนุญาตให้ใช้ชื่อบัญชีเข้าใช้งานระบบสารสนเทศ ตามสิทธิ์ที่ได้รับอนุมัติ ซึ่งหมายถึง พนักงานบริษัท Outsource หรือ Vendor เพื่อใช้ในการปฏิบัติงานบนระบบสารสนเทศ

1.6 ผู้ให้บริการภายนอก/หน่วยงานภายนอก

บุคคล กลุ่มบุคคล ที่หมายถึงคู่ค้า ผู้ให้บริการ ผู้จัดจำหน่ายระบบ หรือ พนักงานสัญญาจ้างที่ได้รับการจ้างจากหน่วยงานภายในองค์กรเพื่อทำงานเฉพาะทาง โดยมีส่วนในความรับผิดชอบตามคำสั่งงานหรือข้อตกลงกันไว้โดยได้รับอนุญาตให้มีสิทธิ์เข้าถึงสถานที่ สินทรัพย์สารสนเทศ และใช้งานระบบสารสนเทศ

1.7 เจ้าของข้อมูล

หมายถึง บุคคลที่ต้องรับผิดชอบในความถูกต้องของข้อมูล ความปลอดภัย และความคล่องตัวในการนำไปใช้ เป็นผู้เห็นชอบที่จะกำหนดการเข้าถึงและสิทธิ์การใช้งานข้อมูลให้กับผู้อื่นในระบบตามความเหมาะสม

1.8 นักศึกษาฝึกงาน

บุคคลที่อยู่ในกระบวนการฝึกอบรมหรือการเรียนรู้ที่เกี่ยวข้องกับงานหรือการทำงานในองค์กร โดยมีระยะเวลาที่กำหนดไว้สำหรับการฝึกงานนั้นๆ

นโยบาย แนวปฏิบัติ และมาตรการ

1.1 นโยบาย

ความต้องการขององค์กรที่กำหนดเป็นเอกสารที่ระบุเป็นข้อกำหนด และแนวทางปฏิบัติเพื่อให้บุคลากรในองค์กรและหน่วยงานภายนอก ทั้งหมดรับทราบในการเห็นชอบที่จะปฏิบัติตามกรอบนโยบายร่วมกัน

1.2 แนวปฏิบัติ

แนวทางที่กล่าวถึงขั้นตอนการปฏิบัติแล้วจะสอดคล้องกับข้อกำหดในนโยบายที่กำหนดไว้ มุ่งเน้นที่การกระทำที่มีประสิทธิ์ภาพ และการปฏิบัติตามที่ได้รับการยอมรับจากบุคคลภายในองค์กร เพื่อให้งานดำเนินไปอย่างราบรื่นและมีประสิทธิ์ภาพมากขึ้น

1.3 มาตรการ

คือการดำเนินการควบคุมที่ถูกกำหนดขึ้นเพื่อรองรับหรือป้องกันความเสี่ยงหรือปัญหาที่เป็นไปได้ มุ่งเน้นที่การบังคับใช้ และการป้องกัน เพื่อลดความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

1.4 มาตรฐาน

กฎระเบียบที่ถูกกำหนดขึ้นเพื่อให้เกิดความสอดคล้องหรือความเป็นไปได้ในการปฏิบัติงาน เช่น มาตรฐาน ISO/IEC 27001:2022

เทคนิคคอล

1.1 SSL

หมายถึงเทคโนโลยีในการเข้ารหัสข้อมูลในการเชื่อมต่อระหว่าง Computer และ Server ผ่าน Web application เพื่อความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่าย

1.2 VPN

หมายถึงการสร้างช่องทางการเชื่อมต่อเครือข่ายส่วนตัวระหว่างอุปกรณ์ต่างๆ ผ่านอินเทอร์เน็ต เพื่อส่งข้อมูลอย่างปลอดภัยและไม่เปิดเผยตัวตนผ่านเครือข่ายสาธารณะ ซึ่งจะทำงานโดยปกปิดที่อยู่ IP ของผู้ใช้และเข้ารหัสข้อมูลเพื่อให้บุคคลที่ไม่ได้รับอนุญาตที่ได้รับข้อมูลดังกล่าวไม่สามารถอ่านได้

1.3 Cloud Service

คือเทคโนโลยีที่ให้บริการระบบคอมพิวเตอร์แบบเครือข่ายออนไลน์ ตั้งแต่การให้บริการการจัดเก็บข้อมูล บริการซอฟต์แวร์และแหล่งทรัพยากรคอมพิวเตอร์ผ่านอินเทอร์เน็ต สามารถใช้แหล่งทรัพยากรคอมพิวเตอร์ที่อยู่บน Cloud ของผู้ให้บริการ Cloud Provider

1.4 Web Service

คือระบบซอฟต์แวร์ที่ออกแบบมาเพื่อสนับสนุนการแลกเปลี่ยนข้อมูล ระหว่างเครื่องคอมพิวเตอร์ผ่านระบบเครือข่าย โดยใช้ภาษาในการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ ระบบที่ออกแบบมา เพื่อสนับสนุนการแลกเปลี่ยนข้อมูล ระหว่างคอมพิวเตอร์ผ่านทางระบบเครือข่าย

1.5 ระบบสารสนเทศ (IT system)

- ระบบที่ประกอบด้วย Hardware Software และ Data ที่มีการสื่อสารระหว่างกันเพื่อดำเนินการประมวลผล จัดเก็บ และบริหารจัดการข้อมูลต่างๆ อย่างมีประสิทธิ์ภาพ โดยมีเป้าหมายในการให้บริการแก่ผู้ใช้งานระบบสารสนเทศในรูปแบบที่ตรงตามความต้องการขององค์กร หรือหน่วยงานต่างๆ
- ระบบสารสนเทศจะประกอบด้วยระบบย่อยหลายระบบ ที่สร้างขึ้นเพื่อวัตถุประสงค์ทางธุรกิจที่ชัดเจนเป็นศูนย์กลางการทำงานของผู้ใช้ระบบสารสนเทศ เพื่อป้อนข้อมูล และนำไปประมวลผล
  - ระบบ PSPro: ระบบสารสนเทศเพื่อใช้ในการบริหารงานขาย ผู้ใช้งานคือหน่วยงานขาย
  - ระบบ Email: ระบบสารสนเทศเพื่อใช้ในการติดต่อสื่อสาร ผู้ใช้งานคือทุกคนในองค์กร
  - ระบบ Humatrix: ระบบสารสนเทศเพื่อใช้ในการบริหารทรัพยากรบุคคล ผู้ใช้งานคือทุกคนในองค์กร
  - ระบบ SAP: ระบบสารสนเทศเพื่อใช้ในการบริหารงานด้าน Enterprise Resource Planning ผู้ใช้งานคือหน่วยงานบัญชี การเงิน และอื่นๆ ที่เกี่ยวข้อง

1.6 ระบบ IT Help Desk Service

เป็นระบบสารสนเทศที่ใช้ในการแจ้งปัญหา หรือขอใช้บริการจากฝ่าย IT ซึ่งข้อมูลการใช้งานระบบจะถูกเก็บบันทึกไว้ใน Website โดยมีระบบการติดตามงาน และประเมินผลเมื่องานสำเร็จ ใช้ในการบันทึกกิจกรรมการดำเนินงานร่วมกับผู้ใช้งานระบบสารสนเทศ

1.7 ข้อมูล

อธิบายถึงกิจกรรมขององค์กร ที่ผ่านระบบสารสนเทศ จากการเก็บรวบรวม วิเคราะห์ ตัดสินใจ และนำไปใช้ในการประมวลผล ข้อมูลอาจเป็นตัวเลข ข้อความ ภาพถ่าย หรือวิดีโอ โดยนำมาใช้งานได้ในหลายๆ รูปแบบตามความต้องการของผู้ใช้งานระบบสารสนเทศ โดยรวมถึง Hard copy Soft copy ทั้ง Online และ Offline

1.8 สินทรัพย์สารสนเทศ

หมายถึงอุปกรณ์ Hardware Software และ Data ที่เกี่ยวข้องการระบบสารสนเทศที่ถูกใช้ในองค์กร

1.9 Disaster recovery plan (DRP)

เป็นแผนการที่องค์กรหรือธุรกิจกำหนดขึ้นเพื่อใช้ในกรณีที่เกิดภัยพิบัติหรือเหตุการณ์ฉุกเฉินที่สามารถทำให้ระบบสำคัญหรือข้อมูลสำคัญขององค์กรเสียหายได้ โดย DRP จะรวมถึงวิธีการกู้คืนข้อมูล ระบบสำคัญ หรือสถานะปกติของธุรกิจที่ถูกสร้างขึ้นเพื่อให้ระบบและธุรกิจสามารถกลับมาทำงานได้โดยรวดเร็วหลังจากการเกิดภัยพิบัติ

1.10 Active Directory (AD)

Active Directory (AD) เป็นการจัดการและบริหารจัดการทรัพยากรในระบบสารสนเทศ เช่น ผู้ใช้งานเครื่องคอมพิวเตอร์ กลุ่มผู้ใช้ และอื่นๆ เพื่อให้ผู้ใช้งานสามารถเข้าถึงทรัพยากรต่างๆ ได้อย่างมีประสิทธิ์ภาพและปลอดภัย

1.11 Security Operation Center (SOC)

เป็นกลุ่มบุคคลที่ใช้ระบบในการตรวจสอบ ติดตาม และตอบสนองต่อความเสี่ยงและการละเมิดความปลอดภัยที่เกิดขึ้นภายในระบบขององค์กร และการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยทันทีเมื่อเกิดขึ้น เพื่อลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้นต่อองค์กร

1.12 Data lost Prevention (DLP)

ระบบที่ใช้ในการรักษาข้อมูลองค์กรมีค่าสูงสุดและเสี่ยงต่อการสูญเสีย ระบบจะไม่อนุญาตให้ข้อมูลดังกล่าวถูกเผยแพร่ออกนอกองค์กร หรือป้องกันการรั่วไหลข้อมูลที่ไม่ได้รับอนุญาต

1.13 Privileged Access Management (PAM)

ระบบที่ใช้ในการจัดการและควบคุมการเข้าถึงและการใช้งานข้อมูลหรือทรัพยากรของผู้ดูแลระบบที่มีสิทธิ์สูงสุดในระบบสารสนเทศขององค์กร

2. บทนโยบาย (Policy Statement)

แนวทางหลักในการจัดทำนโยบาย

วัตถุประสงค์

เพื่อให้นโยบายถูกกำหนดออกมาเป็นเอกสารที่ใช้ในการอ้างอิงและปฏิบัติร่วมกันภายในองค์กร โดยให้ผู้ใช้งานระบบสารสนเทศ และบุคคลที่เกี่ยวข้องได้ รับทราบถึงความสำคัญ หน้าที่ ความรับผิดชอบ และแนวทางการปฏิบัติในการควบคุมความเสี่ยง

หลักการ

1. คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ มีหน้าที่ความรับผิดชอบในการจัดทำนโยบายด้านความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษร
2. คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศมีหน้าที่ความรับผิดชอบในการตรวจทาน และเห็นชอบนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงการเผยแพร่เอกสารนโยบายดังกล่าวให้กับผู้ใช้ระบบสารสนเทศ หน่วยงานภายนอก และผู้ที่เกี่ยวข้องโดยเอกสารนโยบายดังกล่าว จะต้องสามารถเข้าถึงได้
3. คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ มีหน้าที่ความรับผิดชอบในการติดตามผลจากการประกาศใช้ภายในองค์กร เพื่อนำผลที่ได้มาทบทวนและปรับปรุงนโยบาย
4. คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ มีหน้าที่ความรับผิดชอบในการทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญซึ่งส่งผลต่อองค์กร

โครงสร้างของเนื้อหาในเอกสารนโยบาย

หลักการ

1. เอกสารต้องแบ่งแยกหน้าที่ ความรับผิดชอบ (Segregation of Duties) อย่างชัดเจน เพื่อให้มีการสอบทานระหว่างกัน ตาม "ข้อกำหนดแบ่งแยกหน้าที่และความรับผิดชอบต่อความมั่นคงปลอดภัยสารสนเทศ"
2. เอกสารนโยบายจะถูกแบ่งออกเป็นข้อกำหนดต่างๆ และกำหนดแนวปฏิบัติให้สอดคล้อง ดังนี้

ข้อกำหนด: ระบุถึงความต้องการขององค์กรเพื่อรักษาความมั่นคงปลอดภัยสารสนเทศ

แนวปฏิบัติ: ระบุถึงแนวปฏิบัติที่เหมาะสมในการดำเนินงานสอดคล้องกับข้อกำหนด

มาตรการ: คือแนวปฏิบัติที่ลงรายละเอียดชัดเจน เพื่อถูกบังคับใช้ ให้ผู้ใช้งานระบบสารสนเทศยึดถือและปฏิบัติตามอย่างเคร่งครัด

การทบทวนนโยบาย

วัตถุประสงค์

เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องกับนโยบาย แนวปฏิบัติ ข้อกำหนดขององค์กร และเหมาะสมกับบริบทที่เปลี่ยนไป

หลักการ

1. การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ

   นโยบาย แนวปฏิบัติ ข้อกำหนด มาตรการต่างๆ ต้องมีการทบทวนตามรอบระยะเวลาที่กำหนด และสมาชิกของคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศมีส่วนร่วมทางความคิดอย่างอิสระในการนำเสนอแก้ไขและปรับปรุง

2. ความสอดคล้องของนโยบาย แนวทางปฏิบัติ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ

   หน่วยงานภายในองค์กร ต้องกำกับดูแลให้ขั้นตอนปฏิบัติของหน่วยงานตนเองสอดคล้องกับนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ

   ผู้ใช้งานระบบสารสนเทศสามารถให้ข้อมูลป้อนกลับ และนำเสนอต่อคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ เพื่อพิจารณาปรับปรุงตามรอบการทบทวนได้ หากพบว่ามีปัญหาในการปฏิบัติ ที่ส่งผลกระทบที่มีต่อการดำเนินงานทางธุรกิจ และความคุ้มค่าในการลงทุน

3. การทบทวนความสอดคล้องทางเทคนิค

   ฝ่าย IT ต้องรับผิดชอบในการตั้งค่าระบบสารสนเทศ ให้เป็นไปตามนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ

   การตั้งค่าการทำงานของระบบสารสนเทศต้องได้รับการทบทวนอย่างสม่ำเสมอ เพื่อมุ่งไปยังการรักษาความมั่นคงปลอดภัยสารสนเทศตามที่กำหนดไว้ในนโยบายตามรอบการทบทวนที่กำหนด

3. ข้อกำหนดบทบาทหน้าที่และความรับผิดชอบต่อความมั่นคงปลอดภัยสารสนเทศ

คณะกรรมการบริหาร บริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน) หรือ Excom

1. แต่งตั้งคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ
2. มอบหมายหน้าที่ความรับผิดชอบของคณะกรรมบริหารความมั่นคงปลอดภัยสารสนเทศ
3. พิจารณาและเห็นชอบนโยบายที่คณะกรรมบริหารความมั่นคงปลอดภัยสารสนเทศนำเสนอ โดยพิจารณาความสำคัญดังนี้
   - นโยบายที่ถูกจัดทำ ครอบคลุมระบบสารสนเทศที่มีความสำคัญ
   - นโยบายที่ถูกจัดทำ มีทิศทางสอดคล้องกับวัตถุประสงค์ทางธุรกิจขององค์กร
   - นโยบายที่ถูกจัดทำ มีการปฏิบัติสอดคล้องกับกฎหมายที่มีการบังคับใช้
   - นโยบายที่ถูกจัดทำ สามารถถูกปรับปรุงได้อย่างเหมาะสมตามรอบการทบทวน
   - นโยบายที่ถูกจัดทำ ถูกเผยแพร่ และถูกนำไปใช้ทั่วทั้งองค์กร
4. พิจารณาติดตามผลการใช้นโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ

คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ

คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ ได้รับการแต่งตั้งจากคณะกรรมการบริหาร บริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน) โดยสมาชิกต้องประกอบด้วยสายงาน หรือหน่วยงานที่เกี่ยวข้องอย่างน้อย ได้แก่

- CDO Group Digital & Innovation
- LC Legal & Compliance (Legal and DPO)
- IA Internal Audit
- RM Risk Management and Sustainability

โครงสร้างการบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management: ISM)

โครงสร้างการบริหาร ISM

Excom

- อนุมัติแต่งตั้งและมอบหมายหน้าที่ความรับผิดชอบแก่คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Committee: ISM Com)

คณะกรรมการบริหาร ความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Committee: ISM Com)

- กำหนดทิศทางในการดำเนินงานระบบบริหารจัดการด้านความมั่นคงปลอดภัย
- พิจารณาออกนโยบาย วัตถุประสงค์ ขอบเขตของระบบ และเกณฑ์การประเมินประสิทธิภาพรักษาความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน และกฎหมาย
- สนับสนุนทรัพยากรและสั่งการ เพื่อให้สามารถดำเนินงานตามมาตรการควบคุม และแผนจัดการความมั่นคงปลอดภัยสารสนเทศได้ตามกรอบที่กำหนด
- แต่งตั้งและมอบหมายหน้าที่การทำงานให้คณะปฏิบัติงานความมั่นคงปลอดภัยสารสนเทศ (Working team)

คณะปฏิบัติงาน ความมั่นคงปลอดภัยสารสนเทศ (Working team)

- ร่างนโยบายให้เหมาะสมและนำเสนอแก่คณะกรรมการบริหารฯ เพื่อขอความเห็นชอบ และพิจารณาการดำเนินการปรับปรุงตามข้อเสนอแนะของผู้เชี่ยวชาญตามบริบทของบริษัทฯ
- วางแผนประเมินความเสี่ยง และดำเนินการปรับปรุงให้เหมาะสมอย่างต่อเนื่อง และปรับแก้ไขตามผลการประเมินภายใน
- เผยแพร่เกี่ยวกับความปลอดภัยให้กับพนักงานองค์กร เพื่อเพิ่มความตระหนักและความเข้าใจในเรื่องความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

หน้าที่คณะกรรมการความมั่นคงปลอดภัยสารสนเทศแบ่งออกเป็น 2 คณะ ดังนี้

3.1 ฝ่ายบริหารของคณะกรรมการ:

เป็นผู้กำหนดนโยบาย รับรอง และรายงานผลแก่ Excom ให้รับทราบอย่างน้อยปีละ 1 ครั้ง หรือเกิดการเปลี่ยนแปลงที่สำคัญ โดยมี

3.1.1 พิจารณาอบเขต นโยบาย วัตถุประสงค์ ของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ และอนุมัติสั่งการ

3.1.2 พิจารณาจัดหาและสนับสนุนทรัพยากรที่จำเป็น เพื่อให้สามารถดำเนินมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ มาตรการลดความเสี่ยง และบริหารจัดการได้ตามกรอบที่กำหนด

3.1.3 พิจารณา กำหนดแนวทาง และวิธีการประเมินความเสี่ยง เกณฑ์ในการยอมรับความเสี่ยง และระดับความเสี่ยงที่สามารถยอมรับได้

3.1.4 กำหนดให้มีการประเมินความเสี่ยง และพิจารณาผลการประเมินความเสี่ยง

3.1.5 กำหนดให้ติดตามการดำเนินการตรวจสอบภายใน ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามกรอบเวลาที่กำหนด

3.1.6 กำหนดให้ปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อให้บรรลุตามวัตถุประสงค์ที่กำหนด

3.1.7 กำหนดระยะเวลาของ Management Review เพื่อใช้ในประเมินผลการปฏิบัติงานตามนโยบาย และการทบทวนนโยบายอย่างน้อยปีละ 2 ครั้ง หรือกรณีที่มีการเปลี่ยนแปลงที่สำคัญ

3.1.8 กำหนดให้ทบทวนนโยบาย โดยพิจารณาผลการตอบกลับจากผู้ใช้งานระบบสารสนเทศ เพื่อปรับปรุงให้เหมาะสมและเป็นปัจจุบันโดยคำนึงถึงความสมดุลระหว่าง ประสิทธิ์ภาพการดำเนินงานทางธุรกิจ กลยุทธ์องค์กร และความมั่นคงปลอดภัยสารสนเทศ

3.2 ฝ่ายปฏิบัติงานของคณะกรรมการ:

เป็นผู้ร่างนโยบายให้เหมาะสมและนำเสนอแก่คณะกรรมการฝ่ายบริหารเพื่อขอความเห็นชอบ และพิจารณาการดำเนินการปรับปรุงตามข้อเสนอแนะของผู้เชี่ยวชาญให้เหมาะสมกับบริษัท

3.2.1 ร่างนโยบายและนำเสนอแก่คณะบริหารฯ เพื่อขอความเห็นชอบ และพิจารณาการดำเนินการปรับปรุงตามข้อเสนอแนะของผู้เชี่ยวชาญให้เหมาะสมกับบริบทขององค์กร

3.2.2 ดำเนินการเผยแพร่นโยบาย และสร้างความเข้าใจในนโยบายแก่ผู้ใช้งานในองค์กร

3.2.3 จัดอบรม / เข้าร่วมการอบรม เพื่อสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศให้แก่ตนเองและผู้ที่เกี่ยวข้อง

3.2.4 ทำงานร่วมกับสายงานบริหารความเสี่ยงและความยั่งยืน ดังนี้

- กำหนดแนวทางและวิธีการประเมินความเสี่ยง เกณฑ์ในการยอมรับความเสี่ยง และระดับความเสี่ยงที่สามารถยอมรับได้
- ดำเนินมาตรการควบคุมความเสี่ยงตามแผนการปรับลดความเสี่ยง และดำเนินมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศตามนโยบายและกรอบการบริหารความเสี่ยงของบริษัท

3.2.5 ทำงานร่วมกับฝ่ายกฎหมาย

- รับผิดชอบดูข้อกฎหมายที่เกี่ยวข้องกับ พรบ.ตามที่ระบุไว้ในนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศโดยปรับปรุงให้ทันสมัยและเหมาะสมในแต่ละรอบ

3.2.6 ทำงานร่วมกับฝ่ายตรวจสอบภายใน

- ตรวจสอบหน่วยงานภายในองค์กรให้ปฏิบัติตามขั้นตอนปฏิบัติ และแผนการปฏิบัติที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่ได้ออกแบบไว้

3.2.7 ทำงานร่วมกับหน่วยงานภายในองค์กร (BU)

- ตอบคำถาม และสร้างความเข้าใจในรายละเอียดของนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ
- รับผิดชอบเก็บผลการตอบรับหลังจากหน่วยงานต่างๆ ที่ได้ปฏิบัติตามนโยายแล้ว แต่มีความต้องการนำเสนอเพื่อการปรับปรุงที่ดีขึ้น

ผู้บริหารระดับสูงทุกสายงาน ของบริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน) และบริษัทย่อย

1. กำกับดูแลหน่วยงานที่รับผิดชอบ ให้ปฏิบัติงานสอดคล้องตามข้อกำหนดที่ระบุไว้ในนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ
2. กำหนดให้พนักงานในหน่วยงานที่รับผิดชอบ ร่วมมือ เพื่อติดตามผลการปฏิบัติงานตามนโยบายจากฝ่ายตรวจสอบภายใน และสนับสนุนให้หน่วยงานดำเนินการปรับปรุงแก้ไขจากผลสิ่งที่ไม่สอดคล้องโดยระบุเป็นแผนงานและดำเนินตามกรอบเวลาที่กำหนด
3. หากการทบทวนหากพบว่าผลการดำเนินการนโยบายส่งผลกระทบกับการดำเนินงานทางธุรกิจหรือกลยุทธ์ขององค์กรให้แจ้งคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศเพื่อพิจารณาตรวจสอบและปรับปรุง

ผู้บริหารระดับแผนกหรือฝ่าย

1. ทบทวน ทำความเข้าใจ และสามารถอธิบาย นโยบายความมั่นคงปลอดภัยสารสนเทศแก่พนักงานในสังกัดที่ดูแลเพื่อให้พนักงานสามารถปฏิบัติงานได้ถูกต้อง
2. กำหนดบทบาทหน้าที่ และความรับผิดชอบบุคลากร ในการปฏิบัติงานให้สอดคล้องตามข้อกำหนดที่ระบุไว้ในนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ
3. ชี้แจงการเปลี่ยนแปลงที่อาจจะเกิดขึ้นในการดำเนินธุรกิจ กับการปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศในส่วนงานที่รับผิดชอบ แก่ผู้บริหารระดับสูงของสายงาน เพื่อรวบรวมและนำส่งให้คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศรับทราบและพิจารณา
4. ติดตามแผนงานของแผนกหรือฝ่ายของตนเองและดำเนินการตามแผนให้แล้วเสร็จ หากได้รับคำแนะนำจากฝ่ายตรวจสอบภายในว่าปฏิบัติงานไม่สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ

CDO Group Digital & Innovation

1. ควบคุมการดำเนินงานโครงการ IT ทุกโครงการให้เป็นไปตามข้อกำหนดในนโยบายรักษาความมั่นคงปลอดภัย
2. กำกับดูแลและติดตามให้ระบบสารสนเทศขององค์กร ให้ดำเนินงานตามแนวทางปฏิบัติที่สอดคล้องกับนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ
3. ทบทวนการนำนโยบายและแนวทางปฏิบัติที่นำไปใช้งานทุกๆปีและนำเสนอให้คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศพิจารณาปรับปรุง

CHO Group Human Resources

กำหนดแนวทางปฏิบัติงานความมั่นคงปลอดภัยสำหรับสายงานทรัพยากรบุคคลตามให้สอดคล้องตามข้อกำหนดที่ระบุไว้ใน นโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ

RM Risk Management and Sustainability (สายงานบริหารเสี่ยงและความยั่งยืน)

รับผิดชอบกำหนดระยะเวลา แผนงานและจัดเตรียมกำลังคน เพื่อร่วมพิจารณาและให้ความเห็นในประเด็นที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงร่วมทบทวนปรับปรุงนโยบายและแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศในแต่ละปี

IA Internal Audit

รับผิดชอบกำหนดระยะเวลา แผนงาน และจัดเตรียมกำลังคนในการตรวจสอบการปฏิบัติงานของระบบสารสนเทศให้เป็นไปตามนโยบาย และรายงานผลการดำเนินงานแก่คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ โดยถือว่าเป็นส่วนหนึ่งของตารางการตรวจสอบเป็นประจำ

LC Legal & Compliance (Legal and DPO)

รับผิดชอบดูรายละเอียดในข้อกฎหมายที่เกี่ยวข้องกับ พรบ.ตามที่ระบุไว้ในนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศโดยปรับปรุงให้ทันสมัย เพิ่มลด หรือปรับเหมาะสมในแต่ละรอบปี

พนักงานบริษัท

1. ศึกษาและทำความเข้าใจต่อนโยบายและแนวปฏิบัติ รักษาความมั่นคงปลอดภัยสารสนเทศ และแนวปฏิบัติงานต่างๆ ที่ประกาศ เพื่อให้ความร่วมมือในการปฏิบัติตามข้อกำหนดขององค์กร
2. รายงานเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยสารสนเทศ แก่ผู้บังคับบัญชา และส่งข้อมูลให้คณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศเพื่อตรวจสอบและแก้ไข

ผู้ให้บริการภายนอก/หน่วยงานภายนอก

1. รับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. ข้อมูลสารสนเทศที่ได้รับจากการเก็บรวบรวมหรือเข้าถึงในระหว่างที่มีการทำงานกับองค์กร ให้ถือเป็นความลับ ห้ามทำการเปิดเผยแก่บุคคลภายนอกองค์กร ยกเว้นได้รับการยินยอมอย่างชัดเจนเป็นลายลักษณ์อักษรจากหน่วยงานที่จัดจ้าง และผ่านการลงนามเห็นชอบจากคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ
3. รายงานเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยสารสนเทศ แก่หน่วยงานที่จัดจ้างตนเอง และส่งข้อมูลให้คณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศเพื่อตรวจสอบและแก้ไข
4. รับผิดชอบ / ดูแล เจ้าหน้าที่ที่เข้ามาปฏิบัติงาน ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

4. ข้อกำหนดด้านบริหารทรัพยากรบุคคล

การสรรหาบุคลากรก่อนการทำงาน (Prior to employment)

ขอบเขต

ครอบคลุมการดำเนินงานของฝ่าย HR IT Legal PRC และ BU

หลักการ

1. ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)
   - กรณีผู้ให้บริการภายนอก / หน่วยงานภายนอก: PRC ต้องกำหนดในร่างสัญญาที่ระบุหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงาน
   - กรณีพนักงานบริษัท: HR ต้องระบุข้อความในสัญญาจ้างงานระหว่างพนักงานว่าจะไม่เปิดเผยความลับทางการค้าของบริษัท (Non-Disclosure Agreement: NDA) ทั้งนี้ ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

ระหว่างการจ้างงาน (During employment)

ขอบเขต

ครอบคลุมการดำเนินงานของฝ่าย HR IT BU และผู้ใช้งานระบบสารสนเทศ

หลักการ

พนักงานของบริษัทหุกคนต้องได้รับการอบรมเกี่ยวกับเรื่องนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอเพื่อช่วยให้พนักงานรับทราบ และใช้เป็นแนวทางในการปฏิบัติงานที่ตนเองรับผิดชอบได้

การฝึกอบรม

4.1 ขอบเขต

ครอบคลุมการดำเนินงานของฝ่าย HR IT BU และพนักงานบริษัท

4.2 หลักการ

1. ฝ่าย HR และ IT ร่วมกันในจัดฝึกอบรมพนักงาน เพื่อให้พนักงานได้รับความรู้และความเข้าใจในนโยบาย แนวทางปฏิบัติ และมาตราการการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. ฝ่าย HR และ IT ร่วมกันในการจัดฝึกอบรม เผยแพร่ความรู้ที่เกี่ยวข้องสม่ำเสมอ เพื่อสร้างความตระหนักรู้ถึงความมั่นคงปลอดภัยสารสนเทศให้แก่พนักงานอย่างน้อยปีละ1 ครั้งหรือกรณีที่มีการเปลี่ยนแปลงที่มีนัยสำคัญกับองค์กร

การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

ขอบเขต

ครอบคลุมการดำเนินงานของฝ่าย HR IT BU และผู้ใช้งานระบบสารสนเทศ

หลักการ

1. ฝ่าย HR ต้องส่งข้อมูลการพ้นสภาพของพนักงาน และ BU หรือพนักงานต้องส่งการเปลี่ยนแปลงสถานะของพนักงานให้ฝ่าย IT เพื่อดำเนินการปรับปรุง หรือยกเลิกสิทธิ์การเข้าถึงข้อมูลในระบบสารสนเทศขององค์กร
2. พนักงานที่ลาออกต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงานผู้เป็นเจ้าของ เมื่อสิ้นสุดสภาพการเป็นพนักงานหรือสิ้นสุดสัญญา หรือข้อตกลงการปฏิบัติงานให้กับองค์กร
3. เครื่องคอมพิวเตอร์ Tablet มือถือ External Disk ที่ส่งคืนจากพนักงานที่ลาออกหรือสิ้นสุดสัญญา ทาง IT ต้องดำเนินการลบข้อมูลออกก่อนจะนำเครื่องดังกล่าวมอบให้พนักงานท่านอื่นใช้ต่อไป

การบริหารจัดการสิทธิ์บนระบบสารสนเทศของผู้ใช้งานระบบสารสนเทศ

ขอบเขต

ครอบคลุมการดำเนินงานของฝ่าย HR IT BU พนักงานบริษัท ผู้ให้บริการภายนอก นักศึกษาฝึกงาน และผู้ใช้งานระบบสารสนเทศ

หลักการ

กรณีพนักงานต้องการใช้สิทธิ์เพิ่มเติมเข้าถึงข้อมูลหรือระบบสารสนเทศ พนักงานต้องแจ้งขอเปลี่ยนแปลงสิทธิ์ผ่านผู้บังคับบัญชาของตน ผ่านช่องทางที่ฝ่าย IT จัดเตรียมไว้เพื่อนำมาอ้างอิงเป็นหลักฐานได้ในการดำเนินการเพิ่ม ลดและปรับสิทธิ์ของพนักงาน ทั้งนี้ ฝ่าย IT จะต้องทำหน้าที่ในการกลั่นกรองอย่างเหมาะสมก่อนดำเนินการ

5. ข้อกำหนดการบริหารสินทรัพย์สารสนเทศ (IT Asset Management)

วัตถุประสงค์

เพื่อระบุสินทรัพย์สารสนเทศขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการป้องกันสินทรัพย์อย่าง เหมาะสม ซึ่งประกอบไปด้วย Hardware Software Server Network และ Data

ขอบเขต

สินทรัพย์สารสนเทศ หมายถึงอุปกรณ์ Hardware Software และ Data ที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร

1. Hardware
   - Computer
   - Server (On premise on Cloud)
   - Network
   - Tablet
2. Software
   - Application
   - Service Subscription
3. Data
   - Hard Copy
   - Soft Copy
   - Database

การบริหารสินทรัพย์สารสนเทศ

1. การจัดทำบัญชีสินทรัพย์ (Inventory of assets)

ฝ่าย IT ต้องจัดทำทะเบียนสินทรัพย์สารสนเทศทั้งหมดภายในองค์กร และตรวจสอบดูแลปรับปรุงบัญชีรายการทรัพย์สินดังกล่าวอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง รวมถึงการนำข้อมูลทะเบียนสินทรัพย์สารสนเทศมาวิเคราะห์ ประเมินความเสี่ยง และบริหารจัดการความเสี่ยงได้อย่างเหมาะสม

2. ผู้ถือครองสินทรัพย์ (Ownership of assets)

การถือครองสินทรัพย์สารสนเทศต้องกำหนดผู้รับผิดชอบให้ชัดเจน และผู้ถือครองต้องรับผิดชอบความเสียหายที่เกิดขึ้นกับสินทรัพย์ดังกล่าว

3. การใช้สินทรัพย์อย่างเหมาะสม (Acceptable use of assets)

- พนักงานบริษัทต้องเข้าใจแนวปฏิบัติต่างๆ เพื่อให้สามารถใช้สินทรัพย์สารสนเทศได้อย่างถูกต้อง โดยฝ่าย IT จัดทำขึ้นตามแนวปฏิบัติงานในการจัดการ และจัดเก็บทรัพย์สินสารสนเทศเพื่อไม่ให้ข้อมูลสารสนเทศรั่วไหล หรือถูกนำไปใช้ผิดประเภท
- ผู้ใช้งานต้องไม่ทิ้ง หรือปล่อยให้ทรัพย์สินสารสนเทศที่มีความสำคัญ เช่น เอกสารสื่อบันทึกข้อมูล ให้อยู่ในสถานที่ที่ไม่มีความปลอดภัย สถานที่สาธารณะ หรือพบเห็นได้ง่าย เป็นต้น

4. การคืนสินทรัพย์ (Return of assets)

- พนักงานบริษัทที่สิ้นสุดการจ้างงาน หรือสิ้นสุดโครงการต้องคืนสินทรัพย์สารสนเทศที่รับผิดชอบทั้งหมด รวมทั้งกุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้าออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง และ อุปกรณ์ต่าง ๆ
- ฝ่าย IT BU และหัวหน้างานหรือผู้บังคับบัญชา มีหน้าที่ติดตาม Asset ที่อยู่ในความรับผิดชอบของพนักงานในสังกัดตนเองให้ส่งคืน สินทรัพย์สารสนเทศแก่ฝ่าย IT
- พนักงานที่เป็นผู้ถือครองในระบบสารสนเทศประเภท Server Network และ Hardware ใดๆ ซึ่งเป็นส่วนกลางที่ทุกคนในบริษัทใช้ร่วมกัน ก่อนกำหนดพ้นสภาพ จะต้องกำหนดผู้ถือครองให้เป็นปัจจุบันเสมอ โดยให้ผู้ถือครองให้เป็นหัวหน้าลำดับถัดไปก่อนจนกว่าจะมีพนักงานบริษัทใหม่มาทดแทนในตำแหน่งดังกล่าว

5. การดูแลรักษาอุปกรณ์ (Equipment Maintenance)

- ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ
- กำหนดแผนและผู้รับผิดชอบในการดูแล และบำรุงรักษาอุปกรณ์

6. การนำสินทรัพย์ที่ตนเองไม่ใช่ผู้ถือครองออกนอกหน่วยงาน

- การนำไปใช้งานนอกหน่วยต้องมีสิทธิ์ หรือได้อนุญาตจากผู้ถือครองก่อนนำออกไปใช้งาน
- มีบันทึกการนำสินทรัพย์สารสนเทศ ลงนามความยินยอม และบันทึกการส่งคืนเพื่อเก็บเป็นหลักฐานป้องกันการสูญหาย

การจัดการอุปกรณ์ที่ใช้สนับสนุนสินทรัพย์สารสนเทศ (Equipment)

1. การจัดตั้งและการป้องกันอุปกรณ์ (Equipment Siting and Protection)
   - ต้องติดตั้งอุปกรณ์หรือเครื่องมือไว้ในพื้นที่ปลอดภัยและมีการมาตรการป้องกันภัย หรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์ต่างๆ
   - ต้องจัดวางอุปกรณ์สารสนเทศในตำแหน่งที่เหมาะสมเพื่อหลีกเลี่ยงการมองเห็นข้อมูลสำคัญจากบุคคลภายนอกหรือผู้ไม่มีสิทธิ์
2. การดูแลอุปกรณ์ต่างๆ (Supporting Utilities)
   - ต้องมีระบบสนับสนุนการทำงานของระบบควบคุมอุณหภูมิและความชื้นของบริษัทที่เพียงพอต่อการใช้งาน เช่น ระบบกระแสไฟฟ้า การควบคุมอุณหภูมิ เครื่องปรับอากาศ ระบบไฟฟ้าหลัก และสำรอง เป็นต้น
   - ต้องกำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบ และอุปกรณ์สนับสนุนต่างๆ เช่น ระบบกระแสไฟฟ้า ระบบไฟฟ้าสำรอง ระบบควบคุมอุณหภูมิ ระบบความชื้น และระบบปรับอากาศ เป็นต้น เพื่อป้องกันการล้มเหลวของระบบเทคโนโลยีสารสนเทศอันส่งผลต่อความต่อเนื่องในการดำเนินธุรกิจ
3. การเดินสายไฟ และสายเคเบิล (Cabling Security)
   - ต้องกำหนดให้มีการป้องกันการเดินสายไฟฟ้า สายสื่อสาร หรือสายเคเบิ้ลต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต หรือทำให้เกิดความเสียหายกับสายสัญญาณ และส่งผลต่อการทำงานทำให้เกิดการหยุดชะงัก
   - หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของบริษัทในลักษณะที่ผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกสามารถเข้าถึงได้ ซึ่งอาจลักลอบดักจับข้อมูลในสายสัญญาณได้
   - บริเวณที่มีการเดินสายไฟฟ้า หรือสายเคเบิลเข้ามาภายในบริษัท และมีการติดตั้งตู้พักสายต้องล็อคไว้ตลอดเวลา และจำกัดการเข้าใช้งานได้เฉพาะเจ้าหน้าที่ หรือบุคคลที่มีสิทธิ์เท่านั้น
   - ต้องกำหนดให้มีการร้อยสายสัญญาณต่างๆ เข้าไปในท่อเพื่อป้องกันการดักแอบจับสัญญาณการถูกสัตว์กัดแทะ หรือการตัดสายสัญญาณซึ่งทำให้เกิดความเสียหายได้
   - ต้องกำหนดให้มีการเดินสายสัญญาณสื่อสาร และสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการแทรกแซงของสัญญาณซึ่งกันและกัน
   - ต้องกำหนดให้มีการจัดทำป้ายชื่อสำหรับสายสัญญาณ และบนอุปกรณ์ที่มีความสำคัญ เพื่อให้สะดวกในการค้นหาหรือบริหารจัดการเส้นสายสัญญาณที่ต้องการ เช่น ในการแก้ไขปัญหาที่เกิดจากสายสัญญาณมีปัญหา เป็นต้น
   - ต้องกำหนดให้มีการทำผังสายสัญญาณหลักที่ใช้ในการสื่อสารระหว่างชั้นต่างๆ กับอุปกรณ์หลัก ให้ครบถ้วนและถูกต้องรวมทั้งปรับปรุงให้ทันสมัยเสมอ

- ต้องกำหนดให้มีการปิดล็อกห้องที่มีสายสัญญาณสื่อสารต่างๆ เพื่อป้องกันการเข้าถึงโดยบุคคลภายนอกหรือบุคคลที่ไม่มีสิทธิ์

6. ข้อกำหนดการบริหารจัดการข้อมูลภายในองค์กร (Organization Data Management)

วัตถุประสงค์

ข้อมูลถือว่าเป็นส่วนหนึ่งของสินทรัพย์สารสนเทศที่ต้องได้รับการป้องกันที่เหมาะสมสอดคล้องกับความสำคัญที่มีต่อองค์กร

ขอบเขต

ข้อมูลขององค์กรที่มีอยู่ในรูปแบบของเอกสารที่เป็นตั้งแต่ Hard copy Soft copy Database ในรูปแบบ Online และ Offline

หลักการ

การจัดหมวดหมู่ข้อมูล: ต้องมีการกำหนดหมวดหมู่ กำหนดระดับความสำคัญ. กำหนดชั้นความลับ และเจ้าของข้อมูลที่ชัดเจนทั้งองค์กร โดยให้ปฏิบัติตาม "กรอบและนโยบายการกำกับดูแลข้อมูลสำหรับองค์กร" ที่กำหนดขึ้นจากคณะกรรมการและคณะทำงานด้านการกำกับดูแลข้อมูลและการคุ้มครองข้อมูลส่วนบุคคล โดยจะครอบคลุมรายละเอียดดังนี้

1. การจัดหมวดหมู่ข้อมูล (Data Category) แบ่งเป็น Public Personal Business Secret Security
2. การกำหนดชั้นความลับข้อมูล (Data Classification) แบ่งเป็น Open Private Confidential Restricted High Restricted
3. การจัดลำดับความสำคัญของข้อมูล (Data Prioritization)
4. การเข้าถึงและดำเนินการข้อมูล (Data Access and Operation)
5. การสร้าง การรวบรวม และการจัดเก็บรักษาข้อมูล (Data Creation Acquisition and Store)
6. การสำรองข้อมูลหากเกิดเหตุฉุกเฉินโดยข้อมูลจะต้องสามารถใช้งานได้อย่างต่อเนื่อง
7. การเปิดเผยข้อมูลและการรักษาความลับข้อมูล (Data Disclosure and Confidentiality)
8. การจัดเก็บถาวรและการทำลายข้อมูล (Data Archival and Destroy)

การจัดเก็บข้อมูล สำรองข้อมูลและการกู้ข้อมูล

ข้อมูลที่สำคัญที่เกี่ยวข้องกับการดำเนินงานขององค์กรทั้งหมดที่เก็บรักษาอยู่ในเครื่อง คอมพิวเตอร์ของผู้ใช้งาน ผู้ใช้งานต้องดำเนินการทำการจัดเก็บไว้ในเครื่อง Server Cloud Server หรือ Network Drive ตามระบบสารสนเทศที่ผู้ใช้กำลังใช้บริการอยู่ เพื่อประโยชน์ต่อการปกป้องข้อมูล และการสำรองข้อมูลจากบริษัท โดยให้ปฏิบัติตาม "แนวปฏิบัติการจัดเก็บข้อมูล สำรองและกู้ข้อมูล"

การเปิดเผยข้อมูลองค์กร

ต้องกำหนดการควบคุมอย่างเหมาะสม เพื่อรักษาความลับและความปลอดภัยของข้อมูลองค์กรเป็นลายลักษณ์อักษร โดยมีรายละเอียดตาม "มาตราการควบคุมการเปิดเผยข้อมูลองค์กร"

7. ข้อกำหนดความมั่นคงปลอดภัยทางกายภาพ (Physical and Environmental Security)

การควบคุมการเข้าออกทางกายภาพ (Physical entry controls)

วัตถุประสงค์

เพื่อป้องกันไม่ให้บุคคลที่ไม่มีอำนาจเกี่ยวข้องเข้าถึง ล่วงรู้ข้อมูล แก้ไขเปลี่ยนแปลง หรือก่อให้เกิดความเสียหายต่อบริษัท

ขอบเขต

ห้องทำงาน และห้อง Server ขององค์กร

7.1 พื้นที่ Secure Areas

7.1.1 การกำหนดพื้นที่มั่นคงปลอดภัย (**Physical Security Perimeter**)

7.1.1.1 ต้องจัดสภาพแวดล้อมทางกายภาพในการป้องกันบุคคลภายนอกหรือผู้ประสงค์ร้ายบุกรุกเข้าถึงพื้นที่มั่นคงปลอดภัย

7.1.1.2 กำหนดพื้นที่หรือบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas) คือ

- ห้อง Data Center
- สำนักงานออฟฟิศที่เป็นพื้นที่สำหรับการจัดเก็บข้อมูลสำคัญ ยกเว้น สำนักงานประจำโครงการก่อสร้าง

7.1.2 การควบคุมการเข้า-ออกพื้นที่มั่นคงปลอดภัยของ Secure Areas

7.1.2.1 มีการติดตั้งระบบรักษาความปลอดภัยที่เหมาะสม เช่น เครื่องสแกนลายนิ้วมือ ใช้บัตรเข้าออก หรือการล็อคประตูทางเข้า-ออก

7.1.2.2 มีการติดตั้งระบบกล้องวงจรปิด CCTV ให้ครอบคลุมพื้นที่มั่นคงปลอดภัย

7.1.3 การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และเครื่องมือต่างๆ

7.1.3.1 มีการจัดแบ่งและบริหารพื้นที่ที่เป็นห้องทำงานและสิ่งอำนวยความสะดวกตามมาตราฐานความปลอดภัยในบริษัท

7.1.3.2 ต้องมีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ อัคคีภัย ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์ และธรรมชาติ

7.2 พื้นที่ทำงานของพนักงาน

7.2.1 บุคคลภายนอกหรือผู้ให้บริการภายนอกที่ต้องเข้า-ออกพื้นที่ ต้องได้รับอนุญาตผ่านบัตรชั่วคราว

7.2.2 มีการบันทึกการเข้า-ออกพื้นที่มั่นคงปลอดภัยในการเข้าพื้นที่

7.2.3 ต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดย เด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัว หรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยจากบุคคลที่ไม่ได้รับอนุญาต

7.2.4 พนักงานบริษัทต้องรับทราบว่าในพื้นที่ทำงานมีห้ามถ่ายภาพ และห้ามสูบบุหรี่ ในพื้นที่ทำงาน

7.2.5 ห้ามบุคคลภายนอกหรือผู้ให้บริการภายนอกพกพาอาวุธ วัตถุต้องห้าม หรือวัสดุที่อาจเป็นเชื้อเพลิงที่เป็นอันตราย ยกเว้นเครื่องใช้สำนักงานเข้ามาภายในพื้นที่มั่นคงปลอดภัย

7.2.6 ต้องมีการจัดพื้นที่หรือบริเวณส่งสิ่งของ (Loading Areas) หากเป็นไปได้ควรแบ่งแยกพื้นที่ที่เกี่ยวกับการทำงานเพื่อหลีกเลี่ยงการเข้าถึงของบุคคลภายนอกหรือผู้ไม่มีสิทธิ์

7.3 ห้อง Data Center

7.3.1 ต้องควบคุมให้เฉพาะผู้ที่มีสิทธิ์ หรือผู้ที่ได้รับอนุญาตสามารถเข้าออกในพื้นที่

7.3.2 ต้องกำหนดสิทธิ์ และช่วงเวลาในการผ่านเข้าออกพื้นที่

7.3.3 ต้องบันทึกการผ่านเข้าออกในพื้นที่ที่สำคัญ

7.3.4 ต้องดำเนินการทบทวนสิทธิ์อย่างน้อยปีละ 1 ครั้ง

7.3.5 ห้อง Data Center ต้องได้รับสิทธิ์เฉพาะฝ่าย IT และมีระบบ Access Control แยกจากระบบของอาคาร

7.3.6 มีระบบ Monitoring กล้อง CCTV เพื่อตรวจสอบย้อนหลังได้ในพื้นที่ทำงาน และก่อนเข้าห้อง Data Center

8. ข้อกำหนดในการปฏิบัติงานบนระบบสารสนเทศ

หลักการ

ฝ่าย IT ต้องรับผิดชอบทำข้อกำหนด แนวปฏิบัติงาน หรือคู่มือ อย่างใดอย่างหนึ่งของระบบสารสนเทศที่สำคัญ เพื่อป้องกันการเกิดการปฏิบัติงานด้านสารสนเทศที่ผิดพลาด และเพื่อให้สอดคล้องกับนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ

การควบคุมการเปลี่ยนแปลงระบบสารสนเทศ

1. กำหนดให้มีการควบคุมการเปลี่ยนแปลงสารสนเทศต้องมีการขออนุมัติจากผู้บังคับบัญชา ก่อนดำเนินการ โดยต้องมีแผนงาน และแผนสำรองข้อมูลสารสนเทศก่อนการเปลี่ยนแปลงสารสนเทศ
2. ก่อนทำการเปลี่ยนแปลงกับระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย ระบบคอมพิวเตอร์ ซอฟต์แวร์ หรือฐานข้อมูล โดยผู้ดูแลระบบฯ หรือผู้ให้บริการภายนอกต้องดำเนินการขออนุมัติการดำเนินการเปลี่ยนแปลงจากฝ่ายเทคโนโลยีสารสนเทศ
3. การเปลี่ยนแปลงกับระบบเครือข่าย ระบบคอมพิวเตอร์ ซอฟต์แวร์ หรือฐานข้อมูล โดยผู้ให้บริการภายนอกต้องได้รับการควบคุมดูแลจากผู้ดูแลระบบเทคโนโลยีสารสนเทศ
4. ให้ผู้ดูแลระบบปฏิบัติตาม "แนวปฏิบัติการบริหารจัดการการเปลี่ยนแปลง (Change Management)"

การควบคุมผู้ใช้งานและระบบสารสนเทศก่อนเริ่มเข้าใช้งาน

วัตถุประสงค์: เพื่อจำกัดการเข้าถึงข้อมูล และระบบสารสนเทศเฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

1. แนวปฏิบัติการพิสูจน์ตัวตนและรักษาดูแลบัญชีของระบบสารสนเทศ (Authentication Management)
2. แนวปฏิบัติการตั้งค่ารหัสผ่าน (Password Management)

การควบคุมผู้ใช้งานและเชื่อมต่อเข้าระบบสารสนเทศ

วัตถุประสงค์: เพื่อให้ผู้ใช้งานที่ได้รับอนุญาตสามารถปฏิบัติงานในระบบสารสนเทศต่างๆ โดยเชื่อมต่อเข้าระบบ Network ผ่าน WIFI LAN จากที่อาคารสำนักงาน หรือเชื่อมต่อจากนอกสถานที่เป็นการทำงานจากระยะไกล

1. แนวปฏิบัติการใช้ Network WIFI และ Internet
2. แนวปฏิบัติการทำงานระยะไกล (Remote working)

การบริหารจัดการระบบสารสนเทศให้มั่นคงปลอดภัย

วัตถุประสงค์: เพื่อให้ผู้ดูแลจัดการระบบสารสนเทศให้สามารถพร้อมใช้ได้ตลอดเวลา ปลอดภัย ปกป้องข้อมูล โดยมีการดูแลปฏิบัติการเฝ้าระวังและบันทึกข้อมูล log ที่เกิดขึ้นของกลุ่ม Server และ Network รวมถึงมีการวางแผนป้องกันความผิดพลาดจากสูญหายของข้อมูลและระบบ ด้วยการ Backup และ Restore

1. แนวปฏิบัติการเฝ้าระวัง และบันทึกข้อมูล log (Monitoring and Logging)

2. แนวปฏิบัติการสำรองข้อมูลและกู้ข้อมูล(Backup & Restore)
3. แนวปฏิบัติการป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware)
4. แนวปฏิบัติการควบคุมบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privileged Access Management)

การควบคุมการใช้งาน Computer Software และสิทธิ์การเข้าถึงข้อมูล

วัตถุประสงค์: เพื่อให้ผู้ใช้งานสามารถใช้ Computer Software และการ Access Data ตามสิทธิ์ที่ได้รับ

1. แนวปฏิบัติการใช้เครื่องคอมพิวเตอร์
2. แนวปฏิบัติการใช้งาน Tablet
3. แนวปฏิบัติการติดตั้งและใช้งาน Software
4. แนวปฏิบัติการใช้สิทธิ์การเข้าถึงข้อมูล (Data Access Right)

การควบคุมการสื่อสารระหว่างผู้ใช้งาน

1. แนวปฏิบัติการใช้ระบบ Email เพื่อการสื่อสารภายในองค์กร
2. แนวปฏิบัติการใช้ Chat เพื่อการสื่อสารภายในองค์กร

การควบคุมการพัฒนาโครงการ IT

ฝ่าย IT ต้องพิจารณาการแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน ว่าควรจะดำเนินการในโครงการหรือไม่ และเมื่อไร โดยประเมินถึงความคุ้มค่าของราคา และเฟสในการพัฒนาที่ควบคู่ไปกับความต้องการทางธุรกิจ หากพบว่าประเมินแล้วระบบสารสนเทศมีความสำคัญสูง ฝ่าย IT ควรแยกระบบการพัฒนาออกจากระบบการให้บริการจริง เพื่อป้องกันผลกระทบของการเปลี่ยนแปลงข้อมูล ซึ่งจะมีผลกระทบต่อการดำเนินงานในปัจจุบัน

การบริหารขีดความสามารถของทรัพยากรสารสนเทศ (Capacity Management)

1. ต้องมีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถของทรัพยากรสารสนเทศปัจจุบันอย่างสม่ำเสมอ ตามความเหมาะสมของทรัพยากรชนิดต่างๆ เพื่อวางแผนบริหารทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม
2. ต้องมีการวางแผนบริหารทรัพยากรสารสนเทศอย่างน้อยปีละ 1 ครั้ง ตามปีงบประมาณของบริษัท โดยพิจารณาจากความต้องการใช้งานทรัพยากรสารสนเทศในอนาคต สภาพการใช้งานทรัพยากรในปัจจุบัน การเปลี่ยนแปลงของเทคโนโลยี

9. แนวปฏิบัติการเฝ้าระวัง และบันทึกข้อมูล log (Monitoring and Logging)

วัตถุประสงค์

ระบบสารสนเทศต้องถูกออกแบบเพื่อสนับสนุนการบันทึกข้อมูล log เพื่อใช้ติดตามกรณีเกิดเหตุความมั่นคงปลอดภัยอย่าง

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ทุก Server ต้องมีการจัดตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization) เพื่อใช้ในการบันทึก log โดยจะต้องตั้งแหล่งเทียบเวลานาฬิกา เช่น โปรโตคอลเวลาเครือข่าย (Network Time Protocol) ให้เป็นไปตามมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อให้เวลาที่ปรากฏในบันทึกเหตุการณ์ (Event Log) ที่ได้จากระบบเทคโนโลยีสารสนเทศ และอุปกรณ์เครือข่ายคอมพิวเตอร์เป็นเวลาถูกต้อง ตรงกัน และสามารถนำไปใช้ในการตรวจสอบได้ ระบบคอมพิวเตอร์หรือระบบเครือข่ายต้องมีการเก็บบันทึกข้อมูล log ต้องบันทึกข้อมูลกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศ และเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่างๆ เพื่อประโยชน์ในการสืบสวนสอบสวนในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง รวมทั้งให้มีการวิเคราะห์ข้อมูล log ดังกล่าวอย่างสม่ำเสมอ และจัดการแก้ไขข้อผิดพลาดอย่างเหมาะสม
2. การบริหารจัดการข้อมูลเหตุการณ์ (Event Logging)
   - ผู้ดูแลระบบต้องจัดให้มีขั้นตอนการเฝ้าติดตามสังเกตการใช้งานระบบเทคโนโลยีสารสนเทศ และมีการติดตามประเมินผลการติดตามสังเกตดังกล่าวอย่างสม่ำเสมอ
   - ผู้ดูแลระบบต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นระยะเวลาไม่น้อยกว่า 90 วัน
   - ผู้ดูแลระบบต้องกำหนดให้มีการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆ ไม่ให้สามารถถูกแก้ไขโดยไม่ได้รับอนุญาต
   - ผู้ดูแลระบบต้องใช้ระบบและทีมผู้เชียวชาญในการวิเคราะห์ข้อมูล เพื่อใช้ในการป้องกัน และหรือแก้ไขปัญหาที่เกิดขึ้น

10. แนวปฏิบัติการใช้ระบบ Email เพื่อการสื่อสารภายในองค์กร

วัตถุประสงค์

ผู้ใช้ E-mail ของบริษัทภายใต้ชื่อโดเมน (Domain) ที่จดทะเบียนไว้คือ @pruksa.com หรือจดทะเบียนในชื่อของธุรกิจอื่นๆ ของบริษัท พนักงานบริษัทมีหน้าที่ปฏิบัติในการใช้ระบบ E-Mail โดยไม่ขัดกับนโยบายรักษาความมั่นคงปลอดภัย

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบจัดเตรียม E-mail เพื่อสามารถให้สามารถใช้งานทุกสถานที่ ทุกเวลา และทุกอุปกรณ์ ให้กับพนักงานตามความเหมาะสมของหน้าที่และความรับผิดชอบในการปฏิบัติงาน
2. ผู้ดูแลระบบต้องติดตั้งการคัดกรอง Spam Mail ประเภท Cloud Service ป้องกัน E-mail หลอกลวง และ E-mail โฆษณาต่างๆ
3. ผู้ดูแลระบบจะไม่จัดเตรียม E-mail ให้กับ Outsource หรือ vendor เว้นเสียแต่ว่าจะแจ้งเป็นลายลักษณ์อักษรที่โดยให้ชี้แจ้งความจำเป็น ระบุระยะเวลาในการใช้งาน และได้รับความเห็นชอบจากฝ่าย IT
4. ผู้ดูแลระบบจะปิดบัญชีผู้ใช้งาน E-mail ในกรณีที่ลาออก โดยจะถ่ายโอนสิทธิ์ไปยังพนักงานตามที่ต้นสังกัดแจ้งผ่าน ระบบ IT Help Desk Service และข้อมูลจะถูกเก็บไว้ 7 วัน ก่อนถูกลบทิ้ง ยกเว้นจะได้รับคำสั่งให้คงรักษาไว้เพื่อใช้ในการตรวจสอบข้อมูล

แนวปฏิบัติของผู้ใช้งาน

1. ห้ามมิให้ผู้ใช้งานแบ่งปัน E-mail ID ร่วมกับผู้ใช้งานอื่น
2. สำหรับ E-mail ส่วนกลางที่ใช้สำหรับงานเฉพาะ จะต้องได้รับการอนุมัติในใช้งานร่วมกัน จะต้องกำหนดผู้รับผิดชอบที่ชัดเจน
3. ห้ามปลอมแปลงชื่อบัญชีผู้ส่ง หรือบัญชีผู้ใช้งานอื่น
4. ต้องใช้ E-mail ด้วยภาษาเขียนที่สุภาพ ไม่ขัดต่อศีลธรรมอันดีงาม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี คุกคาม ข่มขู่ ส่อไปในทางผิดกฎหมาย
5. ห้ามส่งข้อความที่เป็นความคิดเห็นส่วนบุคคล โดยอ้างเป็นความเห็นของบริษัทฯ หรือก่อให้เกิดความเสียหายต่อบริษัทฯ
6. หน่วยงานของแต่ละ BU หากประเมินว่าพนักงานที่กำลังจะลาออกอาจจะมีพฤติกรรมที่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศให้ดำเนินการแจ้งกับฝ่าย HR ทันที่เพื่อให้เป็นตัวแทนประสานงานกับฝ่าย IT เพื่อดำเนินการตัดสิทธิ์การใช้งานบัญชีตามขั้นตอนของฝ่าย IT

11. แนวปฏิบัติการใช้งาน Storage เพื่อจัดเก็บข้อมูล

วัตถุประสงค์

บริษัทได้จัดเตรียมพื้นที่ในการจัดเก็บข้อมูลให้แก่พนักงาน Cloud Drive หรือ G: โดยแบ่งพื้นที่ออกเป็นส่วนต่างๆ เพื่อการทำงานส่วนตัวและการทำงานร่วมกัน จะถูกเรียกว่า Workspace สามารถทำงานได้ทั้ง online และ offline และมีระบบสำรองข้อมูลอัตโนมัติ ที่สามารถกู้คืนย้อนหลังได้สูงสุด 30 วัน

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบ จัดเตรียม Workspace เพื่อให้พนักงานสามารถจัดเก็บข้อมูลสำหรับการทำงาน ซึ่งพนักงานสามารถเข้าถึงโดยผ่าน online และ offline ได้ โดยใช้โปรแกรม Chrome หรือ Drive Desktop ตามลำดับ โดยพื้นที่จัดเก็บจะแบ่งออกเป็น 2 ส่วน และมี Disk Space รวมกันสูงสุดต่อคนไม่เกิน 300 GB ดังต่อไปนี้
    - My Drive: เป็น Workspace สำหรับพื้นที่ทำงานส่วนตัว
    - Share Drive: เป็น Workspace สำหรับพื้นที่ทำงานส่วนกลาง ผู้ใช้บริการ

แนวปฏิบัติของผู้ใช้งาน

1. พนักงานต้องรับผิดชอบบริหาร Workspace เพื่อเก็บไฟล์ของตนเองให้อยู่ใน Disk Space ที่กำหนด
2. พนักงานที่ใช้ My Drive สามารถกำหนดสิทธิ์ให้เข้าถึงข้อมูลของตนเอง กับคนในบริษัทได้ด้วยตนเอง
3. พนักงานที่ใช้ Share Drive จะไม่สามารถเพิ่มสิทธิ์ให้แก่ผู้ใช้อื่นใน Share Drive ได้เอง จำเป็นต้องแจ้งให้ผู้ดูแลระบบเป็นผู้ที่จะดำเนินการให้สิทธิ์นี้ และต้องผ่านกระบวนการอนุมัติจากเจ้าของข้อมูลก่อน
4. พนักงานต้องปฏิบัติตามนโยบายและแนวปฏิบัติเพื่อรักษาความลับและความปลอดภัยของข้อมูล ดังนั้น ห้ามแชร์ข้อมูลที่อาจเป็นอันตรายหรือข้อมูลที่สามารถเปิดเผยความลับบริษัท หรือส่วนตัว โดยให้ปฏิบัติตาม "มาตราการควบคุมการเปิดเผยข้อมูลองค์กร"
5. พนักงานควรใช้ Cloud Drive สำหรับทำงาน และจัดเก็บข้อมูลสำคัญ เพราะมีระบบช่วยป้องกันการเข้าถึงข้อมูลและกู้ข้อมูลจากการสูญหายได้

12. แนวปฏิบัติการใช้ Chat เพื่อการสื่อสารภายในองค์กร

วัตถุประสงค์

บริษัทจัดเตรียมการสื่อสารแบบ Real Time คือ google chat และส่งเสริมให้พิจารณาใช้ google Chat เป็นหลักในการสื่อสาร อย่างไรก็ตามสามารถใช้โปรแกรมอื่นๆ ได้แต่ต้องปฏิบัติตาม "ข้อควรระวังในการใช้สื่อสารแบบ Real Time" ที่ระบุไว้ใน แนวปฏิบัติการใช้ Chat เพื่อการสื่อสารภายในองค์กร

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบจัดเตรียม Google Chat ให้กับพนักงานทุกคนตาม E-mail
2. ผู้ดูแลระบบไม่ลงโปรแกรม line หรืออื่นๆบนเครื่องคอมพิวเตอร์ของบริษัท แต่จะแนะนำให้พนักงานใช้ Google Chat แทน

แนวปฏิบัติของผู้ใช้งาน

1. พนักงานสามารถใช้โปรแกรม Google Chat สื่อสารพูดคุยกับพนักงานภายในบริษัท เพราะเป็นระบบรักษาความปลอดภัยที่มีมาตรฐานสูง ระบบที่สามารถกำหนดสิทธิ์การเข้าถึง และการจัดการข้อมูลส่วนบุคคลและกลุ่มได้
2. พนักงานต้องตระหนักถึงความไม่ปลอดภัยด้านความลับข้อมูลขององค์กร ในการใช้โปรแกรม Line ดังนั้นต้องปฏิบัติตาม "ข้อควรระวังในการใช้สื่อสารแบบ Real Time"
3. ข้อควรระวังในการใช้สื่อสารแบบ Real Time
   - ความเป็นส่วนตัวและความลับ: ห้ามไม่ให้พนักงานสื่อสารข้อมูลอันเป็นความลับของบริษัท และข้อมูลที่บริษัทมีหน้าที่รักษาความลับ รวมถึงข้อมูลที่อยู่ภายใต้กฎหมาย PDPA
   - ความเหมาะสมของข้อมูลในกลุ่ม: ห้ามไม่ให้พนักงานส่งข้อมูลที่ฝ่าฝืนหรือละเมิดกฎหมาย เช่น เป็นภาพถ่ายหรือวิดีโอที่อาจมีความไม่เหมาะสมหรือก่อให้เกิดปัญหาทางการเมือง ข้อมูลส่วนบุคคลของลูกค้า
   - การสื่อสารกับลูกค้าหรือพันธมิตรธุรกิจ: พนักงานควรพิจารณาว่าการสื่อสารกับลูกค้าหรือพันธมิตรธุรกิจผ่าน Real Time ถือว่าเป็นการสื่อสารแบบไม่เป็นทางการ ดังนั้นเมื่อได้ข้อสรุปที่ควรจะเป็นแล้วควรใช้ E-mail ในการยืนยันอย่างเป็นทางการ

13. แนวปฏิบัติการทำงานระยะไกล (Remote Working)

วัตถุประสงค์

เพื่อส่งเสริมการทำงานแบบระยะทางไกล ฝ่าย IT จัดเตรียมการโยงการทำงานจากนอกสถานที่มายังระบบสารสนเทศภายในบริษัทได้อย่างต่อเนื่อง และมีความมั่นคงปลอดภัย โดยใช้เทคโนโลยีได้แก่ SSL VPN ซึ่งเป็นระบบสนับสนุนการทำงานดังกล่าว

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลออกแบบระบบให้มีช่องการติดต่อกับผู้ใช้งานโดยมีลำดับความสำคัญคือ Cloud Service Web Service (พัฒนาเอง) โดยต้องมีการใช้ SSL เพื่อเข้ารหัสข้อมูลระหว่างการรับส่ง และการระบบการพิสูจน์ตัวตนก่อนเข้าใช้งาน แต่หากพบว่าระบบที่พัฒนาไม่สนับสนุนโปรโตคอลดังกล่าวให้จัดหาระบบ VPN เพื่อใช้ทดแทน
2. ผู้ดูแลระบบจัดเตรียมบัญชี VPN ให้แก่ผู้ใช้งานระบบ ตามตำแหน่งหน้าที่ และความรับผิดชอบในการปฏิบัติงานของตนเอง โดยสามารถเข้าถึงสิทธิ์ต่างๆ จากนอกสถานที่ได้อย่างมั่นคงปลอดภัย โดยแบ่งออกเป็น พนักงานบริษัท outsource และ vendor จะแตกต่างกันโดยมีรายละเอียดดังนี้
   - พนักงานบริษัท: จะได้รับสิทธิ์ในวันที่เริ่มงาน เพื่อให้สามารถใช้งานระบบ VPN จนกว่าจะสิ้นสภาพการเป็นพนักงาน
   - Outsource: จะได้รับสิทธิ์ โดยมีพนักงานบริษัทที่จัดจ้าง Outsource เป็นผู้รับรอง และได้ขออนุมัติการใช้งานตามสายงาน และตามระยะเวลาในสัญญาจ้าง Outsource โดยให้แจ้งขอบัญชีผ่านระบบ IT Help Desk Service
   - Vendor: จะได้รับสิทธิ์โดยมีพนักงานบริษัทที่จัดจ้าง Vendor เป็นผู้รับรอง และขออนุมัติตามสายงาน โดยมีระยะเวลาการใช้งานสูงสุดไม่เกิน 30 วัน โดยให้แจ้งผ่านการขอบัญชีผ่านระบบ IT Help Desk Service
3. ผู้ดูแลระบบต้องออกแบบการเชื่อมระหว่างสถานที่ต่อสถานที่โดยพิจารณา VPN แบบ Site to Site โดยต้องมีกระบวนการพิสูจน์ตัวตนในการเชื่อมต่อระหว่างเครือข่ายบริษัท กับเครือข่ายภายนอกที่ได้รับอนุญาตเท่านั้น

แนวปฏิบัติของผู้ใช้งาน

1. ผู้ใช้งานห้ามเปิดเผย User และ Password ของ VPN แก่บุคคลอื่น หรือ มอบให้บุคคลอื่นเป็นตัวแทนใช้งาน
2. ผู้ใช้งาน VPN Account จะได้รับการใช้งานแต่ละระบบตามเดิมที่ได้รับจากตำแหน่งงานและหน้าที่ของตนเอง
3. การเปลี่ยน password ของ VPN เป็นไปตาม Password policy
4. พนักงานบริษัทต้องเป็นผู้รับผิดชอบผลการดำเนินงานของ Outsource และ Vendor และ หากมีการเปลี่ยนตัวผู้ใช้งาน หรือลาออกก่อนกำหนดต้องแจ้งฝ่าย IT เพื่อทำการระงับหรือยุติการใช้งาน

14. แนวปฏิบัติการใช้ Network WIFI และ Internet

วัตถุประสงค์

เพื่อควบคุมผู้ใช้งานบนเครือข่าย WIFI และ Internet ให้เป็นไปตามนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบต้องออกแบบระบบให้สามารถทำงานได้อย่างต่อเนื่อง และมีความมั่นคงปลอดภัยสารสนเทศ โดยจัดแบ่งแยกระบบเครือข่าย ตามกลุ่มของผู้ใช้งานอย่าง และ 3 Security Zone เป็นอย่างน้อย คือ Private Zone Public Zone และ DMZ Zone
2. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานมีการพิสูจน์ตัวตน ด้วยการใช้รหัสผ่าน (Password) ผ่านระบบActive Directory (AD)
3. ผู้ดูแลระบบการจำกัดเส้นทางการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน หรืออุปกรณ์กระจายสัญญาณ เพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น
4. ผู้ดูแลระบบต้องจัดอุปกรณ์เครือข่ายไว้ในห้องที่มีการควบคุมการเข้าถึง และจะเข้าได้เฉพาะผู้ที่ได้รับ อนุญาตเท่านั้น หรือล๊อคกุญแจเพื่อป้องกันการเชื่อมต่อโดยไม่ได้รับอนุญาต

แนวปฏิบัติของผู้ใช้งาน

1. ผู้ใช้งานจะใช้ username และ password เพื่อเข้าสู่เครื่องขายขององค์กร โดยสามารถใช้บนทุกอุปกรณ์เช่น คอมพิวเตอร์ Tablet และโทรศัพท์มือถือ
2. ผู้ใช้งานต้องรับผิดชอบต่อกิจกรรมที่เกิดขึ้นจากการใช้งานระบบเครือข่ายอินเตอร์เน็ต รวมถึงรับผิดชอบต่อข้อความ คำสั่ง โปรแกรม ซอฟต์แวร์ หรือ ไฟล์งาน ที่เกิดจากการเข้าใช้งานระบบอินเตอร์เน็ตของบริษัท
3. ผู้ใช้งานใช้เครือข่าย internet ของบริษัทเพื่อการทำงานของบริษัทเท่านั้น โดยมีข้อปฏิบัติการใช้งานดังต่อไปนี้
   - ห้ามกระทำการใดๆ เพื่อผลประโยชน์ส่วนตน เช่น เล่นเกมส์ ดาวน์โหลดไฟล์ที่มีขนาดใหญ่ ดำเนินธุรกรรมเพื่อประโยชน์ส่วนตน เป็นต้น หรือ กระทำการที่ผิดหลักจริยธรรม จัดสร้างหน้างานของตนเอง หรือการกระทำที่ไม่เหมาะสมอื่นๆ
   - ห้ามส่งต่อ หรือ จัดเก็บภาพ ข้อมูลลามก อนาจาร หรือข้อมูลที่ไม่เหมาะสมอื่นๆ
   - ห้ามมีส่วนร่วมในการ Post ข้อความผ่าน Social Media ที่ขัดแย้งกับนโยบายและระเบียบข้อบังคับของบริษัท
   - ห้ามทำการดาวน์โหลดโปรแกรมใช้งานที่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา
   - ห้ามกระทำการผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ หรือกฎหมายที่เกี่ยวข้อง

4. บุคคลภายนอกที่เป็น Vendor หรือ Outsource ที่มีสัญญาจ้างงานกับบริษัท หากจำเป็นต้องใช้งานระบบสารสนเทศขององค์กรให้พนักงานที่ดูแล Vendor หรือ Outsource ทำการส่งคำขอที่ได้รับการอนุมัติจากหัวหน้างานให้หน่วยงาน IT โดยในรายละเอียดคำขอต้องระบุระยะเวลาในใช้งานตามจำนวนวันในสัญญาจ้างแต่ไม่เกิน 90 วัน หากเกินวันดังกล่าวจะต้องดำเนินการส่งคำขอใหม่ทุกครั้ง
5. บุคคลภายนอกที่จำเป็นต้องใช้เครือข่าย internet ขององค์กร สามารถขอบริการ Password ชั่วคราวได้ที่ ตู้ KIOSK สร้างบัญชีผู้ใช้งานชั่วคราว ชั้น16 ของอาคาร Pearl โดยใช้บัตรประชาชนเพื่อยืนยันตัวตน โดยจะได้รับ User/password เพื่อใช้งาน 3 ชั่วโมง และได้รับสิทธิ์ในสถานะ Guest สามารถใช้ internet เท่านั้น ไม่สามารถเข้าสู่ระบบใดภายในบริษัทได้

15. แนวปฏิบัติการพิสูจน์ตัวตนและรักษาดูแลบัญชีของระบบ IT

วัตถุประสงค์

ก่อนที่จะสามารถเข้าใช้ระบบ IT ผู้ใช้งานต้องยืนยันว่าเป็นพนักงานบริษัท หรือ บุคคลได้รับการอนุญาต โดยต้องใช้บัญชีผู้ใช้งานและรหัสผ่าน (User/Password) เพื่อยืนยันตัวตน

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบ มีหน้าที่จะจัดเตรียม บัญชีผู้ใช้งาน และรหัสผ่าน (User/Password) ให้กับพนักงานทุกคน หรือบุคคลที่รับอนุญาตให้ใช้ระบบ (Outsource Vendor) ตามบทบาทและหน้าที่ ซึ่งได้รับการอนุมัติจากผู้เกี่ยวข้องตามระยะเวลาที่กำหนด
2. ผู้ดูแลระบบ มีหน้าที่ ปิดบัญชีผู้ใช้งาน หรือลบออกจากระบบเมื่อผู้ใช้งานพ้นสภาพพนักงาน หรือ ครบกำหนดการขอใช้งาน โดยผู้ดูแลระบบจะตรวจสถานะของพนักงานที่ถูกแจ้งพ้นสภาพในการดำเนินงานทุกวัน หรือได้รับแจ้งด่วนจากผู้มีอำนาจสูงสุดของฝ่าย IT
3. ผู้ดูแลระบบ จะดำเนินทบทวน และปรับปรุงข้อมูลของบัญชีผู้ใช้งานให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง และรายงานต่อผู้มีอำนาจสุงสุดของฝ่าย IT

แนวปฏิบัติของผู้ใช้งาน

1. ผู้ใช้งานระบบสารสนเทศมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ห้ามแจกจ่าย และทำให้ผู้อื่นล่วงรู้
2. พนักงานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม เว้นเสียแต่ว่ามีหลักฐานที่พิสูจน์ชัดเจนได้ว่าไม่ได้เป็นผู้กระทำ
3. บัญชีผู้ใช้งานและรหัสผ่าน (User / Password) ที่ได้รับอนุญาตเป็นชั่วคราวสำหรับ Outsource Vendor และ Trainee ระยะเวลาสูงสุดตามเอกสารสัญญาที่แนบ โดยต้องพนักงานบริษัทเป็นผู้ขอผ่านระบบ IT Help Desk Service ซึ่งถือเป็นพนักงานบริษัทที่รับรองนี้ต้องมีส่วนร่วมในความรับผิดชอบต่อการกระทำที่เกิดขึ้น
4. ห้ามลักลอบใช้รหัสผ่าน หรือแกะรหัสของผู้อื่น หรือการกระทำใดๆที่ได้มาซึ่งรหัสผ่านของผู้อื่น
5. แจ้งการละเมิดความปลอดภัยในระบบให้ผู้ดูแลระบบทราบทันที

16. แนวปฏิบัติการตั้งค่ารหัสผ่าน

วัตถุประสงค์

เพื่อสงวนสิทธิ์การเข้าใช้งานระบบสารสนเทศใดๆ ให้สามารถพิสูจน์ได้ว่าเป็นผู้มีสิทธิ์ และป้องกันการเดารหัสผ่านเพื่อแอบอ้าง จึงจำเป็นต้องกำหนดการตั้งค่ารหัสผ่านให้เหมาะสมในการดำเนินงาน

ขอบเขตการให้บริการและแนวปฏิบัติ

ผู้ดูแลระบบควรให้ระบบสารสนเทศผูกบัญชีผู้ใช้งานที่อ้างอิงกับระบบ Active Directory (AD) เพื่อลดภาระในการจดจำบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เสียแต่ว่าระบบดังกล่าวไม่อยู่ใน Environment ของระบบปฏิบัติการ Windows จึงเป็นเหตุให้แยกบัญชีผู้ใช้งาน เช่น ระบบ SAP ระบบ Lotus Note และ ระบบ Email เป็นต้น

1. ผู้ดูแลระบบต้องกำหนดให้ระบบสารสนเทศรองรับการตั้งรหัสตาม Password policy (ยกเว้นระบบสารสนเทศนั้นไม่ได้สนับสนุนการปรับแต่ง)
2. ผู้ดูแลระบบกำหนด password เริ่มต้นให้ชั่วคราว และกำหนดให้ผู้ใช้งานเปลี่ยน password ทันทีเมื่อเข้าใช้งานระบบครั้งแรก
3. ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย

แนวปฏิบัติของผู้ใช้งาน

ผู้ใช้งานระบบสารสนเทศต้องตั้งรหัสผ่านตาม Password policy ซึ่งกำหนดไว้ดังนี้

- รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร
- โดยผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน
- รหัสผ่านจะใช้ซ้ำกับครั้งก่อนๆ ไม่ได้จนกว่าจะผ่านการตั้งรหัสใหม่ไปแล้ว 5 ครั้ง
- รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลา ที่กำหนดไว้คือ 90 วัน

17. แนวปฏิบัติการใช้สิทธิ์การเข้าถึงข้อมูล (Data Access Right)

วัตถุประสงค์

1. ผู้ใช้ระบบจะได้รับสิทธิ์การใช้งานระบบตามระดับและบทบาทของผู้ใช้ที่แตกต่างกัน เพื่อให้ความสอดคล้องกับงานและความรับผิดชอบของแต่ละบุคคลในบริษัท
2. เพื่อให้มีการควบคุมการการขอใช้สิทธิ์เข้าถึงข้อมูลของระบบสารสนเทศ ระหว่างผู้ดูแลระบบและผู้ใช้งานระบบสารสนเทศมีแนวปฏิบัติที่ชัดเจนเป็นไปตามนโยบายจะมีรายละเอียดตาม “มาตราการควบคุมการใช้สิทธิ์การเข้าถึงข้อมูล”

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบจะกำหนดสิทธิ์ในการความเข้าถึงและการใช้งานของผู้ใช้ในระบบต่างๆ และรวมถึงขอบเขตการกระทำที่ผู้ใช้สามารถทำได้ในระบบนั้นๆ
2. ผู้ดูแลระบบกับ BU จะรับผิดชอบจัดทำตารางสิทธิ์สำหรับกลุ่มพนักงานในระบบ เพื่อใช้เป็นมาตราฐานในการกำหนดสิทธิ์ให้กับพนักงานตามกลุ่ม โดยจะมีการทบทวนร่วมกับฝ่าย IT ทุกๆ 1 ปี
3. ผู้ดูแลระบบจะรับผิดชอบในการให้สิทธิ์ ตามตารางสิทธิ์ที่กำหนดร่วมกันไว้ กรณีที่มีการขอสิทธิ์นอกเหนือจากที่ระบุในตารางสิทธิ์ จำเป็นต้องผ่านการอนุมัติผู้บังคับบัญชาของพนักงาน และเจ้าของข้อมูลของระบบนั้นๆ และเก็บบันทึกผลการเปลี่ยนแปลงพร้อมระบุสาเหตุผ่านระบบ IT Help Desk Service
4. ผู้ดูแลระบบมีความจำเป็นในการประเมินสิทธิ์ให้เหมาะสม รวมถึงเครื่องคอมพิวเตอร์และซอฟต์แวร์ที่ใช้อยู่ เมื่อพนักงานได้รับการปรับเปลี่ยนหน้าที่ หรือตำแหน่งงานใหม่

แนวปฏิบัติของผู้ใช้งาน

1. พนักงานต้องใช้สิทธิ์ระบบตามบทบาทที่ได้รับจากบริษัทหรือตำแหน่งงาน เพื่อรักษาความเข้าถึงข้อมูลที่เหมาะสมและลดความเสี่ยงในการกระทำผิดในระบบ
2. พนักงานสามารถเพิ่มสิทธิ์ของตนเองได้แต่ต้องได้รับ การอนุมัติผ่านผู้บังคับบัญชาของพนักงาน และเจ้าของข้อมูลของระบบนั้นๆ โดยแจ้งผ่าน ระบบ IT Help Desk Service
3. พนักงานต้องแจ้งให้ฝ่าย IT รับทราบหากพบว่าสิทธิ์ที่ได้รับไม่ถูกต้อง เนื่องจากเกินจากบทบาทหน้าที่ เพื่อให้ฝ่าย IT ตรวจสอบและทำการแก้ไข

18. แนวปฏิบัติการสำรองข้อมูลและกู้ข้อมูล (Backup & Restore)

วัตถุประสงค์

เพื่อป้องกันการสูญหายของข้อมูล และให้มั่นใจว่าระบบสารสนเทศอยู่ในสภาพพร้อมใช้งาน

หลักการ

1. ต้องจัดให้มีการดูแลอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิ์ภาพสามารถใช้งานได้ตลอดเวลา
2. ต้องกำหนดความถี่ในการทำการสำรองข้อมูลขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยง
3. ต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบเทคโนโลยีสารสนเทศ
4. ต้องมีกระบวนการสำรองข้อมูล และการกู้ข้อมูลของทุกระบบ ต้องมีการทำเอกสาร และมีการตรวจสอบและทดสอบเป็นระยะๆ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบต้องพิจารณาเครื่อง Server ที่เป็น Production และเป็น Server ที่สำคัญต่อ Core Business ต้องได้รับการสำรองข้อมูลวันละ 1 ครั้ง ทั้งหมด 7 วันและสามารถ Restore ย้อนหลังได้ครบทั้ง 7 วัน
2. ผู้ดูแลระบบต้องจัดทำกระบวนการสำรองข้อมูล และการกู้ข้อมูลของทุกระบบ เป็นเอกสาร และมีการตรวจสอบและทดสอบเป็นระยะๆ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์
3. ผู้ดูแลระบบต้องทดสอบสภาพพร้อมใช้ข้อมูลสำรอง โดยวางแผนและกู้ข้อมูลจากระบบสำคัญอย่างน้อยปีละ 1 ครั้ง
4. ฝ่าย IT และสายงานบริหารความเสี่ยงและความยั่งยืน ต้องกำหนดแผนงานในการจัดการทดสอบระบบ Disaster recovery plan (DRP) ปีละ 1 ครั้งเพื่อซักซ้อมการกู้ข้อมูลจากระบบสำคัญๆ เช่น ข้อมูลการขาย และข้อมูลบัญชี

19. แนวปฏิบัติการใช้เครื่องคอมพิวเตอร์

วัตถุประสงค์

บริษัทได้ดำเนินการสนับสนุนให้พนักงานได้มีการใช้งานเครื่องคอมพิวเตอร์ที่มีประสิทธิ์ภาพที่เหมาะสมกับตำแหน่งและภารกิจงานอย่างเต็มที่ โดยในกระบวนการนี้ได้มีการให้ความสำคัญกับการรักษาความลับและความปลอดภัยของข้อมูลที่เกี่ยวข้องกับบริษัทอย่างเคร่งครัด และบริษัทอนุญาตให้นำเครื่องส่วนตัว หรืออุปกรณ์อื่นๆ ของพนักงานมาใช้งานได้ แต่ต้องให้เป็นส่วนหนึ่งของขั้นตอนการดูแลรักษาที่มุ่งเน้นความเป็นอยู่อย่างปลอดภัยและมีความน่าเชื่อถือในทุกๆ ด้าน

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบ จัดเตรียมเครื่องคอมพิวเตอร์แบบเช่าใช้ สำหรับพนักงานโดยแบ่งออกเป็น 3 กลุ่มคือ โดยอ้างอิงนโยบายผู้ใช้งานระบบเทคโนโลยีสารสนเทศ
   - คอมพิวเตอร์ประจำสำหรับผู้ปฏิบัติในสำนักงาน
   - คอมพิวเตอร์ประจำห้องอบรม
   - คอมพิวเตอร์ประจำกลุ่ม Site งานก่อสร้าง และโรงงาน เป็นคอมพิวเตอร์ส่วนกลาง หรือแต่ละบุคคล ให้ คำนึงถึงความถี่ในใช้งาน และความคุ้มค่าในเช่าใช้เครื่องคอมพิวเตอร์
2. ผู้ดูแลระบบจัดหาคอมพิวเตอร์เช่าใช้ที่รวม license ของ Operating System และ MS Office ตลอดอายุสัญญา
3. ผู้ดูแลระบบจัดหาเครื่องคอมพิวเตอร์ที่มี Spec แตกต่างกันตามตำแหน่งและบทบาทหน้าที่ในการทำงานตาม "มาตราการจัดสรร Computer สำหรับพนักงานบริษัท"
4. ผู้ดูแลระบบ จะเปลี่ยนเครื่องคอมพิวเตอร์ใหม่ด้วยเงื่อนไขดังต่อไปนี้
   - เป็นเครื่องคอมพิวเตอร์ที่หมดอายุตามสัญญาการเช่า
   - พนักงานมีการเปลี่ยนหน้าที่ และตำแหน่งงาน
5. ผู้ดูแลระบบคอมพิวเตอร์กำหนดให้เครื่องคอมพิวเตอร์พักหน้าจอ (Screen Saver) แบบที่มีรหัสป้องกันทุก 15 นาที หรือล๊อคหน้าจอเมื่อไม่มีการใช้งาน
6. ผู้ดูแลระบบจะไม่ให้ลง software ที่ผิดลิขสิทธิ์ สำหรับการลง software พิเศษใดๆ ต้องการได้รับการอนุมัติ และมีสิขสิทธิ์ถูกต้องเท่านั้น

แนวปฏิบัติของผู้ใช้งาน

1. พนักงานบริษัท มีหน้าที่ตรวจสอบคอมพิวเตอร์ และอุปกรณ์และความพร้อมก่อนลงนามรับเครื่องคอมพิวเตอร์ หากมีจุดบกพร่องให้บันทึกเป็นข้อตกลงไว้ และพนักงานต้องระมัดระวังและดูแลทรัพย์สินของบริษัทฯ ที่ตนเองใช้งาน หากเกิดความสูญหายโดยประมาทเลินเล่อ ต้องรับผิดชอบชดใช้ต่อความเสียหายนั้น
2. พนักงานบริษัทมีหน้าที่คืนเครื่องคอมพิวเตอร์ เมื่อสิ้นสุดการเป็นพนักงาน โดยแจ้งเรื่องก่อน 7 วัน ที่มีผลการลาออก ถ้าไม่คืนพนักงานต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้น และถ้าหากมีความจำเป็นทำงานถึงวันสุดท้ายให้ทำเอกสารยืนยันมาให้ฝ่ายเทคโนโลยีสารสนเทศ โดยผู้จัดการในสายงานของพนักงานลงนามรับผิดชอบแทนพนักงาน
3. พนักงานบริษัท ที่ทำเครื่องคอมพิวเตอร์สูญหาย ต้องแจ้งฝ่าย IT ทันที เพื่อดำเนินการเปลี่ยนรหัสเข้าเครื่องคอมพิวเตอร์ใหม่ และพนักงานต้องรับผิดชอบค่าใช้จ่ายในกรณีเครื่องสูญหาย โดยนำเอกสารแจ้งความแนบในระบบ IT Help Desk Service
4. ผู้ใช้งานระบบสารสนเทศสามารถนำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้งานในบริษัทได้ แต่จำเป็นต้องทำการลงทะเบียนเพื่อใช้งานโดยแจ้งผ่าน ระบบ IT Help Desk Service และเครื่องคอมพิวเตอร์ที่ถูกนำมาใช้งานจะต้องมีสภาพความพร้อมที่เหมาะสมในการป้องกันการแพร่กระจายของไวรัสและรักษาความลับและปลอดภัยของข้อมูลบริษัทตามหัวข้อ "มาตราการควบคุมการใช้เครื่องคอมพิวเตอร์ส่วนตัว Tablet ส่วนตัว และมือถือ"
5. ห้ามพนักงานทำการ Format เครื่องคอมพิวเตอร์ของบริษัทด้วยตนเองเพื่อมีวัตถุประสงค์ในการลง software ที่ไม่ได้รับอนุญาต
6. กรณีที่ BU หรือ หน่วยงานประสงค์ได้รุ่นที่แตกต่างไปตามที่กำหนดไว้ ผู้บังคับบัญชาของ BU ต้องทบทวนถึงเหตุความจำเป็นอย่างแท้จริง โดยต้องวางแผนจัดเตรียมงบประมาณในส่วนนี้ และทำบันทึกขอแก่ฝ่าย IT โดยผู้บริหารสูงสุดของฝ่าย IT จะเป็นผู้ตัดสินใจตามความจำเป็น ผลกระทบต่อการทำที่ไม่เป็นตามข้อกำหนดและความมั่นคงปลอดภัยสารสนเทศ
7. การป้องกันอุปกรณ์ของผู้ใช้งานที่ไม่มีผู้ดูแล (Unattended User Equipment)
   - ผู้ใช้งานระบบสารสนเทศต้องป้องกันอุปกรณ์ไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ เครื่องคอมพิวเตอร์ และระบบเครือข่ายในช่วงเวลาที่ไม่ได้อยู่กับอุปกรณ์
   - ผู้ใช้งานระบบสารสนเทศต้องออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นการปฏิบัติงาน และปิดเครื่องคอมพิวเตอร์ทุกครั้ง เมื่อเสร็จสิ้นการปฏิบัติงานประจำวัน และหากเป็นเครื่อง Notebook ควรนำเก็บไว้ในตู้ที่มิดชิดและปลอดภัย เพื่อป้องกันการสูญหาย

8. การจัดระเบียบโต๊ะทำงาน และหน้าจออุปกรณ์สารสนเทศ (Clear Desk and Clear Screen Policy)
   - ข้อมูลความลับ หรือข้อมูลที่มีความสำคัญที่บันทึกอยู่ในรูปแบบกระดาษ หรือที่จัดเก็บในสื่อบันทึกข้อมูลทางอิเล็กทรอนิกส์ต้องมีการจัดเก็บอย่างปลอดภัยเมื่อไม่มีความจำเป็นต้องใช้งาน
   - เมื่อไม่ได้ใช้งานต้องล็อคหน้าจอคอมพิวเตอร์ด้วยรหัสผ่าน หรือระบบการยืนยันตัวตนอื่นๆ
   - เอกสารที่มีชั้นความลับ หรือเอกสารสำคัญต้องไม่วางทิ้งไว้บนโต๊ะทำงานตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน
9. กรณีที่เครื่องคอมพิวเตอร์สูญหาย ให้พนักงานบริษัทดำเนินการแจ้งความและนำเอกสารมายื่นให้กับฝ่าย IT พร้อมแจ้งรหัสเข้าคอมพิวเตอร์ และทำการ Reset ใหม่เพื่อป้องกันการเข้าถึงข้อมูลผ่านเครื่องคอมพิวเตอร์ที่สูญหายไป

20. แนวปฏิบัติการใช้ Tablet

วัตถุประสงค์

บริษัทจะเตรียมแท็บเล็ตสำหรับผู้บริหารและพนักงานเพื่อนำเสนอภาพลักษณ์ของบริษัทและการทำงานที่คล่องตัวเพื่อการบริการลูกค้าอย่างเต็มประสิทธิ์ภาพ

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบ จัดเตรียม Tablet แบบเช่าใช้ สำหรับผู้ใช้งานระบบสารสนเทศโดยแบ่งออกเป็น 3 กลุ่มคือ
   - กลุ่มผู้บริหารคณะกรรมการบริหาร บริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน)
   - กลุ่มพนักงานขาย (Android)
   - กลุ่มพนักงาน PC Cons (Android)
2. ผู้ดูแลระบบ จะเปลี่ยน Tablet ให้ใหม่ด้วยเงื่อนไขดังต่อไปนี้
   - เป็นเครื่องที่อายุมากกว่า 4 ปี และมีสภาพชำรุดใช้งานไม่ได้
   - ผู้ใช้งานระบบสารสนเทศมีการเปลี่ยนหน้าที่ และตำแหน่งงาน
3. ผู้ดูแลระบบจะจัดหาคู่ค้าเพื่อทำการเช่าซื้อ Tablet เป็นระยะเวลา 3 ปี โดยรวมค่า Sim Internet และตัวเครื่อง
4. ผู้ดูแลระบบจะจัดหา SIM พิเศษสำหรับกลุ่มเครื่องคณะกรรมการบริหาร บริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน) กรณีเครื่องหมดสัญญาเช่าแล้ว แต่ยังคงต้องใช้อินเตอร์เน็ตต่อ
5. ผู้ดูแลระบบ จะทำหน้าที่จำหน่ายเครื่องกรณี Tablet มีอายุมากกว่า 4 ปี และไม่มีคนใช้งาน
6. ผู้ดูแลระบบจะทำการแจกจ่าย Tablet ที่มีอยู่ในสต็อกให้แก่พนักงานใหม่เป็นอันดับแรก หากพบว่าไม่มี Tablet ที่พร้อมใช้งาน จะดำเนินการสั่งซื้อเพิ่มตามความเหมาะสม
7. กรณีที่ BU หรือ หน่วยงานประสงค์ได้รุ่นที่แตกต่างไปจากที่กำหนดไว้ ต้องทบทวนถึงเหตุความจำเป็นที่กระทบการดำเนินงานของตนเอง โดยต้องจัดเตรียมงบประมาณในส่วนนี้ และทำบันทึกขอแก่ฝ่าย IT โดยผู้บริหารสูงสุดของฝ่าย IT จะเป็นผู้ตัดสินใจตามความจำเป็นของงาน ผลกระทบต่อการทำที่ไม่เป็นตามข้อกำหนด และความมั่นคงปลอดภัยสารสนเทศ

แนวปฏิบัติของผู้ใช้งาน

1. พนักงานบริษัทเมื่อได้รับ Tablet จากการเช่าใช้บริการจากฝ่าย IT ซึ่งจะมีการคิดค่าใช้จ่ายกับต้นสังกัดของพนักงานบริษัท (Cost Center) โดยยี่ห้อและประเภทเครื่องคอมพิวเตอร์ ฝ่าย IT จะเป็นผู้จัดสรรให้เป็นตาม "มาตราการจัดสรร Tablet สำหรับพนักงาน"

2. พนักงานบริษัท มีหน้าที่ตรวจสอบ Tablet และอุปกรณ์และความพร้อมก่อนลงนามรับเครื่องคอมพิวเตอร์ หากมีจุดบกพร่องให้บันทึกเป็นข้อตกลงไว้ และพนักงานต้องระมัดระวังและดูแลทรัพย์สินของบริษัทฯ ที่ตนเองใช้งาน หากเกิดความสูญหายโดยประมาทเลินเล่อ ต้องรับผิดชอบชดใช้ต่อความเสียหายนั้น
3. พนักงานบริษัทมีหน้าที่คืนเครื่อง Tablet เมื่อสิ้นสุดการเป็นพนักงาน โดยแจ้งเรื่องก่อน 7 วันที่มีผลการลาออก ถ้าไม่คืนพนักงานต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้น และถ้าหากมีความจำเป็นทำงานถึงวันสุดท้ายให้ทำเอกสารยืนยันมาให้ฝ่ายเทคโนโลยีสารสนเทศ โดยผู้จัดการในสายงานของพนักงานลงนามรับผิดชอบแทนพนักงาน
4. พนักงานบริษัท ไม่สามารถซื้อ Tablet ถ้าพ้นสภาพพนักงานแล้วต้องส่งคืนเครื่องโดยตรงกับผู้ดูแลระบบ
5. พนักงานบริษัทต้องใช้เครื่อง Tablet ในงานของบริษัทเท่านั้น และปฏิบัติตาม "มาตราการควบคุมการเปิดเผยข้อมูลองค์กร"
6. คณะกรรมการบริหาร บริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน) จะได้รับ iPad เพื่อใช้ในการทำงานทุกท่าน และเมื่อสิ้นกำหนดการเช่าใช้แล้วตามสัญญา เครื่องดังกล่าวจะยกให้เป็นทรัพย์สินของผู้ใช้งาน และจะยังคงได้รับบริการด้าน Internet ไปจนกว่าจะหมดวาระ
7. คณะกรรมการบริหาร บริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน) ลาออก จะต้องคืนเครื่อง iPad หากอุปกรณ์ดังกล่าวยังอยู่ในสัญญาเช่า
8. การจัดหาเครื่องใหม่ทดแทน iPad ของคณะกรรมการบริหาร บริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน) ฝ่าย IT พิจารณาเงื่อนไข เครื่องที่มีอายุ 4 ปี ขึ้นไป และมีสภาพชำรุดและใช้งานไม่ได้ โดยเลขาคณะกรรมการเป็นแจ้งเป็นเอกสารขอแก่ผู้ดูแลระบบ

21. แนวปฏิบัติการติดตั้งและใช้งาน Software

วัตถุประสงค์

บริษัทจัดหา Software และกำหนดแนวทางปฏิบัติให้เป็นมาตรฐานเพื่ออำนวยความสะดวกในการทำงาน และรักษาความลับและความปลอดภัยของข้อมูล ผู้ดูแลระบบจะติดตั้ง Software กลุ่มมาตราฐาน และกลุ่มพิเศษตามตำแหน่งและหน้าที่ในการทำงาน

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบจะต้องติดตั้งเฉพาะที่ซอฟต์แวร์ที่จำเป็นในการใช้งาน และมี License ถูกต้องเท่านั้น
2. ผู้ดูแลระบบต้องทำให้คอมพิวเตอร์บริษัทจะต้องได้รับการติดตั้ง Anti-virus ทุกเครื่อง
3. ผู้ดูแลระบบจะติดตั้ง Software กลุ่มมาตราฐานตามที่ระบุไว้ "มาตราการควบคุมการติดตั้ง Software ทั่วไปและเฉพาะทาง"
4. ผู้ดูแลระบบจะติดตั้ง Software กลุ่มพิเศษเฉพาะทาง ตามที่ระบุไว้ "มาตราการควบคุมการติดตั้ง Software ทั่วไปและเฉพาะทาง"
5. ผู้ดูแลระบบจะติดตั้ง Software ที่ไม่อยู่ในกลุ่มมาตราฐาน กลุ่มพิเศษ กลุ่ม Open source และกลุ่มทดสอบ ก็ต่อเมื่อได้รับการอนุมัติจากผู้บริหารสูงสุดของฝ่าย IT
6. ผู้ดูแลระบบจะดำเนินการถอน Software ที่ไม่ได้รับอนุญาตดังกล่าวออกจากเครื่องคอมพิวเตอร์ของบริษัทฯ ในทันที

แนวปฏิบัติของผู้ใช้งาน

1. พนักงานห้ามติดตั้ง Software ใดๆ ด้วยตนเอง ความเสียหายอันเกิดจากการติดตั้งซอฟต์แวร์ที่ไม่เป็นไปตามข้อกำหนด พนักงานบริษัทฯ ผู้ถือครองเครื่องคอมพิวเตอร์ จะต้องเป็นผู้รับผิดชอบต่อค่าใช้จ่ายนั้น และถือว่ามีความผิดทางวินัย
2. พนักงานสามารถทำการแจ้งรายละเอียดเกี่ยวกับการติดตั้งซอฟต์แวร์เพิ่มเติมในกลุ่มมาตราฐาน กลุ่มพิเศษ กลุ่ม Opensource และกลุ่มทดสอบ ผ่านระบบ IT Help Desk Service โดยฝ่ายที่พนักงานสังกัดต้องมี license หรือ Free Software หากพบว่าไม่มี license และไม่ได้แจ้งให้ฝ่าย IT ตั้ง Budget ไว้ พนักงานต้องเป็นผู้จัดหางบประมาณที่กำหนดไว้ล่วงหน้าไว้ให้แล้ว
3. ผู้ใช้งานจะได้รับแจ้งจากผู้ดูแลระบบเรื่องการดำเนินการถอน Software ที่ไม่ได้รับอนุญาตออกจากเครื่องคอมพิวเตอร์ของบริษัทฯ และพนักงานจะต้องรับผิดชอบต่อการความเสียหายนั้นเช่น ค่าใช้จ่ายด้าน license เป็นต้น

22. แนวปฏิบัติการแจ้งคำร้องและคำขอรับบริการด้านระบบสารสนเทศ

วัตถุประสงค์

ฝ่าย IT นำระบบ IT Help Desk Service มาใช้บันทึกคำร้อง (incident) และคำขอ (request) เนื่องจากเป็นระบบที่มีคุณสมบัติครอบคลุม เช่น การติดตามงาน การมอบหมายงาน และการประเมินผลการให้บริการได้อย่างมีประสิทธิภาพ ซึ่งทำให้การช่วยเหลือด้านเทคโนโลยีเป็นไปอย่างมีระบบ และให้การสนับสนุนทางเทคโนโลยีแก่ผู้ใช้งานได้อย่างทันท่วงที

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบจัดเตรียม ระบบ IT Help Desk Service พร้อมใช้งานผ่าน Web Application หรือ รับสาย Call จากผู้ใช้งานในบริษัท
2. ผู้ดูแลระบบจัดเตรียมคลังข้อมูลและปัญหาที่พบบ่อยเพื่อให้ผู้ใช้งานสามารถค้นหาและแก้ไขปัญหาพื้นฐานด้วยตนเองได้ในขั้นต้น
3. ผู้ดูแลระบบจะรับเรื่องและแก้ไขปัญหาโดยมีขั้นตอนดังต่อไปนี้
   - รับคำขอหรือแจ้งปัญหาจากผู้ใช้งาน: คือผู้ใช้ เปิด ticket ใน ระบบ IT Help Desk Service
   - ประเมินและส่งต่อ: ฝ่าย IT Help Desk จะประเมินข้อมูลที่จำเป็นหากครบถ้วนจะส่งต่อไปยังผู้ดำเนินการอย่างเหมาะสม
   - วิเคราะห์และแก้ไข: ฝ่าย IT ดำเนินการตรวจสอบและวิเคราะห์แนวทางการแก้ไข และอาจจะติดต่อกับ User เพื่อ Remote แก้ไข หรือขอ Confirm ข้อมูล
   - ปิดงานและขอให้กรอกคำพึงพอใจ: เพื่อให้ฝ่าย IT ได้นำข้อมูลนี้ไปปรับปรุงคุณภาพการให้บริการ

แนวปฏิบัติของผู้ใช้งาน

1. ผู้ใช้งานระบบสารสนเทศสามารถเรียกใช้บริการผ่าน Web Application เพื่อขอเปิด Ticket ในระบบ IT Help Desk Service
2. ผู้ใช้งานระบบสารสนเทศสามารถ 02-080-1739 ต่อ 22 เพื่อแจ้งปัญหา หรือรับบริการเปิด Ticket ในระบบให้
3. ผู้ใช้งานระบบสารสนเทศสามารถติดตาม Status งานด้วยตนเองผ่าน ระบบ IT Help Desk Service หรือโทร 02-080-1739 ต่อ 22
4. ผู้ใช้งานสามารถแก้ไขปัญหาในเบื้องต้นด้วยตนเองผ่านการค้นหาคำตอบที่ Knowledge management ที่จัดเตรียมไว้

23. แนวปฏิบัติการใช้งาน Printer

วัตถุประสงค์

บริษัทเช่าระบบ Printer แบบ Multi-function ที่สามารถควบคุมการเข้าถึงการพิมพ์เอกสารได้อย่างมีประสิทธิภาพควบคุมค่าใช้จ่าย และป้องกันการนำเอกสารออกจากระบบโดยไม่ได้รับอนุญาต ดังนั้น ต้องใช้บัตรพนักงานเป็นตัวตรวจสอบและการเข้าถึงเครื่องพิมพ์ นอกจากการพิมพ์แล้วยังสามารถใช้งานฟังก์ชันการสแกนเอกสารเพื่อส่งไปยัง E-mail ของตนเอง และยังสามารถทำการถ่ายสำเนาเอกสารที่หน้าเครื่องได้

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบจะกำหนดให้บัตรพนักงานสามารถพิมพ์เอกสารได้ ทั้งบัตรชั่วคราว และบัตรประจำตัวพนักงาน
2. ผู้ดูแลระบบจะกำหนดสิทธิ์การพิมพ์ตามที่ได้รับมอบหมายจากฝ่าย HR โดยจะลง Driver ให้เครื่องคอมพิวเตอร์ของพนักงานทุกคน
3. ผู้ดูแลระบบจะจัดเตรียม Printer ไว้ตามชั้นต่างๆ ตามคำแนะนำจากฝ่าย HR

แนวปฏิบัติของผู้ใช้งาน

1. พนักงานสามารถใช้ Printer เพื่อการพิมพ์งานตามสิทธิ์ที่พึงได้ เช่น ขาวดำ และสี โดยผู้กำหนดจะเป็นฝ่าย HR โดยระบบจะบันทึกเป็นค่าใช้จ่ายแยกตาม Cost Center ของแต่ละหน่วยงาน
2. การพิมพ์เอกสารผ่านเครื่อง Multi-function ของ Printer พนักงานต้องใช้บัตรพนักงานในนำเอกสารการพิมพ์ออกจาก Printer และต้องไปเก็บเอกสารที่ใช้ในการพิมพ์ไว้เสมอ
3. การใช้กระดาษ Reuse ให้พิจารณาข้อความในเอกสาร ห้ามมีข้อมูลที่เป็นความลับทางการค้าขององค์กร

24. แนวปฏิบัติการบริหารจัดการการเปลี่ยนแปลง (Change Management)

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบต้องแจ้งให้ผู้ใช้งานทราบก่อนทุกครั้งก่อนทำการเปลี่ยนแปลงระบบ
2. ผู้ดูแลระบบ หรือผู้ให้บริการภายนอกต้องมีการประเมินผลกระทบของการเปลี่ยนแปลงระบบก่อนที่จะทำการเปลี่ยนแปลงนั้นเพื่อป้องกันผลกระทบกับการทำงานของระบบที่ใช้ดำเนินงานอยู่ในปัจจุบัน
3. ผู้ดูแลระบบต้องบันทึกรายละเอียดการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศผ่านช่องทางที่กำหนดไว้เช่น ระบบ IT Help Desk Service หรือระบบที่เหมาะสมกว่า
4. ผู้ดูแลระบบ หรือผู้ให้บริการภายนอกต้องมีการทดสอบการเปลี่ยนแปลงนั้นก่อนเสมอ โดยเฉพาะอย่างในกรณีเป็นระบบเทคโนโลยีสารสนเทศที่สำคัญ
5. ผู้ดูแลระบบ หรือผู้ให้บริการภายนอกต้องกำหนดแผนย้อนคืน (Fallback Plan) เพื่อรองรับหากการเปลี่ยนแปลงไม่เป็นไปตามที่คาดคิด
6. ผู้ดูแลระบบ หรือผู้ให้บริการจากภายนอกต้องกำหนดระยะเวลาในการติดตาม การเปลี่ยนแปลงนั้นเพื่อตรวจสอบผลกระทบที่อาจเกิดขึ้นกับระบบหลังจากการเปลี่ยนแปลง

25. แนวปฏิบัติการป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware)

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบต้องให้ทุกเครื่องคอมพิวเตอร์ในบริษัทต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสที่ได้รับการอัพเดตข้อมูลปัจจุบัน
2. ผู้ดูแลระบบต้องจัดการให้เครื่องคอมพิวเตอร์ทุกเครื่องในบริษัทมีการป้องกันไวรัสต้องมีการอัพเดทข้อมูลล่าสุดอยู่เสมอ
3. ผู้ดูแลระบบต้องตรวจสอบไฟล์แนบที่มากับจดหมายอิเล็กทรอนิกส์ (E-mail) หรือไฟล์ที่ได้รับมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรสก่อนใช้งาน
4. ผู้ดูแลระบบต้องบริหารจัดการช่องโหว่ทางเทคนิค โดยติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งาน และประเมินความเสี่ยงของช่องโหว่เหล่านั้น รวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว
5. ผู้ดูแลระบบต้องบริหารการกรองเว็บ (Web Filtering) คัดกรองดังต่อไปนี้
   - Website มุ่งร้ายที่หราบหรือเว็บไซต์ที่ต้องสงสัย เช่น เว็บไซต์ที่กระจายมัลแวร์หรือข้อมูลฟิชชิ่ง
   - Website แบ่งปันข้อมูลที่ผิดกฎหมาย
   - Website มุ่งร้ายที่ได้มาจากข่าวกรองด้านภัยคุกคาม

แนวปฏิบัติของผู้ใช้งาน

1. ผู้ใช้งานต้องระมัดระวังในการดาวน์โหลดแชร์แวร์ หรือฟรีแวร์โดยตรงจากอินเทอร์เน็ต
2. ผู้ใช้งานต้องตรวจสอบว่าเครื่องคอมพิวเตอร์ที่ใช้งานมีโปรแกรมป้องกันไวรัสที่อัพเดตข้อมูลเป็นปัจจุบัน หากพบว่าผิดปกติให้แจ้งผู้ดูแลระบบเพื่อทำการแก้ไข

26. แนวปฏิบัติการควบคุมบัญชีผู้ดูแลระบบที่มีสิทธิ์สูงสุด (Privileged Access Management)

บัญชีผู้ดูแลระบบ บาง Account จะมีสิทธิ์ในการจัดการและควบคุมการเข้าถึงข้อมูลและทรัพยากรสำคัญของระบบสารสนเทศได้ เพื่อสร้างความเชื่อมั่นแก่องค์กรว่า ผู้ดูแลระบบจะไม่ละเมิดข้อมูลความลับขององค์กร และข้อมูลส่วนบุคคล รวมถึงช่วยให้องค์กรสามารถลดความเสี่ยงที่เกิดจากภัยคุกคามภายใน การโจมตีจากภายนอก จึงเป็นการปกป้องทรัพย์สินที่สำคัญและรักษาการปฏิบัติตามนโยบาย

ขอบเขตการให้บริการและแนวปฏิบัติ

1. บัญชีผู้ดูแลระบบจะแบ่งเป็น 3 กลุ่ม ดังนี้ และ Privileged Access Account คือ บัญชีผู้ดูแลระบบที่มีสิทธิ์สูง จะต้องมีควบคุมอย่างเหมาะสม
   - Operational Account: เป็นบัญชีผู้ดูแลระบบที่ใช้ในการสร้าง User Account ปรับและเพิ่มสิทธิ์ของผู้ใช้งานต่อระบบสารสนเทศ Install / Remove Software
   - Agent Account: เป็นบัญชีผู้ดูแลระบบที่มีสิทธิ์พิเศษ ตามวัตถุประสงค์ที่สร้าง โดยผู้ใช้ Account นี้จะเป็นโปรแกรม
   - Privileged Access Account: เป็นบัญชีผู้ดูแลระบบที่มีสิทธิ์สูงสุด สามารถสร้างผู้ดูแลระบบต่างๆ และจัดการระบบสารสนเทศตั้งแต่ สร้างระบบ ปรับระบบ และลบระบบได้
2. ฝ่าย IT ต้องกำหนดบทบาทและความรับผิดชอบของผู้ดูแลระบบที่มีสิทธิ์สูง เช่น ผู้ดูแลระบบ (system administrators) และผู้ใช้งานระดับสูงอื่นๆ เป็น ตารางข้อมูล และปรับปรุงให้ทันสมัยเสมอ โดยให้อยู่ในการตัดสินใจของผู้บริหารสูงสุดของฝ่าย IT
   - ฝ่าย IT ต้องจัดแบ่งระบบเป็นส่วนๆ ระบุว่าการใช้บัญชีผู้ดูแลระบบที่มีสิทธิ์สูงสุดในระบบใดไม่ต้องผ่านขั้นตอนการขออนุญาต หรือต้องขอ และถ้าขออนุญาตต้องกำหนดว่าเป็นระดับใด
   - ฝ่าย IT ต้องมีระบบการตรวจสอบย้อนหลังได้ กรณีมีการตรวจสอบการปฏิบัติงานของการใช้บัญชีผู้ดูแลระบบที่มีสิทธิ์สูงสุด
   - ฝ่าย IT ต้องแยกให้ผู้ดูแลระบบมี 2 Account คือสำหรับผู้ดูแลระบบ และสำหรับการทำงานปกติ
3. ฝ่าย IT ควรจัดหาเทคโนโลยีที่เหมาะสม หรือกำหนดขั้นตอน เพื่อความปลอดภัยของใช้บัญชีผู้ดูแลระบบที่มีสิทธิ์สูงสุด โดยพิจารณาจากความคุ้มค่าการลงทุน และการประเมินความเสี่ยง โดยมีการกำหนดแนวทางดังนี้
   - Administrator Access Control: บัญชีผู้ใช้ที่มีสิทธิ์สูงสุด ต้องจำกัดการเข้าถึงเฉพาะให้กับบุคคลที่จำเป็น และกำหนดการขออนุญาต และระดับการอนุมัติตามความเหมาะสมของระบบสารสนเทศ
   - Secure Storage of Privileged Credentials: จัดเก็บบัญชีและรหัสผ่านสิทธิ์พิเศษในที่ปลอดภัย ทำให้ลดความเสี่ยงจากการงโมยข้อมูล

- Password Expiry and Rotation: ลดความเสี่ยงจากการใช้รหัสผ่านที่เก่าหรือการแอบแฝง โดยการตั้งค่าให้รหัสผ่านสิทธิ์พิเศษหมดอายุตามระยะเวลาที่กำหนด
- Just-In-Time Access: ลดความเสี่ยงจากการให้สิทธิ์ค้างยาวนาน กำหนดให้เข้าถึงสิทธิ์พิเศษได้เฉพาะในเวลาที่จำเป็นเท่านั้น
- Audit and Activity Recording: เพื่อให้สามารถตรวจสอบว่าใครเข้าถึงและดำเนินการใดๆ ไม่เป็นไปตามวัตถุประสงค์กรณีมีข้อสงสัยและเรียกตรวจสอบ จะต้องมีระบบ บันทึกและตรวจสอบการกระทำ

27. มาตราการจัดสรร Computer สำหรับพนักงาน

ชนิด	ประเภทการใช้งาน	คำอธิบายอย่างย่อ
PC02	คอมพิวเตอร์ตั้งโต๊ะสำหรับใช้งานทั่วไปและใช้งานกราฟฟิกพื้นฐาน	สำหรับพนักงาน Band 1-3 (งานออฟฟิศทั่วไป และงานกราฟฟิกพื้นฐาน) - โปรแกรมที่ใช้งาน เช่น MS Office Google Mail SAP PS Pro CSS MS Project Work Flow BPC TM1 S&OP Web App เป็นต้น - สำหรับงานที่มีความจำเป็นต้องใช้งานด้านกราฟฟิก 2 มิติและ 3 มิติ เช่น AutoCAD SketchUp ArcGIS Photoshop เป็นต้น
PC03	คอมพิวเตอร์ตั้งโต๊ะสำหรับใช้งานทั่วไปและใช้งานกราฟฟิกคุณภาพสูง	สำหรับพนักงาน Band 1-3 (งานกราฟฟิก 2 มิติและ 3 มิติระดับสูง) - โปรแกรมที่ใช้งาน เช่น Adobe Creative Cloud All App ALL Plan เป็นต้น
MAC02	คอมพิวเตอร์ตั้งโต๊ะสำหรับใช้งานกราฟฟิกคุณภาพสูง (iMac)	สำหรับพนักงาน band 2-4 (งานกราฟฟิก 2 มิติและ 3 มิติระดับสูง) - โปรแกรมที่ใช้งาน Adobe Creative Cloud All App เป็นต้น
NB01	โน้ตบุ๊คสำหรับใช้งานทั่วไป	สำหรับพนักงาน band 1-2 (งานออฟฟิศทั่วไป) - โปรแกรมที่ใช้งาน เช่น MS Office Google Mail SAP PS Pro CSS Work Flow Web App เป็นต้น
NB02	โน้ตบุ๊คสำหรับใช้งานทั่วไปและทำการวิเคราะห์ข้อมูลในปริมาณมาก	สำหรับพนักงาน band 1-5 (งานออฟฟิศทั่วไป และงานกราฟฟิกพื้นฐาน) - โปรแกรมที่ใช้งาน เช่น MS Office Google Mail SAP PS Pro CSS MS Project Work Flow BPC TM1 S&OP Web App เป็นต้น สำหรับงานที่มีความจำเป็นต้องใช้งานด้านกราฟฟิก 2 มิติและ 3 มิติ เช่น AutoCAD SketchUp ArcGIS Photoshop เป็นต้น
NB03	โน้ตบุ๊คสำหรับใช้งานทั่วไปและใช้งานกราฟฟิกระดับกลาง	สำหรับพนักงาน band 1-5 (งานออฟฟิศทั่วไป และงานกราฟฟิกระดับกลาง) - โปรแกรมที่ใช้งาน เช่น MS Office Google Mail SAP PS Pro CSS MS Project Work Flow Web App เป็นต้น - สำหรับงานที่มีความจำเป็นต้องใช้ดูแบบ 2 มิติ และ 3 มิติ - โปรแกรมที่ใช้งาน เช่น AutoCAD SketchUp Photoshop เป็นต้น - สำหรับพนักงานสังกัดบริษัทดังต่อไปนี้ - บริษัท ซินเนอร์จี โกรท จำกัด - บริษัท คลิก ซิ จำกัด - บริษัท มายเฮาส์ เทค จำกัด

ชนิด	ประเภทการใช้งาน	คำอธิบายอย่างย่อ
NB04	โน้ตบุ๊คสำหรับใช้งานทั่วไปและงานกราฟฟิกคุณภาพสูง	สำหรับพนักงาน band 2-5 (งานออฟฟิศทั่วไป และงานกราฟฟิกระดับสูง) - โปรแกรมที่ใช้งาน เช่น MS Office Google Mail SAP PS Pro CSS MS Project Work Flow Web App เป็นต้น - โปรแกรมที่ใช้งาน เช่น โปรแกรมที่ใช้งานเกี่ยวกับ Adobe Creative Cloud All App ALL Plan เป็นต้น
NB05	โน้ตบุ๊คสำหรับผู้บริหาร	สำหรับผู้บริหาร band 6 ขึ้นไป
MAC01	MacBook	สำหรับพนักงาน band 2-4 (งานกราฟฟิก 2 และ 3 มิติระดับสูง) - โปรแกรมที่ใช้งาน Adobe Creative Cloud All App เป็นต้น

28. มาตราการจัดสรร Tablet สำหรับพนักงาน

ชนิด	ประเภทการใช้งาน	คำอธิบายอย่างย่อ
TL01	Tablet สำหรับงานขาย	สำหรับใช้งานเสนอขาย จัดเก็บข้อมูลลูกค้า และเพื่อกิจกรรมส่งเสริมการขาย
TL02	Tablet สำหรับพนักงานฝ่าย PC Cons.	สำหรับใช้งานการการดำเนินงานติดตั้งแผ่น Precast บนระบบ I-Construction

29. มาตราการควบคุมการใช้เครื่องคอมพิวเตอร์ส่วนตัว Tablet ส่วนตัว และมือถือ

แนวปฏิบัติของผู้ใช้งาน

1. ลงทะเบียนและการอนุญาต
   - ผู้ใช้งานเครื่องคอมพิวเตอร์ส่วนตัว ต้องลงทะเบียนก่อนนำเครื่องคอมพิวเตอร์เข้ามาใช้งานในบริษัทผ่าน ระบบ IT Help Desk Service
   - ผู้ใช้งานมือถือ และ Tablet ไม่จำเป็นต้องลงทะเบียนแต่ให้ปฏิบัติตาม "การตรวจสอบความพร้อม"
2. การตรวจสอบความพร้อม
   - คอมพิวเตอร์ส่วนตัวที่นำมาใช้ในบริษัทจำเป็นต้องมีการติดตั้งโปรแกรม Anti-virus ของตนเองโดยอยู่ในสภาพที่พร้อมทำงานได้ตลอดเวลา
   - ผู้ใช้งานมือถือ และ Tablet จำเป็นต้องลงโปรแกรม Device Policy เมื่อต้องการใช้ระบบ Email เพื่อควบคุมเครื่องให้มีความพร้อมในการปกป้องข้อมูล
3. ยินยอมรับข้อกำหนดการใช้งานดังต่อไปนี้
   - เมื่อผู้ใช้งานดำเนินการเชื่อมต่อกับเครือข่ายของบริษัท หรือเข้าถึงแอปพลิเคชัน หรือข้อมูลบริษัทต้องเป็นไปตามหลักเกณฑ์และข้อกำหนดที่ได้รับมอบหมายในการทำงาน ห้ามทำการเชื่อมต่อไปยังระบบอื่นๆ ที่ไม่ได้ระบุไว้
   - ผู้ใช้งานห้ามนำข้อมูลของบริษัทเก็บไว้ที่เครื่องคอมพิวเตอร์ส่วนตัว เว้นเสียแต่ว่าจะทำงานชั่วคราว และต้องดำเนินการลบทิ้งเมื่อใช้งานเสร็จแล้ว
   - ผู้ใช้งานห้ามนำเครื่องมือส่วนตัวที่มีซอฟต์แวร์ที่ละเมิดลิขสิทธิ์เข้ามาใช้งานในบริษัท หากมีความเสียหายที่เกิดจากการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบ

30. มาตราการควบคุมการติดตั้ง Software ทั่วไปและเฉพาะทาง

Standard Software

No.	รายการ
1	Window 10 Pro x64
2	Microsoft Office
3	Adobe Reader 11
4	Front Pack 11
5	IZArc
6	Java (up to date)
7	Vstor_redist
8	K-LITE MEGA CODEC PACK
9	VLC Media Player
10	Lotus Notes
11	Team Viewer 11
12	Front Pruksa (เลือก All Users)
13	Google Chrome
14	Star CAT Agent
15	VPN Check Point
16	TIFF viewer
17	VIA Software
18	PhotoViewer
19	GoogleDriveFSSetup (Drive G:)
20	CrowdStrike Antivirus
21	All Driver Fuji
22	iCon PRD
23	Icon2017_x64 (Copy Folder ไปไว้ C:\Windows แล้ว Send to Desktop ด้วย)
24	Fuji Printer (Ysoft_client)
25	.NET Framework 3.5
26	SMB 1.0
27	SMB Direct
28	Telnet Client
29	TFTP Client

Special Software

No.	รายการ
1	Microsoft Office 356 Business STD
2	Microsoft Office 356 Enterprise
3	Autodesk Civil 3D
4	Autodesk AutoCAD LT
5	Autodesk including
6	SketchUp Pro
7	Microsoft Project STD
8	Microsoft Project Pro
9	Adobe Acrobat Pro
10	Adobe Creative Cloud All Ap
11	Adobe Photoshop
12	Adobe illustrator
13	ArcGIS
14	Tableau
15	BPC ERP
16	GStarCAD
17	Lumion
18	All Plan Planbar

31. มาตราการควบคุมการเปิดเผยข้อมูลองค์กร

วัตถุประสงค์

เพื่อให้ข้อมูลที่ถูกนำไปเปิดเผยผ่านการคัดกรองและไตร่ตรองอย่างอย่างเหมาะสม ซึ่งเป็นส่วนหนึ่งที่สำคัญในการรักษาความลับข้อมูลขององค์กร

ขอบเขตการให้บริการและแนวปฏิบัติ

1. ผู้ดูแลระบบจะปฏิบัติตาม "กรอบและนโยบายการกำกับดูแลข้อมูลสำหรับองค์กร" ที่กำหนดโดยคณะกรรมการและคณะทำงานด้านการกำกับดูแลข้อมูลและการคุ้มครองข้อมูลส่วนบุคคล
2. ผู้ดูแลระบบจะกำหนดสิทธิ์และระดับการเข้าถึงข้อมูลสำหรับบุคคลภายในองค์กร โดยให้สิทธิ์เฉพาะเจาะจงตามบทบาทหรือความจำเป็น และจำกัดการเข้าถึงข้อมูลให้เฉพาะผู้ที่มีความจำเป็นเท่านั้น โดยอ้างอิงจาก “มาตราการควบคุมการใช้สิทธิ์การเข้าถึงข้อมูล”

แนวปฏิบัติของผู้ใช้งาน

1. พนักงานบริษัทต้องความเข้าใจและปฏิบัติตาม"กรอบและนโยบายการกำกับดูแลข้อมูลสำหรับองค์กร" และปฏิบัติตาม "มาตราการควบคุมการเปิดเผยข้อมูลองค์กร"
2. พนักงานบริษัทต้องตระหนักถึงความสำคัญของข้อมูล ดังนี้

- ผู้ใช้งานระบบสารสนเทศการสร้างข้อมูลใดๆ ในบริษัท ข้อมูลเหล่านั้นถูกพิจารณาว่าเป็นทรัพย์สินสารสนเทศของบริษัท พนักงานต้องปฏิบัติต่อข้อมูล ด้วยความระมัดระวังในการแจกจ่ายข้อมูล โดยให้ตระหนักว่าจะเปิดเผยข้อมูลผ่านการแชร์ให้กลุ่มผู้รับที่มีความจำเป็นต้องรับรู้รับทราบในข้อมูลนั้นเท่านั้น
- ห้ามผู้ใช้งานระบบสารสนเทศเข้าถึงข้อมูลและแก้ไขข้อมูลโดยไม่ได้รับอนุญาต: บริษัทกำหนดสิทธิ์และการอนุญาตให้เข้าถึงอย่างเหมาะสมแล้ว ผู้ใช้งานควรได้รับอนุญาตเฉพาะตามบทบัญญัติที่เกี่ยวข้องกับงานของพวกเขา และต้องมีหลักฐานการเข้าถึงข้อมูลโดยได้รับอนุญาตจากเจ้าของข้อมูลผ่าน ระบบ IT Help Desk Service ก่อน
- ห้ามผู้ใช้งานเปิดเผยข้อมูลความลับ: การเปิดเผยข้อมูลที่เกี่ยวข้องกับความลับเป็นความผิดทางวินัย ทุกคนควรรับรู้ถึงความลับของข้อมูลและมีความรับผิดชอบในการรักษาความลับนั้นๆ ไม่ว่าจะเป็นข้อมูลธุรกิจ เอกสารทางการเงิน แผนภูมิกลยุทธ์ หรือข้อมูลส่วนบุคคลของลูกค้า รวมทั้งข้อมูลที่เป็นส่วนตัวของพนักงาน รายละเอียดอยู่ในหัวข้อ "พนักงานต้องรับทราบรายการข้อมูลที่ห้ามเปิดเผยแก่ภายนอกบริษัท"

- ห้ามผู้ใช้ทำการสำเนาหรือนำข้อมูลใดๆ ของบริษัทไปใช้เพื่อเอื้อให้กับประโยชน์ส่วนตัว ที่ไม่เกี่ยวข้องกับการดำเนินธุริจกิจขององค์กร: ผู้ใช้งานที่มีสิทธิ์ใช้ข้อมูลนั้น ห้ามนำข้อมูลบริษัทไปใช้เพื่อสร้างประโยชน์ส่วนตัว เช่น การเอื้อประโยชน์ให้กับคู่ค้าบางรายในการประมูล หรือการกระทำใดๆที่ทำให้เกิดความเปราะบางต่อข้อมูลและการต่อรองทางธุรกิจ
- ห้ามผู้ใช้งานห้ามทำให้ข้อมูลเกิดความเสียหายหรือความเสี่ยง: ผู้ใช้งานที่มีสิทธิ์ใช้ข้อมูลบริษัทนั้น ห้ามสร้างความเสียหายกับข้อมูลของบริษัท รวมถึงการนำข้อมูลไปใช้ในทางที่อาจเสี่ยงต่อความปลอดภัยหรือความเป็นส่วนตัว

3. พนักงานต้องรับทราบรายการข้อมูลที่ห้ามเปิดเผยแก่ภายนอกบริษัทดังต่อไปนี้

- ข้อมูลส่วนบุคคล: ข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของบุคคลอื่น ซึ่งอาจมีข้อมูลส่วนตัว เช่น ชื่อเต็ม ที่อยู่ เลขประจำตัวประชาชน หมายเลขโทรศัพท์ ฯลฯ
- ข้อมูลทางการเงิน: ข้อมูลที่เกี่ยวข้องกับการเงินของบริษัทหรือลูกค้า เช่น ข้อมูลบัญชีธนาคาร เลขบัตรเครดิต
- ความลับธุรกิจ: ข้อมูลที่เกี่ยวข้องกับความลับของธุรกิจ เช่น แผนธุรกิจ กลยุทธ์การตลาด ข้อมูลลูกค้าที่ไม่เปิดเผย
- ข้อมูลเทคโนโลยีและรหัส: ข้อมูลเกี่ยวกับเทคโนโลยี รหัส หรือคีย์เข้ารหัส เช่น รหัสเข้าสู่ระบบ รหัสผ่าน
- ข้อมูลที่เป็นความลับตามกฎหมาย: ข้อมูลที่ต้องเก็บเป็นความลับตามกฎหมาย เช่น ข้อมูลทางการแพทย์ ข้อมูลทางกฎหมาย
- ข้อมูลที่มีลิขสิทธิ์: ข้อมูลที่มีลิขสิทธิ์เช่น ภาพถ่าย เนื้อหาสร้างสรรค์
- ข้อมูลที่มีความลับตามสัญญา: ข้อมูลที่เป็นความลับตามสัญญาหรือข้อตกลง
- ข้อมูลเอกสารภายในบริษัทที่สำคัญ: เช่น เอกสารเทียบราคากลาง P3

32. มาตราการควบคุมการใช้สิทธิ์การเข้าถึงข้อมูล

อ้างอิง

IT Knowledge Management ที่ใช้งานภายในองค์กร

แนวการปฏิบัติร่วมกันภายในฝ่าย IT

เมื่อผู้ใช้งานระบบสารสนเทศต้องการขอสิทธิ์เพิ่มให้ฝ่าย IT ในส่วนต่างๆ ปฏิบัติงานร่วมกันผ่าน ระบบ IT Help Desk Service ตามมาตรการดังภาพที่แนบ