นโยบายและแนวปฏิบัติ
ด้านการบริหารจัดการข้อมูลสารสนเทศ
กลุ่มบริษัทแอสเซนด์

รายการปรับปรุงแก้ไขนโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูลสารสนเทศ
เครือเจริญโภคภัณฑ์

ครั้งที่	ผู้รับผิดชอบ	สาระสำคัญ	ทบทวนโดย	อนุมัติโดย	วันที่มีผลบังคับใช้
1	ด้านธรรมาภิบาล บจก. เครือเจริญโภคภัณฑ์	ปรับ Template ตามนโยบายและแนวปฏิบัติที่ได้รับความเห็นชอบจากคณะกรรมการขับเคลื่อนการกำกับดูแลกิจการ ความเสี่ยงและการตรวจสอบ บจก. เครือเจริญโภคภัณฑ์ และได้รับอนุมัติจากคณะกรรมการบริหาร บจก. เครือเจริญโภคภัณฑ์ในเดือนสิงหาคม 2564	-	-	สิงหาคม 2564
2					

หมายเหตุ รายการปรับปรุงแก้ไขนโยบายเป็นเอกสารที่ใช้เพื่อการบริหารจัดการภายในเท่านั้น

รายการปรับปรุงแก้ไขนโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูลสารสนเทศ
กลุ่มบริษัทแอสเซนด์

ครั้งที่	ผู้รับผิดชอบ	สาระสำคัญ	ทบทวนโดย	อนุมัติโดย	วันที่มีผลบังคับใช้
1	ระบุชื่อหน่วยงานที่รับผิดชอบของกลุ่มธุรกิจ/บริษัท	• ปรับตามการปรับปรุงแก้ไขนโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูลสารสนเทศเครือเจริญโภคภัณฑ์ ครั้งที่ 1	คณะกรรมการขับเคลื่อน/หน่วยงานที่เกี่ยวข้อง	คณะกรรมการบริหาร หรือผู้บริหารสูงสุด	วัน เดือน ปีถัดจากวัน เดือน ปีที่นโยบายและแนวปฏิบัติระดับเครือมีผลบังคับใช้
2					

สารบัญ

นโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูลสารสนเทศ กลุ่มบริษัทแอสเซนด์

1. ความสำคัญ

ข้อมูลสารสนเทศถือเป็นสินทรัพย์ที่มีค่าของกลุ่มบริษัทแอสเซนด์จึงต้องมีการกำกับดูแลข้อมูลสารสนเทศอย่างเป็นระบบและมีประสิทธิภาพ มีความน่าเชื่อถือถูกต้องสมบูรณ์ซึ่งเป็นการป้องกันความเสี่ยงจากความเสียหาย ปกป้องทรัพย์สินของกลุ่มบริษัทแอสเซนด์และช่วยลดการสูญหายของข้อมูล ส่งผลให้การตัดสินใจทางธุรกิจมีประสิทธิภาพรวมถึงเพิ่มขีดความสามารถทางการแข่งขัน

2. ขอบเขตนโยบาย

นโยบายและแนวปฏิบัตินี้ใช้บังคับกับเครือเจริญโภคภัณฑ์ ต่อไปนี้เรียกว่า “เครือฯ” หมายถึง บริษัท เครือเจริญโภคภัณฑ์ จำกัด และบริษัทในเครือทุกบริษัท ซึ่ง “บริษัท” ที่จะกล่าวถึงในเอกสารฉบับนี้ให้หมายถึง บริษัทหนึ่ง ๆ ที่นำเอาเอกสารฉบับนี้ไปบังคับใช้ ทั้งนี้จะมีการทบทวนโยบายฉบับนี้อย่างน้อยปีละหนึ่งครั้ง หรือกรณีมีเหตุอันสมควร

3. วัตถุประสงค์

เพื่อให้บุคลากรเข้าใจบทบาทหน้าที่และร่วมกันปกป้องข้อมูลสารสนเทศของกลุ่มบริษัทแอสเซนด์มิให้รั่วไหลหรือนำข้อมูลไปใช้ในทางที่ผิด

4. หน้าที่และความรับผิดชอบ

สำหรับบุคลากรใช้เป็นแนวทางในการประสานงานภายในบริษัท

4.1 คณะกรรมการบริษัท

4.1.1 กำหนดให้มีนโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูลสารสนเทศ

4.1.2 กำกับดูแลให้มีการนำนโยบายและแนวปฏิบัติไปปฏิบัติอย่างเป็นรูปธรรม

4.2 ผู้บริหาร

4.2.1 จัดให้มีระเบียบปฏิบัติให้เหมาะสมกับบริบทของแต่ละบริษัท โดยให้สอดคล้องกับบริบทของบริษัท และข้อกำหนดกฎหมายของแต่ละประเทศที่บริษัทดำเนินธุรกิจ

4.2.2 จัดให้มีโครงสร้างผู้รับผิดชอบ เช่น หน่วยงาน หรือบุคคลผู้รับผิดชอบเพื่อดูแลข้อมูลและระบบสารสนเทศ

4.2.3 กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ

4.2.4 มั่นใจว่ามีการบริหารความเสี่ยงจากการใช้ข้อมูลสารสนเทศ

4.2.5 มั่นใจว่ามีการรายงานผลการปฏิบัติงานตามนโยบายฯ รวมถึงรายงานปัญหาจากการใช้ข้อมูลสารสนเทศ

4.3 **หน่วยงาน/บุคคลผู้รับผิดชอบดูแลข้อมูลและระบบสารสนเทศ**

4.3.1 ปฏิบัติตามแนวปฏิบัติ ข้อ 5.2 การบริหารจัดการความเสี่ยง

4.3.2 ปฏิบัติตามแนวปฏิบัติ ข้อ 5.3 การบริหารจัดการข้อมูลสารสนเทศ

4.3.3 ปฏิบัติตามแนวปฏิบัติ ข้อ 5.4 การแลกเปลี่ยนข้อมูลสารสนเทศกับบุคคลภายนอก

4.3.4 ปฏิบัติตามแนวปฏิบัติ ข้อ 5.8 การทำลายข้อมูลสารสนเทศ

4.3.5 รายงานผลการปฏิบัติงานตามนโยบายและแนวปฏิบัติ และระเบียบปฏิบัติ รวมถึงรายงานปัญหาจากการใช้ข้อมูลสารสนเทศ

4.4 **ฝ่ายเทคโนโลยีสารสนเทศ**

4.4.1 ดูแลรักษาเทคโนโลยีสำหรับระบบข้อมูลสารสนเทศ

4.4.2 ควบคุมการเข้าถึงระบบข้อมูลสารสนเทศและเครือข่าย

4.4.3 รักษาความปลอดภัยของข้อมูลสารสนเทศ

4.4.4 จัดให้มีการเก็บสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง

4.5 **หน่วยงานตรวจสอบภายใน**

4.5.1 ตรวจสอบให้มีการบริหารจัดการข้อมูลสารสนเทศตามนโยบายฯ

4.5.2 ให้คำแนะนำและให้ความรู้แก่บุคลากรเพื่อให้เกิดการปฏิบัติตามนโยบายฯ

4.6 **พนักงาน**

4.6.1 รักษาความลับและปกป้องความปลอดภัยของข้อมูลส่วนตัว รวมทั้งข้อมูลสารสนเทศของเครือเจริญโภคภัณฑ์ ลูกค้าและคู่ค้าธุรกิจและพันธมิตรทางธุรกิจ

4.6.2 จัดทำข้อมูลสารสนเทศ บันทึกและรายงานให้มีความถูกต้อง น่าเชื่อถือ

4.6.3 ปกป้องทรัพย์สินทางปัญญาของกลุ่มบริษัทแอสเซนด์ และไม่ละเมิดสิทธิในทรัพย์สินทางปัญญาของผู้อื่น

4.6.4 ปฏิบัติตามนโยบายฯ กฎหมาย และมาตรฐานสากลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลสารสนเทศ

5. แนวปฏิบัติ

5.1 ให้ปฏิบัติตามแนวทางตามมาตรฐานสากลเกี่ยวกับการใช้เทคโนโลยีสารสนเทศซึ่งประกอบด้วยหลัก 4 ประการ คือ Privacy, Accuracy, Property และ Accessibility (PAPA) โดยมีรายละเอียด ดังนี้

5.1.1 ความเป็นส่วนตัวของข้อมูลสารสนเทศ (Information Privacy)
ลักษณะของข้อมูลที่เป็นส่วนตัว เช่น หมายเลขบัตรประจำตัวประชาชน วันเดือนปีเกิด ชื่อบัญชีผู้ใช้งาน (account) และรหัสผ่าน (password)

1) รักษาความลับและปกป้องความปลอดภัยของข้อมูลส่วนตัวของบุคลากร ลูกค้า คู่ค้าธุรกิจ และพันธมิตรทางธุรกิจ
2) ไม่ใช้ข้อมูลของลูกค้าจากแหล่งต่างๆ เพื่อผลประโยชน์ทางการตลาดหรือนำไปสร้างฐานข้อมูลประวัติลูกค้าขึ้นมาใหม่แล้วนำไปขายให้กับบริษัทอื่น
3) เก็บรักษาชื่อบัญชีผู้ใช้งาน (account) และรหัสผ่าน (password) ที่เกี่ยวข้องกับระบบข้อมูลสารสนเทศกลุ่มบริษัทแอสเซนด์ไว้เป็นส่วนตัวและสร้างให้เป็นเอกลักษณ์
4) ไม่จด password ไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่นที่ไม่ได้รับอนุญาต และง่ายต่อการถอดรหัสผ่าน
5) กรณีที่มีความจำเป็นต้องบอก password แก่ผู้อื่นเพื่อเข้าดำเนินการในระบบข้อมูลสารสนเทศ หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านทันที

5.1.2 ความถูกต้องของข้อมูล (Information Accuracy)

1) การจัดทำข้อมูลสารสนเทศให้มีความถูกต้องและน่าเชื่อถือนั้น ข้อมูลควรได้รับการตรวจสอบความถูกต้องก่อนที่จะนำเข้าฐานข้อมูล รวมถึงการปรับปรุงข้อมูลให้มีความทันสมัยอยู่เสมอ
2) แหล่งที่มาของข้อมูลต้องมีความน่าเชื่อถือและตรวจสอบได้ เช่น หน่วยงานภาครัฐ องค์กรอื่นที่เชื่อถือได้ เป็นต้น

5.1.3 ความเป็นเจ้าของ (Information Property)

1) กลุ่มบริษัทแอสเซนด์เป็นเจ้าของในทรัพย์สินทางปัญญาที่บุคลากรได้พัฒนาหรือสร้างขึ้นไม่ว่าจะทั้งหมดหรือบางส่วน
2) ไม่ละเมิดหรือเปิดเผยโดยไม่ได้รับอนุญาตในทรัพย์สินทางปัญญาและลิขสิทธิ์ของงานที่ทำร่วมกัน
3) ไม่ใช้งาน ทำซ้ำ ตีพิมพ์หรือเผยแพร่รูปภาพ บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิด ลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทแอสเซนด์
4) ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ตซึ่งรวมถึงการอัพเดทโปรแกรมต่างๆ ซอฟต์แวร์ที่ใช้ในระบบข้อมูลสารสนเทศของกลุ่มบริษัทแอสเซนด์ต้องไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น
5) ปกป้องทรัพย์สินทางปัญญาของกลุ่มบริษัทแอสเซนด์โดยไม่เปิดเผยก่อนได้รับอนุญาต
6) ปกป้องทรัพย์สินทางปัญญาโดยไม่ใช้ผิดวิธีหรือผิดกฎหมาย และเมื่อใช้ ต้องแน่ใจว่าได้ประทับตราหรือแสดงเครื่องหมายการค้า หรือเครื่องหมายบริการหรือสัญลักษณ์ลิขสิทธิ์ เช่น การใช้ ®, ™, © (20xx) เป็นต้น
7) แจ้งให้กลุ่มบริษัทแอสเซนด์ทราบถึงการค้นพบ การประดิษฐ์ เช่น โปรแกรมคอมพิวเตอร์ สิ่งประดิษฐ์ทางเทคโนโลยีและผลงานนวัตกรรม รวมไปถึงข้อมูลจำเพาะ
8) ให้ความช่วยเหลือกลุ่มบริษัทแอสเซนด์เพื่อให้ได้มาซึ่งสิทธิบัตร ลิขสิทธิ์ หรือปกป้องเครื่องหมายการค้าที่เป็นทรัพย์สินทางปัญญาของกลุ่มบริษัทแอสเซนด์

5.1.4 การเข้าถึงข้อมูล (Data Accessibility)

1) การใช้งานระบบสารสนเทศ เช่น ระบบคอมพิวเตอร์ แอปพลิเคชัน อีเมล ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น ผู้บริหารต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศก่อนเข้าใช้ระบบฯ ของผู้ใช้งานให้เหมาะสมกับงานและหน้าที่ความรับผิดชอบ
2) ผู้บริหารทบทวนสิทธิการเข้าถึงข้อมูลและระบบฯ ปีละหนึ่งครั้งหรือเมื่อต้องเปลี่ยนสิทธิของผู้ใช้งาน เช่น การเลื่อนตำแหน่ง โดยผู้บริหารต้องอนุมัติเลื่อนขั้นในระบบฯ
3) ผู้รับมอบอำนาจจากผู้บริหารเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบฯ

4) บันทึกรายละเอียดการเข้าถึงข้อมูลและระบบฯ รวมถึงการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ ทั้งของผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

5) บันทึกและติดตามการใช้งานระบบฯ และเฝ้าระวังการละเมิดความปลอดภัยที่มีต่อข้อมูลและระบบฯ ที่สำคัญ

5.2 การบริหารจัดการความเสี่ยง

5.2.1 ระบุและประเมินความเสี่ยง

5.2.2 จัดลำดับความสำคัญของความเสี่ยงและบริหารความเสี่ยงสำคัญที่ต้องดำเนินการก่อน

5.2.3 กำหนดมาตรการจัดการความเสี่ยงและดำเนินการตามมาตรการ

5.3 การบริหารจัดการข้อมูลสารสนเทศ

5.3.1 การจัดระดับความลับข้อมูลสารสนเทศ (Classification of Information) โดยพิจารณาจากระดับความเสี่ยงต่อความมั่นคงปลอดภัย ผลกระทบต่อมูลค่าผลกระทบต่อความเสียหายทางทรัพย์สินและภาพพจน์บริษัทโดยแบ่งตามประเภทดังต่อไปนี้

1) **เอกสารลับพิเศษ (Special Control)** [สีม่วง] เป็นข้อมูลสารสนเทศที่ส่งผลกระทบต่อการดำเนินยุทธศาสตร์ทางธุรกิจและก่อให้เกิดความเสียเปรียบในการแข่งขันเชิงธุรกิจอย่างร้ายแรง ถ้าเกิดการรั่วไหลของข้อมูลออกมาจะก่อให้เกิดความเสียหายต่อภาพพจน์ของบริษัทในระดับสากล เช่น

- ข้อมูลความลับทางการค้า (Trade Secret)
- แผนกลยุทธ์ทางธุรกิจ
- แผนการตลาด / การพัฒนาผลิตภัณฑ์
- แผนควบรวมกิจการ

2) **เอกสารลับ (Confidential)** [สีแดง] เป็นข้อมูลสารสนเทศที่ส่งผลกระทบต่อการดำเนินธุรกิจและความก้าวหน้าของธุรกิจ องค์กรอาจถูกฟ้องร้องเรียกค่าเสียหาย ถ้าเกิดการรั่วไหลของข้อมูลและก่อให้เกิดความเสียหายต่อภาพพจน์บริษัทในระดับประเทศ เช่น

- เอกสารทางการตลาด (ที่ยังไม่เปิดเผยต่อสาธารณะ)
- ข้อมูลส่วนบุคคล
- ข้อมูลลูกค้า

3) **เอกสารใช้ภายในเท่านั้น (Internal Use Only)** [สีเหลือง] เป็นข้อมูลสารสนเทศที่อนุญาตให้ใช้ภายในบริษัทในเครือฯ เท่านั้น ส่งผลกระทบต่อการปฏิบัติงานประจำวันและอาจทำให้เกิดความเสียหายต่อภาพพจน์ เช่น
   - ประกาศภายใน/นโยบายต่างๆ
   - ระเบียบ/คู่มือปฏิบัติงาน
   - บันทึกการปฏิบัติงานประจำวัน
4) **เอกสารเปิดเผย (Public)** [สีเขียว] เป็นข้อมูลสารสนเทศที่พิจารณาแล้วเห็นว่าไม่มีผลกระทบต่อองค์กร สามารถเปิดเผยต่อบุคคลภายนอกได้ เช่น
   - ข้อมูลด้านความยั่งยืน
   - ข้อมูลประชาสัมพันธ์
   - โปรโมชั่นทางการค้าต่างๆ

ทั้งนี้ เอกสารหรือสิ่งตีพิมพ์ไม่ว่าจะทั้งหมดหรือบางส่วนที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับ ซึ่งมีการกำหนดชั้นความลับไว้ ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับ

5.3.2 การจัดเก็บข้อมูลสารสนเทศและอุปกรณ์

1) ผู้บริหารและผู้รับผิดชอบดูแลข้อมูลสารสนเทศเป็นผู้กำหนดระยะเวลาจัดเก็บข้อมูลสารสนเทศตามระดับความลับ
2) จัดเก็บข้อมูลสำรองในสื่อบันทึกข้อมูลและจัดทำรายการบันทึกให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน
3) รักษาความปลอดภัยของระบบสารสนเทศและอุปกรณ์ซึ่งบรรจุข้อมูลสารสนเทศของบริษัท เช่น โทรศัพท์มือถือ แล็ปท็อป แท็บเล็ต เป็นต้น และต้องระมัดระวังเป็นพิเศษในการใช้งานอุปกรณ์ดังกล่าวนอกสถานประกอบการ รวมทั้งจัดเก็บไว้ในที่ที่มีกุญแจล็อคหลังการใช้งาน
4) ตั้งรหัสผ่าน (password) ล็อคหน้าจอซึ่งบรรจุข้อมูลสารสนเทศของกลุ่มบริษัทแอสเซนด์เมื่อต้องการออกจากระบบสารสนเทศหรือเสร็จสิ้นงาน
5) รายงานฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อข้อมูลสารสนเทศหรืออุปกรณ์ ซึ่งบรรจุข้อมูลสารสนเทศของกลุ่มบริษัทแอสเซนด์สูญหายหรือถูกขโมย

5.3.3 การนำอุปกรณ์ส่วนตัวมาใช้ในสถานประกอบการ

อุปกรณ์สื่อสารไร้สายเป็นสิ่งสำคัญต่อการสื่อสารทางธุรกิจและช่วยเพิ่มประสิทธิผลการทำงาน นอกจากนี้การใช้อุปกรณ์สื่อสารไร้สายของพนักงานที่เพิ่มขึ้นทำให้ต้อง

มีการขออนุญาตเชื่อมต่อกับเครือข่ายของบริษัท การอนุมัติการใช้อุปกรณ์ส่วนตัวและแอปพลิเคชั่นให้เป็นไปตามแต่ละบริษัทกำหนด

บุคลากรที่ใช้อุปกรณ์สื่อสารไร้สายส่วนตัวต้องปฏิบัติ ดังต่อไปนี้

1) งานที่ได้พัฒนาขึ้นบนอุปกรณ์ส่วนตัวถือเป็นทรัพย์สินทางปัญญาของกลุ่มบริษัทแอสเซนด์
2) อุปกรณ์สื่อสารไร้สายส่วนตัวให้ฝ่ายเทคโนโลยีสารสนเทศตั้งค่าระบบและติดตั้งโปรแกรมพื้นฐานก่อนการเข้าถึงเครือข่าย
3) อุปกรณ์สื่อสารไร้สายจะต้องตั้งรหัสผ่านสำหรับการเข้าถึงข้อมูลของกลุ่มบริษัทแอสเซนด์เพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต และจะต้องไม่วางทิ้งไว้ในที่สาธารณะ
4) ต้องสำรองข้อมูลที่เกี่ยวข้องกับกลุ่มบริษัทแอสเซนด์เป็นประจำเพื่อป้องกันการสูญหาย
5) แจ้งให้บริษัทในเครือฯ ทราบในกรณีที่อุปกรณ์ที่เก็บข้อมูลของกลุ่มบริษัทแอสเซนด์สูญหายหรือถูกขโมย
6) รับผิดชอบค่าใช้จ่ายใดๆ ที่เกี่ยวข้องกับอุปกรณ์ส่วนตัว
7) รับผิดชอบต่อความเสี่ยงที่ข้อมูลส่วนตัวหรือข้อมูลของกลุ่มบริษัทแอสเซนด์บนอุปกรณ์ส่วนตัวจะสูญหายอันเกิดจากความล้มเหลวของระบบปฏิบัติการ ไวรัส โปรแกรมประสงค์ร้าย (malware) หรือข้อผิดพลาดใด ๆ ของซอฟต์แวร์และตัวอุปกรณ์
8) ส่งคืนหรือทำลายข้อมูลของกลุ่มบริษัทแอสเซนด์ที่อยู่ในอุปกรณ์สื่อสารไร้สายส่วนตัวเมื่อสิ้นสุดการเป็นพนักงาน
9) กลุ่มบริษัทแอสเซนด์สงวนสิทธิ์ในการตัดสัญญาณการเชื่อมต่อเครือข่ายหรืองดให้บริการโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

5.3.4 การสำรองข้อมูล

1) จัดให้มีขั้นตอนการปฏิบัติการเก็บสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้องทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศโดยจัดทำเป็นลายลักษณ์อักษร
2) สำรองข้อมูลในระบบข้อมูลสารสนเทศและ Hard Drives ของกลุ่มบริษัทแอสเซนด์มาไว้ที่สื่อบันทึกข้อมูล เช่น USB Drives, External Hard Disk และแผ่นดิสก์ ให้เป็นปัจจุบันอย่างสม่ำเสมอ

3) ดูแลรักษาสื่อบันทึกข้อมูลโดยการสำรองข้อมูลลงในสื่อบันทึกข้อมูลใหม่และทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมออย่างน้อยปีละหนึ่งครั้ง เพื่อป้องกันการเสื่อมสภาพ รวมทั้งมีวิธีการนำข้อมูลกลับมาใช้งานใหม่

5.3.5 สร้างรหัสลับ (Encryption) เมื่อส่งข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษระหว่างหน่วยงาน/บริษัท

5.4 การแลกเปลี่ยนข้อมูลสารสนเทศกับบุคคลภายนอก

5.4.1 ในกรณีที่จำเป็นต้องให้ข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษแก่บุคคลภายนอกหรือบุคคลที่ไม่ได้รับอนุญาตต้องได้รับการตรวจสอบความถูกต้องของข้อมูลจากผู้รับผิดชอบดูแลข้อมูลสารสนเทศและต้องได้รับอนุญาตจากผู้บริหาร รวมทั้งบุคคลภายนอกจะต้องลงนามในข้อตกลงห้ามเปิดเผยข้อมูล (Non Disclosure Agreement หรือ NDA)

5.4.2 สร้างรหัสลับ (Encryption) เมื่อส่งข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษให้กับบุคคลภายนอก

5.5 การใช้อินเทอร์เน็ต

5.5.1 ไม่ใช้อินเทอร์เน็ตของบริษัทในเวลาทำงานเพื่อใช้ดำเนินธุรกิจส่วนตัวซึ่งไม่เกี่ยวกับงานของกลุ่มบริษัทแอสเซนด์

5.5.2 ไม่ใช้อินเทอร์เน็ตในทางที่ละเมิดกฎหมายลิขสิทธิ์ เช่น การดาวน์โหลดโปรแกรม ไฟล์เพลง ไฟล์ภาพยนตร์ รูปภาพหรือข้อความของบุคคลอื่นบนเว็บไซต์โดยไม่ได้รับอนุญาตและนำไปใช้เพื่อแสวงหาผลประโยชน์โดยไม่ได้รับอนุญาตจากเจ้าของ

5.5.3 ไม่ใช้อินเทอร์เน็ตเพื่อกระทำการใดๆ ซึ่งขัดต่อจรรยาบรรณธุรกิจของกลุ่มบริษัทแอสเซนด์

5.5.4 ไม่ใช้อินเทอร์เน็ตของกลุ่มบริษัทแอสเซนด์ซึ่งทำให้การใช้งานอินเทอร์เน็ตของบุคคลอื่นช้าลง เช่น ดาวน์โหลดไฟล์จำนวนมากเกินไป

5.6 การใช้อีเมล

5.6.1 ห้ามส่งอีเมลแก่บุคคลอื่นโดยปลอมแปลงแหล่งที่มาของการส่งอีเมล อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น

5.6.2 ห้ามส่งอีเมลที่มีข้อความหรือรูปภาพ ซึ่งก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ มีเนื้อหาผิดกฎหมาย สร้างความอับอาย คุกคาม ก้าวร้าว สร้างความเกลียดชังหรือสนับสนุนให้มีการกระทำผิดกฎหมาย

5.6.3 ระมัดระวังเมื่อจำเป็นต้องเปิดอีเมลจากผู้ส่งที่ไม่รู้จักซึ่งอาจพบโปรแกรมประสงค์ร้าย (malware) การหลอกเก็บข้อมูลที่มาจากอีเมลหลอกลวง (phishing) รวมถึงระมัดระวังอีเมลจากผู้ที่ไม่รู้จักและแจ้งฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อพบอีเมลที่ต้องสงสัย

5.6.4 ระมัดระวังในการเปิดลิงค์ซึ่งอาจพบโปรแกรมประสงค์ร้าย (malware) เช่น ไวรัส spyware trojan เป็นต้น

5.6.5 ไม่ส่งอีเมลทางธุรกิจโดยใช้สำเนาลับ (Blind Carbon Copy: Bcc)

5.6.6 ตั้งค่าอีเมลทางธุรกิจที่ส่งออกทุกฉบับให้มี E-mail Signature

5.6.7 ใช้อีเมลส่วนตัว (Gmail, Yahoo Mail) นอกเวลางานหรือในเวลาพักกลางวัน

5.7 การใช้สื่อสังคมออนไลน์ (Social Media)

โปรดดูรายละเอียดในนโยบายและแนวทางปฏิบัติในการใช้สื่อสังคมออนไลน์ของกลุ่มบริษัทแอสเซนด์

5.8 การทำลายข้อมูลสารสนเทศ

5.8.1 ข้อมูลสารสนเทศที่จัดพิมพ์เป็นเอกสารในรูปแบบกระดาษหรือวัตถุใดๆ ซึ่งอยู่ในระดับเอกสารใช้ภายในเท่านั้น เอกสารลับและเอกสารลับพิเศษ เมื่อไม่ต้องการแล้วให้ทำลายโดยเครื่องทำลายเอกสารเท่านั้น ส่วนเอกสารเปิดเผยให้ทิ้งลงถังขยะหรือเครื่องทำลายเอกสาร

5.8.2 ย้ายข้อมูลสารสนเทศที่สำคัญแล้วจึงลบข้อมูลสารสนเทศเป็นการถาวรก่อนทำลายสื่อบันทึก

5.9 การตรวจสอบการรั่วไหลของข้อมูลสารสนเทศ

ในกรณีที่เกิดการรั่วไหลของข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษ ผู้บริหารที่รับผิดชอบต้องแต่งตั้งคณะกรรมการสอบสวนเพื่อสอบสวนและตรวจสอบหาสาเหตุความผิดพลาด พร้อมทั้งปรับปรุงวิธีจัดเก็บข้อมูลสารสนเทศไม่ให้รั่วไหลและระบบการป้องกันการรั่วไหลของข้อมูลสารสนเทศ ตลอดจนรายงานให้ผู้บริหารรับทราบ

6. การฝึกอบรม

จัดให้มีการสื่อสารและถ่ายทอดนโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูลสารสนเทศผ่านการฝึกอบรม การประชุม หรือกิจกรรมในรูปแบบต่าง ๆ ให้แก่กรรมการ ผู้บริหารและพนักงานและให้มีการประเมินประสิทธิผลอย่างต่อเนื่อง

7. การแจ้งเบาะแส

ร้องเรียนหรือแจ้งเบาะแสเมื่อพบเห็นการกระทำที่เชื่อได้ว่าเป็นการละเมิดนโยบายและแนวปฏิบัตินี้ โดยขั้นตอนให้เป็นไปตามนโยบายและแนวปฏิบัติเกี่ยวกับการแจ้งเบาะแส ทั้งนี้ผู้ร้องเรียนหรือผู้แจ้งเบาะแสจะได้รับความคุ้มครองและข้อมูลจะถูกเก็บเป็นความลับ โดยไม่มีผลต่อตำแหน่งงานทั้งในระหว่างดำเนินการสอบสวนและหลังเสร็จสิ้นกระบวนการ

8. การขอคำแนะนำ

ในกรณีที่มีข้อสงสัยว่าการกระทำนั้นอาจฝ่าฝืนกฎหมาย ระเบียบ นโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูลสารสนเทศสามารถขอคำแนะนำจากผู้บังคับบัญชา หน่วยงานหรือบุคคลผู้รับผิดชอบด้านการบริหารจัดการข้อมูลสารสนเทศ ด้านกำกับการปฏิบัติตามกฎเกณฑ์หรือด้านกฎหมายก่อนตัดสินใจหรือดำเนินการใด ๆ

9. บทลงโทษ

ในกรณีที่เกิดการสอบสวน พนักงานทุกคนต้องให้ความร่วมมือกับหน่วยงานภายในและภายนอกอย่างเต็มที่ ทั้งนี้หากผู้บริหารและพนักงานกระทำการใด ๆ ที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายฉบับนี้ไม่ว่าทางตรงหรือทางอ้อม ผู้บริหารและพนักงานจะถูกพิจารณาโทษทางวินัยตามระเบียบข้อบังคับการทำงาน

10. กฎหมาย กฎระเบียบและนโยบายที่เกี่ยวข้อง

10.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

10.2 พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537

10.3 นโยบายและแนวทางปฏิบัติในการใช้สื่อสังคมออนไลน์ของกลุ่มบริษัทแอสเซนด์

10.4 ISO/IEC 27001:2013 (Information Security Management System: ISMS)

11. ภาคผนวก

นโยบายและแนวปฏิบัตินี้ ประกอบด้วยภาคผนวก ดังต่อไปนี้

11.1 ภาคผนวก ก ตัวอย่างเอกสารปกตามระดับความลับของข้อมูล

11.2 ภาคผนวก ข ตัวอย่างการใช้กระดาษระดับความลับของข้อมูล

ภาคผนวก ก

ตัวอย่างเอกสารปกตามระดับความลับของข้อมูล

เอกสารลับพิเศษ

(SPECIAL CONTROL)

ตราสัญลักษณ์บริษัท

เอกสารปกใช้ปะหน้าปิดทับเอกสารลับพิเศษ

การเปิดเผยเอกสารลับพิเศษนี้ ส่งผลกระทบต่อยุทธศาสตร์การดำเนินธุรกิจและก่อให้เกิดความเสียเปรียบในการแข่งขันเชิงธุรกิจอย่างร้ายแรงทำให้เกิดความเสียหายต่อภาพพจน์ขององค์กรในระดับสากล

หน้าที่ความรับผิดชอบของผู้ครอบครอง

1. ผู้ถือครองมีหน้าที่รับผิดชอบความปลอดภัยของเอกสารลับพิเศษนี้
2. มีการป้องกันที่จำเป็นเพื่อไม่ให้เอกสารถูกเปิดเผยโดยไม่ได้รับอนุญาต โดยการไม่ทิ้งเอกสารไว้ลำพัง ยกเว้นเมื่อเก็บรักษาในสถานที่ปลอดภัย
3. การเปิดเผยเอกสารจะให้เฉพาะผู้ที่มีสิทธิรับรู้เท่านั้น

การเก็บ

เมื่อไม่มีการใช้งานจากเอกสารให้ใส่ในหีบห่อหรือแฟ้มเอกสารระบุด้านหน้าว่า **“SPECIAL CONTROL (เอกสารลับพิเศษ)”** และให้เก็บไว้ในตู้นิรภัยที่ตั้งไว้ในพื้นที่ที่มีการควบคุมการเข้า-ออก เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

การทำสำเนา

เอกสารลับพิเศษห้ามทำสำเนา แยกชิ้น หรือทำขึ้นมาใหม่ โดยไม่ได้รับอนุญาต

การทำลาย

ห้ามทิ้งถังขยะ ให้ทำลายโดยเครื่องทำลายเอกสารและเผาเท่านั้น

(ใบปะหน้านี้จะไม่เป็นความลับเมื่อถูกแยกจากเอกสารลับพิเศษ)

เอกสารลับพิเศษ

(SPECIAL CONTROL)

เอกสารลับ

(CONFIDENTIAL)

ตราสัญลักษณ์บริษัท

เอกสารปกปะหน้าใช้ปิดทับเอกสารลับ

การเปิดเผยเอกสารลับนี้ ส่งผลกระทบต่อการประกอบธุรกิจและความก้าวหน้าขององค์กร อาจถูกฟ้องร้องเรียกค่าเสียหาย เกิดความเสียหายต่อภาพพจน์ในระดับประเทศ

หน้าที่ความรับผิดชอบของผู้ครอบครอง

1. ผู้ถือครองมีหน้าที่รับผิดชอบความปลอดภัยของเอกสารลับนี้
2. มีการป้องกันที่จำเป็นเพื่อไม่ให้เอกสารถูกเปิดเผยโดยไม่ได้รับอนุญาต โดยการไม่ทิ้งเอกสารไว้ลำพัง ยกเว้นเมื่อเก็บรักษาในสถานที่ปลอดภัย
3. การเปิดเผยเอกสารจะให้เฉพาะผู้ที่มีสิทธิรับรู้เท่านั้น

การเก็บ

เมื่อไม่มีการใช้งานจากเอกสารให้ใส่ในหีบห่อหรือแฟ้มเอกสารระบุด้านหน้าว่า “**CONFIDENTIAL (เอกสารลับ)**” และให้เก็บไว้ในตู้เอกสารที่ปิดล็อกด้วยกุญแจที่มั่นคงที่ตั้งไว้ในพื้นที่ที่มีการควบคุมการเข้า-ออก เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

การทำสำเนา

เอกสารลับห้ามทำสำเนา แยกชิ้น หรือทำขึ้นมาใหม่ โดยไม่ได้รับอนุญาต

การทำลาย

ห้ามทิ้งถังขยะ ให้ทำลายโดยเครื่องทำลายเอกสารเท่านั้น

(ใบปะหน้านี้จะไม่เป็นความลับเมื่อถูกแยกจากเอกสารลับ)

เอกสารลับ

(CONFIDENTIAL)

เอกสารใช้ภายในเท่านั้น

ตราสัญลักษณ์บริษัท

เอกสารปกปะหน้าใช้ปิดทับเอกสารใช้ภายในเท่านั้น

การเปิดเผยเอกสารใช้ภายในเท่านั้น ส่งผลกระทบต่อการปฏิบัติงานประจำวัน อาจทำให้เกิดความเสียหายต่อภาพพจน์ เป็นข้อมูลที่อนุญาตให้ใช้ภายในหน่วยงานเท่านั้น

หน้าที่ความรับผิดชอบของผู้ครอบครอง

1. ผู้ถือครองมีหน้าที่รับผิดชอบความปลอดภัยของเอกสารใช้ภายในเท่านั้น
2. มีการป้องกันที่จำเป็นเพื่อไม่ให้เอกสารถูกเปิดเผยโดยไม่ได้รับอนุญาต โดยการไม่ทิ้งเอกสารไว้ลำพัง ยกเว้นเมื่อเก็บรักษาในสถานที่ปลอดภัย
3. การเปิดเผยเอกสารจะให้เฉพาะผู้ที่มีสิทธิรับรู้ตามหน้าที่ความรับผิดชอบเท่านั้น

การเก็บ

เมื่อไม่มีการใช้งานจากเอกสารให้ใส่ในหีบห่อหรือแฟ้มเอกสารระบุด้านหน้าว่า " INTERNAL USE ONLY **(เอกสารใช้ภายในเท่านั้น)**" และให้เก็บไว้ในตู้เอกสารที่ปิดล็อกด้วยกุญแจ

การทำสำเนา

เอกสารใช้ภายในเท่านั้น สามารถทำสำเนา แยกชิ้น หรือทำขึ้นมาใหม่ โดยต้องได้รับอนุญาตจากผู้มีหน้าที่รับผิดชอบเท่านั้น

การทำลาย

ให้ทำลายโดยเครื่องทำลายเอกสารเท่านั้น

(ใบปะหน้านี้จะไม่เป็นความลับเมื่อถูกแยกจากเอกสารใช้ภายในเท่านั้น)

เอกสารใช้ภายในเท่านั้น

(INTERNAL USE ONLY)

เอกสารเปิดเผย

(PUBLIC)

ตราสัญลักษณ์บริษัท

เอกสารปกปะหน้าใช้ปิดทับเอกสารเปิดเผย

เป็นข้อมูลที่พิจารณาแล้วเห็นว่าไม่มีผลกระทบต่อองค์กร สามารถเปิดเผยสู่บุคคลภายนอกได้

หน้าที่ความรับผิดชอบของผู้ครอบครอง

ผู้ครอบครองเอกสารสามารถเปิดเผยสู่สาธารณะได้ตามความเหมาะสม

การเก็บ

เมื่อไม่มีการใช้งานเอกสารให้ใส่ในหีบห่อหรือแฟ้มเอกสารระบุด้านหน้าว่า "PUBLIC (**เอกสารเปิดเผย**)" และให้เก็บไว้ในตู้เอกสาร

การทำสำเนา

เอกสารเปิดเผย สามารถทำสำเนา คัดลอก แยกชิ้น หรือทำใหม่ได้ ตามความเหมาะสม

การทำลาย

ให้ทำลายโดยทิ้งลงถังขยะให้เรียบร้อย หรือเครื่องทำลายเอกสาร

(ใบปะหน้านี้จะไม่เป็นความลับ)

เอกสารเปิดเผย

(PUBLIC)

ภาคผนวก ข

ตัวอย่างการใช้กระดาษระดับความลับของข้อมูล

ตราสัญลักษณ์
บริษัท

เอกสารลับพิเศษ / **SPECIAL CONTROL**

เอกสารลับพิเศษ / **SPECIAL CONTROL**

ตราสัญลักษณ์
บริษัท

ตราสัญลักษณ์
บริษัท

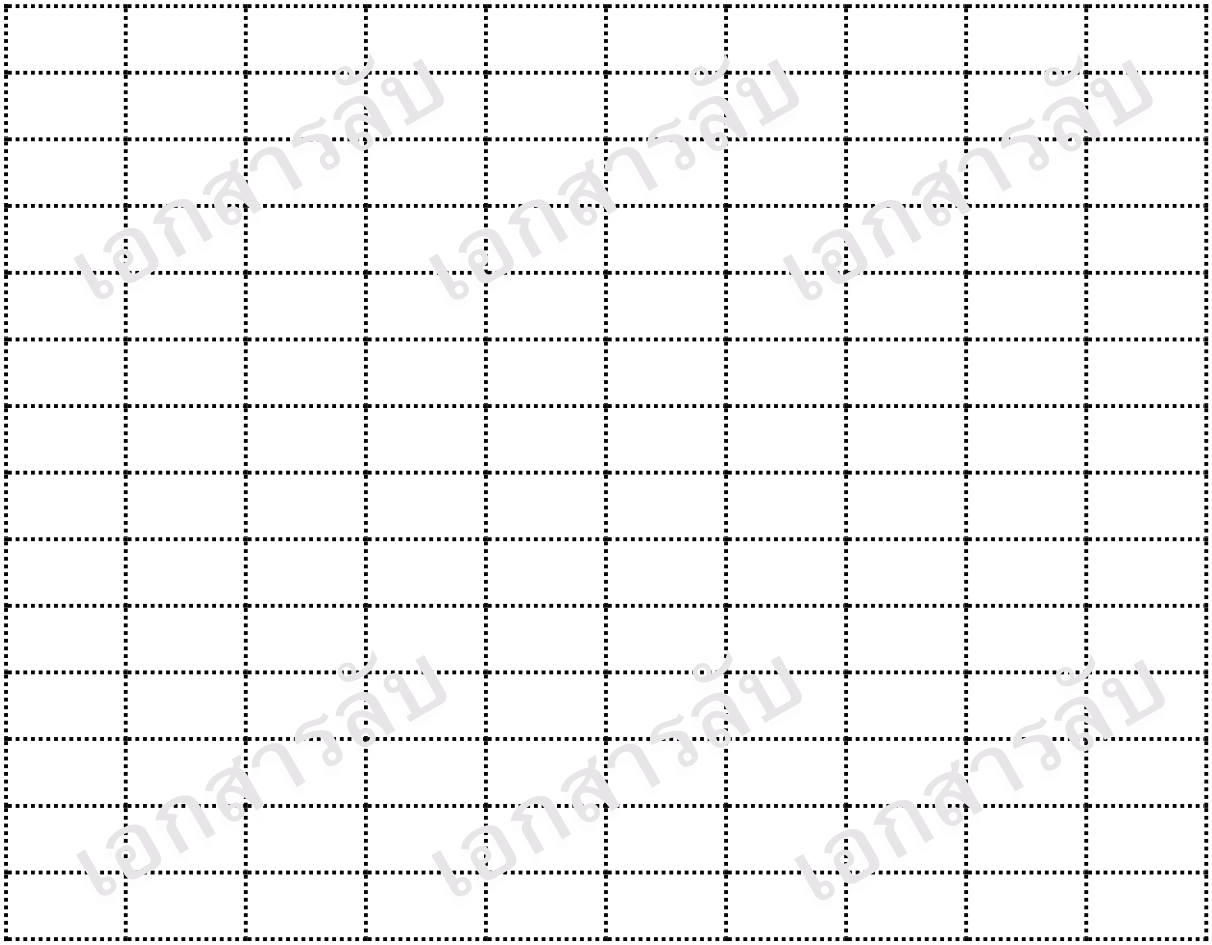
ใช้ภายในเท่านั้น/ (Internal Use Only)

ใช้ภายในเท่านั้น/ (Internal Use Only)

Page 1 of .....

ตราสัญลักษณ์
บริษัท

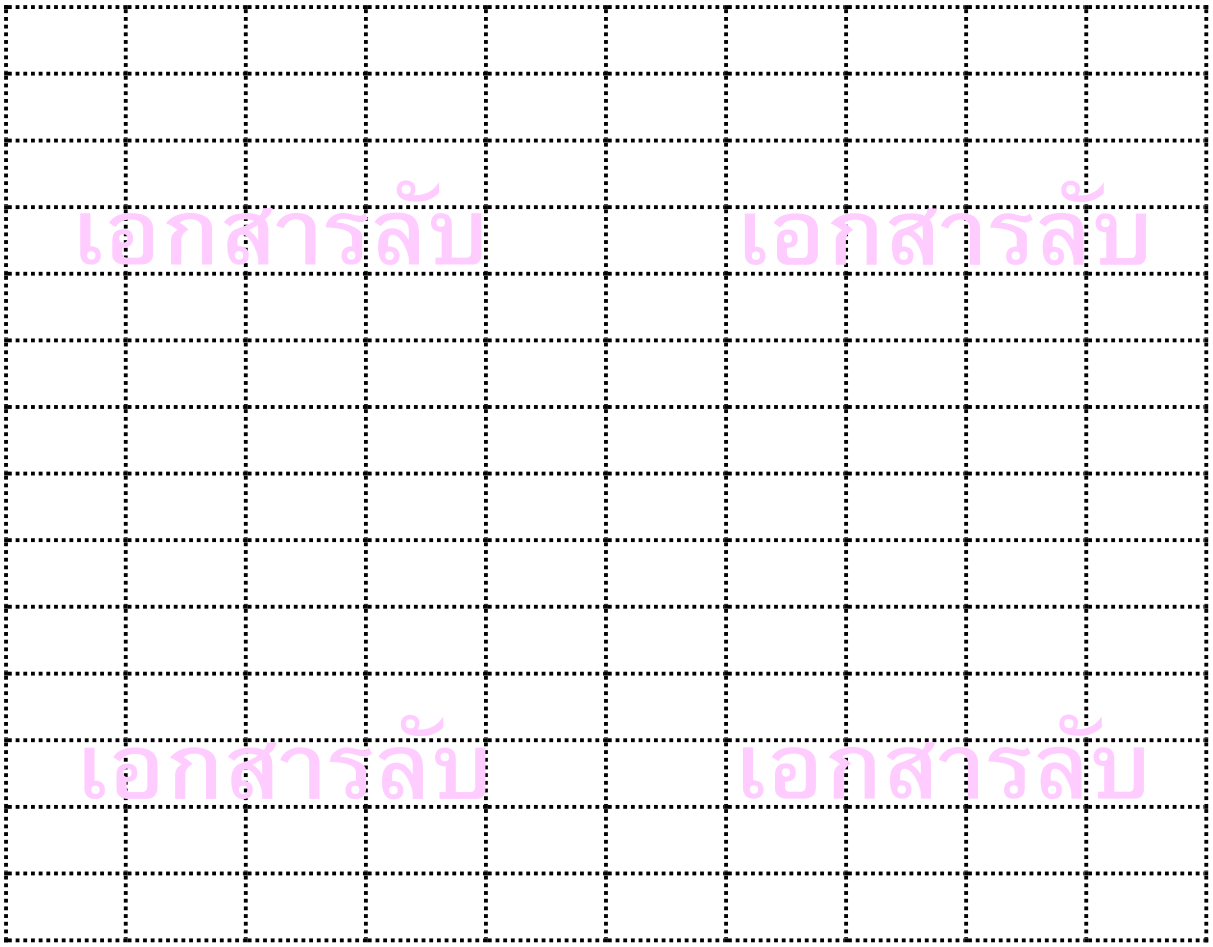
เปิดเผย



เอกสารลับพิเศษ / SPECIAL CONTROL

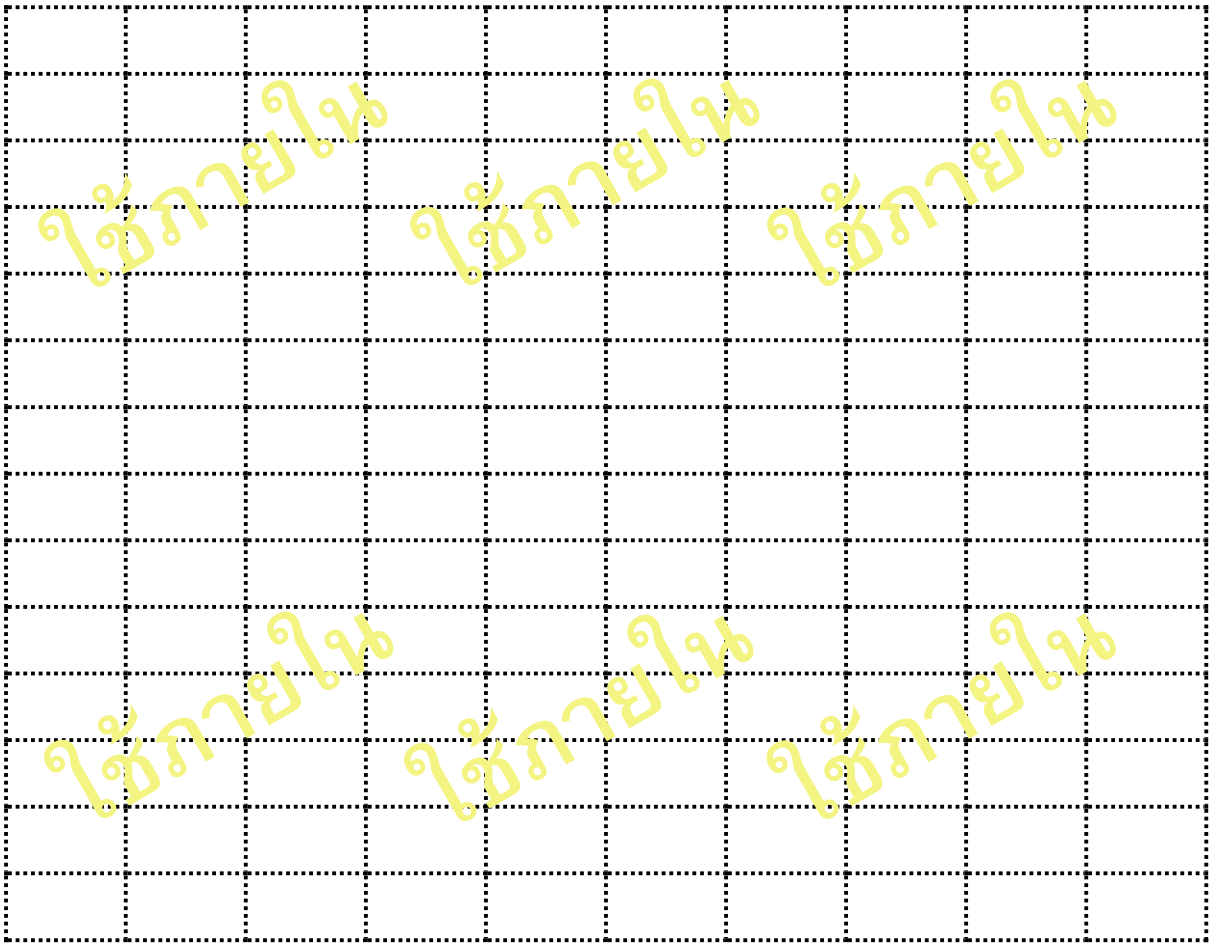
ตราสัญลักษณ์บริษัท

เอกสารลับ / **CONFIDENTIAL**



เอกสารลับ / **CONFIDENTIAL**

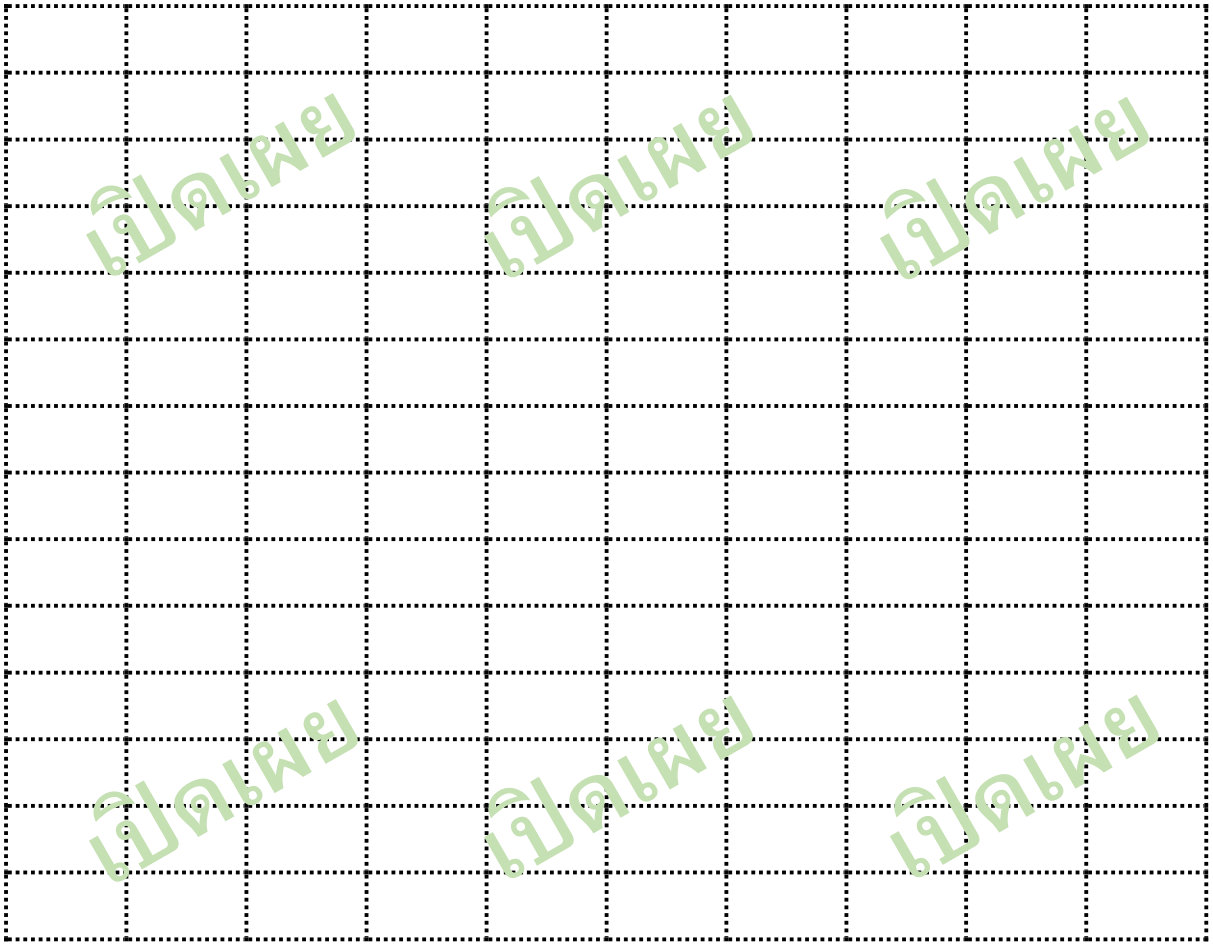
ตราสัญลักษณ์บริษัท



ใช้ภายในเท่านั้น / **Internal Use Only**

ตราสัญลักษณ์บริษัท

เปิดเผย / **Public**



เปิดเผย / **Public**