



นโยบายและแนวปฏิบัติ
เรื่องการบริหารจัดการข้อมูลสารสนเทศ



สารบัญ

1. ความสำคัญ	3
2. วัตถุประสงค์	3
3. หน้าที่และความรับผิดชอบ	3
4. แนวปฏิบัติ	5
5. นโยบายที่เกี่ยวข้อง	11
6. กฎหมาย ข้อกำหนดและมาตรฐานสากลที่เกี่ยวข้อง	11
7. การทบทวนนโยบาย	11
ภาคผนวก 1 : ตัวอย่าง เอกสารปกตามระดับความลับของข้อมูล	12
ภาคผนวก 2 : ตัวอย่าง การใช้กระดาษระดับความลับของข้อมูล	16



นโยบายและแนวปฏิบัติเรื่องการบริหารจัดการข้อมูลสารสนเทศ

1. ความสำคัญ

ข้อมูลสารสนเทศถือเป็นสินทรัพย์ที่มีค่าของเครือเจริญโภคภัณฑ์ จึงต้องมีการกำกับดูแลข้อมูลสารสนเทศอย่างเป็นระบบและมีประสิทธิภาพ มีความน่าเชื่อถือถูกต้องสมบูรณ์ซึ่งเป็นการป้องกันความเสี่ยงจากความเสียหาย ปกป้องทรัพย์สินของเครือเจริญโภคภัณฑ์ และช่วยลดการสูญหายของข้อมูล ส่งผลให้การตัดสินใจทางธุรกิจมีประสิทธิภาพรวมถึงเพิ่มขีดความสามารถทางการแข่งขัน

2. วัตถุประสงค์

เพื่อให้บุคลากรเข้าใจบทบาทหน้าที่และร่วมกันปกป้องข้อมูลสารสนเทศของเครือเจริญโภคภัณฑ์ มิให้รั่วไหลหรือนำข้อมูลไปใช้ในทางที่ผิด

3. หน้าที่และความรับผิดชอบ

สำหรับบุคลากรใช้เป็นแนวทางในการประสานงานภายในบริษัท

3.1 คณะกรรมการ

- 3.1.1 กำหนดให้มีนโยบายและแนวปฏิบัติเรื่องการบริหารจัดการข้อมูลสารสนเทศ
- 3.1.2 กำกับดูแลให้มีการนำนโยบายและแนวปฏิบัติไปปฏิบัติอย่างเป็นรูปธรรม

3.2 ผู้บริหาร

- 3.2.1 จัดให้มีระเบียบปฏิบัติให้เหมาะสมกับบริบทของแต่ละบริษัท โดยให้สอดคล้องกับบริบทของบริษัท และข้อกำหนดกฎหมายของแต่ละประเทศที่บริษัทดำเนินธุรกิจ
- 3.2.2 จัดให้มีโครงสร้างผู้รับผิดชอบ เช่น หน่วยงาน หรือบุคคลผู้รับผิดชอบเพื่อดูแลข้อมูลและระบบสารสนเทศ
- 3.2.3 กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ
- 3.2.4 มั่นใจว่ามีการบริหารความเสี่ยงจากการใช้ข้อมูลสารสนเทศ
- 3.2.5 มั่นใจว่ามีการรายงานผลการปฏิบัติงานตามนโยบายฯ รวมถึงรายงานปัญหาจากการใช้ข้อมูลสารสนเทศ



3.3 หน่วยงาน/บุคคลผู้รับผิดชอบดูแลข้อมูลและระบบสารสนเทศ

- 3.3.3 ปฏิบัติตามแนวปฏิบัติ ข้อ 4.2 การบริหารจัดการความเสี่ยง
- 3.3.4 ปฏิบัติตามแนวปฏิบัติ ข้อ 4.3 การบริหารจัดการข้อมูลสารสนเทศ
- 3.3.5 ปฏิบัติตามแนวปฏิบัติ ข้อ 4.4 การแลกเปลี่ยนข้อมูลสารสนเทศกับบุคคลภายนอก
- 3.3.6 ปฏิบัติตามแนวปฏิบัติ ข้อ 4.8 การทำลายข้อมูลสารสนเทศ
- 3.3.7 รายงานผลการปฏิบัติงานตามนโยบายและแนวปฏิบัติ และระเบียบปฏิบัติ รวมถึงรายงานปัญหาจากการใช้ข้อมูลสารสนเทศ

3.4 ฝ่ายเทคโนโลยีสารสนเทศ

- 3.4.3 ดูแลรักษาเทคโนโลยีสำหรับระบบข้อมูลสารสนเทศ
- 3.4.4 ควบคุมการเข้าถึงระบบข้อมูลสารสนเทศและเครือข่าย
- 3.4.5 รักษาความปลอดภัยของข้อมูลสารสนเทศ
- 3.4.6 จัดให้มีการเก็บสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง

3.5 ด้านตรวจสอบธรรมาภิบาล สำหรับบริหารความยั่งยืน และฝ่ายทรัพยากรบุคคลของแต่ละบริษัทในเครือฯ

- 3.5.3 ตรวจสอบให้มีการบริหารจัดการข้อมูลสารสนเทศตามนโยบายฯ
- 3.5.4 ให้คำแนะนำและให้ความรู้แก่บุคลากรเพื่อให้เกิดการปฏิบัติตามนโยบายฯ

3.6 พนักงาน

- 3.6.3 รักษาความลับและปกป้องความปลอดภัยของข้อมูลส่วนตัว รวมทั้งข้อมูลสารสนเทศของเครือเจริญโภคภัณฑ์ ลูกค้าและคู่ค้าธุรกิจและพันธมิตรทางธุรกิจ
- 3.6.4 จัดทำข้อมูลสารสนเทศ บันทึกและรายงานให้มีความถูกต้อง น่าเชื่อถือ
- 3.6.5 ปกป้องทรัพย์สินทางปัญญาของเครือเจริญโภคภัณฑ์ และไม่ละเมิดสิทธิในทรัพย์สินทางปัญญาของผู้อื่น
- 3.6.6 ปฏิบัติตามนโยบายฯ กฎหมาย และมาตรฐานสากลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลสารสนเทศ



4. แนวปฏิบัติ

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

4.1.1 ความเป็นส่วนตัวของข้อมูลสารสนเทศ (Information Privacy)

ลักษณะของข้อมูลที่เป็นส่วนตัว เช่น หมายเลขบัตรประจำตัวประชาชน วันเดือนปีเกิด ชื่อบัญชีผู้ใช้งาน (account) และรหัสผ่าน (password)

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

4.1.2 ความถูกต้องของข้อมูล (Information Accuracy)

- 1) การจัดทำข้อมูลสารสนเทศให้มีความถูกต้องและน่าเชื่อถือนั้น ข้อมูลควรได้รับการตรวจสอบความถูกต้องก่อนที่จะนำเข้าสู่ฐานข้อมูล รวมถึงการปรับปรุงข้อมูลให้มีความทันสมัยอยู่เสมอ
- 2) แหล่งที่มาของข้อมูลต้องมีความน่าเชื่อถือและตรวจสอบได้ เช่น หน่วยงานภาครัฐ องค์กรอื่นที่เชื่อถือได้ เป็นต้น

4.1.3 ความเป็นเจ้าของ (Information Property)

- 1) บริษัทในเครือฯ เป็นเจ้าของในทรัพย์สินทางปัญญาที่บุคลากรได้พัฒนาหรือสร้างขึ้นไม่ว่าจะทั้งหมดหรือบางส่วน
- 2) ไม่ละเมิดหรือเปิดเผยโดยไม่ได้รับอนุญาตในทรัพย์สินทางปัญญาและลิขสิทธิ์ของงานที่ทำร่วมกัน



4.2 การบริหารจัดการความเสี่ยง

4.2.1 ระบุและประเมินความเสี่ยง

4.2.2 จัดลำดับความสำคัญของความเสี่ยงและบริหารความเสี่ยงสำคัญที่ต้องดำเนินการก่อน

4.2.3 กำหนดมาตรการจัดการความเสี่ยงและดำเนินการตามมาตรการ

4.3 การบริหารจัดการข้อมูลสารสนเทศ

4.3.1 การจัดระดับความลับข้อมูลสารสนเทศ (Classification of Information) โดยพิจารณาจากระดับความเสี่ยงต่อความมั่นคงปลอดภัย ผลกระทบต่อมูลค่า ผลกระทบต่อความเสียหายทางทรัพย์สินและภาพพจน์บริษัทโดยแบ่งตามประเภทดังต่อไปนี้

- 1) **เอกสารลับพิเศษ (Special Control) [สีม่วง]** เป็นข้อมูลสารสนเทศที่ส่งผลกระทบต่อ การดำเนินยุทธศาสตร์ทางธุรกิจและก่อให้เกิดความเสียหายเปรียบเทียบในการแข่งขันเชิงธุรกิจอย่างร้ายแรง ถ้าเกิดการรั่วไหลของข้อมูลออกมาจะก่อให้เกิดความเสียหายต่อภาพพจน์ของบริษัทในระดับสากล เช่น
 - ข้อมูลความลับทางการค้า (Trade Secret)
 - แผนกลยุทธ์ทางธุรกิจ
 - แผนการตลาด / การพัฒนาผลิตภัณฑ์
 - แผนควบรวมกิจการ
- 2) **เอกสารลับ (Confidential) [สีแดง]** เป็นข้อมูลสารสนเทศที่ส่งผลกระทบต่อ การดำเนินธุรกิจและความก้าวหน้าของธุรกิจ องค์กรอาจถูกฟ้องร้องเรียกค่าเสียหาย ถ้าเกิดการรั่วไหลของข้อมูลและก่อให้เกิดความเสียหายต่อภาพพจน์บริษัทในระดับประเทศ เช่น
 - เอกสารทางการตลาด (ที่ยังไม่เปิดเผยต่อสาธารณะ)
 - ข้อมูลส่วนบุคคล
 - ข้อมูลลูกค้า
- 3) **เอกสารใช้ภายในเท่านั้น (Internal Use Only) [สีเหลือง]** เป็นข้อมูลสารสนเทศที่อนุญาตให้ใช้ภายในบริษัทในเครือข่าย เท่านั้น ส่งผลกระทบต่อ การปฏิบัติงานประจำวันและอาจทำให้เกิดความเสียหายต่อภาพพจน์ เช่น
 - ประกาศภายใน/นโยบายต่างๆ
 - ระเบียบ/คู่มือปฏิบัติงาน
 - บันทึกการปฏิบัติงานประจำวัน



- 4) **เอกสารเปิดเผย (Public)** [สีเขียว] เป็นข้อมูลสารสนเทศที่พิจารณาแล้วเห็นว่าไม่มีผลกระทบต่อองค์กร สามารถเปิดเผยต่อบุคคลภายนอกได้ เช่น
- ข้อมูลด้านความยั่งยืน
 - ข้อมูลประชาสัมพันธ์
 - โปรโมชันทางการค้าต่างๆ

ทั้งนี้ เอกสารหรือสิ่งตีพิมพ์ไม่ว่าจะทั้งหมดหรือบางส่วนที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับซึ่งมีการกำหนดชั้นความลับไว้ ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับ

4.3.2 การจัดเก็บข้อมูลสารสนเทศและอุปกรณ์

- 1) ผู้บริหารและผู้รับผิดชอบดูแลข้อมูลสารสนเทศเป็นผู้กำหนดระยะเวลาจัดเก็บข้อมูลสารสนเทศตามระดับความลับ
- 2) จัดเก็บข้อมูลสำรองในสื่อบันทึกข้อมูลและจัดทำรายการบันทึกให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน
- 3) รักษาความปลอดภัยของระบบสารสนเทศและอุปกรณ์ ซึ่งบรรจุข้อมูลสารสนเทศของบริษัท เช่น โทรศัพท์มือถือ แล็ปท็อป แท็บเล็ต เป็นต้น และต้องระมัดระวังเป็นพิเศษในการใช้งานอุปกรณ์ดังกล่าวนอกสถานประกอบการรวมทั้งจัดเก็บไว้ในที่ที่มีกุญแจล็อกหลังการใช้งาน
- 4) ตั้งรหัสผ่าน (password) ล็อกหน้าจอซึ่งบรรจุข้อมูลสารสนเทศของเครื่องเจริญโภคภัณฑ์เมื่อต้องการออกจากระบบสารสนเทศหรือเสร็จสิ้นงาน
- 5) รายงานฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อข้อมูลสารสนเทศหรืออุปกรณ์ซึ่งบรรจุข้อมูลสารสนเทศของเครื่องเจริญโภคภัณฑ์สูญหายหรือถูกขโมย

4.3.3 การนำอุปกรณ์ส่วนตัวมาใช้ในสถานประกอบการ

อุปกรณ์สื่อสารไร้สายเป็นสิ่งสำคัญต่อการสื่อสารทางธุรกิจและช่วยเพิ่มประสิทธิภาพการทำงาน นอกจากนี้การใช้อุปกรณ์สื่อสารไร้สายของพนักงานที่เพิ่มขึ้นทำให้ต้องมีการขออนุญาตเชื่อมต่อกับเครือข่ายของบริษัท การอนุมัติการใช้อุปกรณ์ส่วนตัวและแอปพลิเคชันให้เป็นไปตามแต่ละบริษัทกำหนด

บุคลากรที่ใช้อุปกรณ์สื่อสารไร้สายส่วนตัวต้องปฏิบัติ ดังต่อไปนี้

- 1) งานที่ได้พัฒนาขึ้นบนอุปกรณ์ส่วนตัวถือเป็นทรัพย์สินทางปัญญาของเครื่องเจริญโภคภัณฑ์
- 2) อุปกรณ์สื่อสารไร้สายส่วนตัวให้ฝ่ายเทคโนโลยีสารสนเทศตั้งค่าระบบและติดตั้งโปรแกรมพื้นฐานก่อนการเข้าถึงเครือข่าย



- 3) อุปกรณ์สื่อสารไร้สายจะต้องตั้งรหัสผ่านสำหรับการเข้าถึงข้อมูลของเครื่องเจริญโภคภัณฑ์เพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต และจะต้องไม่วางทิ้งไว้ในที่สาธารณะ
- 4) ต้องสำรองข้อมูลที่เกี่ยวข้องกับเครื่องเจริญโภคภัณฑ์เป็นประจำเพื่อป้องกันการสูญหาย
- 5) แจ้งให้บริษัทในเครือฯ ทราบในกรณี que อุปกรณ์ที่เก็บข้อมูลของเครื่องเจริญโภคภัณฑ์สูญหายหรือถูกขโมย
- 6) รับผิดชอบค่าใช้จ่ายใดๆ ที่เกี่ยวข้องกับอุปกรณ์ส่วนตัว
- 7) รับผิดชอบต่อความเสี่ยงที่ข้อมูลส่วนตัวหรือข้อมูลของเครื่องเจริญโภคภัณฑ์ บนอุปกรณ์ส่วนตัวจะสูญหายอันเกิดจากความล้มเหลวของระบบปฏิบัติการ ไวรัส โปรแกรมประสงค์ร้าย (malware) หรือข้อผิดพลาดใดๆ ของซอฟต์แวร์และตัวอุปกรณ์
- 8) ส่งคืนหรือทำลายข้อมูลของเครื่องเจริญโภคภัณฑ์ที่อยู่ในอุปกรณ์สื่อสารไร้สายส่วนตัวเมื่อสิ้นสุดการเป็นพนักงาน
- 9) บริษัทในเครือฯ สงวนสิทธิ์ในการตัดสินญาณการเชื่อมต่อเครือข่ายหรืองดให้บริการโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

4.3.4 การสำรองข้อมูล

- 1) จัดให้มีขั้นตอนการปฏิบัติการเก็บสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้องทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศโดยจัดทำเป็นลายลักษณ์อักษร
- 2) สำรองข้อมูลในระบบข้อมูลสารสนเทศและ Hard Drives ของเครื่องเจริญโภคภัณฑ์มาไว้ที่สื่อบันทึกข้อมูล เช่น USB Drives, External Hard Disk และแผ่นดิสก์ ให้เป็นปัจจุบันอย่างสม่ำเสมอ
- 3) ดูแลรักษาสื่อบันทึกข้อมูลโดยการสำรองข้อมูลลงในสื่อบันทึกข้อมูลใหม่และทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมออย่างน้อยปีละหนึ่งครั้งเพื่อป้องกันการเสื่อมสภาพ รวมทั้งมีวิธีการนำข้อมูลกลับมาใช้งานใหม่

4.3.5 สร้างรหัสลับ (Encryption) เมื่อส่งข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษระหว่างหน่วยงาน/บริษัท

4.4 การแลกเปลี่ยนข้อมูลสารสนเทศกับบุคคลภายนอก

- 4.4.1 ในกรณีที่จำเป็นต้องให้ข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษแก่บุคคลภายนอกหรือบุคคลที่ไม่ได้รับอนุญาตต้องได้รับการตรวจสอบความถูกต้อง



ของข้อมูลจากผู้รับผิดชอบดูแลข้อมูลสารสนเทศและต้องได้รับอนุญาตจากผู้บริหาร รวมทั้งบุคคลภายนอกจะต้องลงนามในข้อตกลงห้ามเปิดเผยข้อมูล (Non Disclosure Agreement หรือ NDA)

4.4.2 สร้างรหัสลับ (Encryption) เมื่อส่งข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษ ให้กับบุคคลภายนอก

4.5 การใช้อินเทอร์เน็ต

4.5.1 ไม่ใช้อินเทอร์เน็ตของบริษัทในเวลาทำงานเพื่อใช้ดำเนินธุรกิจส่วนตัวซึ่งไม่เกี่ยวกับงานของเครือเจริญโภคภัณฑ์

4.5.2 ไม่ใช้อินเทอร์เน็ตในทางที่ละเมิดกฎหมายลิขสิทธิ์ เช่น การดาวน์โหลดโปรแกรมไฟล์เพลง ไฟล์ภาพยนตร์ รูปภาพหรือข้อความของบุคคลอื่นบนเว็บไซต์โดยไม่ได้รับอนุญาตและนำไปใช้เพื่อแสวงหาผลประโยชน์โดยไม่ได้รับอนุญาตจากเจ้าของ

4.5.3 ไม่ใช้อินเทอร์เน็ตเพื่อกระทำการใดๆ ซึ่งขัดต่อจรรยาบรรณธุรกิจของเครือเจริญโภคภัณฑ์

4.5.4 ไม่ใช้อินเทอร์เน็ตของเครือเจริญโภคภัณฑ์ซึ่งทำให้การใช้งานอินเทอร์เน็ตของบุคคลอื่นช้าลง เช่น ดาวน์โหลดไฟล์จำนวนมากเกินไป

4.6 การใช้อีเมล

4.6.1 ห้ามส่งอีเมลแก่บุคคลอื่นโดยปลอมแปลงแหล่งที่มาของการส่งอีเมล อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น

4.6.2 ห้ามส่งอีเมลที่มีข้อความหรือรูปภาพซึ่งก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ มีเนื้อหาผิดกฎหมาย สร้างความอับอาย คุกคาม ก้าวร้าว สร้างความเกลียดชังหรือสนับสนุนให้มีการกระทำผิดกฎหมาย

4.6.3 ระมัดระวังเมื่อจำเป็นต้องเปิดอีเมลจากผู้ส่งที่ไม่รู้จักซึ่งอาจพบโปรแกรมประสงค์ร้าย (malware) การหลอกเก็บข้อมูลที่มาจากอีเมลหลอกลวง (phishing) รวมถึงระมัดระวังอีเมลจากผู้ที่ไม่รู้จักและแจ้งฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อพบอีเมลที่ต้องสงสัย

4.6.4 ระมัดระวังในการเปิดลิ้งค์ซึ่งอาจพบโปรแกรมประสงค์ร้าย (malware) เช่น ไวรัส spyware trojan เป็นต้น

4.6.5 ไม่ส่งอีเมลทางธุรกิจโดยใช้สำเนาลับ (Blind Carbon Copy: Bcc)

4.6.6 ตั้งค่าอีเมลทางธุรกิจที่ส่งออกทุกฉบับให้มี E-mail Signature



- 4.6.7 ใช้อีเมลส่วนตัว (Gmail, Yahoo Mail) นอกเวลางานหรือในเวลาพักกลางวัน
- 4.7 การใช้สื่อสังคมออนไลน์ (Social Media)
โปรดดูรายละเอียดในนโยบายและแนวทางปฏิบัติในการใช้สื่อสังคมออนไลน์ของบริษัทใน
เครือเจริญโภคภัณฑ์
- 4.8 การทำลายข้อมูลสารสนเทศ
- 4.8.1 ข้อมูลสารสนเทศที่จัดพิมพ์เป็นเอกสารในรูปแบบกระดาษหรือวัตถุใดๆ ซึ่งอยู่ใน
ระดับเอกสารใช้ภายในเท่านั้น เอกสารลับและเอกสารลับพิเศษ เมื่อไม่ต้องการแล้ว
ให้ทำลายโดยเครื่องทำลายเอกสารเท่านั้น ส่วนเอกสารเปิดเผยให้ทิ้งลงถังขยะหรือ
เครื่องทำลายเอกสาร
- 4.8.2 ย้ายข้อมูลสารสนเทศที่สำคัญแล้วจึงลบข้อมูลสารสนเทศเป็นการถาวรก่อนทำลาย
สื่อบันทึก
- 4.9 การตรวจสอบการรั่วไหลของข้อมูลสารสนเทศ
ในกรณีที่เกิดการรั่วไหลของข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษ ผู้บริหารที่
รับผิดชอบต้องแต่งตั้งคณะกรรมการสอบสวนเพื่อสอบสวนและตรวจสอบหาสาเหตุความ
ผิดพลาด พร้อมทั้งปรับปรุงวิธีจัดเก็บข้อมูลสารสนเทศไม่ให้รั่วไหลและระบบการป้องกัน
การรั่วไหลของข้อมูลสารสนเทศ ตลอดจนรายงานให้ผู้บริหารรับทราบ

5. นโยบายที่เกี่ยวข้อง

นโยบายและแนวทางปฏิบัติในการใช้สื่อสังคมออนไลน์ของบริษัทในเครือเจริญโภคภัณฑ์

6. กฎหมาย ข้อกำหนดและมาตรฐานสากลที่เกี่ยวข้อง

- 6.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
- 6.2 พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537
- 6.3 ISO/IEC 27001:2013 (Information Security Management System: ISMS)

7. การทบทวนนโยบาย

ด้านธรรมาภิบาล สำนักบริหารความยั่งยืน ธรรมาภิบาลและสื่อสารองค์กร สำนักกำกับกับการปฏิบัติตาม
กฎเกณฑ์ เครือเจริญโภคภัณฑ์ และหน่วยงานที่เกี่ยวข้องจากบริษัทในเครือเจริญโภคภัณฑ์ จะร่วมกัน
ทบทวนนโยบายฉบับนี้อย่างน้อยปีละหนึ่งครั้ง



ภาคผนวก 1 : ตัวอย่างเอกสารปกตามระดับความลับของข้อมูล

เอกสารลับพิเศษ

(SPECIAL CONTROL)

ตราสัญลักษณ์บริษัท

เอกสารปกใช้ปะหน้าปิดทับเอกสารลับพิเศษ

การเปิดเผยเอกสารลับพิเศษนี้ ส่งผลกระทบต่อยุทธศาสตร์การดำเนินธุรกิจและก่อให้เกิดความเสียหายเปรียบในการแข่งขันเชิงธุรกิจอย่างร้ายแรงทำให้เกิดความเสียหายต่อภาพพจน์ขององค์กรในระดับสากล

หน้าที่ความรับผิดชอบของผู้ครอบครอง

1. ผู้ถือครองมีหน้าที่รับผิดชอบความปลอดภัยของเอกสารลับพิเศษนี้
2. มีการป้องกันที่จำเป็นเพื่อไม่ให้เอกสารถูกเปิดเผยโดยไม่ได้รับอนุญาต โดยการไม่ทิ้งเอกสารไว้ลำพัง ยกเว้นเมื่อเก็บรักษาในสถานที่ปลอดภัย
3. การเปิดเผยเอกสารจะให้เฉพาะผู้ที่มีสิทธิรับรู้เท่านั้น

การเก็บ

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

การทำสำเนา

เอกสารลับพิเศษห้ามทำสำเนา แยกชิ้น หรือทำขึ้นมาใหม่ โดยไม่ได้รับอนุญาต

การทำลาย

ห้ามทิ้งถังขยะ ให้ทำลายโดยเครื่องทำลายเอกสารและเผาเท่านั้น

(ใบปะหน้าี้จะไม่เป็นความลับเมื่อถูกแยกจากเอกสารลับพิเศษ)

(SPECIAL CONTROL)



เอกสารลับ

(CONFIDENTIAL)

ตราสัญลักษณ์บริษัท

เอกสารปกปะหน้าใช้ปิดทับเอกสารลับ

การเปิดเผยเอกสารลับนี้ ส่งผลกระทบต่อการประกอบธุรกิจและความก้าวหน้าขององค์กร อาจถูกฟ้องร้องเรียกค่าเสียหาย เกิดความเสียหายต่อภาพพจน์ในระดับประเทศ

หน้าที่ความรับผิดชอบของผู้ครอบครอง

1. ผู้ถือครองมีหน้าที่รับผิดชอบความปลอดภัยของเอกสารลับนี้
2. มีการป้องกันที่จำเป็นเพื่อไม่ให้เอกสารถูกเปิดเผยโดยไม่ได้รับอนุญาต โดยการไม่ทิ้งเอกสารไว้ลำพัง ยกเว้นเมื่อเก็บรักษาในสถานที่ปลอดภัย
3. การเปิดเผยเอกสารจะให้เฉพาะผู้ที่มีสิทธิรับรู้เท่านั้น

การเก็บ

เมื่อไม่มีการใช้งานจากเอกสารให้ใส่ในหีบห่อหรือแฟ้มเอกสารระบุด้านหน้าว่า “**CONFIDENTIAL (เอกสารลับ)**” และให้เก็บไว้ในตู้เอกสารที่ปิดล็อกด้วยกุญแจที่มั่นคงที่ตั้งไว้ในพื้นที่ที่มีการควบคุม การเข้า-ออก เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

การทำสำเนา

เอกสารลับห้ามทำสำเนา แยกชิ้น หรือทำขึ้นมาใหม่ โดยไม่ได้รับอนุญาต

การทำลาย

ห้ามทิ้งถังขยะ ให้ทำลายโดยเครื่องทำลายเอกสารเท่านั้น

(ใบปะหน้านี้จะไม่เป็นความลับเมื่อถูกแยกจากเอกสารลับ)

เอกสารลับ

(CONFIDENTIAL)



เอกสารใช้ภายในเท่านั้น

(INTERNAL USE ONLY)

ตราสัญลักษณ์บริษัท

เอกสารปกปะหน้าใช้ปิดทับเอกสารใช้ภายในเท่านั้น

การเปิดเผยเอกสารใช้ภายในเท่านั้น ส่งผลกระทบต่อการทำงานประจำวัน 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 2 : ตัวอย่างการใช้กระดาษระดับความลับของข้อมูล

ตราสัญลักษณ์ บริษัท	เอกสารลับพิเศษ / SPECIAL CONTROL
เอกสารลับพิเศษ	
เอกสารลับพิเศษ / SPECIAL CONTROL	Page 1 of



ตราสัญลักษณ์
บริษัท

เอกสารลับ / **CONFIDENTIAL**

เอกสารลับ

เอกสารลับ / **CONFIDENTIAL**

Page 1 of



ตราสัญลักษณ์
บริษัท

ใช้ภายในเท่านั้น/ (Internal Use Only)

ใช้ภายในเท่านั้น

ใช้ภายในเท่านั้น/ (Internal Use Only)

Page 1 of



ตราสัญลักษณ์
บริษัท

เปิดเผย / PUBLIC

เปิดเผย

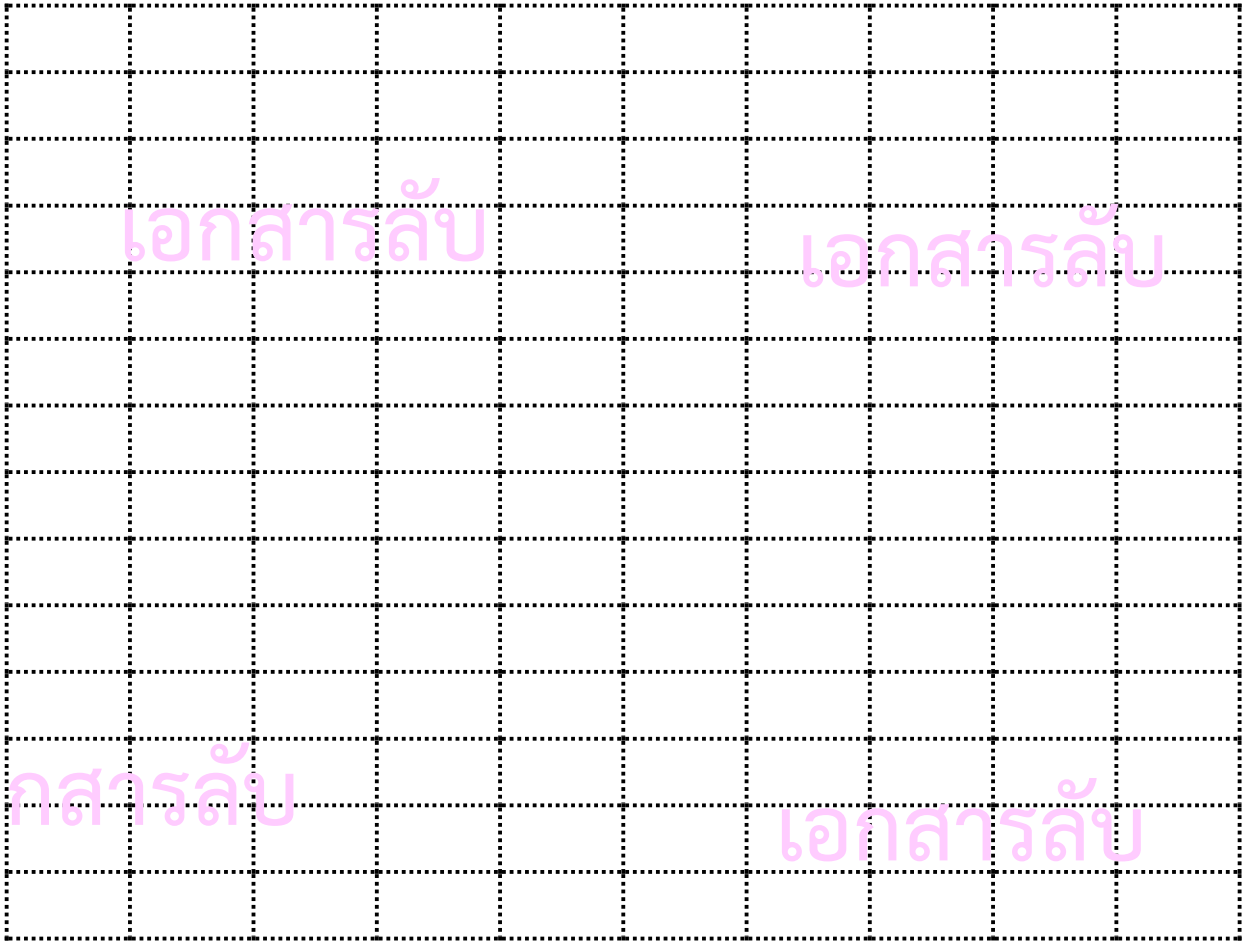
เปิดเผย / PUBLIC

Page 1 of



ตราสัญลักษณ์บริษัท

เอกสารลับ / CONFIDENTIAL



เอกสารลับ / CONFIDENTIAL

