นโยบายและแนวปฏิบัติ

ด้านการบริหารจัดการข้อมูลสารสนเทศ

กลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน)

นโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูลสารสนเทศ
กลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน)

1. ความสำคัญ

ข้อมูลสารสนเทศถือเป็นสินทรัพย์ที่มีค่าของกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน)จึงต้องมีการกำกับดูแลข้อมูล สารสนเทศอย่างเป็นระบบและมีประสิทธิภาพ มีความน่าเชื่อถือถูกต้องสมบูรณ์ซึ่งเป็นการป้องกัน ความเสี่ยงจากความเสียหาย ปกป้องทรัพย์สินของกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) และช่วยลดการสูญหายของ ข้อมูล ส่งผลให้การตัดสินใจทางธุรกิจมีประสิทธิภาพรวมถึงเพิ่มขีดความสามารถทางการแข่งขัน

2. ขอบเขตนโยบาย

นโยบายและแนวปฏิบัตินี้ใช้บังคับกับกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) ต่อไปนี้เรียกว่า “กลุ่มบริษัทฯ” หมายถึง บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) และบริษัทย่อยในกลุ่มบริษัททุกบริษัท ส่วน “บริษัท” ที่จะกล่าวถึงในเอกสารฉบับนี้ให้หมายถึง บริษัทหนึ่งๆ ที่นำเอาเอกสารฉบับนี้ไปบังคับใช้ ทั้งนี้จะมีการทบทวนโยบายฉบับนี้ อย่างน้อยปีละหนึ่งครั้ง หรือกรณีมีเหตุอันสมควร

3. วัตถุประสงค์

เพื่อให้บุคลากรเข้าใจบทบาทหน้าที่และร่วมกันปกป้องข้อมูลสารสนเทศของกลุ่ม บริษัท พรีเมียร์ ควอลิตี้สตาร์ช จำกัด (มหาชน) มิให้รั่วไหลหรือนำข้อมูลไปใช้ในทางที่ผิด

4. หน้าที่และความรับผิดชอบ

สำหรับบุคลากรใช้เป็นแนวทางในการประสานงานภายในบริษัท

4.1 **คณะกรรมการบริษัท**

4.1.1 กำหนดให้มีนโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูลสารสนเทศ

4.1.2 กำกับดูแลให้มีการนำนโยบายและแนวปฏิบัติไปปฏิบัติอย่างเป็นรูปธรรม

4.2 **ผู้บริหาร**

4.2.1 จัดให้มีระเบียบปฏิบัติให้เหมาะสมกับบริบทของแต่ละบริษัท โดยให้สอดคล้องกับ บริบทของบริษัท และข้อกำหนดกฎหมายของแต่ละประเทศที่บริษัทดำเนินธุรกิจ

4.2.2 จัดให้มีโครงสร้างผู้รับผิดชอบ เช่น หน่วยงาน หรือบุคคลผู้รับผิดชอบเพื่อดูแล ข้อมูลและระบบสารสนเทศ

4.2.3 กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ

4.2.4 มั่นใจว่ามีการบริหารความเสี่ยงจากการใช้ข้อมูลสารสนเทศ

4.2.5 มั่นใจว่ามีการรายงานผลการปฏิบัติงานตามนโยบายฯ รวมถึงรายงานปัญหาจาก การใช้ข้อมูลสารสนเทศ

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 ควบคุมการเข้าถึงระบบข้อมูลสารสนเทศและกลุ่มบริษัทข่าย

4.4.3 รักษาความปลอดภัยของข้อมูลสารสนเทศ

4.4.4 จัดให้มีการเก็บสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง

4.5 **หน่วยงานตรวจสอบภายใน**

4.5.1 ตรวจสอบให้มีการบริหารจัดการข้อมูลสารสนเทศตามนโยบายฯ

4.5.2 ให้คำแนะนำแนะนำและให้ความรู้แก่บุคลากรเพื่อให้เกิดการปฏิบัติตามนโยบายฯ

4.6 **พนักงาน**

4.6.1 รักษาความลับและปกป้องความปลอดภัยของข้อมูลส่วนตัว รวมทั้งข้อมูล สารสนเทศของกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) ลูกค้าและคู่ค้าธุรกิจและพันธมิตรทางธุรกิจ

4.6.2 จัดทำข้อมูลสารสนเทศ บันทึกและรายงานให้มีความถูกต้อง น่าเชื่อถือ

4.6.3 ปกป้องทรัพย์สินทางปัญญาของกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) และไม่ละเมิดสิทธิใน ทรัพย์สินทางปัญญาของผู้อื่น

4.6.4 ปฏิบัติตามนโยบายฯ กฎหมาย และมาตรฐานสากลที่เกี่ยวข้องกับการบริหาร จัดการข้อมูลสารสนเทศ

5. แนวปฏิบัติ

5.1 ให้ปฏิบัติตามแนวทางตามมาตรฐานสากลเกี่ยวกับการใช้เทคโนโลยีสารสนเทศซึ่ง ประกอบด้วยหลัก 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 เพื่อผลประโยชน์ทางการตลาดหรือ นำไปสร้างฐานข้อมูลประวัติลูกค้าขึ้นมาใหม่แล้วนำไปขายให้กับบริษัทอื่น
3) เก็บรักษาชื่อบัญชีผู้ใช้งาน (account) และรหัสผ่าน (password) ที่เกี่ยวข้อง กับระบบข้อมูลสารสนเทศกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) ไว้เป็นส่วนตัวและสร้างให้เป็น เอกลักษณ์
4) ไม่จด password ไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น ที่ไม่ได้รับอนุญาต และง่ายต่อการถอดรหัสผ่าน
5) กรณีที่มีความจำเป็นต้องบอก password แก่ผู้อื่นเพื่อเข้าดำเนินการในระบบ ข้อมูลสารสนเทศ หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านทันที

5.1.2. ความถูกต้องของข้อมูล (Information Accuracy)

1) การจัดทำข้อมูลสารสนเทศให้มีความถูกต้องและน่าเชื่อถือนั้น ข้อมูลควรได้รับ การตรวจสอบความถูกต้องก่อนที่จะนำเข้าฐานข้อมูล รวมถึงการปรับปรุง ข้อมูลให้มีความทันสมัยอยู่เสมอ
2) แหล่งที่มาของข้อมูลต้องมีความน่าเชื่อถือและตรวจสอบได้เช่น หน่วยงาน ภาครัฐ องค์กรอื่นที่เชื่อถือได้ เป็นต้น

5.1.3 ความเป็นเจ้าของ (Information Property)

1) กลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) เป็นเจ้าของในทรัพย์สินทางปัญญาที่บุคลากรได้พัฒนา หรือสร้างขึ้นไม่ว่าจะทั้งหมดหรือบางส่วน
2) ไม่ละเมิดหรือเปิดเผยโดยไม่ได้รับอนุญาตในทรัพย์สินทางปัญญาและลิขสิทธิ์ ของงานที่ทำร่วมกัน
3) ไม่ใช้งาน ทำซ้ำตีพิมพ์หรือเผยแพร่รูปภาพ บทความ หนังสือ หรือเอกสาร ใดๆ ที่เป็นการละเมิด ลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบ เทคโนโลยีสารสนเทศของกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน)
4) ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ตซึ่งรวมถึง การอัพเดทโปรแกรมต่างๆ ซอฟต์แวร์ที่ใช้ในระบบข้อมูลสารสนเทศของกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) ไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น
5) ปกป้องทรัพย์สินทางปัญญาของกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) โดยไม่เปิดเผยก่อนได้รับ อนุญาต
6) ปกป้องทรัพย์สินทางปัญญาโดยไม่ใช้ผิดวิธีหรือผิดกฎหมาย และเมื่อใช้ ต้องแน่ใจว่าได้ประทับตราหรือแสดงเครื่องหมายการค้า หรือเครื่องหมายบริการ หรือสัญลักษณ์ลิขสิทธิ์ เช่น การใช้ ®, ™, © (20xx) เป็นต้น
7) แจ้งให้กลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) ทราบถึงการค้นพบ การประดิษฐ์ เช่น โปรแกรม คอมพิวเตอร์ สิ่งประดิษฐ์ทางเทคโนโลยีและผลงานนวัตกรรม รวมไปถึงข้อมูล จำเพาะ
8) ให้ความช่วยเหลือกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) เพื่อให้ได้มาซึ่งสิทธิบัตร ลิขสิทธิ์ หรือ ปกป้องเครื่องหมายการค้าที่เป็นทรัพย์สินทางปัญญาของกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน)

5.1.4 การเข้าถึงข้อมูล (Data Accessibility)

1) การใช้งานระบบสารสนเทศ เช่น ระบบคอมพิวเตอร์ แอปพลิเคชัน อีเมล ระบบกลุ่มบริษัทข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น ผู้บริหารต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศก่อนเข้าใช้ ระบบฯ ของผู้ใช้งานให้เหมาะสมกับงานและหน้าที่ความรับผิดชอบ
2) ผู้บริหารทบทวนสิทธิการเข้าถึงข้อมูลและระบบฯ ปีละหนึ่งครั้งหรือเมื่อต้อง เปลี่ยนสิทธิของผู้ใช้งาน เช่น การเลื่อนตำแหน่ง โดยผู้บริหารต้องอนุมัติเลื่อน ขั้นในระบบฯ
3) ผู้รับมอบอำนาจจากผู้บริหารเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ การเข้าถึงข้อมูลและระบบฯ
4) บันทึกรายละเอียดการเข้าถึงข้อมูลและระบบฯ รวมถึงการแก้ไขเปลี่ยนแปลง สิทธิต่างๆ ทั้งของผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานใน การตรวจสอบหากมีปัญหาเกิดขึ้น
5) บันทึกและติดตามการใช้งานระบบฯ และเฝ้าระวังการละเมิดความปลอดภัย ที่มีต่อข้อมูลและระบบฯ ที่สำคัญ

5.2 การบริหารจัดการความเสี่ยง

5.2.1 ระบุและประเมินความเสี่ยง

5.2.2 จัดลำดับความสำคัญของความเสี่ยงและบริหารความเสี่ยงสำคัญที่ต้องดำเนินการ ก่อน

5.2.3 กำหนดมาตรการจัดการความเสี่ยงและดำเนินการตามมาตรการ

5.3 การบริหารจัดการข้อมูลสารสนเทศ

5.3.1 การจัดระดับความลับข้อมูลสารสนเทศ (Classification of Information) โดย พิจารณาจากระดับความเสี่ยงต่อความมั่นคงปลอดภัย ผลกระทบต่อมูลค่า ผลกระทบต่อความเสียหายทางทรัพย์สินและภาพพจน์บริษัทโดยแบ่งตามประเภท ดังต่อไปนี้

1) เอกสารลับพิเศษ (Special Control) [สีม่วง] เป็นข้อมูลสารสนเทศที่ส่งผล กระทบต่อการดำเนินยุทธศาสตร์ทางธุรกิจและก่อให้เกิดความเสียเปรียบใน การแข่งขันเชิงธุรกิจอย่างร้ายแรง ถ้าเกิดการรั่วไหลของข้อมูลออกมาจะ ก่อให้เกิดความเสียหายต่อภาพพจน์ของบริษัทในระดับสากล เช่น

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

2) **เอกสารลับ (Confidential)** [สีแดง] เป็นข้อมูลสารสนเทศที่ส่งผลกระทบต่อ การดำเนินธุรกิจและความก้าวหน้าของธุรกิจ องค์กรอาจถูกฟ้องร้องเรียก ค่าเสียหาย ถ้าเกิดการรั่วไหลของข้อมูลและก่อให้เกิดความเสียหายต่อภาพพจน์ บริษัทในระดับประเทศ เช่น

- เอกสารทางการตลาด (ที่ยังไม่เปิดเผยต่อสาธารณะ)
- ข้อมูลส่วนบุคคล
- ข้อมูลลูกค้า

3) **เอกสารใช้ภายในเท่านั้น (Internal Use Only)** [สีเหลือง] เป็นข้อมูล สารสนเทศที่อนุญาตให้ใช้ภายในบริษัทในกลุ่มบริษัทฯ เท่านั้น ส่งผลกระทบต่อ การปฏิบัติงานประจำวันและอาจทำให้เกิดความเสียหายต่อภาพพจน์ เช่น

- ประกาศภายใน/นโยบายต่างๆ
- ระเบียบ/คู่มือปฏิบัติงาน
- บันทึกการปฏิบัติงานประจำวัน

4) **เอกสารเปิดเผย (Public)** [สีเขียว] เป็นข้อมูลสารสนเทศที่พิจารณาแล้วเห็นว่า ไม่มีผลกระทบต่อองค์กร สามารถเปิดเผยต่อบุคคลภายนอกได้ เช่น

- ข้อมูลด้านความยั่งยืน
- ข้อมูลประชาสัมพันธ์
- โปรโมชั่นทางการค้าต่างๆ

ทั้งนี้ เอกสารหรือสิ่งตีพิมพ์ไม่ว่าจะทั้งหมดหรือบางส่วนที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับ ซึ่งมีการกำหนดชั้นความลับไว้ ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับ

5.3.2 การจัดเก็บข้อมูลสารสนเทศและอุปกรณ์

1) ผู้บริหารและผู้รับผิดชอบดูแลข้อมูลสารสนเทศเป็นผู้กำหนดระยะเวลาจัดเก็บ ข้อมูลสารสนเทศตามระดับความลับ
2) จัดเก็บข้อมูลสำรองในสื่อบันทึกข้อมูลและจัดทำรายการบันทึกให้สามารถแสดง ถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรอง ข้อมูลไว้อย่างชัดเจน
3) รักษาความปลอดภัยของระบบสารสนเทศและอุปกรณ์ซึ่งบรรจุข้อมูล สารสนเทศของบริษัท เช่น โทรศัพท์มือถือ แล็ปท็อป แท็บเล็ต เป็นต้น และต้อง ระมัดระวังเป็นพิเศษในการใช้งานอุปกรณ์ดังกล่าวนอกสถานประกอบการ รวมทั้งจัดเก็บไว้ในที่ที่มีกุญแจล็อคหลังการใช้งาน

4) ตั้งรหัสผ่าน (password) ล็อคหน้าจอซึ่งบรรจุข้อมูลสารสนเทศของกลุ่มบริษัท เมื่อต้องการออกจากระบบสารสนเทศหรือเสร็จสิ้นงาน
5) รายงานฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อข้อมูลสารสนเทศหรืออุปกรณ์ซึ่ง บรรจุข้อมูลสารสนเทศของกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) สูญหายหรือถูกขโมย

5.3.3 การนำอุปกรณ์ส่วนตัวมาใช้ในสถานประกอบการ

อุปกรณ์สื่อสารไร้สายเป็นสิ่งสำคัญต่อการสื่อสารทางธุรกิจและช่วยเพิ่มประสิทธิผลการทำงาน นอกจากนี้การใช้อุปกรณ์สื่อสารไร้สายของพนักงานที่เพิ่มขึ้นทำให้ต้องมีการขออนุญาตเชื่อมต่อกับกลุ่มบริษัทข่ายของบริษัท การอนุมัติการใช้อุปกรณ์ส่วนตัวและแอปพลิเคชั่นให้เป็นไปตามแต่ละบริษัทกำหนด

บุคลากรที่ใช้อุปกรณ์สื่อสารไร้สายส่วนตัวต้องปฏิบัติ ดังต่อไปนี้

1) งานที่ได้พัฒนาขึ้นบนอุปกรณ์ส่วนตัวถือเป็นทรัพย์สินทางปัญญาของ กลุ่มบริษัท
2) อุปกรณ์สื่อสารไร้สายส่วนตัวให้ฝ่ายเทคโนโลยีสารสนเทศตั้งค่าระบบและติดตั้งโปรแกรมพื้นฐานก่อนการเข้าถึงกลุ่มบริษัทข่าย
3) อุปกรณ์สื่อสารไร้สายจะต้องตั้งรหัสผ่านสำหรับการเข้าถึงข้อมูล ของ กลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) เพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต และ จะต้องไม่วางทิ้งไว้ในที่สาธารณะ
4) ต้องสำรองข้อมูลที่เกี่ยวข้องกับกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) เป็นประจำเพื่อป้องกัน การสูญหาย
5) แจ้งให้บริษัทใน กลุ่มบริษัทฯ ทราบในกรณีที่อุปกรณ์ที่เก็บข้อมูลของ กลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) สูญหายหรือถูกขโมย
6) รับผิดชอบค่าใช้จ่ายใดๆ ที่เกี่ยวข้องกับอุปกรณ์ส่วนตัว
7) รับผิดชอบต่อความเสี่ยงที่ข้อมูลส่วนตัวหรือข้อมูลของกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) บน อุปกรณ์ส่วนตัวจะสูญหายอันเกิดจากความล้มเหลวของระบบปฏิบัติการ ไวรัส โปรแกรมประสงค์ร้าย (malware) หรือข้อผิดพลาดใด ๆ ของซอฟต์แวร์และ ตัวอุปกรณ์
8) ส่งคืนหรือทำลายข้อมูลของกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) ที่อยู่ในอุปกรณ์สื่อสาร ไร้สายส่วนตัวเมื่อสิ้นสุดการเป็นพนักงาน
9) กลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) สงวนสิทธิ์ในการตัดสัญญาณการเชื่อมต่อกลุ่มบริษัทข่ายหรือ งดให้บริการโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

5.3.4 การสำรองข้อมูล

1) จัดให้มีขั้นตอนการปฏิบัติการเก็บสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศโดยจัดทำเป็นลายลักษณ์ อักษร
2) สำรองข้อมูลในระบบข้อมูลสารสนเทศและ Hard Drives ของบริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) มาไว้ที่สื่อบันทึกข้อมูล เช่น Cloud Storage , NAS Storage
3) ดูแลรักษาสื่อบันทึกข้อมูลโดยการสำรองข้อมูลลงในสื่อบันทึกข้อมูลใหม่และ ทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมออย่างน้อยปี ละหนึ่งครั้ง เพื่อป้องกันการเสื่อมสภาพ รวมทั้งมีวิธีการนำข้อมูลกลับมาใช้งานใหม่

5.3.5 สร้างรหัสลับ (Encryption) เมื่อส่งข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษระหว่างหน่วยงาน/บริษัท

5.4 การแลกเปลี่ยนข้อมูลสารสนเทศกับบุคคลภายนอก

5.4.1. ในกรณีที่จำเป็นต้องให้ข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษแก่บุคคลภายนอกหรือบุคคลที่ไม่ได้รับอนุญาตต้องได้รับการตรวจสอบความถูกต้อง ของข้อมูลจากผู้รับผิดชอบดูแลข้อมูลสารสนเทศและต้องได้รับอนุญาตจากผู้บริหาร รวมทั้งบุคคลภายนอกจะต้องลงนามในข้อตกลงห้ามเปิดเผยข้อมูล (Non Disclosure Agreement หรือ NDA)

5.4.2. สร้างรหัสลับ (Encryption) เมื่อส่งข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษให้กับบุคคลภายนอก

5.5 การใช้อินเทอร์เน็ต

5.5.1. ไม่ใช้อินเทอร์เน็ตของบริษัทในเวลาทำงานเพื่อใช้ดำเนินธุรกิจส่วนตัวซึ่งไม่เกี่ยวกับงานของกลุ่มบริษัท

5.5.2. ไม่ใช้อินเทอร์เน็ตในทางที่ละเมิดกฎหมายลิขสิทธิ์เช่น การดาวน์โหลดโปรแกรม ไฟล์เพลง ไฟล์ภาพยนตร์ รูปภาพหรือข้อความของบุคคลอื่นบนเว็บไซต์โดยไม่ได้ รับอนุญาตและนำไปใช้เพื่อแสวงหาผลประโยชน์โดยไม่ได้รับอนุญาตจากเจ้าของ

5.5.3. ไม่ใช้อินเทอร์เน็ตเพื่อกระทำการใดๆ ซึ่งขัดต่อจรรยาบรรณธุรกิจของกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน)

5.5.4. ไม่ใช้อินเทอร์เน็ตของกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน) ซึ่งทำให้การใช้งานอินเทอร์เน็ตของ บุคคลอื่นช้าลง เช่น ดาวน์โหลดไฟล์จำนวนมากเกินไป

5.6 การใช้อีเมล

5.6.1. ห้ามส่งอีเมลแก่บุคคลอื่นโดยปลอมแปลงแหล่งที่มาของการส่งอีเมล อันเป็น การรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น

5.6.2. ห้ามส่งอีเมลที่มีข้อความหรือรูปภาพ ซึ่งก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ มีเนื้อหาผิดกฎหมาย สร้างความอับอาย คุกคาม ก้าวร้าว สร้างความเกลียดชังหรือสนับสนุนให้มีการกระทำผิดกฎหมาย

5.6.3. ระมัดระวังเมื่อจำเป็นต้องเปิดอีเมลจากผู้ส่งที่ไม่รู้จักซึ่งอาจพบโปรแกรมประสงค์ ร้าย (malware) การหลอกเก็บข้อมูลที่มาจากอีเมลหลอกลวง (phishing) รวมถึงระมัดระวังอีเมลจากผู้ที่ไม่รู้จักและแจ้งฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อพบอีเมล ที่ต้องสงสัย

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)

โปรดดูรายละเอียดในนโยบายและแนวทางปฏิบัติในการใช้สื่อสังคมออนไลน์ของกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน)

5.8 การทำลายข้อมูลสารสนเทศ

5.8.1. ข้อมูลสารสนเทศที่จัดพิมพ์เป็นเอกสารในรูปแบบกระดาษหรือวัตถุใดๆ ซึ่งอยู่ใน ระดับเอกสารใช้ภายในเท่านั้น เอกสารลับและเอกสารลับพิเศษ เมื่อไม่ต้องการแล้ว ให้ทำลายโดยเครื่องทำลายเอกสารเท่านั้น ส่วนเอกสารเปิดเผยให้ทิ้งลงถังขยะหรือเครื่องทำลายเอกสาร

5.8.2. ย้ายข้อมูลสารสนเทศที่สำคัญแล้วจึงลบข้อมูลสารสนเทศเป็นการถาวรก่อนทำลาย สื่อบันทึก

5.8.3. ข้อมูลการบันทึกการประชุมในรูปแบบอิเลคทรอนิคส์ให้เก็บไว้เป็นเวลา 1 ปี โดยต้องมีการบันทึกรายงานการประชุมและได้รับการรับรองรายงานแล้ว หากไม่มีการบันทึกรายงานการประชุม ให้เก็บไว้เป็นระยะเวลา 2 ปี

5.8.4. เทปเสียงบันทึกการประชุม ให้ทำลายทิ้ง ภายหลังการถอดเสียงเป็นรายงานการประชุมและได้รับการรับรองรายงานแล้ว

5.9 การตรวจสอบการรั่วไหลของข้อมูลสารสนเทศ

ในกรณีที่เกิดการรั่วไหลของข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษ ผู้บริหารที่ รับผิดชอบต้องแต่งตั้งคณะกรรมการสอบสวนเพื่อสอบสวนและตรวจสอบหาสาเหตุ ความผิดพลาด พร้อมทั้งปรับปรุงวิธีจัดเก็บข้อมูลสารสนเทศไม่ให้รั่วไหลและระบบ การป้องกันการรั่วไหลของข้อมูลสารสนเทศ ตลอดจนรายงานให้ผู้บริหารรับทราบ

6. การฝึกอบรม

จัดให้มีการสื่อสารและถ่ายทอดนโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูลสารสนเทศ ผ่านการฝึกอบรม การประชุม หรือกิจกรรมในรูปแบบต่าง ๆ ให้แก่กรรมการ ผู้บริหารและพนักงานและ ให้มีการประเมินประสิทธิผลอย่างต่อเนื่อง

7. การแจ้งเบาะแส

ร้องเรียนหรือแจ้งเบาะแสเมื่อพบเห็นการกระทำที่เชื่อได้ว่าเป็นการละเมิดนโยบายและ แนวปฏิบัตินี้ โดยขั้นตอนให้เป็นไปตามนโยบายและแนวปฏิบัติเกี่ยวกับการแจ้งเบาะแส ทั้งนี้ผู้ร้องเรียน หรือผู้แจ้งเบาะแสจะได้รับความคุ้มครองและข้อมูลจะถูกเก็บเป็นความลับ โดยไม่มีผลต่อตำแหน่งงาน ทั้งในระหว่างดำเนินการสอบสวนและหลังเสร็จสิ้นกระบวนการ

8. การขอคำแนะนำแนะนำ

ในกรณีที่มีข้อสงสัยว่าการกระทำนั้นอาจฝ่าฝืนกฎหมาย ระเบียบ นโยบายและแนวปฏิบัติด้าน การบริหารจัดการข้อมูลสารสนเทศสามารถขอคำแนะนำแนะนำจากผู้บังคับบัญชา หน่วยงานหรือบุคคลผู้รับผิดชอบด้านการบริหารจัดการข้อมูลสารสนเทศ ด้านกำกับการปฏิบัติตามกฎเกณฑ์หรือด้าน กฎหมายก่อนตัดสินใจหรือดำเนินการใด ๆ

9. บทลงโทษ

ในกรณีที่เกิดการสอบสวน พนักงานทุกคนต้องให้ความร่วมมือกับหน่วยงานภายในและภายนอก อย่างเต็มที่ ทั้งนี้หากผู้บริหารและพนักงานกระทำการใด ๆ ที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามนโยบาย ฉบับนี้ไม่ว่าทางตรงหรือทางอ้อม ผู้บริหารและพนักงานจะถูกพิจารณาโทษทางวินัยตามระเบียบ ข้อบังคับการทำงาน

10. กฎหมาย กฎระเบียบและนโยบายที่เกี่ยวข้อง

10.1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

10.2. พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537

10.3. นโยบายและแนวทางปฏิบัติในการใช้สื่อสังคมออนไลน์ของบริษัทในกลุ่ม บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน)

10.4. ISO 27001, ISO 9001

นโยบายฉบับนี้ มีผลบังคับใช้ตั้งแต่วันที่ 15 พฤษภาคม 2567 เป็นต้นไป

ลงชื่อ .....

(นายมนตรี มหาพฤกษ์พงศ์)

ประธานกรรมการบริษัท

บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด (มหาชน)

ภาคผนวก

นิยามชั้นความลับของเอกสาร

เอกสารลับพิเศษ

(Secret)

การเปิดเผยเอกสารลับพิเศษ นี้ จะส่งผลกระทบต่อยุทธศาสตร์การดำเนินธุรกิจของกลุ่มบริษัท และก่อให้เกิดความเสียเปรียบในการแข่งขันเชิงธุรกิจอย่างร้ายแรงทำให้เกิดความเสียหายต่อภาพพจน์ขององค์กร

หน้าที่ความรับผิดชอบของผู้ครอบครอง

1. ผู้ถือครองเอกสาร มีหน้าที่รับผิดชอบความปลอดภัยของเอกสารลับพิเศษ
2. มีการป้องกันที่จำเป็นเพื่อไม่ให้เอกสารถูกเปิดเผยโดยไม่ได้รับอนุญาต โดยการไม่ทิ้งเอกสารไว้ในสถานที่ที่เปิดเผย เข้าถึงได้โดยง่าย ต้องเก็บเอกสารไว้ในสถานที่ที่ปลอดภัย
3. การเปิดเผยเอกสารจะให้ได้เฉพาะผู้ที่มีสิทธิรับรู้เท่านั้น
4. กรณีเป็นเอกสาร Electronic จะต้องมีการตั้งรหัส (Encrypted)

การจัดเก็บเอกสาร

เมื่อไม่มีการใช้งาน ให้เก็บเอกสารไว้ในแฟ้ม ที่การระบุ Secret อย่างชัดเจน และให้จัดเก็บไว้ในตู้นิรภัยที่ตั้งไว้ในพื้นที่ที่มีการควบคุมการเข้า-ออก เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

การทำสำเนา

เอกสารลับพิเศษ ห้ามทำสำเนา แยกชิ้น หรือทำขึ้นใหม่ โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาของผู้รับผิดชอบ

การทำลาย

ห้ามทิ้งถังขยะ ให้ทำลายโดยเครื่องทำลายเอกสารเท่านั้น

เอกสารลับ

(Confidential)

การเปิดเผยเอกสารลับ จะส่งผลกระทบต่อการประกอบธุรกิจและความก้าวหน้าขององค์กร อาจทำให้บริษัทถูกฟ้องร้องเรียกค่าเสียหาย เกิดความเสียหายต่อภาพพจน์ ในระดับหนึ่ง

หน้าที่ความรับผิดชอบของผู้ครอบครอง

1. ผู้ถือครองมีหน้าที่รับผิดชอบความปลอดภัยของเอกสารฉบับนี้
2. มีการป้องกันที่จำเป็น เพื่อไม่ให้เอกสารถูกเปิดเผยโดยไม่รับอนุญาต โดยการไม่ทิ้งเอกสารไว้ลำพัง และมีการเก็บรักษาเอกสารไว้ในที่ปลอดภัย
3. การเปิดเผยเอกสารจะให้เฉพาะผู้มีสิทธิรับรู้เท่านั้น

การเก็บ

เมื่อไม่มีการใช้งานจากเอกสารให้ใส่ในแฟ้ม ที่มีตราประทับ Confidential หรือ เอกสารลับ อย่าง ชัดเจน และให้เก็บไว้ในตู้เอกสารที่ปิดล็อคด้วยกุญแจและตั้งอยู่ในพื้นที่ที่มีการควบคุมการเข้า-ออก เฉพาะผู้ได้รับอนุญาตเท่านั้น

การทำสำเนา

เอกสารลับเฉพาะนี้ ห้ามทำสำเนา แยกชิ้น หรือทำขึ้นใหม่ โดยไม่ได้รับอนุญาต

การทำลาย

ห้ามทิ้งขยะ ให้ทำลายโดยเครื่องทำลายเอกสารเท่านั้น

เอกสารใช้ภายในเท่านั้น

Internal Use Only

การเปิดเผย เอกสารใช้ภายในเท่านั้น ส่งผลกระทบต่อการปฏิบัติงานประจำวัน อาจทำให้เกิดความเสียหายต่อภาพพจน์ เป็นข้อมูลอนุญาตเพื่อใช้งานภายในเท่านั้น

<u>หน้าที่ความรับผิดชอบของผู้ครอบครอง</u>

1. ผู้ถือครองมีหน้าที่รับผิดชอบการถือครองเอกสาร
2. มีการป้องกันที่จำเป็น เพื่อไม่ให้เอกสารถูกเปิดเผยโดยไม่รับอนุญาต โดยการไม่ทิ้งเอกสารไว้ลำพัง และมีการเก็บรักษาเอกสารไว้ในที่ปลอดภัย
3. การเปิดเผยเอกสารจะให้เฉพาะผู้มีสิทธิรับรู้ตามหน้าที่ความรับผิดชอบเท่านั้น

<u>การเก็บ</u>

เมื่อไม่มีการใช้เงินเอกสารแล้ว ให้เก็บเข้าแฟ้มเอกสาร เข้าตู้เอกสารที่มีการระบุ Internal Use Only หรือ เอกสารใช้งานภายในเท่านั้น และเก็บปิดล็อกด้วยกุญแจ

<u>การทำสำเนา</u>

ใช้งานภายในเท่านั้น สามารถทำสำเนา แยกชิ้น หรือทำขึ้นใหม่ โดยได้รับอนุมัติจากผู้มีหน้าที่รับผิดชอบในเนื้อหาของเอกสารนั้นๆ เท่านั้น

<u>การทำลาย</u>

ให้ทำลายโดยเครื่องทำลายเอกสารเท่านั้น