บริษัท เอเชียนน้ำมันปาล์ม จำกัด (มหาชน)
ASIAN PALM OIL PUBLIC COMPANY LIMITED
99 หมู่ที่ 2 ตำบลอ่าวลึกใต้ อำเภออ่าวลึก จังหวัดกระบี่ 81110
TEL : +66(0) 75 681 355 E-MAIL : INFO@ASIANPALMOIL.COM
เลขประจำตัวผู้เสียภาษี : 0107566000275

นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

1. ผู้รับผิดชอบ

- ฝ่ายเทคโนโลยีสารสนเทศ
- ผู้ดูแลระบบที่ได้รับมอบหมาย

2. นิยาม

1) บริษัท หมายถึง บริษัท เอเชียนน้ำมันปาล์ม จำกัด (มหาชน)
2) Active Directory Server (AD) หมายถึง เครื่องเซิฟเวอร์ที่ทำหน้าที่เก็บข้อมูลเกี่ยวกับ Object ต่างๆ เช่น ผู้ใช้งาน (User) กลุ่ม (Group) คอมพิวเตอร์ (Computer) หรือนโยบายรักษาความปลอดภัย (Security Policy) เป็นต้น
3) “ฝ่ายเทคโนโลยี” หมายความว่า ฝ่ายเทคโนโลยี ของ บริษัท เอเชียนน้ำมันปาล์ม จำกัด (มหาชน)
4) “ส่วนจัดการอาคารและบริเวณ” หมายความว่า ส่วนจัดการอาคารและบริเวณ ของ บริษัท เอเชียนน้ำมันปาล์ม จำกัด (มหาชน)
5) “ผู้ใช้งาน” หมายความว่า กรรมการบริษัท ผู้บริหาร ผู้ใช้งาน ผู้ใช้งานภายนอก และผู้ใช้งานภายนอก ที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเครือข่ายของ
6) “ผู้ใช้งานภายนอก” หมายความว่า บุคคล หรือนิติบุคคลที่เป็นคู่สัญญาของบริษัท ที่เข้ามาดำเนินกิจกรรมภายในบริษัท
7) “ผู้ดูแลระบบ” หมายความว่า ผู้จัดการฝ่ายเทคโนโลยี หรือผู้ใช้งานอื่น ที่ได้รับมอบหมายจากผู้บังคับบัญชาระดับผู้บริหารสายงานบริหาร (Chief Administrative Officer) ขึ้นไป ให้มีหน้าที่รับผิดชอบในการพัฒนา แก้ไข ปรับปรุง และดูแล รักษาระบบสารสนเทศ และระบบเครือข่าย ที่ใช้งานอยู่ในบริษัท หรือหน่วยงานที่มีหน้าที่ และรับผิดชอบในการดูแลระบบสารสนเทศ และระบบเครือข่าย โดยตรง
8) “สารสนเทศ” หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ เอกสาร แผนผัง แผนที่ ภาพถ่าย ฟิล์ม การบันทึกภาพ การบันทึกเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
9) “ระบบสารสนเทศ” หมายความว่า ระบบงานของบริษัท ที่ใช้จัดเก็บ ประมวลผลข้อมูล และเผยแพร่สารสนเทศซึ่งทำงานประสานกันระหว่างฮาร์ดแวร์ ซอฟท์แวร์ ข้อมูล ผู้ใช้งาน และกระบวนการประมวลผล ให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร และการสนับสนุนกลไกการทำงานของบริษัท

10) “ระบบเครือข่าย” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของบริษัท ได้ เช่น ระบบ LAN ระบบ Wireless ระบบ Intranet ระบบ Internet และระบบการสื่อสารอื่นๆ

11) “สินทรัพย์” หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับ บริษัท ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ บุคลากร ฮาร์ดแวร์ ซอฟท์แวร์ คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์ระบบเครือข่าย เลขไอพี หรือซอฟท์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อบริษัท

12) “ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ” หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายของบริษัท โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้าม ปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

13) “สิทธิ์ของผู้ใช้งาน” หมายความว่า ระดับชั้นของการเข้าถึงข้อมูลสารสนเทศของผู้ใช้งาน และผู้ใช้งานภายนอก ได้แก่ สิทธิ์ทั่วไป สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ และระบบเครือข่ายของบริษัท

14) “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ

15) “บัญชีผู้ใช้งาน” หมายความว่า บัญชีรายชื่อ (Username) และรหัสผ่าน (Password) สำหรับผู้ใช้งานผู้ใช้งานภายนอก และผู้ใช้งานภายนอก

16) “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือ เครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

17) “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ซึ่งอาจทำให้ระบบของบริษัทถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

18) “การเข้ารหัส (Encryption)” หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ ข้อมูลผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้ จะต้องมี โปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

19) “การยืนยันตัวตน (Authentication)” หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไปแล้ว เป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน

20) “SSL (Secure Socket Layer)” หมายความว่า เทคโนโลยีการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์หรือ Application ที่ใช้งาน

21) “VPN (Virtual Private Network)” หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยใช้การรับส่งข้อมูลจริง ซึ่งในการรับส่งข้อมูลจะทำการเข้ารหัสเฉพาะ โดยผ่านเครือข่ายอินเทอร์เน็ตทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

3. สาระสำคัญของแนวทางปฏิบัติ

3.1 การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

- **ฝ่ายเทคโนโลยีสารสนเทศ แบ่งแยกอำนาจหน้าที่ ดังนี้**
  - ผู้บริหารระดับสูง ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท
  - ผู้จัดการฝ่ายเทคโนโลยี ต้องกำหนดมอบหมายหน้าที่ให้กับผู้ใช้งานในฝ่ายเทคโนโลยี รับผิดชอบการดูแลระบบสารสนเทศที่บริษัทใช้งานให้มีความมั่นคงปลอดภัยของระบบสารสนเทศ และควบคุมการปฏิบัติงาน เพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท
  - ผู้จัดการฝ่ายเทคโนโลยี เป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแล ติดตาม และทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท
  - ผู้ใช้งานฝ่ายเทคโนโลยี ที่ได้รับมอบหมายเป็นผู้ดูแลระบบระดับ Administrator รับผิดชอบต่อระบบที่ดูแลนั้น จะต้องทำหน้าที่ตรวจสอบดูแลระบบความปลอดภัยในการใช้งานของระบบด้วย และเมื่อมีสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด จะต้องดำเนินการแก้ไขและรายงานต่อผู้บังคับบัญชา
  - ผู้ใช้งาน และหน่วยงานทั้งภายในและภายนอก ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของบริษัท ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท รวมทั้งจะต้องไม่กระทำการละเมิดต่อกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- ส่วนบริหารระบบ (System Administrator) บริษัท มีบุคลากรที่คอยดูแลระบบคอมพิวเตอร์ภายใน และมีบุคลากรสำรองในตำแหน่งเจ้าหน้าที่คอมพิวเตอร์ (it support) หากในกรณีจำเป็นสามารถทำงานทดแทนกันได้

- ส่วนของระบบงาน บริษัท ได้เช่าใช้บริการซอฟต์แวร์ผ่านทางเว็บไซต์ ได้แก่ โปรแกรมบัญชี TRCLOUD โปรแกรมซ่อมบำรุง Factorium โปรแกรมบริหารงานบุคคล Tigersoft โปรแกรมเครื่องชั่งน้ำหนัก Quick Weight Enterprise, Headquarters System, Grader ซอฟต์แวร์ Google Workspace
- บุคลากรในฝ่ายเทคโนโลยีสารสนเทศมี Job Description (JD) ซึ่งระบุหน้าที่ความรับผิดชอบของแต่ละหน้าที่งานอย่างชัดเจน

3.2 การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)

3.2.1 การควบคุมการเข้าออกศูนย์คอมพิวเตอร์

- บริษัท มีศูนย์คอมพิวเตอร์โดยผู้ที่เข้าได้มีเพียงผู้ดูแลระบบ (System Administrator) เท่านั้นหากพนักงานในฝ่ายเทคโนโลยีสารสนเทศ หรือบุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องจะต้องขออนุญาตผู้ดูแลระบบ (System Administrator) และลงบันทึกการเข้าใช้ห้องเซิฟเวอร์ในบันทึกทุกครั้ง
- บริษัท จัดให้มีตู้เซิฟเวอร์ไว้เก็บอุปกรณ์เครือข่ายและเครื่องเซิฟเวอร์ ซึ่งมีการล๊อคกุญแจป้องกันความปลอดภัยจากบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึง โดยมีกุญแจ 3 ชุดซึ่งจะเก็บไว้ที่หัวหน้าแผนกเทคโนโลยีสารสนเทศ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ รองประธานเจ้าหน้าที่บริหารสายงานบัญชีและการเงิน คนละ 1 ชุด และระบบ Access Control
- เพิ่ม/แก้ไข/ลบ สิทธิการเข้าถึงห้องคอมพิวเตอร์ โดยผู้มีอำนาจจัดการที่ได้รับการแต่งตั้งอนุมัติ ทำการเพิ่มลายนิ้วมือที่เครื่องสแกนนิ้วหน้าห้องควบคุมคอมพิวเตอร์ พิจารณาตามความเหมาะสม ตำแหน่งหน้าที่ ที่เกี่ยวข้อง
- ต้องมีระบบเก็บบันทึกการเข้าออก Data Center Room โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคลและเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
- ห้ามนำอาหาร เครื่องดื่ม รวมถึงอุปกรณ์ที่ไม่เกี่ยวข้องเข้าไป หรือนำไปจัดเก็บไว้ภายในห้อง Data Center

3.2.2 การป้องกันความเสียหาย

- บริษัท มีถังดับเพลิงในห้องเซิฟเวอร์ เพื่อใช้ในการดับเพลิงเบื้องต้น ในกรณีที่สามารถควบคุมเพลิงได้ หากเกินการความคุมให้แจ้งคณะกรรมการความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (คปอ.)
- บริษัท มีเครื่องสำรองไฟที่สามารถปรับแรงดันความคงที่ของกระแสไฟฟ้า และสามารถสำรองไฟฟ้าได้ถึง 30 นาทีขึ้นไป
- บริษัท มีเครื่องดำเนินไฟฟ้า Generator

- บริษัท มีระบบปรับอากาศและความชื้นจำนวน 2 ตัว รวมถึงเครื่องตรวจวัดอุณหภูมิและความชื้น ควบคุมอุณหภูมิไม่เกิน 22-25 องศาเซลเซียส และค่าความชื้นประมาณร้อยละ 40-60 เพื่อปรับให้เหมาะสมกับคุณลักษณะของระบบคอมพิวเตอร์
- ผู้ดูแลระบบจะต้องเข้าตรวจเช็คศูนย์คอมพิวเตอร์อย่างน้อยทุกๆ 1 สัปดาห์ เพื่อตรวจสอบความผิดปกติของระบบของการป้องกันความเสียหายในศูนย์คอมพิวเตอร์ โดยจะตรวจสอบตามรายการดังนี้
  - Hardware ตรวจสอบสถานะไฟต่างๆ บนเซิฟเวอร์ และอุปกรณ์เน็ตเวิร์คแต่ละตัวทำงานปกติหรือไม่
  - Software การทำงานของ Software บน Server แต่ละตัวทำงานปกติหรือไม่
  - Backup ตรวจสอบ Log File Backup ให้อยู่ในสถานะสำเร็จ
  - Environment สิ่งแวดล้อม อุณหภูมิ ความชื้น ร่องรอยน้ำหยดของเครื่องปรับอากาศ
  - Security เก็บ Log บุคคลที่เข้ามาปฏิบัติงานกับห้องเซิฟเวอร์
  - Network ตรวจสอบว่า Link online หรือไม่ สายเคเบิลมีร่องรอยชำรุดหรือไม่

3.2.3 การกำหนดสิทธิการเข้าใช้ข้อมูลใน FILE GOOGLE DRIVE

โครงสร้างการใช้งาน File Sharing

โครงสร้างหลัก	โครสร้างย่อย	สิทธิ์การใช้งานในระดับ Read-only	สิทธิ์การใช้งานในระดับ Edit	คำอธิบาย
COMPANYDATA	ฟอร์มเอกสารบริษัท	All Users		เก็บข้อมูลทั่วไปของบริษัท เช่น ประกาศวันหยุด ซึ่งสามารถเข้าถึงข้อมูลโดยพนักงานทุกคน
	APO Logo	All Users		เก็บข้อมูลโลโก้บริษัท
	APO WEEKLY	All Users		รายงานการประชุมประจำสัปดาห์
	Presentation	All Users		Presentation สำหรับรับภายนอก
	RSPO	All Users		วิสาหกิจชุมชนแปลงใหญ่ปาล์มน้ำมัน RSPO
	Video	All Users		สื่อคู่มือ

โครงสร้างหลัก	โครสร้างย่อย	สิทธิ์การใช้งานในระดับ Read-only	สิทธิ์การใช้งานในระดับ Edit	คำอธิบาย
DEPARTMENTDATA	ACCOUNT & FINANCE DEPARTMENT		ACCOUNT STAFF, CFO	เก็บข้อมูลในแต่ละแผนก โดยแยกเป็นรายแผนก ผู้ใช้งานสามารถเข้าถึงข้อมูลได้เฉพาะแผนกของตนเองและระหว่างแผนกตามที่ได้รับอนุญาตเท่านั้น (สำหรับ STAFF คือ ตั้งแต่ STAFF ขึ้นไป)
	Production Department		PRODUCTION STAFF, PRO, CFO, CEO	
	APO ส่งเสริมคุณภาพ		PRODUCTION STAFF, FFB PURCHASE MANAGER	
	IT Department		IT STAFF	
	Company Secretary		SECRETARY STAFF, CFO, CEO	
	Weighting Department		SCALES STAFF, CEO, CFO,PRO	
	BIOGAS Department		BIOGAS STAFF, PRO, CFO, CEO, SP	
DEPARTMENTDATA	ธุรการ		ADMINISTRATIVE STAFF, CFO, CEO, SP, PRO	เก็บข้อมูลในแต่ละแผนก โดยแยกเป็นรายแผนก ผู้ใช้งานสามารถเข้าถึงข้อมูลได้เฉพาะแผนกของตนเองและระหว่างแผนกตามที่ได้รับอนุญาตเท่านั้น (สำหรับ STAFF คือ ตั้งแต่ STAFF ขึ้นไป)
	ใบรับเงิน		ACCOUNT STAFF	
	ข้อมูลงานคลัง		WAREHOUS STAFF	
	Human Resource Department		HR STAFF, PRO, SP, AC, CFO, CEO	
	ISO		SCERETARY STAFF, PRODUCTION STAFF, PRO, SP, CFO, CEO	
	Sales		SCALES STAFF, SP, AC, CFO, CEO	
	การเงินและลานเท		ACCOUNT STAFF, SCALES	

- บริษัท มีระบบ TRCLOUD ในการจัดเก็บข้อมูลซึ่งสามารถควบคุมความถูกต้องของข้อมูลที่ใช้จัดเก็บ ผู้ให้บริการใช้ระบบฐานข้อมูล Cloud Digital Ocean ที่ได้มาตรฐาน ซึ่งมีการป้องกันความปลอดภัยของข้อมูลเทียบเท่าระดับสากล เว็บไซต์มีการเข้ารหัส SSL เพื่อความปลอดภัยในการส่งข้อมูลระหว่างเว็บไซต์กับระบบฐานข้อมูล
- การแจ้งซ่อมในลักษณะจะต้องมีการเปลี่ยนอะไหล่ กู้ข้อมูล หรือทำลายข้อมูลจะต้องมีการเขียนใบคำขอแจ้งซ่อม และได้รับการอนุมัติจากหัวหน้าแผนก ขึ้นไปเท่านั้น
- บริษัท มีมาตรการรักษาความปลอดภัยข้อข้อมูล ในการนำคอมพิวเตอร์ออกนอกบริษัท ดังนี้
  - หากมีการนำคอมพิวเตอร์ของบริษัท ออกไปนอกบริษัทหากเป็นระดับต่ำกว่าระดับผู้จัดการ(Manager) จะต้องได้รับการอนุญาตและกรอกใบคำขอนำคอมพิวเตอร์ออกนอกบริษัทไว้เป็นลายลักษณ์อักษรทุกครั้ง
  - หากมีการนำคอมพิวเตอร์ส่งซ่อมภายนอกบริษัท จะต้องถอดสื่อบันทึก (Hard disk, SSD) ออกก่อน
- หากมีพนักงานลาออกฝ่าย HR จะมีการแจ้งข้อมูลทาง Email และฝ่ายเทคโนโลยีสารสนเทศก็จะทำการ Disable user และยกเลิกสิทธิการใช้งานระบบคอมพิวเตอร์ของบุคคลนั้นทันทีหลังจากหมดสภาพการเป็นพนักงาน เพื่อความปลอดภัยของข้อมูลบริษัท และรองรับ พ.ร.บ.คอมพิวเตอร์ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้บริษัท เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ไว้เกิน 90 วันแต่ไม่เกิน 2 ปีเป็นกรณีพิเศษเฉพาะราย โดยจะมีการทำ Memo ขออนุญาตการลบข้อมูลจากระดับผู้อำนวยการของบุคคลนั้น ผู้อำนวยการส่วนงานสนับสนุนธุรกิจ และประธานเจ้าหน้าที่บริหาร (CEO)
- บริษัท ได้ทำการติดตั้ง FIREWALL เพื่อความปลอดภัยของการเชื่อมต่อกับระบบภายนอกทั้งหมดตลอดเวลา และมีการเก็บ LOG การใช้งานการเชื่อมต่อกับระบบภายนอกอย่างละเอียดไม่น้อยกว่า 90 วัน ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้บริษัท เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ไว้เกิน 90 วันแต่ไม่เกิน 2 ปีเป็นกรณีพิเศษเฉพาะราย

3.2.4 การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege)

- ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
- ต้องกำหนดสิทธิการใช้ข้อมูลและระบบสารสนเทศ เช่น สิทธิการใช้โปรแกรมระบบสารสนเทศ (Application System) สิทธิการใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และ

ความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

- ในกรณีมีความจำเป็นต้องใช้ User ที่มีสิทธิพิเศษ ต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ ในการพิจารณาว่าการควบคุม User ที่มีสิทธิพิเศษมีความรัดกุมเพียงพอหรือไม่นั้น บริษัทจะใช้ปัจจัยประกอบการพิจารณาในภาพรวมดังต่อไปนี้
  - ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่
  - ควรควบคุมการใช้งานของผู้ใช้งานที่มีสิทธิ์พิเศษอย่างเข้มงวด เช่น จำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
  - ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
  - ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น
- ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิและหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log Out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น
- ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ Share Files เป็นต้น จะต้องเป็นการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว และเจ้าของข้อมูลต้องมีหลักฐานการให้สิทธิดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น ให้มีสิทธิใช้งานระบบสารสนเทศและระบบเครือข่ายในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติ และต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- การใช้งานเครื่องคอมพิวเตอร์และระบบคอมพิวเตอร์ ไม่ว่าเป็นระยะเวลาตลอดการทำงานในตำแหน่งนั้นๆ หรือเป็นลักษณะการขอใช้ชั่วคราวจะต้องยื่นใบคำขอ และมีการอนุมัติจากระดับหัวหน้าแผนกขึ้นไปเท่านั้น
- ระบบงานไทเกอร์ซอฟท์ได้กำหนดสิทธิ์การใช้งานตาม Role
- ระบบ Factorium งานซ่อม งานPM มีการกำหนดสิทธิ์ให้เป็นไปตามหน้าที่ผู้รับผิดชอบ
- โปรแกรมชั่งน้ำหนัก Quick Weight Enterprise มีการจัดการควบคุมสิทธิ์โดยแบ่งตามหน้าที่งาน

- บริษัท ได้กำหนดสิทธิ์การใช้งานโปรแกรม TRCLOUD ไว้ดังนี้
  - โปรแกรม TRCLOUD ได้แบ่งระดับการใช้งานตาม Role ดังนี้

Role Profile	สิทธิในการใช้งาน
Admin	SYSTEM ADMINISTRATOR, DEVELOPER
Accountant	CFO AC ACCOUNT MANAGER, ACCOUNT, PURCHASE STAFF, PURCHASE MANAGER
Manager	CEO SP PRO MANAGER
Manager Day to Day	
Staff	USER STAFF
Staff Day to Day	
Staff View Only	

- นอกจากนี้โปรแกรม TRCLOUD ยังได้แบ่งสิทธิในการใช้งานเพิ่มเติมตามสิทธิการใช้งานรายบุคคลอีกด้วย
- สิทธิในการใช้งานอินเทอร์เน็ตของบริษัท จะถูกแบ่งดังนี้
  - ผู้ใช้งาน (User) ที่ Login คอมพิวเตอร์ผ่าน AD จะถูกเรียกว่าจะสามารถใช้งานอินเทอร์เน็ตได้ผ่าน Policy single sign-on บน Firewall
  - ผู้ใช้งาน (User) ที่ไม่ได้ Login คอมพิวเตอร์ผ่าน AD หากเป็นพนักงานจะต้องผ่านขั้นตอนระบุตัวตน (Authentication) โดยสามารถใช้ User Password บน AD ได้เลย และจะต้อง Login ใหม่ทุกๆ 24 ชั่วโมง
  - ผู้ใช้งาน (User) ที่ไม่ได้ Login คอมพิวเตอร์ผ่าน AD และไม่ได้เป็นพนักงานจะต้องขอ User Password ที่ฝ่ายเทคโนโลยีสารสนเทศบริษัท เพื่อลงชื่อรับ User Password สำหรับใช้งานชั่วคราวเป็นระยะเวลา 24 ชั่วโมง
- ระบบ TRCLOUD จะต้องมีการทบทวนสิทธิการใช้งานของ User อย่างน้อยปีละ 2 ครั้ง โดยระดับผู้อำนวยการส่วนงาน
- ระบบ Tigersoft จะต้องจัดทำการทบทวนสิทธิการใช้งานของ user อย่างน้อยปีละ 2 ครั้ง โดยระดับผู้อำนวยการส่วนงาน
- ระบบ Factorium จะต้องจัดทำการทบทวนสิทธิการใช้งานของ user อย่างน้อยปีละ 1 ครั้ง โดยระดับผู้อำนวยการส่วนงาน

- ระบบ Quick Weight Enterprise จะต้องจัดทำการทบทวนสิทธิการใช้งานของ user อย่างน้อยปีละ 2 ครั้ง โดยระดับผู้อำนวยการส่วนงาน

3.3 การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์และระบบเครือข่าย (Information and Network Security)

3.3.1 การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)

- ฝ่ายเทคโนโลยีสารสนเทศมีการตรวจสอบสถานะต่างๆบนเซิฟเวอร์เช่น Service ต่างๆ บน AD Server Firewall และ ระบบ TRCLOUD ในทุกๆวัน และระบบ Backup ของทุกเซิฟเวอร์อย่างน้อยทุกๆ 3 วัน เป็นต้น
- ฝ่ายเทคโนโลยีสารสนเทศมีการเปิด Service และ Policy บน Firewall ตามที่จำเป็นเท่านั้นเพื่อป้องกันความปลอดภัยของระบบคอมพิวเตอร์แม่ข่าย
- ฝ่ายเทคโนโลยีสารสนเทศมีการใช้ Antivirus สำหรับเครื่องแม่ข่าย (Server) ทั้ง AD Server และมีการต่ออายุ Maintenance Agreement(MA) ของทุกๆ Solution ทุกปีตาม Budget Plan

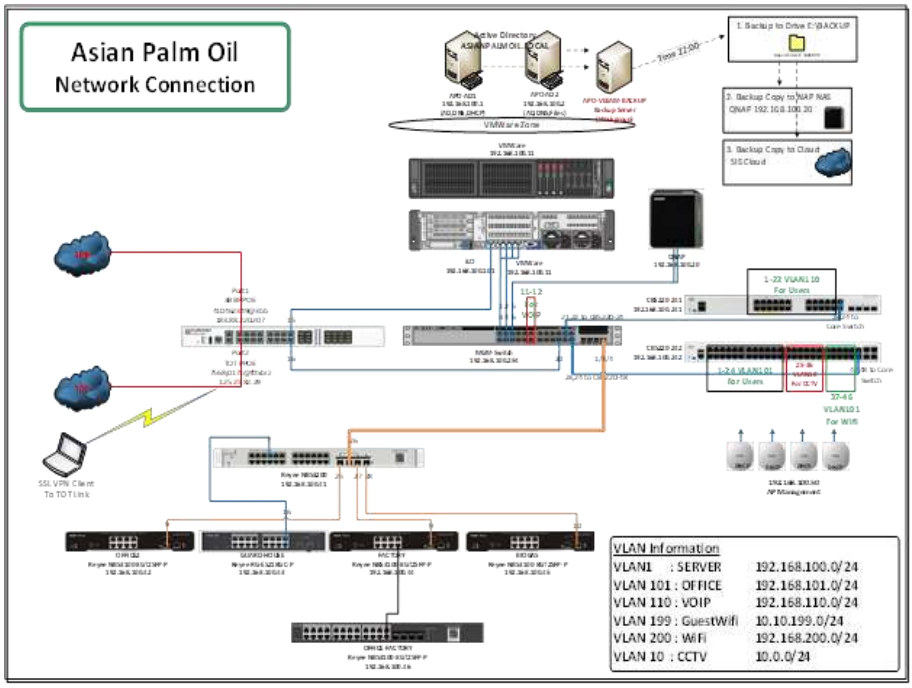
3.3.2 ไวรัสคอมพิวเตอร์ (Computer Virus)

- บริษัท ห้ามมิให้พนักงานติดตั้งโปรแกรมต่างๆด้วยตนเองเพื่อป้องกันโปรแกรมที่ผิดลิขสิทธิ์และไวรัสที่อาจแฝงมากับโปรแกรมต่างๆได้
- บริษัท มีการติดตั้ง Antivirus ให้กับเครื่องของผู้ใช้งานทุกเครื่องเพื่อป้องกันไวรัส ทั้งจาก Thumb drive, Flash drive หรือแผ่น CD, DVD ต่างๆ
- บริษัท ได้มีการใช้ Firewall ในการป้องกันไวรัสจากการใช้งานอินเตอร์เน็ตของผู้ใช้งานด้วย policy ต่างๆ โดยการเพิ่ม Security Profile บน Policy การใช้งานอินเตอร์เน็ตของผู้ใช้งาน เช่น Antivirus, Web application, Web filter, Anti-Spam, Application Control, IPS เป็นต้น

3.3.3 การบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network)

- ฝ่ายเทคโนโลยีสารสนเทศมีการจัดทำแบ่งแยกโซนตามสัดส่วนการใช้งาน ดังนี้
  - Server Zone
  - Client Zone

ซึ่งมี Network Diagram ดังนี้



- Computer Diagram

ซึ่งมี Computer Diagram ดังนี้

- บริษัท มี FIREWALL ในการป้องกันระบบ รวมไปถึงการควบคุมการใช้งานอินเตอร์เน็ต และ Centralize Log ซึ่งจะเก็บ Log ตาม พ.ร.บ คอมพิวเตอร์ ซึ่งสามารถเก็บข้อมูลจราจรได้ไม่ต่ำกว่า 90 วัน และรองรับ พรบ.คอมพิวเตอร์ ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้บริษัท เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ไว้เกิน 90 วันแต่ไม่เกิน 2 ปีเป็นกรณีพิเศษเฉพาะราย
- ฝ่ายเทคโนโลยีสารสนเทศ จะมีการตรวจสอบ Log ในด้านการพยายามโจมตีระบบจากบุคคลอยู่สม่ำเสมอทุกวัน

3.3.4 การควบคุมการเปลี่ยนแปลง (Change Control)

กรณีมีการเปลี่ยนแปลงหรือติดตั้ง Program Network ให้กับระบบคอมพิวเตอร์ จะมีขั้นตอนการดำเนินการดังนี้

- มีการเสนออนุมัติเป็นบันทึก (Memo) เสนอผู้บริหาร
- หลังจากผ่านการอนุมัติ ให้มีการขอซื้อผ่านฝ่ายจัดซื้อทั่วไป
- วิเคราะห์ผลกระทบ และทดสอบระบบก่อนใช้จริง
- ติดตั้งระบบ ใช้งานจริง และติดตามผลการใช้งาน

3.3.5 การสำรองข้อมูล และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)

- การสำรองข้อมูลของระบบคอมพิวเตอร์บริษัท มีดังนี้
  - AD Server / File Sever มีการสำรองไว้ใน QNAP NAS โดยมีการตั้งเวลาการสำรองข้อมูลตอนเวลา 20.00 นาฬิกา ของทุกวัน และสำรองไว้บน SIS Cloud เวลา 10.00นาฬิกา ของทุกวัน
  - TRCLOUD มีการสำรองไว้ใน QNAP NAS เวลา 03.00นาฬิกา ของทุกวัน และผู้ให้บริการจะทำการสำรองข้อมูลในทุกวันอาทิตย์ เวลา 03.00นาฬิกา
  - Email Google Workspace มีการสำรองไว้ใน NAS Synology
- ฝ่ายเทคโนโลยีสารสนเทศได้มีการจัดทำแผนสำรองในสถานการณ์ฉุกเฉินเพื่อเป็นการเตรียมความพร้อมในยามที่เกิดสถานการณ์ฉุกเฉินก็จะสามารถกู้ข้อมูลกลับมาได้ภายในไม่เกิน 48 ชั่วโมง

3.3.6 บันทึกเพื่อการตรวจสอบ (Audit Log)

- ฝ่ายเทคโนโลยีสารสนเทศได้มีการเก็บ Log การใช้งานทั้ง Server Log และ Traffic Log ไว้ไม่ต่ำกว่า 90 วัน ตาม พรบ.คอมพิวเตอร์ และ รองรับ พรบ.คอมพิวเตอร์ ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้บริษัท เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ไว้เกิน 90 วันแต่ไม่เกิน 2 ปีเป็นกรณีพิเศษเฉพาะราย

- ฝ่ายเทคโนโลยีสารสนเทศได้มีการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ Log file จะเก็บข้อมูลการเข้าออกใช้งานอินเตอร์เน็ตของทุกคนในองค์กร
- ฝ่ายเทคโนโลยีสารสนเทศจะมีการสอบทาน Log ทุก 30 วัน และมีการนำเสนอในที่ประชุมประจำเดือน

3.3.7 การอบรมและความตระหนักของผู้ใช้งาน (User's Training and Awareness)

- ฝ่ายเทคโนโลยีสารสนเทศ มีแผนที่จะจัดการอบรมพนักงานในขั้นตอนการรักษาความปลอดภัยเบื้องต้นจากการใช้งานระบบคอมพิวเตอร์ของบริษัท โดยจะร่วมกับฝ่ายทรัพยากรบุคคลจัดอบรมพนักงานใหม่ในช่วงของการปฐมนิเทศ และพนักงานปัจจุบันในช่วงเดือนธันวาคมของทุกปี

3.3.8 การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

- ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดเส้นทางการเชื่อมต่อระบบเครือข่ายเพื่อการเข้าใช้งานระบบอินเทอร์เน็ต โดยต้องผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall หรือ Proxy เป็นต้น
- เครื่องคอมพิวเตอร์ของบริษัท ก่อนทำการเชื่อมต่อระบบเครือข่าย ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการก่อน
- การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL(Secure Socket Layer) การใช้ VPN (Virtual Private Network) ต้องมีเอกสารคำขอเปิดสิทธิ VPN และผ่านการอนุมัติตามอำนาจดำเนินการของบริษัท หากเกิดข้อมูลรั่วไหลจากการ VPN จะต้องถูกพิจารณาบทลงโทษทางวินัยตามระเบียบบริษัท
- หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น
- ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยของบริษัท
- ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับของบริษัท ยกเว้นเป็นไปตามหลักเกณฑ์การเปิดเผยอย่างเป็นทางการของบริษัท
- ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดเพื่อปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา
- ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำไปใช้งาน

- ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของบริษัท เพื่อประโยชน์ในเชิงธุรกิจส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมอันดี เว็บไซต์ที่มีเนื้อหาเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เว็บไซต์ที่เป็นภัยต่อสังคม เว็บไซต์ลามกอนาจาร เป็นต้น
- ผู้ใช้งานจะต้องใช้ระบบอินเทอร์เน็ต ในลักษณะที่ไม่เป็นการละเมิดของบุคคลอื่นๆ และจะต้องไม่ก่อให้เกิดความเสียหายขึ้นต่อบริษัท รวมทั้งจะต้องไม่กระทำการใดอันเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ หรือกฎหมายที่เกี่ยวข้องโดยเด็ดขาด ทั้งนี้ การใช้ระบบอินเทอร์เน็ตเพื่อการปฏิบัติงานของบริษัทในทุกกรณี ผู้ใช้งานจะต้องปฏิบัติตามขั้นตอนการปฏิบัติที่บริษัทกำหนดไว้อย่างเคร่งครัด

ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่รับผิดชอบในการจัดนโยบายในการควบคุมการเข้าถึงสารสนเทศเป็นลายลักษณ์อักษร โดยมีเนื้อหาดังนี้

a. การควบคุมรหัสผ่าน (Password Control)

- ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบสารสนเทศที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น บริษัท จะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม
  - บริษัท มีการบังคับให้พนักงานเปลี่ยน password การเข้าใช้งานระบบ AD อินเตอร์เน็ต ไฟล์เซิฟเวอร์ (File Server) และอีเมล์บริษัท ทุกๆ 90 วัน หรือ 3 เดือนผ่าน Security Policy ของเครื่องเซิฟเวอร์นั้นๆ
  - บริษัท ได้กำหนดให้รหัสผ่านของผู้ใช้งาน (user) มีความยากต่อการคาดเดาผ่าน Security Policy ของเครื่องเซิฟเวอร์นั้นๆ มีคลาสอักขระอย่างน้อยสามในห้าคลาสต่อไปนี้ ตัวอักษรตัวพิมพ์เล็ก (a-z) ตัวอักษรตัวพิมพ์ใหญ่ (A-Z)ตัวเลข (0-10) อักขระ “พิเศษ” (เช่น @#$%^&*()_+|~-=\`{}[]:";'<>/ เป็นต้น) รหัสผ่านประกอบด้วยอักขระน้อยกว่า 8 ตัวขึ้นไป
  - บริษัท ได้กำหนดให้รหัสผ่านถูกซ่อนไม่ให้มองเห็นเมื่อมีการเข้าสู่ระบบโดยใช้คีย์บอร์ด
  - บริษัท มีการจัดเก็บประวัติของรหัสผ่านเพื่อป้องกันไม่ให้มีการใช้รหัสผ่านซ้ำกับรหัสที่เคยใช้ไปแล้ว
  - บริษัท กำหนดให้ผู้ใช้งาน (user) จะต้องเปลี่ยนรหัสผ่านทันทีในการเข้าสู่ระบบครั้งแรก

- บริษัท กำหนดให้ระบบมีการล๊อคผู้ใช้ออกจากระบบหลังจากมีความพยายามในการเข้าถึง (Account Lockout) เกิน 3 ครั้ง

- ต้องมีระบบการเข้ารหัส (Encryption) ไฟล์ที่เก็บรหัสผ่านเพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง
- ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิใช้งานระบบแล้ว เช่น บัญชีรายชื่อของผู้ใช้งานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือเปลี่ยน รหัสผ่าน เป็นต้น

b. การควบคุมการเข้าถึงของผู้ให้บริการภายนอก (IT OUTSOURCING)

- บริษัท มีนโยบาย ให้ผู้ให้บริการภายนอกจะต้องกรอกใบคำขอเปิดสิทธิใช้งานระบบคอมพิวเตอร์ และจะต้องมีการอนุมัติจากผู้บริหารของบริษัท ก่อนที่จะสร้าง Active Directory Object(User Password) ตามระยะเวลาที่ขอใช้ และมีการ Monitor การใช้งานทุกครั้ง
- บริษัท มีนโยบายการ Remote Support จากผู้ให้บริการภายนอกโดยจะต้องแจ้งให้หัวหน้าแผนกเทคโนโลยีสารสนเทศ และผู้บังคับบัญชาในสายงาน เพื่ออนุมัติและมีการ Monitor การใช้งานทุกครั้ง
- บริษัท มีนโยบายให้ผู้บริการภายนอกจะต้องกรอกใบคำขอยกเลิกสิทธิใช้งานระบบสารสนเทศทุกครั้ง และจะต้องมีการเซ็นอนุมัติจากผู้บริหารของบริษัท ก่อนทำการ Disable ในระบบจนครบ 90วัน จึงทำการลบข้อมูล

3.3.9 ระดับความสำคัญของระบบงานสารสนเทศ

- Internet/Network บริษัท มีการใช้โปรแกรมหลักผ่านระบบ Cloud จึงมีความสำคัญ
- Server AD บริษัท ได้มีการนำเอา Active Directory เข้ามาควบคุม Policy และ File Sever

3.3.10 การควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ (Computer and Peripheral Access Control)

- ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท ต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน

- ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัท เพื่อประกอบธุรกิจการค้า หรือบริการใดๆ ที่เป็นของส่วนตัวและไม่เหมาะสม
- ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ของบริษัท เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงาน
- ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบ หรือหน่วยงานที่รับผิดชอบ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงให้มีสภาพเดิม
- ผู้ใช้งานต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อน ชื้น มีฝุ่นละออง และต้องระวังการตกกระทบ
- ไม่ใช้หรือวางอุปกรณ์คอมพิวเตอร์ทุกชนิดใกล้สิ่งที่เป็นของเหลว ใกล้สนามแม่เหล็ก ไฟฟ้าแรงสูง ในที่มีการสั่นสะเทือน และในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส
- ในการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ควรทำด้วยความระมัดระวัง ไม่วางของหนักทับ หรือโยน
- ไม่เคลื่อนย้ายเครื่องขณะที่ฮาร์ดดิสก์กำลังทำงาน หรือขณะเปิดใช้งานอยู่
- หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ และควรเช็ดทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน
- การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท
- ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

3.3.11 การควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License)

- ข้อกำหนดสำหรับผู้ดูแลระบบ
  - มีหน้าที่รับผิดชอบในการควบคุม ดูแลการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนจัดสรรการใช้งานโปรแกรมคอมพิวเตอร์ภายในบริษัท ตามสิทธิการใช้งานที่กำหนด
  - มีหน้าที่รับผิดชอบในการติดตั้ง และอัพเกรดโปรแกรมคอมพิวเตอร์ให้แก่ผู้ใช้งาน ตามวันเวลาที่นัดหมาย
  - ทำการถอดและยกเลิกสิทธิการใช้งานโปรแกรมคอมพิวเตอร์ทันที เมื่อบริษัท และ/หรือหน่วยงาน แจ้งยกเลิกและ/หรือย้ายสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์
- ต้องใช้โปรแกรมคอมพิวเตอร์อย่างเช่นวิญญูชนพึงจะใช้ทรัพย์สินของตนเอง โดยไม่นำไปใช้ในทางที่ผิดกฎหมายหรือละเมิดกฎหมายต่อบุคคลอื่นอันเป็นต้นเหตุให้เกิดความเสียหายขึ้นกับบริษัท
- โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัท เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งาน
- ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัดทำขึ้นโดยไม่ได้รับอนุญาต โดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำความผิดทางกฎหมาย
- ห้ามนำโปรแกรมคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมายมาติดตั้งใช้งานบนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด กรณีผู้ใช้งานนำโปรแกรมคอมพิวเตอร์อื่นใดนอกเหนือไปจากโปรแกรมที่บริษัท มีอยู่ มาใช้งานบนระบบคอมพิวเตอร์ ไม่ว่าจะมี Licensed Software หรือ Freeware ก็ตาม หากมีความเสียหายหรือละเมิดเกิดขึ้นผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว
- การติดตั้งใช้งาน การยกเลิกการใช้งาน การโอนย้าย และการคืนเครื่องคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์ ให้ผู้ใช้งานขอแจ้งความประสงค์ในแต่ละกรณีให้ผู้มีอำนาจพิจารณาอนุมัติ และผู้ดูแลระบบเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามที่ได้รับอนุมัติในแต่ละกรณี

3.4 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)

3.4.1 จัดทำคู่มือหรือขั้นตอนปฏิบัติงานเกี่ยวกับระบบสารสนเทศที่สำคัญของบริษัท เพื่อป้องกันความผิดพลาดในการปฏิบัติงานด้านสารสนเทศ

3.4.2 กำหนดให้มีการควบคุมการเปลี่ยนแปลงสารสนเทศ เช่น ต้องมีการขออนุมัติจากผู้บังคับบัญชาก่อนดำเนินการเป็นต้น

3.4.3 ต้องมีการสำรองข้อมูลสารสนเทศก่อนการเปลี่ยนแปลงสารสนเทศ

3.4.4 ตรวจสอบติดตามทรัพยากรของระบบสารสนเทศ เช่น CPU, Memory, Hard Disk ว่าเพียงพอหรือไม่ และนำข้อมูลการตรวจสอบติดตามมาวางแผนการเพิ่มหรือลดทรัพยากรในอนาคต

3.4.5 ระบบที่มีความสำคัญสูง ควรแยกระบบการพัฒนาออกจากระบบการให้บริการจริง เพื่อป้องกันการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

3.4.6 ต้องสำรวจข้อมูล จัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรองและความถี่ในการสำรองข้อมูล

3.4.7 ข้อมูลที่มีความสำคัญสูง ต้องจัดให้มีความถี่การสำรองมาก และควรจัดให้มีการสำรองข้อมูลภายนอกบริษัท

3.4.8 ต้องทดสอบสภาพพร้อมใช้งานระบบสำรองของระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

3.4.9 ต้องมีมาตรการป้องกันโปรแกรมไม่ประสงค์ดี เช่น

- เครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องคอมพิวเตอร์แบบพกพาส่วนบุคคล ก่อนเชื่อมต่อระบบเครือข่ายของบริษัท ต้องติดตั้งโปรแกรมป้องกันไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราว์เซอร์
- ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการและโปรแกรมที่ใช้งาน ที่ได้มีการออก Patch และ/หรือ Hotfix อย่างสม่ำเสมอ โดยสามารถดาวน์โหลดจากเว็บไซต์ของเจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่
- ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอีเมล จะต้องตรวจสอบไวรัส โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง
- ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ที่ทางบริษัทได้จัดเตรียมไว้ให้ หากต้องการติดตั้งซอฟต์แวร์อื่นนอกเหนือจากที่บริษัทเตรียมไว้ให้ ต้องแจ้งฝ่ายเทคโนโลยีเพื่อตรวจสอบความปลอดภัยก่อนการติดตั้ง

3.5 การใช้งานจดหมายอิเล็กทรอนิกส์

3.5.1 ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ จะต้องไม่กระทำการละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายที่เกี่ยวข้อง และนโยบายและข้อกำหนดเกี่ยวกับเทคโนโลยีสารสนเทศที่บริษัทกำหนด

3.5.2 หน่วยงานหรือผู้ใช้งานผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัท จะต้องใช้จดหมายอิเล็กทรอนิกส์ เพื่อผลประโยชน์ของบริษัท

3.5.3 ผู้ใช้งานจะได้รับสิทธิ์ในการใช้บริการจดหมายอิเล็กทรอนิกส์ โดยทางผู้ดูแลระบบจะเป็นผู้ทำการลงทะเบียนผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ ตามรายชื่อผู้ใช้งานที่ได้รับแจ้งมาจากฝ่ายทรัพยากรบุคคล

3.5.4 ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่าน หรือรับส่งข้อความ

3.5.5 การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง หรือบัญชีผู้ใช้งานอื่น

3.5.6 การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการตามภารกิจของบริษัท ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทขัดข้อง และต้องได้รับอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

3.5.7 การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อศีลธรรมอันดีงาม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความคิดเห็นส่วนบุคคล โดยอ้างเป็นความเห็นของบริษัท หรือก่อให้เกิดความเสียหายต่อบริษัท

3.5.8 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรมอันดีงาม ความมั่นคงของประเทศ กฎหมาย หมิ่นต่อสถาบันพระมหากษัตริย์ หรือกระทบต่อการดำเนินงานของบริษัท ตลอดจนเป็นการรบกวนผู้ใช้งานอื่นรวมทั้งผู้รับบริการของบริษัท

3.5.9 ห้ามผู้ใช้บริการนำที่อยู่จดหมายอิเล็กทรอนิกส์ ไปใช้ในกิจการงานส่วนบุคคล เช่น ธุรกิจส่วนตัว ใช้สมัครเครือข่ายสังคมออนไลน์ เป็นต้น หากตรวจพบว่ามีการกระทำดังกล่าว ให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์หรือเจ้าของผู้ใช้บริการ เป็นผู้รับผิดชอบการกระทำดังกล่าว

3.5.10 ห้ามกระทำการอันที่จะสร้างปัญหาในการใช้ทรัพยากรของระบบ เช่น การสร้างจดหมายลูกโซ่ (Chain mail) การส่งจดหมายจำนวนมาก (Spam mail) การส่งจดหมายต่อเนื่อง (Letter bomb) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์ เป็นต้น

3.5.11 ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของบริษัทให้กับบุคคลอื่นหรือหน่วยงานที่ไม่เกี่ยวข้องกับภารกิจของบริษัท

3.5.12 การส่งข้อมูลข่าวสารที่เป็นความลับบริษัท ควรมีการเข้ารหัสข้อมูลข่าวสารนั้น

3.5.13 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้ง

3.5.14 กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับการบริการชั่วคราวแก่ผู้ใช้งานนั้นๆ เพื่อทำการสอบสวน และตรวจสอบสาเหตุ

3.5.15 หากผู้ใช้บริการพบการกระทำที่ไม่เหมาะสม หรือเข้าข่ายการกระทำความผิด เกิดขึ้นในบริษัท ให้แจ้งเบาะแสไปที่ช่องทางการรับแจ้งเบาะแสของบริษัท E-Mail : info@asianpalmoil.com

3.6 แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของ IT (Information Security Policy)

3.6.1 ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งที่ผิดกฎหมาย หรือขัดต่อศีลธรรมอันดี เป็นต้น

3.6.2 ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้ของผู้อื่น ทั้งที่ได้รับอนุญาต และไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้

3.6.3 ห้ามเข้าใช้ระบบคอมพิวเตอร์และข้อมูลที่มีการป้องกันการเข้าถึงของผู้อื่น เพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอก

3.6.4 ห้ามเผยแพร่ข้อมูลของผู้อื่น หรือของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูลนั้นๆ

3.6.5 ห้ามก่อกวน ขัดขวาง หรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของบริษัทเกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์ การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) เป็นต้น

3.6.6 ห้ามลักลอบดักรับข้อมูลในเครือข่ายคอมพิวเตอร์ของบริษัท และของผู้อื่นที่อยู่ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์

3.6.7 ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ หรือเปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสก่อนทุกครั้ง

3.6.8 ผู้ใช้ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีใช้งานและรหัสผ่านของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

กระบวนการควบคุมทรัพย์สินสารสนเทศ

วัตถุประสงค์

1) เพื่อเป็นแนวทางในการกำกับดูแล ตรวจสอบ และติดตามด้านการควบคุมทรัพย์สินสารสนเทศ ให้มีความสอดคล้องกับระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2) เพื่อสื่อสารชี้แจงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่บริษัทควรมีมาตรการบริหารจัดการความเสี่ยงนั้นอย่างเหมาะสม
3) เพื่อให้บริษัทบริหารจัดการและปฏิบัติงานภายใต้ความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

คำนิยาม

- **ลิขสิทธิ์** หมายถึง สิทธิ์แต่ผู้เดียวที่กฎหมายรับรองให้ผู้สร้างสรรค์กระทำการใด ๆ เกี่ยวกับงานที่ตนได้ทำขึ้น อันได้แก่ สิทธิ์ที่จะทำซ้ำ ดัดแปลง หรือนำออกโฆษณา ไม่ว่าในรูปลักษณะอย่างใดหรือวิธีใด รวมทั้งอนุญาตให้ผู้อื่นนำงานนั้นไปใช้ได้
- **ระบบคอมพิวเตอร์** หมายถึง ขั้นตอนการปฏิบัติงานของคอมพิวเตอร์ที่มีการกำหนดอย่างชัดเจนว่าต้องทำอะไรบ้าง เพื่อให้ได้ผลออกมาตามที่ต้องการ ขั้นตอนการปฏิบัติงานจะประกอบด้วย ข้อมูลนำเข้า การประมวลผล ผลลัพธ์ และข้อมูลป้อนกลับ ซึ่งมีความสัมพันธ์เชื่อมโยงกัน ดังนั้นเมื่อกล่าวถึงระบบคอมพิวเตอร์สิ่งสำคัญของระบบจึงได้แก่ ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์(Software) และบุคลากร (Peopleware)
- **ทรัพย์สินทางด้านสารสนเทศ** หมายถึง อุปกรณ์อิเล็กทรอนิกส์ เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง หรืออุปกรณ์ที่สามารถเชื่อมต่อกับระบบเครือข่ายของบริษัท และรวมไปถึง ซอฟต์แวร์ และโปรแกรมประยุกต์ที่ได้รับการจัดซื้อ หรือจัดทำขึ้นมาเพื่อใช้ในการประกอบกิจการของบริษัท

ข้อกำหนด

1) กำหนดความเป็นเจ้าของทรัพย์สินสารสนเทศ

- ***กำหนดบุคคล หรือหน่วยงานผู้รับผิดชอบ*** ข้อมูลและทรัพย์สินทั้งหมดด้านเทคโนโลยีสารสนเทศ และการสื่อสารของบริษัท***อย่างชัดเจน***

2) การอนุญาตให้ใช้ทรัพย์สินสารสนเทศ

- พนักงานของบริษัท***จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน*** รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัย และคงความถูกต้อง โดยหมายรวมถึงข้อมูล และระบบสารสนเทศของบริษัท
- ผู้ใช้งาน***ต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ของบริษัทอย่างระมัดระวัง*** และให้การปกป้องเสมือนเป็นทรัพย์สินของตน

- เครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งหมดของบริษัท***ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งาน*** และ***ต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของการล็อคหน้าจอ หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง***
- ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าระบบเครือข่ายของบริษัท รวมถึง***ต้องไม่ติดตั้งซอฟต์แวร์ใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัท***ก่อนได้รับอนุญาตจากผู้มีอำนาจ

  อุปกรณ์คอมพิวเตอร์ของบริษัท***ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ*** ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้น และ***พนักงานต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์บนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด***

3) การอนุญาตให้ใช้งานทรัพย์สินด้านซอฟต์แวร์

- ***ห้ามพนักงานทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของ บริษัท*** โดยให้พนักงานที่ใช้งานระบบสารสนเทศลงนามในเอกสารข้อตกลง
- รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งาน***ต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยหัวหน้าแผนก IT*** เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของบริษัทเท่านั้น

4) การจัดหมวดหมู่ข้อมูลและทรัพย์สินสารสนเทศ

- การ***จัดทำป้ายชื่อแสดงรหัสทรัพย์สินของอุปกรณ์สารสนเทศ***ที่เกี่ยวข้องกับการบริหารด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งทรัพย์สินซอฟต์แวร์ และทรัพย์สินอุปกรณ์
- เมื่อมีการจัดซื้อและส่งมอบแล้ว แผนก IT จะทำการ***เก็บข้อมูลรายละเอียดของอุปกรณ์ต่าง ๆ ก่อนการส่งมอบให้กับเจ้าของเครื่อง***
- หากมีการโอนย้ายทรัพย์สิน ***แผนก IT ต้องทำการแจ้งฝ่ายที่เกี่ยวข้อง*** เพื่อแก้ไขข้อมูลที่มีอยู่ให้เป็นปัจจุบัน

เอกสารที่เกี่ยวข้อง

เอกสารที่ใช้ภายในบริษัท		เอกสารภายนอก
เอกสารที่มีเลขทะเบียนคุม	**เอกสารที่ไม่มีเลขทะเบียนคุม**	
ชื่อเอกสาร	**ชื่อเอกสาร**	**ชื่อเอกสาร**
ทะเบียนควบคุมทรัพย์สินสารสนเทศ	-ไม่มี-	-ไม่มี-

ผู้ที่เกี่ยวข้อง

- แผนก IT
- แผนกที่เกี่ยวข้อง

การส่งมอบ รับคืน และซ่อมทรัพย์สินทางด้านสารสนเทศ

วัตถุประสงค์

1) เพื่อเป็นแนวทางในการกำกับดูแล ตรวจสอบ และติดตามกระบวนการส่งมอบ รับคืนทรัพย์สินทางด้านสารสนเทศ ให้มีความสอดคล้องกับระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2) เพื่อสื่อสารชี้แจงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่บริษัทควรมีมาตรการบริหารจัดการความเสี่ยงนั้นอย่างเหมาะสม
3) เพื่อให้บริษัทบริหารจัดการและปฏิบัติงานภายใต้ความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

คำนิยาม

- **ผู้ที่มีความประสงค์** หมายถึง พนักงานภายในบริษัท หรือ บุคคลที่ต้องการใช้การปฏิบัติงานในบริษัท
- **ทรัพย์สินทางด้านสารสนเทศ** หมายถึง อุปกรณ์อิเล็กทรอนิกส์ เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง หรืออุปกรณ์ที่สามารถเชื่อมต่อกับระบบเครือข่ายของบริษัท และรวมไปถึง ซอฟต์แวร์ และโปรแกรมประยุกต์ที่ได้รับการจัดซื้อ หรือจัดทำขึ้นมาเพื่อใช้ในการประกอบกิจการของบริษัท
- **ทะเบียนควบคุมทรัพย์สินสารสนเทศ** หมายถึง ข้อมูลทรัพย์สินสารสนเทศที่มีทั้งหมดซึ่งจัดเก็บโดยแผนก IT

ข้อกำหนด

1) ควบคุมการขอใช้งานทรัพย์สินทางด้านสารสนเทศ

- ***เมื่อมีการเปลี่ยนแปลงหรือเพิ่มพนักงานใหม่*** เจ้าหน้าที่ HR หรือผู้มีความประสงค์ต้องการยืมอุปกรณ์สารสนเทศชั่วคราว***ต้องจัดทำ “แบบฟอร์มส่งมอบและรับคืนทรัพย์สินทางด้านสารสนเทศ” ทุกครั้ง***
- เจ้าหน้าที่ IT ***นำอุปกรณ์สารสนเทศไปส่งมอบให้ผู้มีความประสงค์ และทำการแก้ไข “ทะเบียนควบคุมทรัพย์สินสารสนเทศ” ทุกครั้ง*** เมื่อมีการเปลี่ยนแปลง

2) ควบคุมการคืนทรัพย์สินทางด้านสารสนเทศ

- หน่วยงานเจ้าของทรัพย์สิน***ต้องทำการขอคืนอุปกรณ์ทางด้านสารสนเทศทุกครั้ง*** เมื่อมีพนักงานลาออกหรือผู้มีความประสงค์ต้องการคืนอุปกรณ์สารสนเทศยืมชั่วคราว
- เจ้าหน้าที่ IT ***ต้องทำการอนุมัติและตรวจสอบทุกครั้ง*** เมื่อมีการคืนอุปกรณ์ทางด้านสารสนเทศ
- เจ้าหน้าที่ IT ***ต้องทำการแก้ไข “ทะเบียนควบคุมทรัพย์สินสารสนเทศ” ทุกครั้ง*** เมื่อมีการเปลี่ยนแปลง

3) ควบคุมการซ่อมทรัพย์สินทางด้านสารสนเทศ

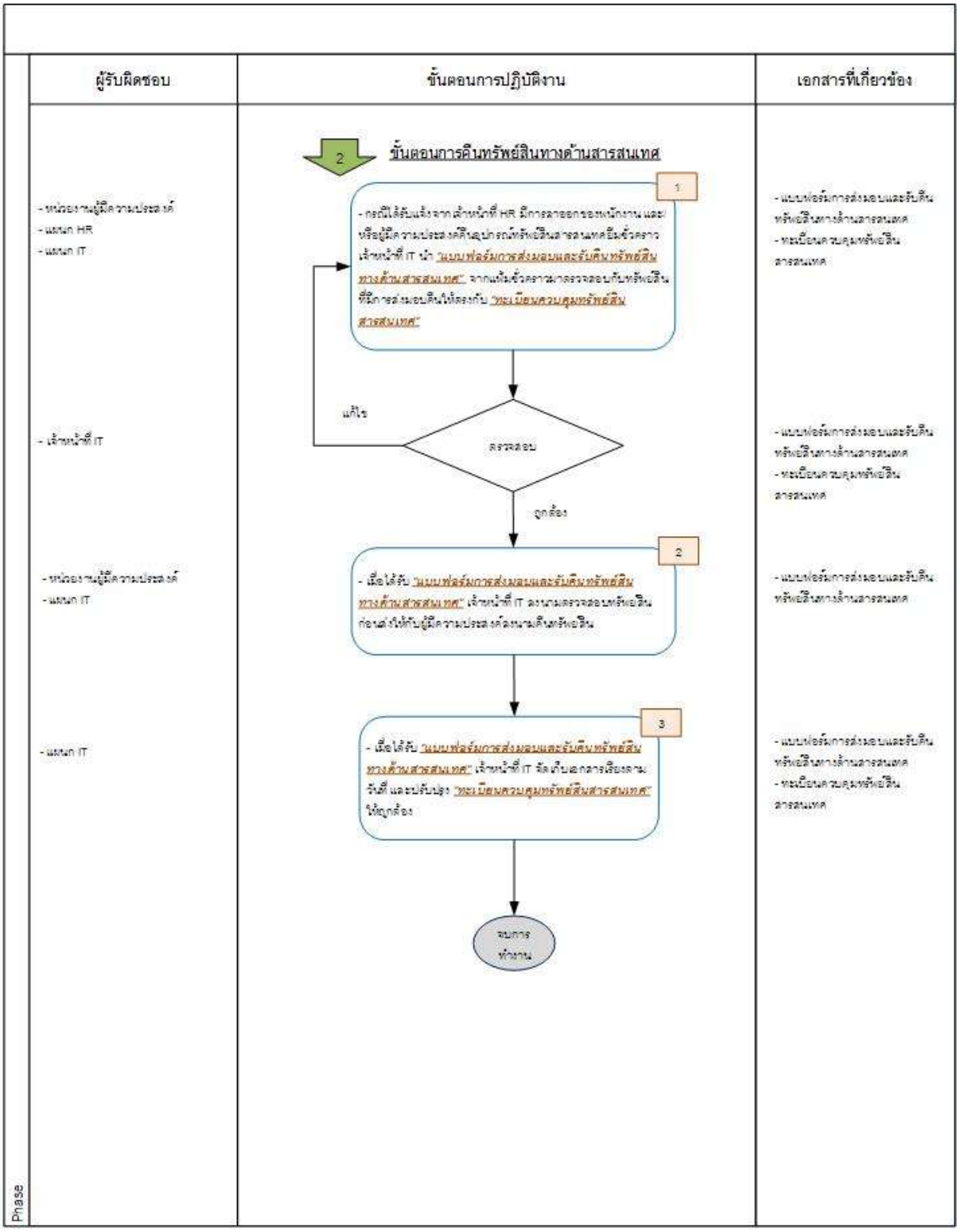
- หน่วยงานเจ้าของทรัพย์สิน***ต้องจัดทำ "แบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ" โดยระบุปัญหาที่เกิดขึ้น***
- เจ้าหน้าที่ IT ทำการ***ตรวจสอบซ่อมบำรุงอุปกรณ์สารสนเทศ และหัวหน้าแผนก IT พิจารณาเพิ่มเติมหากอุปกรณ์สารสนเทศไม่สามารถซ่อมได้***

เอกสารที่เกี่ยวข้อง

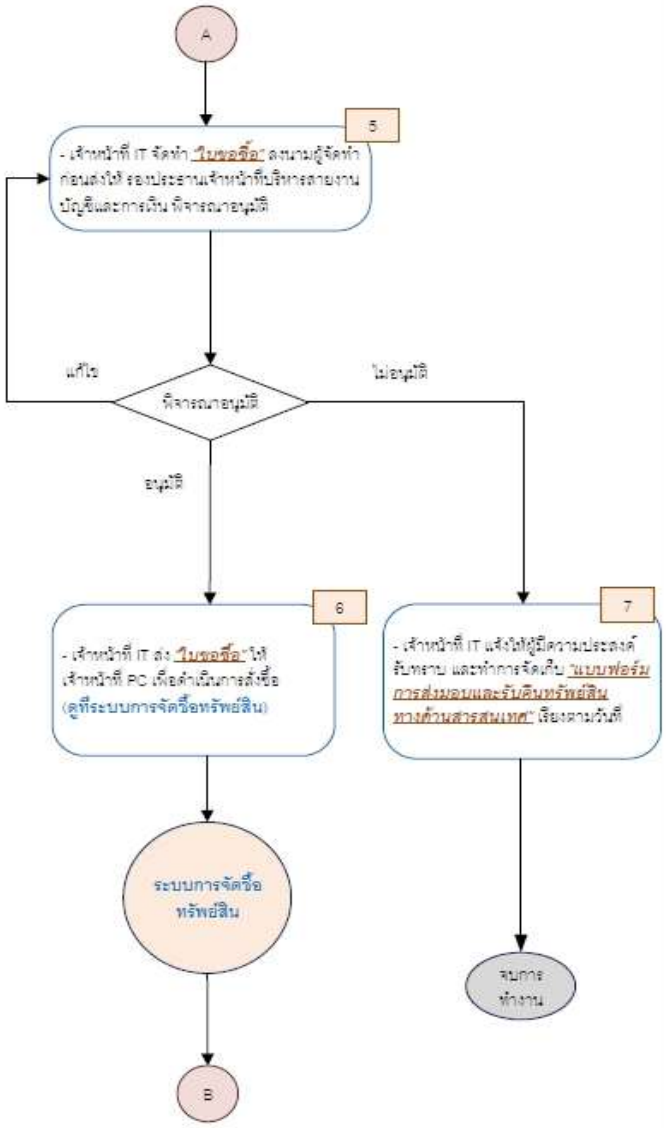
เอกสารที่ใช้ภายในบริษัท		**เอกสารภายนอก**
เอกสารที่มีเลขทะเบียนคุม	**เอกสารที่ไม่มีเลขทะเบียนคุม**	
ชื่อเอกสาร	**ชื่อเอกสาร**	**ชื่อเอกสาร**
แบบฟอร์มการส่งมอบและรับคืนทรัพย์สินทางด้านสารสนเทศ	-ไม่มี-	-ไม่มี-
แบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ		
ทะเบียนควบคุมทรัพย์สินสารสนเทศ		

ผู้ที่เกี่ยวข้อง

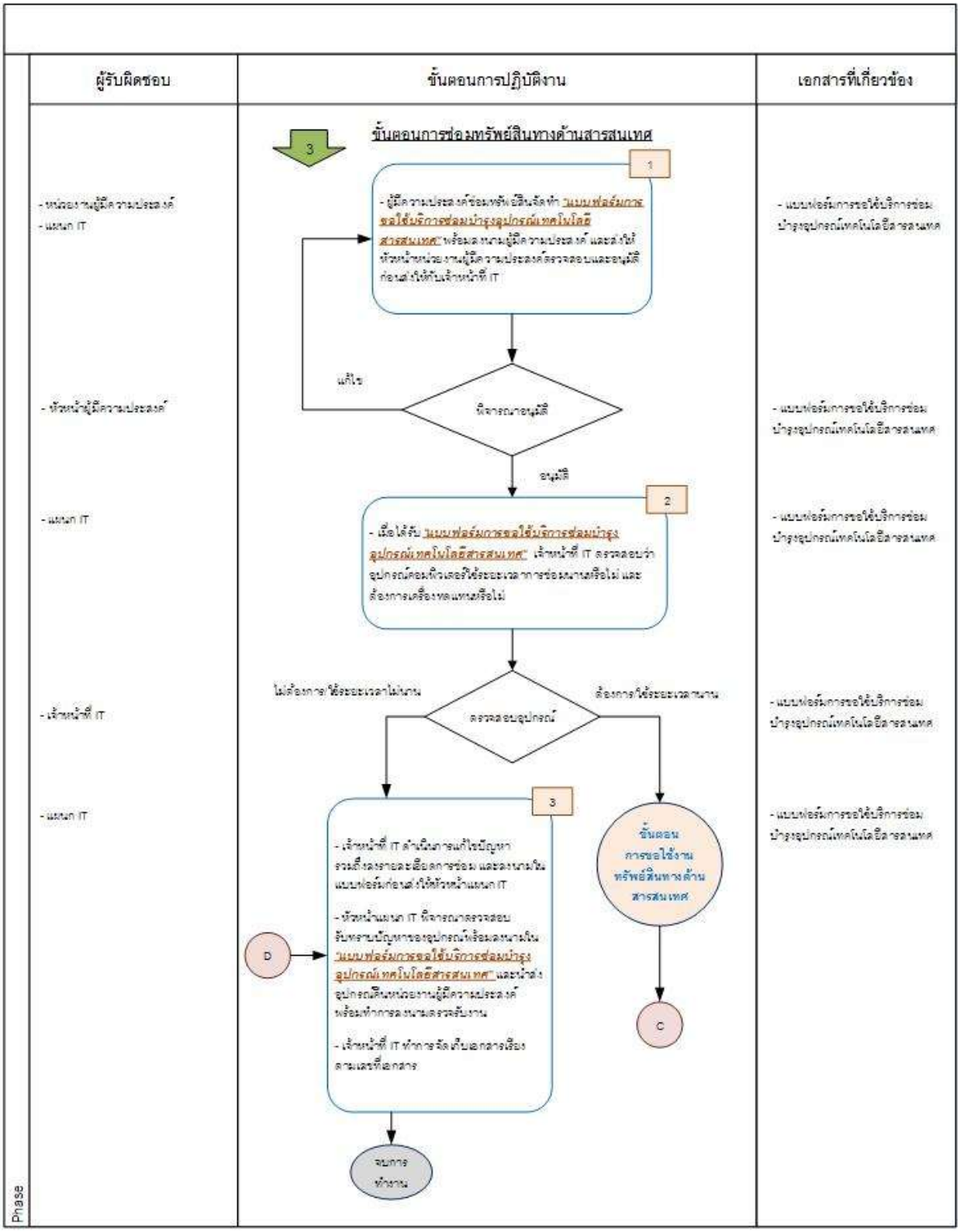
- แผนก IT
- แผนก HR
- แผนก PC
- แผนกที่เกี่ยวข้อง

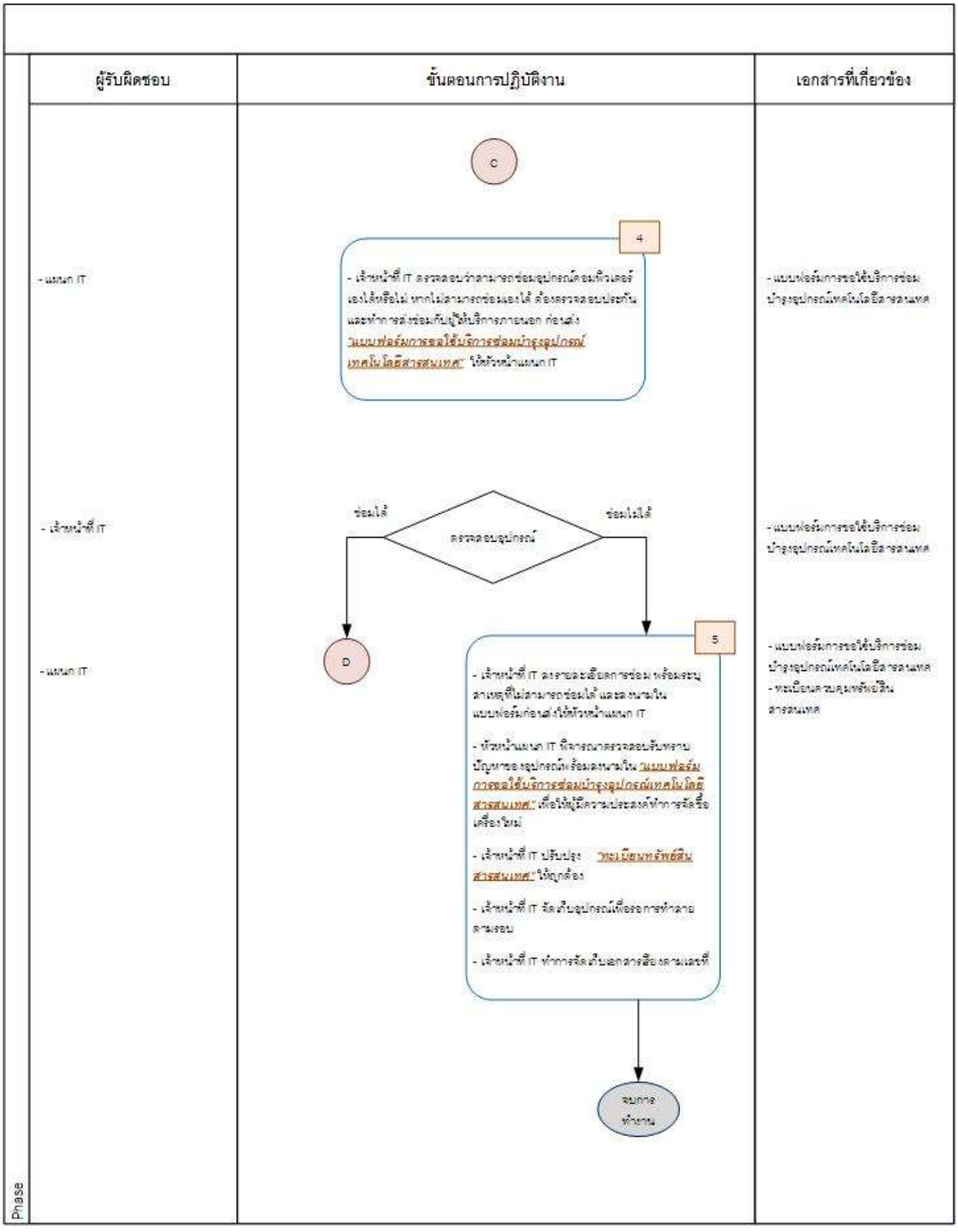

ผู้รับผิดชอบ
ขั้นตอนการปฏิบัติงาน
เอกสารที่เกี่ยวข้อง
2
ขั้นตอนการคืนทรัพย์สินทางด้านสารสนเทศ
1
- กรณีได้รับแจ้งจากเจ้าหน้าที่ HR มีการลาออกของพนักงาน และ/หรือผู้มีความประสงค์คืนอุปกรณ์ทรัพย์สินสารสนเทศยืมตัวคราว เจ้าหน้าที่ IT นำ "แบบฟอร์มการส่งมอบและรับคืนทรัพย์สินทางด้านสารสนเทศ" จากแท็บตัวคราวมาตรวจสอบกับทรัพย์สินที่มีการส่งมอบคืนให้ตรงกับ "ทะเบียนควบคุมทรัพย์สินสารสนเทศ"
- หน่วยงานผู้มีความประสงค์
- แผนก HR
- แผนก IT
- แบบฟอร์มการส่งมอบและรับคืนทรัพย์สินทางด้านสารสนเทศ
- ทะเบียนควบคุมทรัพย์สินสารสนเทศ
แก้ไข
ตรวจสอบ
- เจ้าหน้าที่ IT
ถูกต้อง
2
- เมื่อได้รับ "แบบฟอร์มการส่งมอบและรับคืนทรัพย์สินทางด้านสารสนเทศ" เจ้าหน้าที่ IT ตรวจสอบทรัพย์สินก่อนส่งให้กับผู้มีความประสงค์คืนทรัพย์สิน
- หน่วยงานผู้มีความประสงค์
- แผนก IT
- แบบฟอร์มการส่งมอบและรับคืนทรัพย์สินทางด้านสารสนเทศ
3
- เมื่อได้รับ "แบบฟอร์มการส่งมอบและรับคืนทรัพย์สินทางด้านสารสนเทศ" เจ้าหน้าที่ IT จัดเก็บเอกสารเรียงตามวันที่ และปรับปรุง "ทะเบียนควบคุมทรัพย์สินสารสนเทศ" ให้ถูกต้อง
- แผนก IT
- แบบฟอร์มการส่งมอบและรับคืนทรัพย์สินทางด้านสารสนเทศ
- ทะเบียนควบคุมทรัพย์สินสารสนเทศ
จบการทำงาน
Phase

ผู้รับผิดชอบ	ขั้นตอนการปฏิบัติงาน	เอกสารที่เกี่ยวข้อง
- แผนก IT	5 - เจ้าหน้าที่ IT จัดทำ "ใบขอซื้อ" ลงนามผู้จัดทำ ก่อนส่งให้ รองประธานเจ้าหน้าที่บริหารสายงานบัญชีและการเงิน พิจารณาอนุมัติ	- ใบขอซื้อ
- หัวหน้าแผนก IT	แก้ไข / ไม่อนุมัติ — พิจารณาอนุมัติ — อนุมัติ	- ใบขอซื้อ
- แผนก IT - แผนก PC -หน่วยงานผู้มีความประสงค์	6 - เจ้าหน้าที่ IT ส่ง "ใบขอซื้อ" ให้เจ้าหน้าที่ PC เพื่อดำเนินการสั่งซื้อ (ดูที่ระบบการจัดซื้อทรัพย์สิน) 7 - เจ้าหน้าที่ IT แจ้งให้ผู้มีความประสงค์รับทราบ และทำการจัดเก็บ "แบบฟอร์มการส่งมอบและรับคืนทรัพย์สินทางด้านสารสนเทศ" เรียงตามวันที่	- ใบขอซื้อ - แบบฟอร์มการส่งมอบและรับคืนทรัพย์สินทางด้านสารสนเทศ



Phase


ผู้รับผิดชอบ
ขั้นตอนการปฏิบัติงาน
เอกสารที่เกี่ยวข้อง
ขั้นตอนการซ่อมทรัพย์สินทางด้านสารสนเทศ
3
1
- หน่วยงานผู้มีความประสงค์
- แผนก IT
- ผู้มีความประสงค์ซ่อมทรัพย์สินจัดทำ วแบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ พร้อมลงนามผู้มีความประสงค์ และส่งให้หัวหน้าหน่วยงานผู้มีความประสงค์ตรวจสอบและอนุมัติก่อนส่งให้กับเจ้าหน้าที่ IT
- แบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ
แก้ไข
- หัวหน้าผู้มีความประสงค์
พิจารณาอนุมัติ
- แบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ
อนุมัติ
2
- แผนก IT
- เมื่อได้รับ วแบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ เจ้าหน้าที่ IT ตรวจสอบว่าอุปกรณ์คอมพิวเตอร์ใช้ระยะเวลาการซ่อมนานหรือไม่ และต้องการเครื่องทดแทนหรือไม่
- แบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ
ไม่ต้องการใช้ระยะเวลาไม่นาน
ต้องการใช้ระยะเวลานาน
- เจ้าหน้าที่ IT
ตรวจสอบอุปกรณ์
- แบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ
3
- แผนก IT
- เจ้าหน้าที่ IT ดำเนินการแก้ไขปัญหา รวมถึงลงรายละเอียดการซ่อม และลงนามในแบบฟอร์มก่อนส่งให้หัวหน้าแผนก IT
- หัวหน้าแผนก IT พิจารณาตรวจสอบรับทราบปัญหาของอุปกรณ์พร้อมลงนามใน วแบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ และนำส่งอุปกรณ์คืนหน่วยงานผู้มีความประสงค์ พร้อมทำการลงนามตรวจรับงาน
- เจ้าหน้าที่ IT ทำการจัดเก็บเอกสารเรียงตามเลขที่เอกสาร
- แบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ
ขั้นตอนการขอใช้งานทรัพย์สินทางด้านสารสนเทศ
D
C
จบการทำงาน
Phase


ผู้รับผิดชอบ
ขั้นตอนการปฏิบัติงาน
เอกสารที่เกี่ยวข้อง
C
4
- เจ้าหน้าที่ IT ตรวจสอบว่าสามารถซ่อมอุปกรณ์คอมพิวเตอร์เองได้หรือไม่ หากไม่สามารถซ่อมเองได้ ต้องตรวจสอบประกันและทำการส่งซ่อมกับผู้ให้บริการภายนอก ก่อนส่ง "แบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ" ให้หัวหน้าแผนก IT
- แผนก IT
- แบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ
ซ่อมได้
ตรวจสอบอุปกรณ์
ซ่อมไม่ได้
- เจ้าหน้าที่ IT
- แบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ
D
5
- เจ้าหน้าที่ IT ลงรายละเอียดการซ่อม พร้อมระบุสาเหตุที่ไม่สามารถซ่อมได้ และลงนามในแบบฟอร์มก่อนส่งให้หัวหน้าแผนก IT
- หัวหน้าแผนก IT พิจารณาตรวจสอบรับทราบปัญหาของอุปกรณ์พร้อมลงนามใน "แบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ" เพื่อให้ผู้มีความประสงค์ทำการจัดซื้อเครื่องใหม่
- เจ้าหน้าที่ IT ปรับปรุง "ทะเบียนทรัพย์สินสารสนเทศ" ให้ถูกต้อง
- เจ้าหน้าที่ IT จัดเก็บอุปกรณ์เพื่อรอการทำลายตามรอบ
- เจ้าหน้าที่ IT ทำการจัดเก็บเอกสารอย่างตามเดิม
- แผนก IT
- แบบฟอร์มการขอใช้บริการซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ
- ทะเบียนควบคุมทรัพย์สินสารสนเทศ
จบการทำงาน
Phase

การขอเพิ่ม ลบ และแก้ไขบัญชีผู้ใช้งาน

วัตถุประสงค์

1) เพื่อเป็นแนวทางในการกำกับดูแล ตรวจสอบ และติดตามการขอเพิ่ม แก้ไข และ ลบบัญชีผู้ใช้งาน ให้มีความสอดคล้องกับระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2) เพื่อสื่อสารชี้แจงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่บริษัทควรมีมาตรการบริหารจัดการความเสี่ยงนั้นอย่างเหมาะสม
3) เพื่อให้บริษัทบริหารจัดการและปฏิบัติงานภายใต้ความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

คำนิยาม

- **ผู้ที่มีความประสงค์** หมายถึง พนักงานภายในบริษัท หรือ บุคคลที่ต้องการใช้การปฏิบัติงานในบริษัท
- **หัวหน้าหน่วยงาน** หมายถึง ผู้มีอำนาจในหน่วยงานนั้น ๆ และเป็นงานที่อยู่ในงานรับผิดชอบของหน่วยงานนั้น ๆ
- **ผู้ดูแลระบบ** หมายถึง ผู้ทำหน้าที่บริหารและจัดการระบบคอมพิวเตอร์ในองค์กร สร้าง ออกแบบและบำรุงรักษาบัญชีผู้ใช้
- **บัญชีผู้ใช้งาน** หมายถึง บัญชีผู้ใช้งานเป็นสิ่งที่ใช้สำหรับยืนยันความถูกต้องของตัวบุคคลนั้น ๆ ในการเข้าถึงข้อมูลของบริษัท

ข้อกำหนด

1) การเปลี่ยนรหัสการใช้งาน

- ***กำหนดรหัสการใช้งานให้เป็นรหัสผ่านที่สามารถระบุตัวตนของแต่ละคน***เพื่อแยกการทำงาน รวมถึงสามารถที่จะติดตามและรู้การทำงานของแต่ละผู้ใช้งานได้หากเกิดปัญหาขึ้น
- ***กำหนดให้ทำการเปลี่ยนรหัสการใช้งานครั้งแรกเพื่อป้องกันบุคคลอื่นเข้าโดยไม่ได้รับอนุญาต*** โดยใช้ Password Policy ที่ใช้งานด้วยกันทั้งบริษัท

2) การเพิ่มบัญชีผู้ใช้งาน

- เมื่อมีพนักงานเข้าใหม่หรือต้องการแก้ไขสิทธิ์การใช้งาน ผู้มีความประสงค์จัดทำ ***"แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ"*** พร้อมทั้งจัดส่งให้แผนก IT หรือผู้ดูแลระบบ
- เจ้าหน้าที่ IT หรือผู้ดูแลระบบ ***ทำการสร้างบัญชีผู้ใช้งานพื้นฐานในระบบ หรือแก้ไขบัญชีผู้ใช้งานตาม "แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ"*** โดยระบุผู้ใช้งานอย่างชัดเจน
- เจ้าหน้าที่ IT หรือผู้ดูแลระบบ ***ทำการบันทึกไว้เป็นหลักฐานว่าได้มีการจัดทำผู้ใช้งานใหม่และส่งให้กับผู้ใช้งาน***

3) การลบบัญชีผู้ใช้งาน

- เมื่อมีพนักงานลาออก ***<u>เจ้าหน้าที่ HR ที่มีหน้าที่รับผิดชอบจัดเตรียมรายชื่อพนักงานลาออก</u>*** จัดส่งให้เจ้าหน้าที่ IT หรือผู้ดูแลระบบ เพื่อระงับบัญชีผู้ใช้งานในระบบสารสนเทศ
- เจ้าหน้าที่ IT หรือผู้แลระบบ***<u>ตรวจเช็คข้อมูลและสำรองข้อมูลก่อนทำการลบบัญชี</u>***
- หากต้องการจะใช้งานรหัสผู้ใช้งานที่ลาออกแล้ว ***<u>ต้องทำการอนุมัติโดยหัวหน้าแผนก IT หรือผู้มีอำนาจอนุมัติ</u>***

4) การแก้ไขบัญชีผู้ใช้งาน

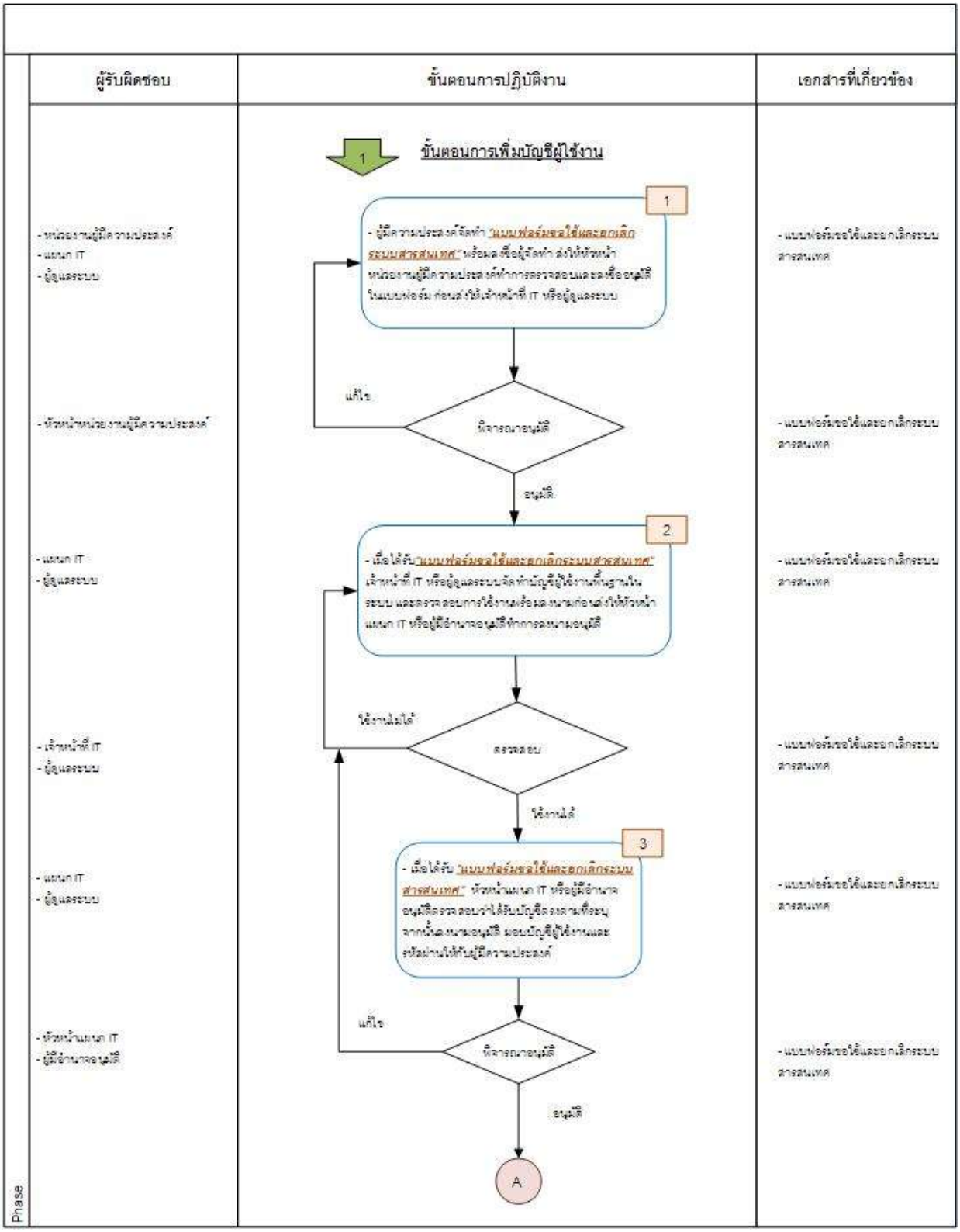
- เมื่อผู้มีความประสงค์ต้องการแก้ไขสิทธิ์การใช้งาน ***<u>ผู้มีความประสงค์จัดทำ “แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ”</u>*** พร้อมทั้งจัดส่งให้เจ้าหน้าที่ IT หรือผู้ดูแลระบบ
- เจ้าหน้าที่ IT หรือผู้ดูแลระบบ ***<u>ทำการแก้ไขบัญชีผู้ใช้งานตาม “แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ”</u>*** พร้อมแจ้งให้ผู้มีความประสงค์รับทราบ
- เจ้าหน้าที่ IT หรือผู้ดูแลระบบ***<u>ทำการบันทึกไว้เป็นหลักฐานว่าได้มีการแก้ไขบัญชีผู้ใช้งานและส่งให้กับผู้ใช้งาน</u>***

เอกสารที่เกี่ยวข้อง

เอกสารที่ใช้ภายในบริษัท		**เอกสารภายนอก**
เอกสารที่มีเลขทะเบียนคุม	**เอกสารที่ไม่มีเลขทะเบียนคุม**	
ชื่อเอกสาร	**ชื่อเอกสาร**	**ชื่อเอกสาร**
แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ	-ไม่มี-	-ไม่มี-
รายงานรายชื่อพนักงานลาออก		

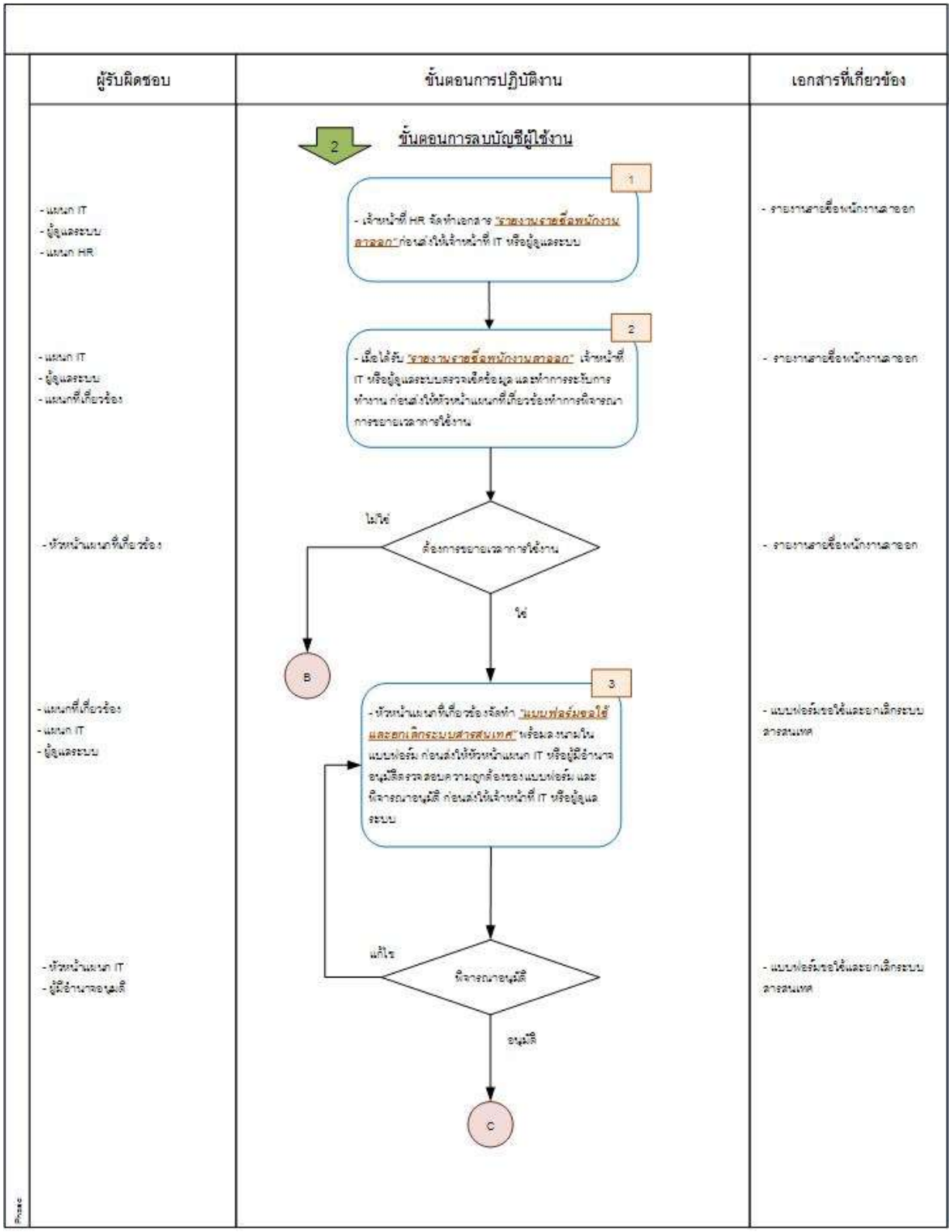
ผู้ที่เกี่ยวข้อง

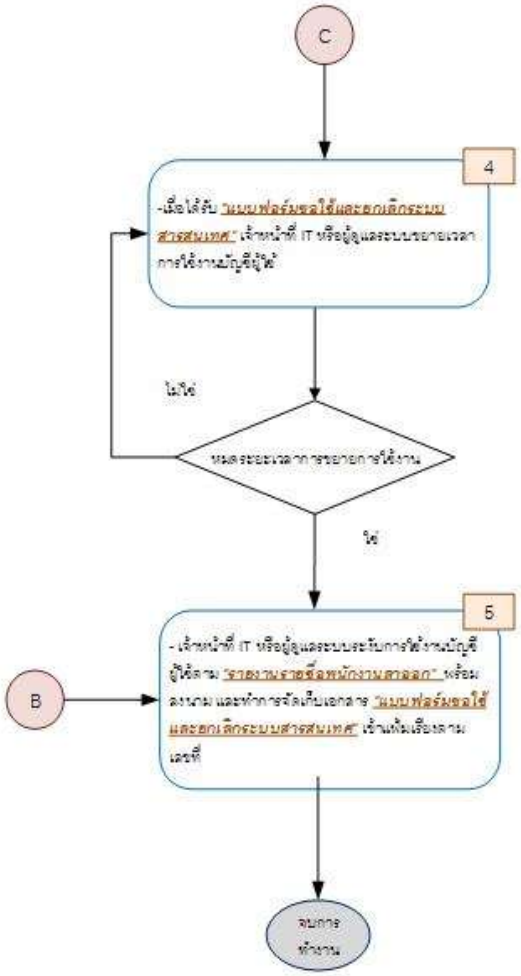
- แผนก IT
- แผนก HR
- แผนกที่เกี่ยวข้อง


ผู้รับผิดชอบ
ขั้นตอนการปฏิบัติงาน
เอกสารที่เกี่ยวข้อง
ขั้นตอนการเพิ่มบัญชีผู้ใช้งาน
1
- หน่วยงานผู้มีความประสงค์
- แผนก IT
- ผู้ดูแลระบบ
- ผู้มีความประสงค์จัดทำ "แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ" พร้อมลงชื่อผู้จัดทำ ส่งให้หัวหน้าหน่วยงานผู้มีความประสงค์ทำการตรวจสอบและลงชื่ออนุมัติในแบบฟอร์ม ก่อนส่งให้เจ้าหน้าที่ IT หรือผู้ดูแลระบบ
- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
แก้ไข
- หัวหน้าหน่วยงานผู้มีความประสงค์
พิจารณาอนุมัติ
- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
อนุมัติ
2
- แผนก IT
- ผู้ดูแลระบบ
- เมื่อได้รับ "แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ" เจ้าหน้าที่ IT หรือผู้ดูแลระบบจัดทำบัญชีผู้ใช้งานขั้นพื้นฐานในระบบ และตรวจสอบการใช้งานเรียบร้อย นำมาก่อนส่งให้หัวหน้าแผนก IT หรือผู้มีอำนาจอนุมัติทำการลงนามอนุมัติ
- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
ใช้งานไม่ได้
- เจ้าหน้าที่ IT
- ผู้ดูแลระบบ
ตรวจสอบ
- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
ใช้งานได้
3
- แผนก IT
- ผู้ดูแลระบบ
- เมื่อได้รับ "แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ" หัวหน้าแผนก IT หรือผู้มีอำนาจอนุมัติตรวจสอบว่าได้รับบัญชีตามที่ระบุจากนั้นลงนามอนุมัติ มอบบัญชีผู้ใช้งานและรหัสผ่านให้กับผู้มีความประสงค์
- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
แก้ไข
- หัวหน้าแผนก IT
- ผู้มีอำนาจอนุมัติ
พิจารณาอนุมัติ
- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
อนุมัติ
A
Phase

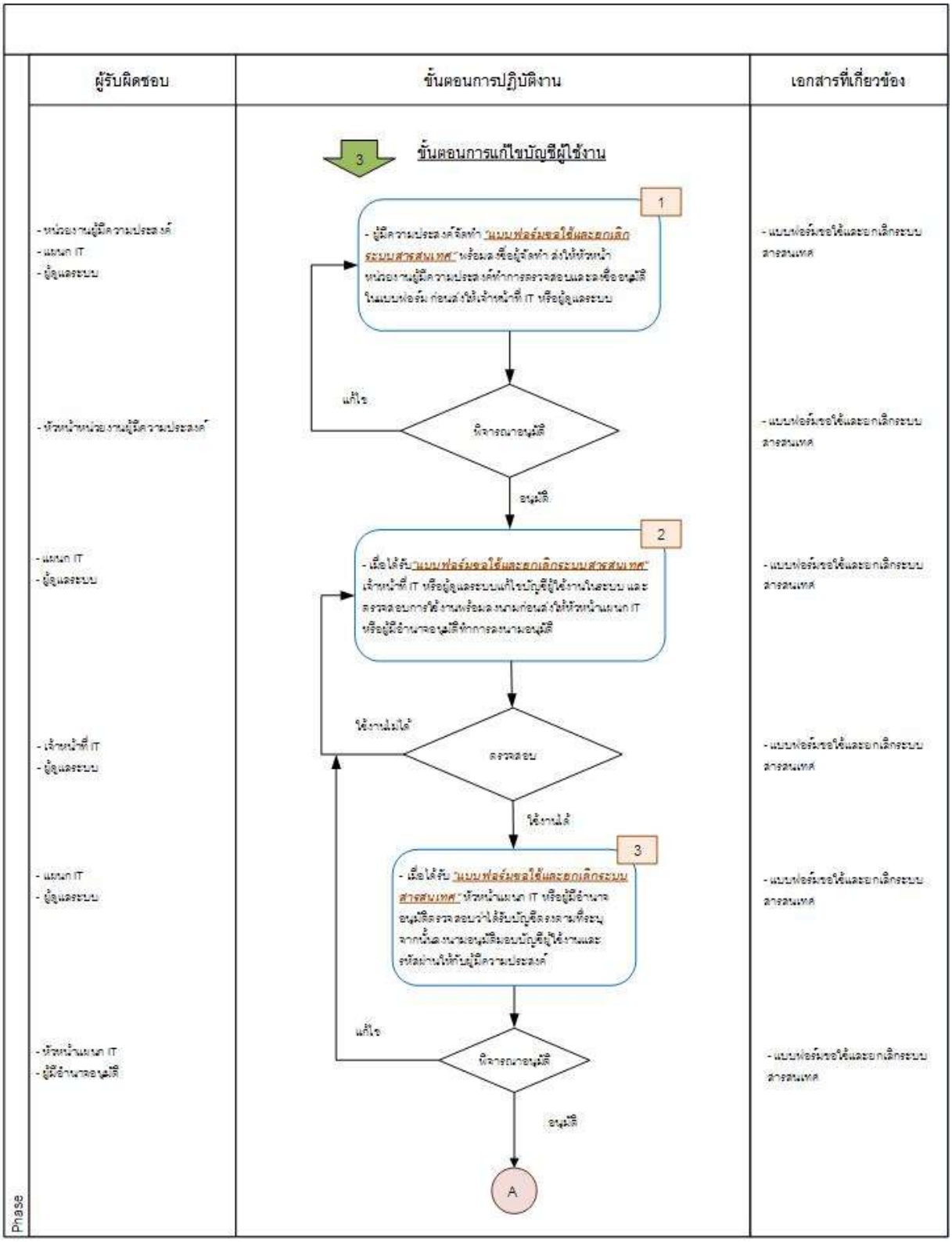
ผู้รับผิดชอบ	ขั้นตอนการปฏิบัติงาน	เอกสารที่เกี่ยวข้อง
- หน่วยงานผู้มีความประสงค์ - แผนก IT - ผู้ดูแลระบบ		- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ - แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ

Phase


ผู้รับผิดชอบ
ขั้นตอนการปฏิบัติงาน
เอกสารที่เกี่ยวข้อง
2
ขั้นตอนการลบบัญชีผู้ใช้งาน
1
- เจ้าหน้าที่ HR จัดทำเอกสาร "รายงานรายชื่อพนักงานลาออก" ก่อนส่งให้เจ้าหน้าที่ IT หรือผู้ดูแลระบบ
- แผนก IT
- ผู้ดูแลระบบ
- แผนก HR
- รายงานรายชื่อพนักงานลาออก
2
- เมื่อได้รับ "รายงานรายชื่อพนักงานลาออก" เจ้าหน้าที่ IT หรือผู้ดูแลระบบตรวจเช็คข้อมูล และทำการระงับการทำงาน ก่อนส่งให้หัวหน้าแผนกที่เกี่ยวข้องทำการพิจารณาการขยายเวลาการใช้งาน
- แผนก IT
- ผู้ดูแลระบบ
- แผนกที่เกี่ยวข้อง
- รายงานรายชื่อพนักงานลาออก
ไม่ใช่
ต้องการขยายเวลาการใช้งาน
- หัวหน้าแผนกที่เกี่ยวข้อง
- รายงานรายชื่อพนักงานลาออก
ใช่
B
3
- หัวหน้าแผนกที่เกี่ยวข้องจัดทำ "แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ" พร้อมลงนามในแบบฟอร์ม ก่อนส่งให้หัวหน้าแผนก IT หรือผู้มีอำนาจอนุมัติตรวจสอบความถูกต้องของแบบฟอร์ม และพิจารณาอนุมัติ ก่อนส่งให้เจ้าหน้าที่ IT หรือผู้ดูแลระบบ
- แผนกที่เกี่ยวข้อง
- แผนก IT
- ผู้ดูแลระบบ
- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
แก้ไข
พิจารณาอนุมัติ
- หัวหน้าแผนก IT
- ผู้มีอำนาจอนุมัติ
- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
อนุมัติ
C

ผู้รับผิดชอบ	ขั้นตอนการปฏิบัติงาน	เอกสารที่เกี่ยวข้อง
- แผนก IT - ผู้ดูแลระบบ		- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
- เจ้าหน้าที่ IT - ผู้ดูแลระบบ		- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
- แผนก IT - ผู้ดูแลระบบ		- รายงานลายชื่อพนักงานลาออก - แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ

Phase


ผู้รับผิดชอบ
ขั้นตอนการปฏิบัติงาน
เอกสารที่เกี่ยวข้อง
3
ขั้นตอนการแก้ไขบัญชีผู้ใช้งาน
1
- ผู้มีความประสงค์จัดทำ "แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ" พร้อมลงชื่อผู้จัดทำ ส่งให้หัวหน้าหน่วยงานผู้มีความประสงค์ทำการตรวจสอบและลงชื่ออนุมัติในแบบฟอร์ม ก่อนส่งให้เจ้าหน้าที่ IT หรือผู้ดูแลระบบ
- หน่วยงานผู้มีความประสงค์
- แผนก IT
- ผู้ดูแลระบบ
- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
แก้ไข
พิจารณาอนุมัติ
- หัวหน้าหน่วยงานผู้มีความประสงค์
- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
อนุมัติ
2
- เมื่อได้รับ "แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ" เจ้าหน้าที่ IT หรือผู้ดูแลระบบแก้ไขบัญชีผู้ใช้งานในระบบ และตรวจสอบการใช้งานพร้อมลงนามก่อนส่งให้หัวหน้าแผนก IT หรือผู้มีอำนาจอนุมัติทำการลงนามอนุมัติ
- แผนก IT
- ผู้ดูแลระบบ
- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
ใช้งานไม่ได้
ตรวจสอบ
- เจ้าหน้าที่ IT
- ผู้ดูแลระบบ
- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
ใช้งานได้
3
- เมื่อได้รับ "แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ" หัวหน้าแผนก IT หรือผู้มีอำนาจอนุมัติตรวจสอบว่าได้รับบัญชีรายการที่ระบุจากนั้นลงนามอนุมัติมอบบัญชีผู้ใช้งานและรหัสผ่านให้กับผู้มีความประสงค์
- แผนก IT
- ผู้ดูแลระบบ
- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
แก้ไข
พิจารณาอนุมัติ
- หัวหน้าแผนก IT
- ผู้มีอำนาจอนุมัติ
- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
อนุมัติ
A
Phase

ผู้รับผิดชอบ	ขั้นตอนการปฏิบัติงาน	เอกสารที่เกี่ยวข้อง
- หน่วยงานผู้มีความประสงค์ - แผนก IT - ผู้ดูแลระบบ	A 4 - เมื่อได้รับ "แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ" และบัญชีผู้ใช้งานผู้มีความประสงค์ทำการลงนามในแบบฟอร์ม ก่อนส่งให้เจ้าหน้าที่ IT หรือผู้ดูแลระบบ	- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ
- แผนก IT - ผู้ดูแลระบบ	5 -เมื่อได้รับ "แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ" เจ้าหน้าที่ IT หรือผู้ดูแลระบบจัดเก็บเอกสารเรียงตามเลขที่ จบการทำงาน	- แบบฟอร์มขอใช้และยกเลิกระบบสารสนเทศ

Phase

การขอแก้ไข และเปลี่ยนแปลงระบบงาน

วัตถุประสงค์

1) เพื่อเป็นแนวทางในการกำกับดูแล ตรวจสอบ และติดตามการขอแก้ไข และ เปลี่ยนแปลงระบบงาน ให้มีความสอดคล้องกับระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2) เพื่อสื่อสารชี้แจงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่บริษัทควรมีมาตรการบริหารจัดการความเสี่ยงนั้นอย่างเหมาะสม
3) เพื่อให้บริษัทบริหารจัดการและปฏิบัติงานภายใต้ความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

คำนิยาม

- **ผู้ร้องขอระบบ** หมายถึง บุคคลที่ต้องการแก้ไข เปลี่ยนแปลงระบบ เพื่อใช้ในการปฏิบัติงาน
- **หัวหน้าหน่วยงาน** หมายถึง ผู้มีอำนาจในหน่วยงานนั้น ๆ และเป็นงานที่อยู่ในงานรับผิดชอบของหน่วยงานนั้น ๆ
- **ผู้พัฒนาระบบ** หมายถึง ผู้มีหน้าที่ แก้ไข เปลี่ยนแปลงระบบตามที่ได้รับการร้องขอ

ข้อกำหนด

1) **วิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย**
   - กำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือซื้อมาใช้งาน
   - แผนก IT จะต้องทำการวิเคราะห์ระบบที่จะพัฒนาขึ้นมาใช้งานว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย
2) **การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ**
   - กำหนดความมั่นคงปลอดภัยให้กับไฟล์ต่าง ๆ ของระบบที่ให้บริการไว้อย่างชัดเจน
3) **การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ**
   - ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบจะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้น ๆ
   - แผนก IT ทำการบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ แจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง
4) **การตรวจสอบการทำงานของแอพพลิเคชั่นภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ**
   - ทำการตรวจสอบทางเทคนิคภายหลังจากที่ทำการเปลี่ยนแปลงระบบปฏิบัติการเพื่อดูว่าแอพพลิเคชั่นที่ทำงานอยู่บนระบบปฏิบัติการนั้น ทำงานผิดปกติไม่สามารถใช้งานได้ หรือมีปัญหาทางด้านความมั่นคงปลอดภัยเกิดขึ้น

5) การจำกัดการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต

- ต้องหลีกเลี่ยงการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต หากจำเป็นต้องแก้ไข ต้องทำตามความจำเป็นเท่านั้น และต้องมีการควบคุมการแก้ไขนั้นอย่างเข้มงวด

6) กระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์

- คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ์ในการแก้ไขระบบ
- ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
- ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
- เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ
- ต้องมีการเก็บรายละเอียดของคำขอไว้
- ต้องมีการจัดเก็บเอกสารการร้องขอเป็นระบบ

7) การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

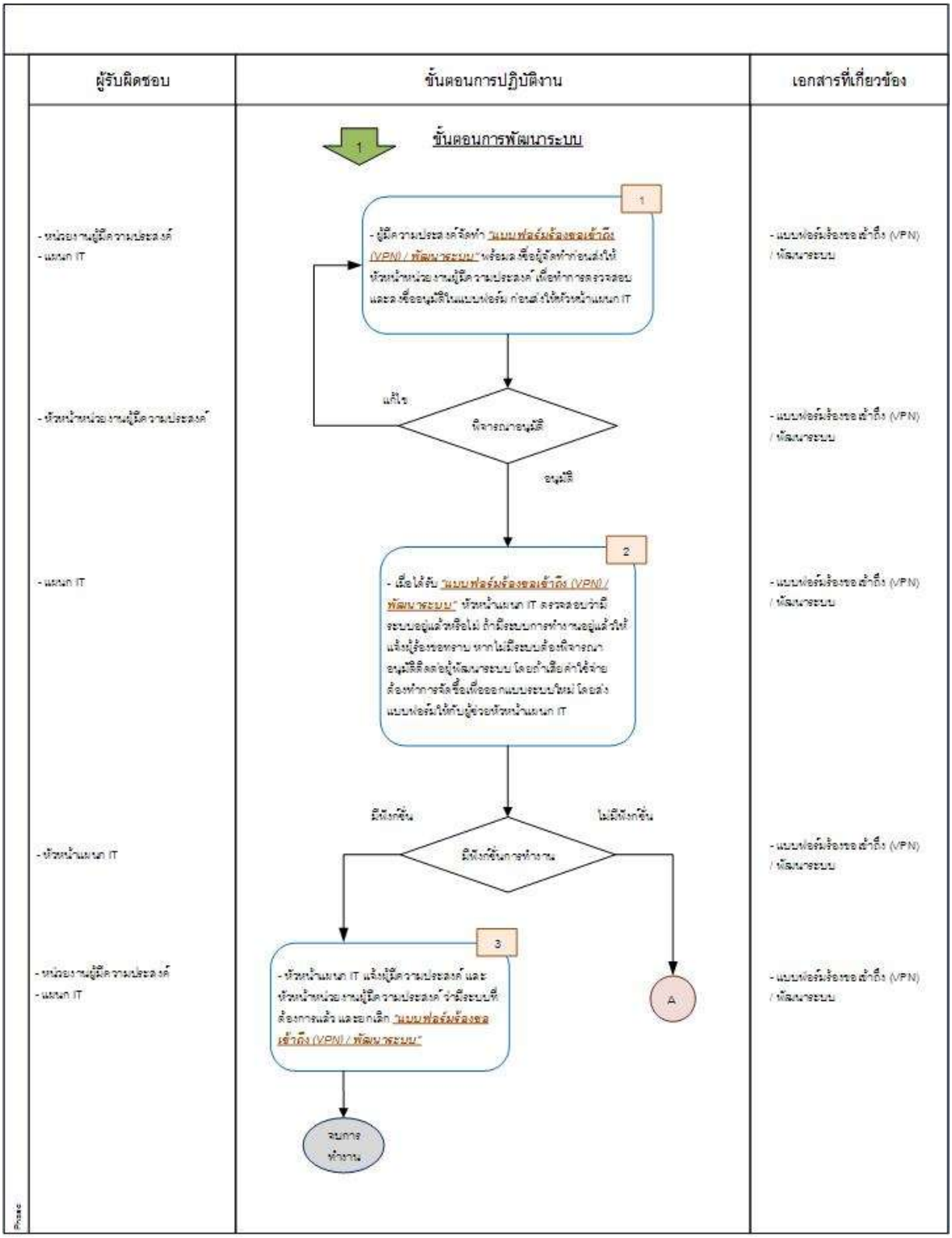
- ต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบโดยละเอียดก่อนติดตั้งใช้งานจริง
- ต้องมีการรับรองคุณภาพของระบบในการทำงานจริง
- ต้องมีการกำหนดขอบเขตในการจ้างพัฒนาระบบอย่างชัดเจน

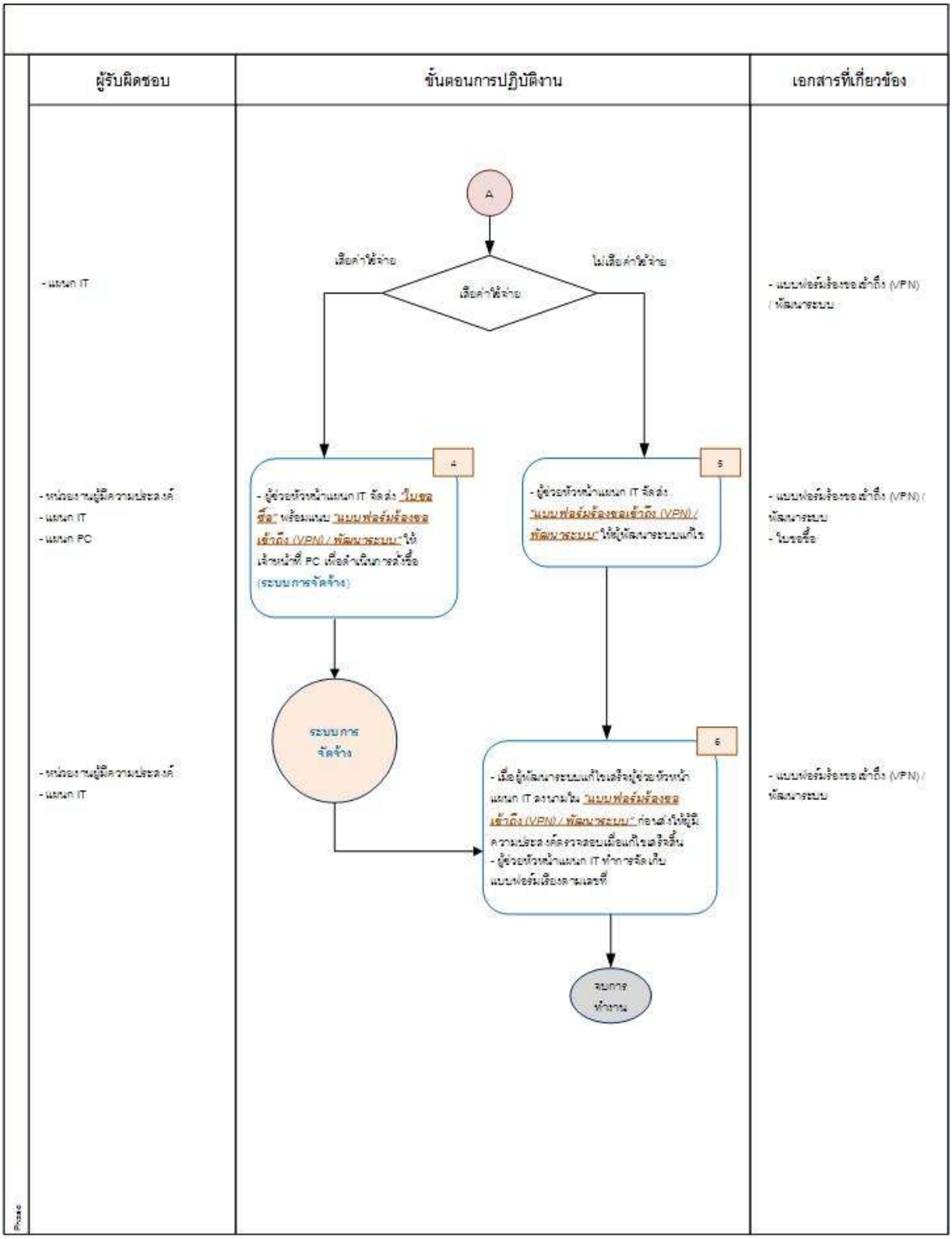
เอกสารที่เกี่ยวข้อง

เอกสารที่ใช้ภายในบริษัท		**เอกสารภายนอก**
เอกสารที่มีเลขทะเบียนคุม	**เอกสารที่ไม่มีเลขทะเบียนคุม**	
ชื่อเอกสาร	**ชื่อเอกสาร**	**ชื่อเอกสาร**
แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ	-ไม่มี-	-ไม่มี-
	ใบขอซื้อ	

ผู้ที่เกี่ยวข้อง

- แผนก IT
- แผนก PC
- แผนกที่เกี่ยวข้อง


ผู้รับผิดชอบ
ขั้นตอนการปฏิบัติงาน
เอกสารที่เกี่ยวข้อง
ขั้นตอนการพัฒนาระบบ
1
- หน่วยงานผู้มีความประสงค์
- แผนก IT
- แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ
- ผู้มีความประสงค์จัดทำ "แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ" พร้อมลงชื่อผู้จัดทำก่อนส่งให้หัวหน้าหน่วยงานผู้มีความประสงค์ เพื่อทำการตรวจสอบและลงชื่ออนุมัติในแบบฟอร์ม ก่อนส่งให้หัวหน้าแผนก IT
- หัวหน้าหน่วยงานผู้มีความประสงค์
- แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ
แก้ไข
พิจารณาอนุมัติ
อนุมัติ
- แผนก IT
- แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ
2
- เมื่อได้รับ "แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ" หัวหน้าแผนก IT ตรวจสอบว่ามีระบบอยู่แล้วหรือไม่ ถ้ามีระบบการทำงานอยู่แล้วให้แจ้งผู้ร้องขอทราบ หากไม่มีระบบต้องพิจารณาอนุมัติติดต่อผู้พัฒนาระบบ โดยถ้าเสียค่าใช้จ่ายต้องทำการจัดซื้อเพื่อออกแบบระบบใหม่ โดยส่งแบบฟอร์มให้กับผู้ช่วยหัวหน้าแผนก IT
มีพักขั้น
ไม่มีพักขั้น
มีพักขั้นการทำงาน
- หัวหน้าแผนก IT
- แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ
3
- หัวหน้าแผนก IT แจ้งผู้มีความประสงค์ และหัวหน้าหน่วยงานผู้มีความประสงค์ ว่ามีระบบที่ต้องการแล้ว และยกเลิก "แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ"
A
- หน่วยงานผู้มีความประสงค์
- แผนก IT
- แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ
จบการทำงาน


ผู้รับผิดชอบ
ขั้นตอนการปฏิบัติงาน
เอกสารที่เกี่ยวข้อง
A
เสียค่าใช้จ่าย
ไม่เสียค่าใช้จ่าย
เสียค่าใช้จ่าย
- แผนก IT
- แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ
4
- ผู้ช่วยหัวหน้าแผนก IT จัดส่ง "ใบขอซื้อ" พร้อมแนบ "แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ" ให้เจ้าหน้าที่ PC เพื่อดำเนินการสั่งซื้อ (ระบบการจัดจ้าง)
5
- ผู้ช่วยหัวหน้าแผนก IT จัดส่ง "แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ" ให้ผู้พัฒนาระบบแก้ไข
- หน่วยงานผู้มีความประสงค์
- แผนก IT
- แผนก PC
- แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ
- ใบขอซื้อ
ระบบการจัดจ้าง
6
- เมื่อผู้พัฒนาระบบแก้ไขเสร็จผู้ช่วยหัวหน้าแผนก IT ดำเนินการ "แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ" ก่อนส่งให้ผู้มีความประสงค์ตรวจสอบเพื่อแก้ไขเสร็จสิ้น
- ผู้ช่วยหัวหน้าแผนก IT ทำการจัดเก็บแบบฟอร์มเรียงตามเลขที่
- หน่วยงานผู้มีความประสงค์
- แผนก IT
- แบบฟอร์มร้องขอเข้าถึง (VPN) / พัฒนาระบบ
จบการทำงาน

การสอบทานสิทธิ์ผู้ใช้งาน

วัตถุประสงค์

1) เพื่อเป็นแนวทางในการกำกับดูแล ตรวจสอบ และติดตามกระบวนการสอบทานสิทธิ์ผู้ใช้งานให้มีความสอดคล้องกับระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2) เพื่อสื่อสารชี้แจงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่บริษัทควรมีมาตรการบริหารจัดการความเสี่ยงนั้นอย่างเหมาะสม
3) เพื่อให้บริษัทบริหารจัดการและปฏิบัติงานภายใต้ความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

คำนิยาม

- **สิทธิ์** หมายถึง อำนาจที่จะกระทำการใด ๆ ตามที่ได้รับมอบหมายจากบริษัท/ผู้มีอำนาจในบริษัท
- **ผู้ที่มีความประสงค์** หมายถึง พนักงานภายในบริษัท หรือ บุคคลที่ต้องการใช้การปฏิบัติงานในบริษัท
- **หัวหน้าหน่วยงาน** หมายถึง ผู้มีอำนาจในหน่วยงานนั้น ๆ และเป็นงานที่อยู่ในงานรับผิดชอบของหน่วยงานนั้น ๆ
- **ผู้สอบทาน** หมายถึง ผู้ตรวจสอบข้อมูล หนังสือ ข้อความ ให้ตรงกับต้นฉบับ

ข้อกำหนด

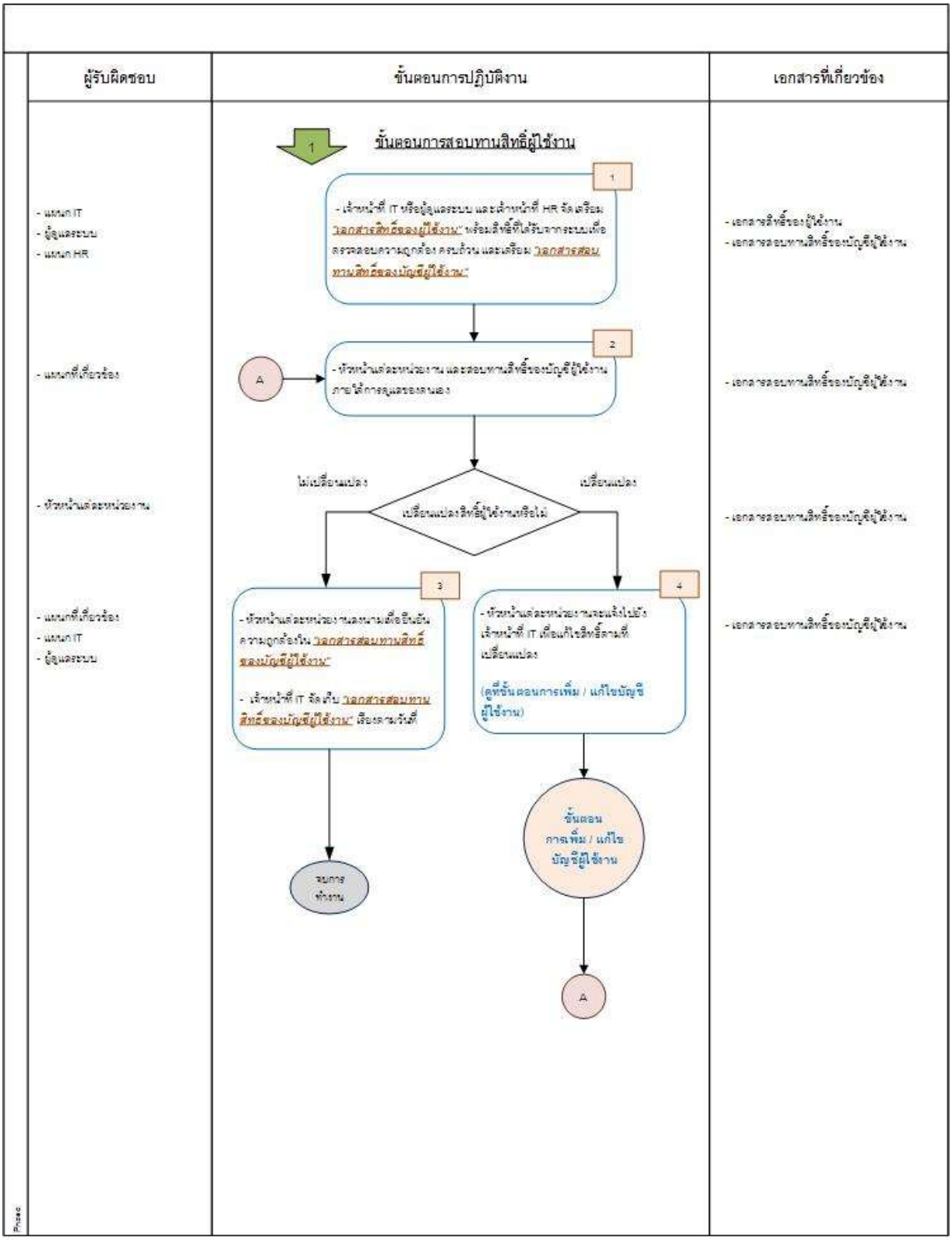
- ***กำหนดผู้ใช้งาน ให้ใช้แยกในแต่ละส่วนการใช้งาน***เพื่อที่สามารถควบคุมและดูแลการใช้งานได้อย่างถูกต้อง
- ***กำหนดขั้นตอนการเข้าถึงในการใช้งานให้เป็นของผู้ใช้งานแต่ละคน***เพื่อแยกการทำงานรวมถึงสามารถที่จะติดตามและรู้การทำงานของแต่ละผู้ใช้งานได้หากเกิดปัญหาขึ้น
- ***กำหนดสิทธิ์ได้ถูกต้องกับการทำงาน***
- หากผู้ใช้งาน***มีสิทธิ์ในระบบถูกต้อง***จะทำการตอบกลับ เพื่อ***ไม่ต้องเปลี่ยนแปลงสิทธิ์การทำงาน***
- หากผู้ใช้งาน***มีสิทธิ์ในระบบไม่ถูกต้อง*** จะทำการตอบกลับ เพื่อ***เปลี่ยนแปลงสิทธิ์การทำงานให้ถูกต้องกับการทำงาน***

เอกสารที่เกี่ยวข้อง

เอกสารที่ใช้ภายในบริษัท		เอกสารภายนอก
เอกสารที่มีเลขทะเบียนคุม	**เอกสารที่ไม่มีเลขทะเบียนคุม**	
ชื่อเอกสาร	**ชื่อเอกสาร**	**ชื่อเอกสาร**
เอกสารสิทธิ์ของผู้ใช้งาน	-ไม่มี-	-ไม่มี-
เอกสารสอบทานสิทธิ์ของบัญชีผู้ใช้งาน		

ผู้ที่เกี่ยวข้อง

- แผนก IT
- แผนก HR
- แผนกที่เกี่ยวข้อง


ผู้รับผิดชอบ
ขั้นตอนการปฏิบัติงาน
เอกสารที่เกี่ยวข้อง
ขั้นตอนการสอบทานสิทธิ์ผู้ใช้งาน
1
- เจ้าหน้าที่ IT หรือผู้ดูแลระบบ และเจ้าหน้าที่ HR จัดเตรียม "เอกสารสิทธิ์ของผู้ใช้งาน" พร้อมสิทธิ์ที่ได้รับจากระบบเพื่อตรวจสอบความถูกต้อง ครบถ้วน และเสร็จแล้ว "เอกสารสอบทานสิทธิ์ของบัญชีผู้ใช้งาน"
- แผนก IT
- ผู้ดูแลระบบ
- แผนก HR
- เอกสารสิทธิ์ของผู้ใช้งาน
- เอกสารสอบทานสิทธิ์ของบัญชีผู้ใช้งาน
2
A
- หัวหน้าแต่ละหน่วยงาน และสอบทานสิทธิ์ของบัญชีผู้ใช้งานภายใต้การดูแลของตนเอง
- แผนกที่เกี่ยวข้อง
- เอกสารสอบทานสิทธิ์ของบัญชีผู้ใช้งาน
ไม่เปลี่ยนแปลง
เปลี่ยนแปลง
เปลี่ยนแปลงสิทธิ์ผู้ใช้งานหรือไม่
- หัวหน้าแต่ละหน่วยงาน
- เอกสารสอบทานสิทธิ์ของบัญชีผู้ใช้งาน
3
- หัวหน้าแต่ละหน่วยงานลงนามเพื่อยืนยันความถูกต้องใน "เอกสารสอบทานสิทธิ์ของบัญชีผู้ใช้งาน"
- เจ้าหน้าที่ IT จัดเก็บ "เอกสารสอบทานสิทธิ์ของบัญชีผู้ใช้งาน" เรียงตามวันที่
- แผนกที่เกี่ยวข้อง
- แผนก IT
- ผู้ดูแลระบบ
4
- หัวหน้าแต่ละหน่วยงานจะแจ้งไปยังเจ้าหน้าที่ IT เพื่อแก้ไขสิทธิ์ตามที่เปลี่ยนแปลง
(ดูที่ขั้นตอนการเพิ่ม / แก้ไขบัญชีผู้ใช้งาน)
- เอกสารสอบทานสิทธิ์ของบัญชีผู้ใช้งาน
จบการทำงาน
ขั้นตอนการเพิ่ม / แก้ไขบัญชีผู้ใช้งาน
A

การสำรอง และกู้คืนข้อมูล

วัตถุประสงค์

1) เพื่อเป็นแนวทางในการกำกับดูแล ตรวจสอบ และติดตามกระบวนการสำรอง และ กู้คืนข้อมูลให้มีความสอดคล้องกับระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2) เพื่อสื่อสารชี้แจงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่บริษัทควรมีมาตรการบริหารจัดการความเสี่ยงนั้นอย่างเหมาะสม
3) เพื่อให้บริษัทบริหารจัดการและปฏิบัติงานภายใต้ความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

คำนิยาม

- **ผู้มีความประสงค์** หมายถึง บุคคลที่ต้องการข้อมูลเก่าที่ไม่มีอยู่ในระบบแล้วหรือมีการลบออกโดยไม่ได้มีการเก็บในเครื่อง เพื่อใช้ในการปฏิบัติงาน
- **หัวหน้าหน่วยงาน** หมายถึง ผู้มีอำนาจในหน่วยงานนั้น ๆ และเป็นงานที่อยู่ในงานรับผิดชอบของหน่วยงานนั้น ๆ
- **ผู้ดูแลระบบ** หมายถึง ผู้ทำหน้าที่บริหารและจัดการระบบคอมพิวเตอร์ในองค์กร สร้าง ออกแบบและบำรุงรักษาบัญชีผู้ใช้
- **สำรองข้อมูล** หมายถึง การสำรองข้อมูลเพื่อทำสำเนาและหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย
- **กู้คืนข้อมูล** หมายถึง กระบวนการที่ทำให้ข้อมูลที่สูญหาย, ข้อมูลที่เสียหาย และข้อมูลที่ไม่สามารถใช้งานได้จากสื่อบันทึกข้อมูลให้กลับมาใช้งานได้ตามปกติ

ข้อกำหนด

1) กระบวนการสำรองข้อมูล

- ***กำหนดกระบวนการสำรองข้อมูล*** โดย

1. โปรแกรม Tiger Soft

- ทำการสำรองข้อมูลเดือนละ 1 ครั้ง

2. โปรแกรม TR Cloud

- ทำการสำรองข้อมูลทุกวัน เวลา 03.00 น.

3. โปรแกรม Factoriam
4. โปรแกรม Headquarters System

- ***<u>เจ้าหน้าที่อาวุโส IT ทำการบันทึกและลงนามไว้เป็นหลักฐาน</u>***ว่าได้ทำการสำรองข้อมูลครบถ้วน รวมถึงวันเวลา ที่การสำรองข้อมูลเสร็จสิ้น ***<u>ผู้ช่วยหัวหน้าแผนก IT ตรวจสอบความถูกต้องพร้อมลงนาม</u>***

2) **กระบวนการกู้คืนข้อมูล**

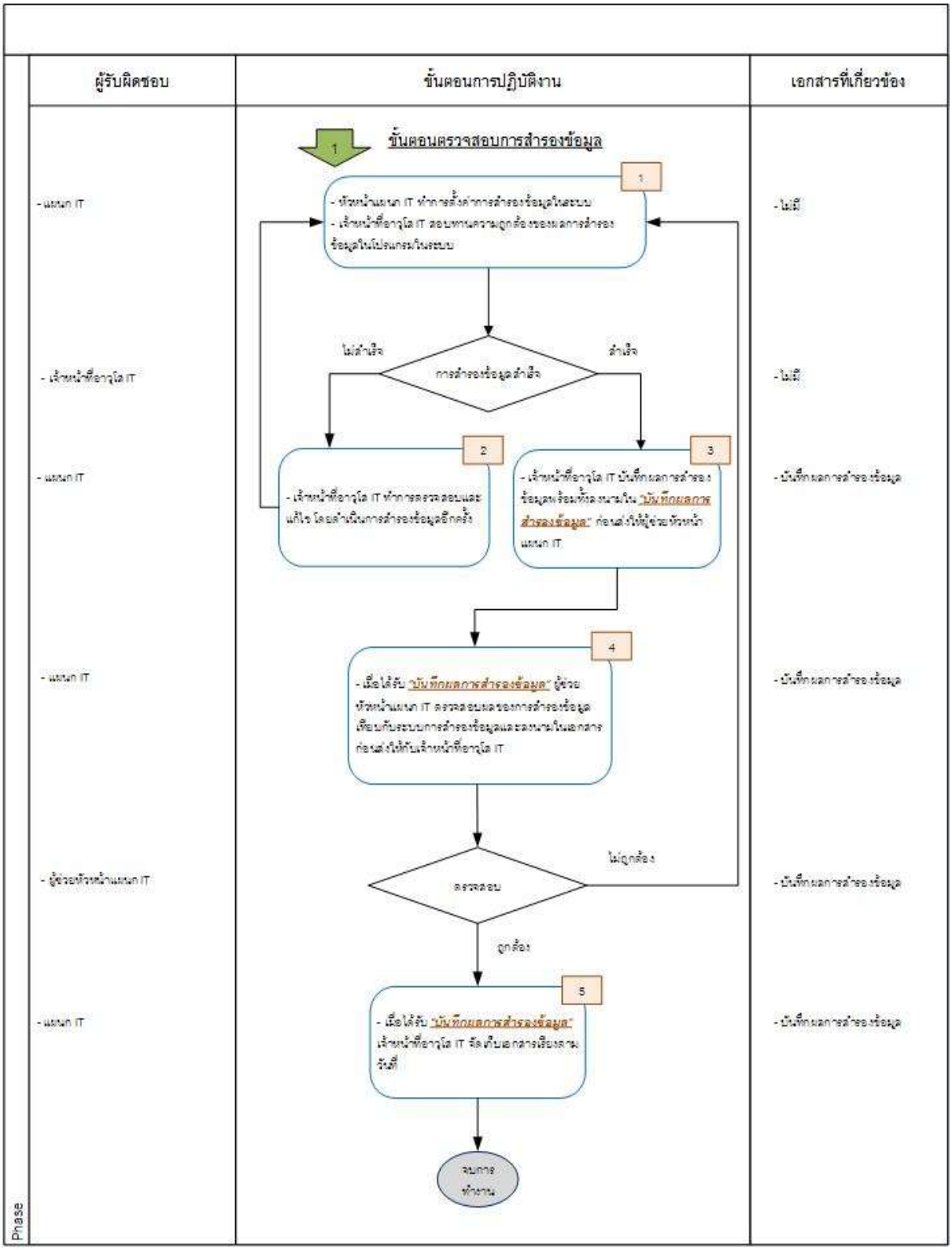
- ผู้มีความประสงค์จัดทำ ***<u>“แบบฟอร์มการขอกู้คืนข้อมูล” และต้องได้รับการอนุมัติจากผู้จัดการฝ่ายขึ้นไป</u>***
- ***<u>“แบบฟอร์มการขอกู้คืนข้อมูล” ต้องได้รับการอนุมัติจากผู้มีอำนาจอนุมัติทุกครั้ง</u>*** ก่อนทำการกู้คืนข้อมูล
- เจ้าหน้าที่อาวุโส IT ***<u>ทำการกู้คืนข้อมูลจากระบบ และต้องทำการตรวจสอบข้อมูล</u>*** ก่อนทำการส่งข้อมูลให้กับผู้มีความประสงค์ขอกู้คืนข้อมูล
- ***<u>ผู้ที่มีความประสงค์ขอข้อมูลต้องทำการตรวจสอบข้อมูลและลงนามยอมรับข้อมูลที่ทำการกู้คืน</u>***

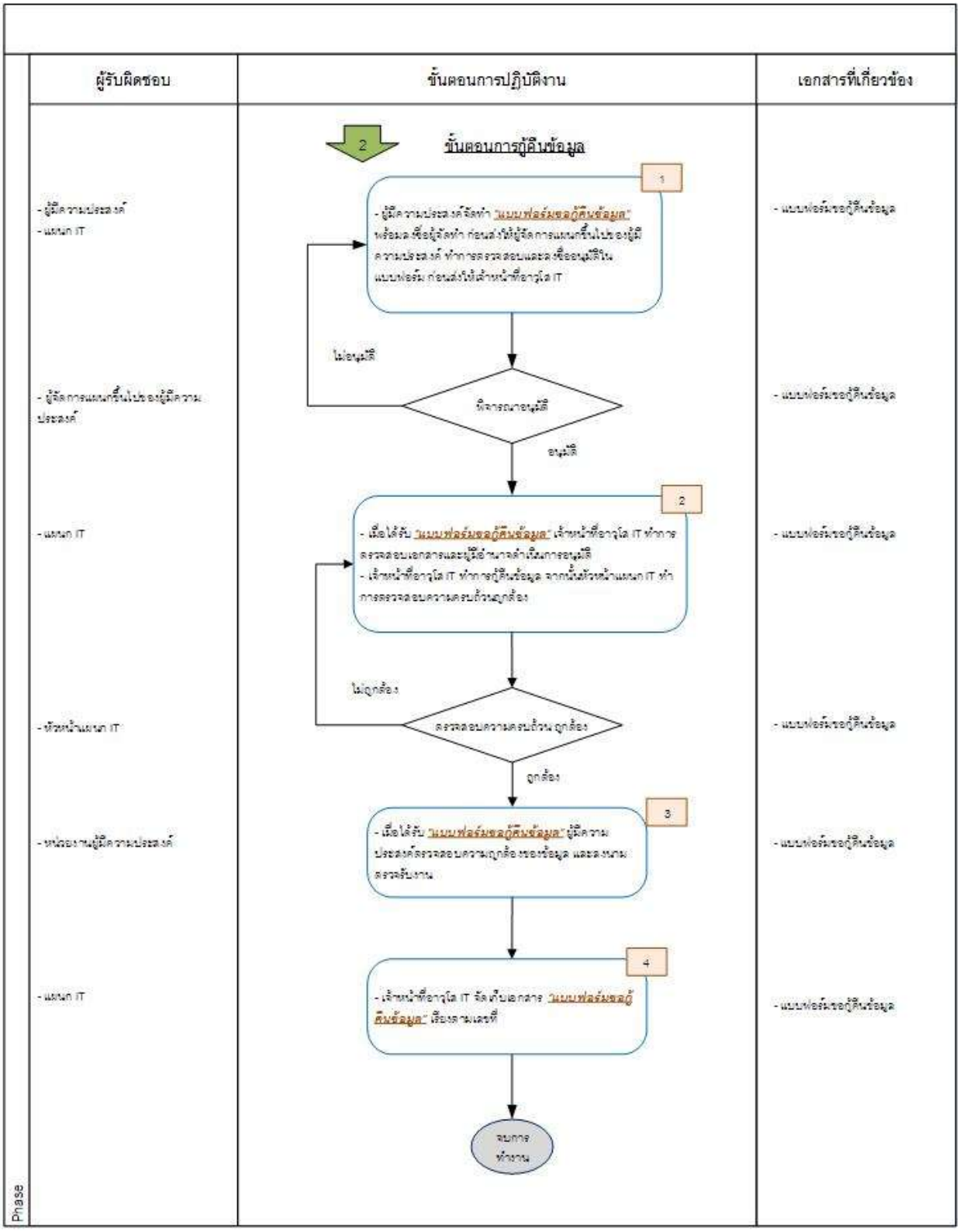
เอกสารที่เกี่ยวข้อง

เอกสารที่ใช้ภายในบริษัท		**เอกสารภายนอก**
เอกสารที่มีเลขทะเบียนคุม	**เอกสารที่ไม่มีเลขทะเบียนคุม**	
ชื่อเอกสาร	**ชื่อเอกสาร**	**ชื่อเอกสาร**
บันทึกผลการสำรองข้อมูล	-ไม่มี-	-ไม่มี-
แบบฟอร์มขอกู้คืนข้อมูล		

ผู้ที่เกี่ยวข้อง

- แผนก IT
- แผนกที่เกี่ยวข้อง


ผู้รับผิดชอบ
ขั้นตอนการปฏิบัติงาน
เอกสารที่เกี่ยวข้อง
ขั้นตอนตรวจสอบการสำรองข้อมูล
- แผนก IT
- เจ้าหน้าที่อาวุโส IT
- แผนก IT
- แผนก IT
- ผู้ช่วยหัวหน้าแผนก IT
- แผนก IT
- ไม่มี
- ไม่มี
- บันทึกผลการสำรองข้อมูล
- บันทึกผลการสำรองข้อมูล
- บันทึกผลการสำรองข้อมูล
- บันทึกผลการสำรองข้อมูล
1
- หัวหน้าแผนก IT ทำการตั้งค่าการสำรองข้อมูลในระบบ
- เจ้าหน้าที่อาวุโส IT สอบทานความถูกต้องของผลการสำรองข้อมูลในโปรแกรมในระบบ
การสำรองข้อมูลสำเร็จ
ไม่สำเร็จ
สำเร็จ
2
- เจ้าหน้าที่อาวุโส IT ทำการตรวจสอบและแก้ไข โดยดำเนินการสำรองข้อมูลอีกครั้ง
3
- เจ้าหน้าที่อาวุโส IT บันทึกผลการสำรองข้อมูลพร้อมทั้งลงนามใน "บันทึกผลการสำรองข้อมูล" ก่อนส่งให้ผู้ช่วยหัวหน้าแผนก IT
4
- เมื่อได้รับ "บันทึกผลการสำรองข้อมูล" ผู้ช่วยหัวหน้าแผนก IT ตรวจสอบผลของการสำรองข้อมูลเทียบกับระบบการสำรองข้อมูลและลงนามในเอกสารก่อนส่งให้กับเจ้าหน้าที่อาวุโส IT
ตรวจสอบ
ไม่ถูกต้อง
ถูกต้อง
5
- เมื่อได้รับ "บันทึกผลการสำรองข้อมูล" เจ้าหน้าที่อาวุโส IT จัดเก็บเอกสารเรียงตามวันที่
จบการทำงาน
Phase


ผู้รับผิดชอบ
ขั้นตอนการปฏิบัติงาน
เอกสารที่เกี่ยวข้อง
2
ขั้นตอนการคืนข้อมูล
1
- ผู้มีความประสงค์
- แผนก IT
- ผู้มีความประสงค์จัดทำ "แบบฟอร์มขอคืนข้อมูล" พร้อมลงชื่อผู้จัดทำ ก่อนส่งให้ผู้จัดการแผนกขึ้นไปของผู้มีความประสงค์ ทำการตรวจสอบและลงชื่ออนุมัติใน แบบฟอร์ม ก่อนส่งให้เจ้าหน้าที่อาวุโส IT
- แบบฟอร์มขอคืนข้อมูล
ไม่อนุมัติ
- ผู้จัดการแผนกขึ้นไปของผู้มีความประสงค์
พิจารณาอนุมัติ
- แบบฟอร์มขอคืนข้อมูล
อนุมัติ
2
- แผนก IT
- เมื่อได้รับ "แบบฟอร์มขอคืนข้อมูล" เจ้าหน้าที่อาวุโส IT ทำการตรวจสอบเอกสารและผู้มีอำนาจลำดับในการอนุมัติ
- เจ้าหน้าที่อาวุโส IT ทำการคืนข้อมูล จากนั้นหัวหน้าแผนก IT ทำการตรวจสอบความครบถ้วนถูกต้อง
- แบบฟอร์มขอคืนข้อมูล
ไม่ถูกต้อง
- หัวหน้าแผนก IT
ตรวจสอบความครบถ้วน ถูกต้อง
- แบบฟอร์มขอคืนข้อมูล
ถูกต้อง
3
- หน่วยงานผู้มีความประสงค์
- เมื่อได้รับ "แบบฟอร์มขอคืนข้อมูล" ผู้มีความประสงค์ตรวจสอบความถูกต้องของข้อมูล และลงนามตรวจรับงาน
- แบบฟอร์มขอคืนข้อมูล
4
- แผนก IT
- เจ้าหน้าที่อาวุโส IT จัดเก็บเอกสาร "แบบฟอร์มขอคืนข้อมูล" เรียงตามเลขที่
- แบบฟอร์มขอคืนข้อมูล
จบการทำงาน
Phase

การทำลายสื่อบันทึกข้อมูล

วัตถุประสงค์

1) เพื่อเป็นแนวทางในการกำกับดูแล ตรวจสอบ และติดตามกระบวนการการทำลายสื่อบันทึกข้อมูลให้มีความสอดคล้องกับระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2) เพื่อสื่อสารชี้แจงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่บริษัทควรมีมาตรการบริหารจัดการความเสี่ยงนั้นอย่างเหมาะสม
3) เพื่อให้บริษัทบริหารจัดการและปฏิบัติงานภายใต้ความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ
4) เพื่อป้องกันไม่ให้ข้อมูลสารสนเทศที่สำคัญของบริษัทรั่วไหลสู่ภายนอก

คำนิยาม

- **<u>สื่อบันทึกข้อมูล</u>** หมายถึง อุปกรณ์ที่ใช้ในการเก็บข้อมูลสารสนเทศ, ข้อมูลทั่วไป, ไฟล์ข้อมูล, รูปภาพ, วีดีโอ, ไฟล์เสียง ฯลฯ ของบริษัท ไม่ว่าจะเป็น ฮาร์ดดิสก์, แฟลชไดร์ฟ (Flash Drive), เอสเอสดี (SSD - Solid State Disk), เมมโมรี่การ์ด (Memory Card) เป็นต้น
- **<u>ทำลาย</u>** หมายถึง กระบวนการ/วิธี/ขั้นตอน ที่ทำให้เกิดความเสียหาย, พัง, สลาย, สุญเสียสภาพทางกายภาพของวัตถุ ฯลฯ จนทำให้ไม่สามารถนำกลับมาใช้ประโยชน์ได้อีก
- **<u>ผู้ทำลาย</u>** หมายถึง เจ้าหน้าอาวุโส IT ที่ได้รับมอบหมาย หรือบุคคลภายนอกที่ได้รับการอนุมัติให้กระทำการแทนเจ้าหน้าที่ของบริษัท

ข้อกำหนด

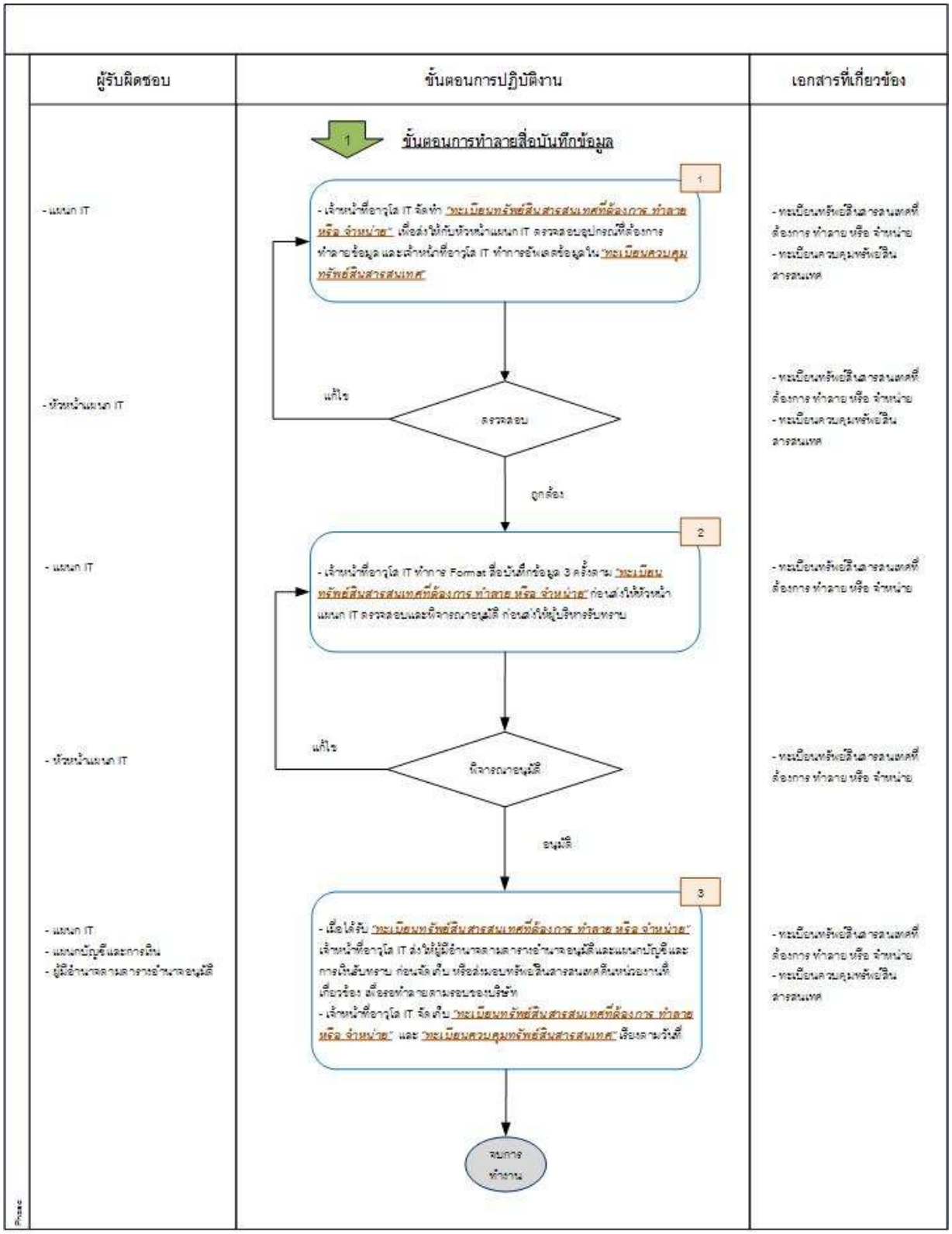
- เจ้าหน้าที่อาวุโส IT จัดทำ ***<u>“ทะเบียนทรัพย์สินสารสนเทศที่ต้องการทำลาย หรือ จำหน่าย”</u>*** (เครื่องเสีย, เครื่องที่เตรียมไปบริจาค, เครื่องที่รอตัดจำหน่าย)
  a. หัวหน้าแผนก IT ***<u>ตรวจสอบ “ทะเบียนทรัพย์สินสารสนเทศที่ต้องการทำลาย หรือ จำหน่าย” และเจ้าหน้าที่อาวุโส IT ทำการปรับปรุง “ทะเบียนควบคุมทรัพย์สินสารสนเทศ” ทุกครั้ง</u>***
  b. เจ้าหน้าที่อาวุโส IT ***<u>ต้องแจ้งให้ผู้มีอำนาจตามตารางอนุมัติและส่วนงานบัญชีและการเงินรับทราบทุกครั้ง</u>*** ก่อนจัดเก็บ หรือส่งมอบทรัพย์สินสารสนเทศคืนหน่วยงานที่เกี่ยวข้องเพื่อรอการทำลายตามรอบ

เอกสารที่เกี่ยวข้อง

เอกสารที่ใช้ภายในบริษัท		**เอกสารภายนอก**
เอกสารที่มีเลขทะเบียนคุม	**เอกสารที่ไม่มีเลขทะเบียนคุม**	
ชื่อเอกสาร	**ชื่อเอกสาร**	**ชื่อเอกสาร**
ทะเบียนทรัพย์สินสารสนเทศที่ต้องการทำลาย หรือ จำหน่าย	-ไม่มี-	-ไม่มี-
ทะเบียนควบคุมทรัพย์สินสารสนเทศ		

ผู้ที่เกี่ยวข้อง

- แผนก IT
- แผนกบัญชีและการเงิน
- แผนกที่เกี่ยวข้อง
- ผู้มีอำนาจตามตารางอนุมัติ


ผู้รับผิดชอบ
ขั้นตอนการปฏิบัติงาน
เอกสารที่เกี่ยวข้อง
1
ขั้นตอนการทำลายสื่อบันทึกข้อมูล
1
- แผนก IT
- เจ้าหน้าที่อาวุโส IT จัดทำ "ทะเบียนทรัพย์สินสารสนเทศที่ต้องการ ทำลาย หรือ จำหน่าย" เพื่อส่งให้กับหัวหน้าแผนก IT ตรวจสอบอุปกรณ์ที่ต้องการทำลายข้อมูล และเจ้าหน้าที่อาวุโส IT ทำการอัพเดตข้อมูลใน "ทะเบียนควบคุมทรัพย์สินสารสนเทศ"
- ทะเบียนทรัพย์สินสารสนเทศที่ต้องการ ทำลาย หรือ จำหน่าย
- ทะเบียนควบคุมทรัพย์สินสารสนเทศ
- หัวหน้าแผนก IT
แก้ไข
ตรวจสอบ
ถูกต้อง
- ทะเบียนทรัพย์สินสารสนเทศที่ต้องการ ทำลาย หรือ จำหน่าย
- ทะเบียนควบคุมทรัพย์สินสารสนเทศ
2
- แผนก IT
- เจ้าหน้าที่อาวุโส IT ทำการ Format สื่อบันทึกข้อมูล 3 ครั้งตาม "ทะเบียนทรัพย์สินสารสนเทศที่ต้องการ ทำลาย หรือ จำหน่าย" ก่อนส่งให้หัวหน้าแผนก IT ตรวจสอบและพิจารณาอนุมัติ ก่อนส่งให้ผู้บริหารรับทราบ
- ทะเบียนทรัพย์สินสารสนเทศที่ต้องการ ทำลาย หรือ จำหน่าย
- หัวหน้าแผนก IT
แก้ไข
พิจารณาอนุมัติ
อนุมัติ
- ทะเบียนทรัพย์สินสารสนเทศที่ต้องการ ทำลาย หรือ จำหน่าย
3
- แผนก IT
- แผนกบัญชีและการเงิน
- ผู้มีอำนาจลงนามการอำนาจอนุมัติ
- เมื่อได้รับ "ทะเบียนทรัพย์สินสารสนเทศที่ต้องการ ทำลาย หรือ จำหน่าย" เจ้าหน้าที่อาวุโส IT ส่งให้ผู้มีอำนาจลงนามการอำนาจอนุมัติและแผนกบัญชีและการเงินรับทราบ ก่อนจัดเก็บ หรือส่งมอบทรัพย์สินสารสนเทศคืนหน่วยงานที่เกี่ยวข้อง เพื่อรอทำลายตามรอบของบริษัท
- เจ้าหน้าที่อาวุโส IT จัดเก็บ "ทะเบียนทรัพย์สินสารสนเทศที่ต้องการ ทำลาย หรือ จำหน่าย" และ "ทะเบียนควบคุมทรัพย์สินสารสนเทศ" เรียบร้อยวันที่
- ทะเบียนทรัพย์สินสารสนเทศที่ต้องการ ทำลาย หรือ จำหน่าย
- ทะเบียนควบคุมทรัพย์สินสารสนเทศ
จบการทำงาน

การขอใช้งานอินเตอร์เน็ตบุคคลภายนอก

วัตถุประสงค์

1) เพื่อเป็นแนวทางในการกำกับดูแล ตรวจสอบ และติดตามกระบวนการขอใช้งานอินเตอร์เน็ตบุคคลภายนอกของบริษัทให้มีความสอดคล้องกับระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2) เพื่อสื่อสารชี้แจงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่บริษัทควรมีมาตรการบริหารจัดการความเสี่ยงนั้นอย่างเหมาะสม
3) เพื่อให้บริษัทบริหารจัดการและปฏิบัติงานภายใต้ความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

คำนิยาม

- **เครือข่ายไร้สาย** หมายถึง การเชื่อมต่ออินเทอร์เน็ตโดยการรับสัญญาณจากอุปกรณ์ Smartphone, Notebook, Tablet เป็นต้น
- **ผู้ใช้** หมายถึง ผู้ให้บริการจากภายนอก (Outsource), ผู้ขาย (Vendors) และตัวแทน (Agent) ที่ต้องการเชื่อมต่ออินเทอร์เน็ต หรือระบบภายในบริษัท
- **การใช้บริการจากภายนอก (Outsource)** หมายถึง การโอนย้ายหน้าที่การทำงานและความรับผิดชอบอาจเป็นในส่วนกระบวนการทางธุรกิจ โดยเป็นภาระหน้าที่ของผู้ให้บริการจากภายนอก

ข้อกำหนด

- เมื่อบุคคลผู้มาติดต่อมีความประสงค์ขอใช้เครือข่ายไร้สาย ***ต้องติดต่อแผนก IT ทุกครั้งเมื่อต้องการใช้งาน***
- ***เจ้าหน้าที่ IT กำหนดบัญชีและรหัสผู้ใช้งาน พร้อมทั้งระบุระยะเวลาในการใช้งานและปรับปรุง “ทะเบียนควบคุมการใช้อินเตอร์เน็ตจากบุคคลภายนอก” ให้ถูกต้อง***

เอกสารที่เกี่ยวข้อง

เอกสารที่ใช้ภายในบริษัท		เอกสารภายนอก
เอกสารที่มีเลขทะเบียนคุม	เอกสารที่ไม่มีเลขทะเบียนคุม	
ชื่อเอกสาร	ชื่อเอกสาร	ชื่อเอกสาร
ทะเบียนควบคุมการใช้อินเตอร์เน็ตจากบุคคลภายนอก	-ไม่มี-	-ไม่มี-

ผู้ที่เกี่ยวข้อง

- แผนก IT
- หน่วยงานที่เกี่ยวข้อง

การเข้า-ออกห้องแม่ข่ายระบบสารสนเทศจากบุคคลภายนอก

วัตถุประสงค์

1) เพื่อเป็นแนวทางในการกำกับดูแล ตรวจสอบ และติดตามกระบวนการเข้า-ออกห้องแม่ข่ายระบบสารสนเทศจากบุคคลภายนอกให้มีความสอดคล้องกับระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2) เพื่อควบคุมการเข้าถึง และ สื่อสารชี้แจงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่บริษัทควรมีมาตรการบริหารจัดการความเสี่ยงนั้นอย่างเหมาะสม
3) เพื่อให้บริษัท บริหารจัดการและปฏิบัติงานภายใต้ความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ
4) เพื่อเป็นกรอบมาตรฐานการดำเนินงานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

คำนิยาม

- **ผู้ที่มีความประสงค์** หมายถึง บุคคลภายนอกที่ต้องการเข้าออกห้องแม่ข่ายระบบสารสนเทศ
- **ผู้จัดการฝ่ายขึ้นไป** หมายถึง ผู้มีอำนาจในหน่วยงานนั้น ๆ และเป็นงานที่อยู่ในงานรับผิดชอบของหน่วยงานนั้น ๆ
- **ห้องแม่ข่ายระบบสารสนเทศ (Server)** หมายถึง สถานที่สำหรับจัดเก็บเครื่องแม่ข่ายที่มีการติดตั้งระบบเทคโนโลยีสารสนเทศที่สำคัญ อุปกรณ์เครือข่ายหลัก และระบบสำรองไฟ (UPS)

ข้อกำหนด

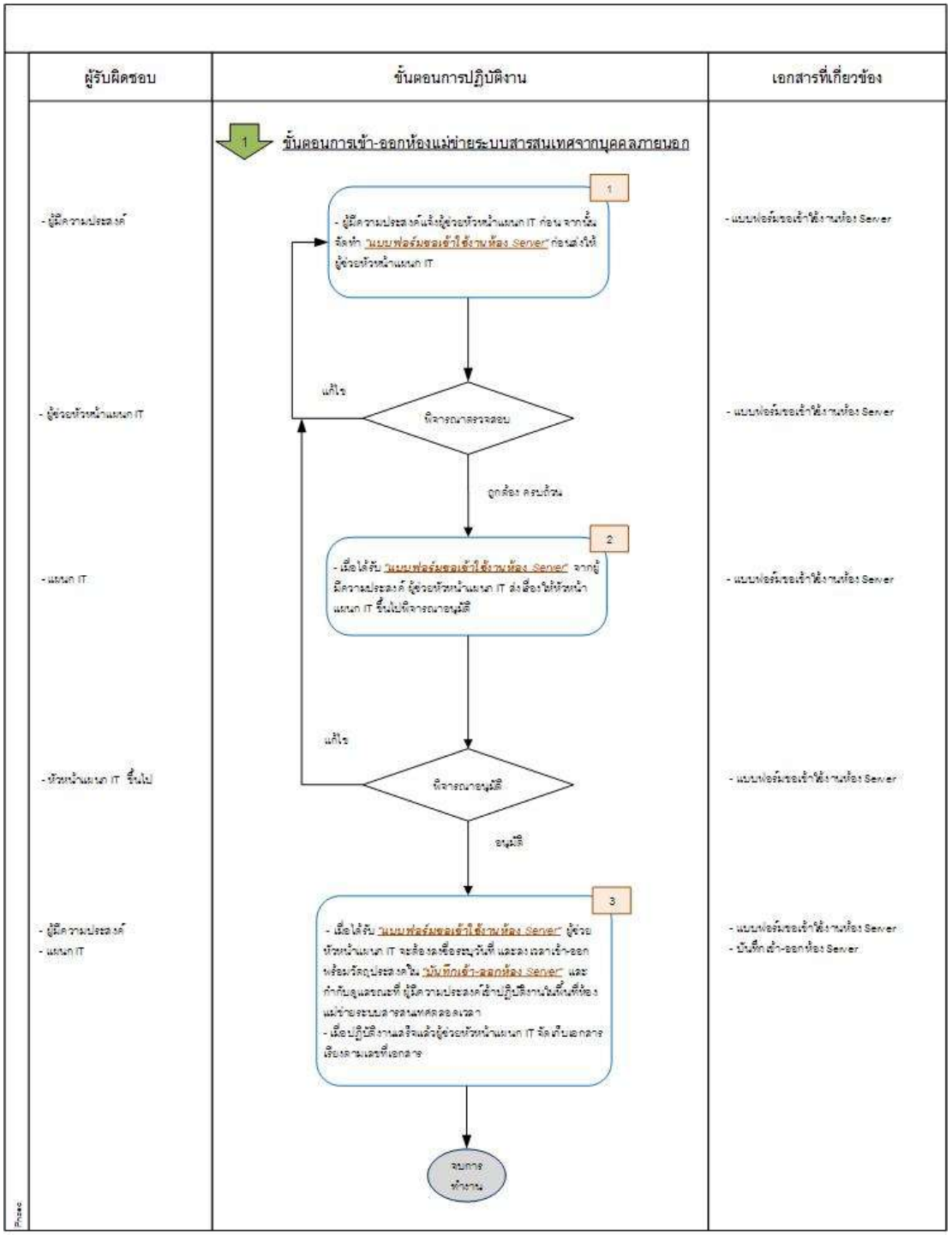
- ***กำหนดผู้เข้า-ออกห้องแม่ข่ายระบบสารสนเทศ (Server)*** เพื่อที่สามารถควบคุมและดูแลการเข้า-ออกห้องแม่ข่ายระบบสารสนเทศ (Server) ได้อย่างถูกต้อง
- กำหนดให้มีการบันทึกเป็นหลักฐาน ***เพื่อที่จะสามารถติดตามและรู้การเข้า – ออกห้องแม่ข่ายระบบสารสนเทศ (Server)***
- ***กำหนดให้มีผู้ช่วยหัวหน้าแผนก IT กำกับ ดูแลการเข้า – ออกห้องแม่ข่ายระบบสารสนเทศ (Server) จากบุคคลภายนอกทุกครั้ง และตลอดเวลาที่เข้ามาปฏิบัติงาน***

เอกสารที่เกี่ยวข้อง

เอกสารที่ใช้ภายในบริษัท		**เอกสารภายนอก**
เอกสารที่มีเลขทะเบียนคุม	**เอกสารที่ไม่มีเลขทะเบียนคุม**	
ชื่อเอกสาร	**ชื่อเอกสาร**	**ชื่อเอกสาร**
แบบฟอร์มขอเข้าใช้งานห้อง Server	-ไม่มี-	-ไม่มี-
บันทึกเข้า-ออกห้อง Server		

ผู้ที่เกี่ยวข้อง

- แผนก IT
- หน่วยงานที่เกี่ยวข้อง


ผู้รับผิดชอบ
ขั้นตอนการปฏิบัติงาน
เอกสารที่เกี่ยวข้อง
1 ขั้นตอนการเข้า-ออกห้องแม่ข่ายระบบสารสนเทศจากบุคคลภายนอก
- ผู้มีความประสงค์
- ผู้ช่วยหัวหน้าแผนก IT
- แผนก IT
- หัวหน้าแผนก IT ขึ้นไป
- ผู้มีความประสงค์
- แผนก IT
1
- ผู้มีความประสงค์แจ้งผู้ช่วยหัวหน้าแผนก IT ก่อน จากนั้นจัดทำ "แบบฟอร์มขอเข้าใช้งานห้อง Server" ก่อนส่งให้ผู้ช่วยหัวหน้าแผนก IT
- แบบฟอร์มขอเข้าใช้งานห้อง Server
แก้ไข
พิจารณาตรวจสอบ
ถูกต้อง ครบถ้วน
2
- เมื่อได้รับ "แบบฟอร์มขอเข้าใช้งานห้อง Server" จากผู้มีความประสงค์ ผู้ช่วยหัวหน้าแผนก IT ส่งต่อให้หัวหน้าแผนก IT ขึ้นไปพิจารณาอนุมัติ
- แบบฟอร์มขอเข้าใช้งานห้อง Server
แก้ไข
พิจารณาอนุมัติ
อนุมัติ
3
- เมื่อได้รับ "แบบฟอร์มขอเข้าใช้งานห้อง Server" ผู้ช่วยหัวหน้าแผนก IT จะต้องเชื่อระบุวันที่ และเวลาเข้า-ออก พร้อมวัตถุประสงค์ใน "บันทึกเข้า-ออกห้อง Server" และกำกับดูแลระหว่างที่ผู้มีความประสงค์เข้าปฏิบัติงานในพื้นที่ห้องแม่ข่ายระบบสารสนเทศตลอดเวลา
- เมื่อปฏิบัติงานเสร็จแล้วผู้ช่วยหัวหน้าแผนก IT จัดเก็บเอกสารเรียงตามเลขที่เอกสาร
- แบบฟอร์มขอเข้าใช้งานห้อง Server
- บันทึกเข้า-ออกห้อง Server
จบการทำงาน

นโยบายนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ประกาศ และบริษัทอาจทบทวนหรือปรับปรุงได้ตามความเหมาะสมกับสภาวะการดำเนินธุรกิจในแต่ละปี นโยบายนี้ได้รับอนุมัติโดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 6/2568 เมื่อวันที่ 11 พฤศจิกายน 2568

พล.อ. ร. กสิวุฒิ

(พลเอก ดร.รุจ กสิวุฒิ)

ประธานกรรมการบริษัท

บริษัท เอเชียนน้ำมันปาล์ม จำกัด (มหาชน)