

นโยบายการจัดลำดับชั้นข้อมูลของบริษัท

เนื่องด้วยพนักงานที่ปฏิบัติงานให้กับ บริษัท ฟรอนท์ไลน์ เอ็นจิเนียริง จำกัด (“บริษัท”) ทุกคนต้องมีความรับผิดชอบในการปกป้อง ดูแลข้อมูลสำคัญของบริษัทให้มีความถูกต้อง เป็นความลับ มีความสมบูรณ์ของข้อมูลสำคัญของบริษัท ดังนั้น พนักงานของบริษัทจึงมีหน้าที่รับผิดชอบต่อการควบคุมข้อมูลสำคัญของบริษัท มิให้รั่วไหลจากการเข้าถึง นำออก รวมไปถึงการนำเข้าสู่ข้อมูลไปเผยแพร่ให้เป็นไปตามนโยบายที่กำหนด และสอดคล้องกับการธุรกิจของกลุ่มบริษัท

โดยข้อมูลสำคัญที่เป็นทรัพย์สินของบริษัท แบ่งออกเป็น 3 ประเภทดังต่อไปนี้

1. ข้อมูลสาธารณะ (Public)
2. ข้อมูลที่เป็นงานเฉพาะภายในบริษัทเท่านั้น (Official User Only)
3. ข้อมูลที่เป็นความลับ (Confidential)

การจำแนกประเภทเอกสาร

1. ข้อมูลสาธารณะ (Public)

“ข้อมูลสาธารณะ (Public)” จัดเป็นข้อมูลที่เปิดเผยให้บุคคลทั่วไปสามารถเข้าถึงได้ โดยไม่มีข้อจำกัดทางด้านนโยบายของกลุ่มบริษัท หรือข้อจำกัดทางด้านกฎหมายเกี่ยวกับการเข้าถึงหรือการใช้งานข้อมูลดังกล่าว โดยตัวอย่างของข้อมูลสาธารณะ เช่น ข้อมูลแถลงข่าวที่เผยแพร่ต่อสาธารณะชน ข้อมูลแผนที่ขององค์กร ข้อมูลที่ปรากฏในข่าว หนังสือพิมพ์และนิตยสารต่าง ๆ เป็นต้น

2. ข้อมูลใช้งานเฉพาะภายในบริษัทเท่านั้น (Official User Only)

ข้อมูลที่ต้องได้รับความคุ้มครองอันเนื่องจากข้อกฎหมาย ข้อบังคับ กรรมสิทธิ จริยธรรม หรือสิทธิส่วนบุคคลและต้องได้รับการป้องกันการเข้าถึง แก้ไข เปลี่ยนแปลงหรือส่งออก การจัดเก็บ รวมถึงการนำไปใช้งานอื่น ๆ โดยผู้ที่มิได้รับอนุญาต

“ข้อมูลที่ใช้ภายในเฉพาะภายในบริษัทเท่านั้น (Official User Only)” หรือข้อมูล เป็นข้อมูลที่ถูกจำกัดเฉพาะพนักงานบริษัทที่ได้รับสิทธิในการเข้าถึงข้อมูลดังกล่าวเท่านั้น เช่น ข้อมูลพนักงาน ข้อมูลลูกค้าหรือผู้สนับสนุนที่ไม่มีข้อมูลความลับ เป็นต้น โดยข้อมูลที่ถูกจัดอยู่ในประเภท “ข้อมูลที่ใช้ภายในเฉพาะภายในบริษัทเท่านั้น (Official User Only)” จะต้องมีการควบคุมข้อมูล ดังต่อไปนี้

- ในกรณีที่ข้อมูลที่เป็นเอกสาร สำเนา ข้อมูลจะต้องเก็บในพื้นที่ ที่มีการควบคุมทางกายภาพเพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต ที่เหมาะสม เพียงพอต่อการรักษาข้อมูลความลับ เช่น เก็บในตู้เอกสารที่มีฉนวนกันความร้อน เป็นต้น โดยข้อมูลจะต้องถูกเข้าถึงหรือนำไปใช้ได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- ในกรณีที่เก็บข้อมูลในรูปแบบอิเล็กทรอนิกส์ จะถูกจัดเก็บไว้ใน Share Drive ของบริษัท โดยจำแนกตามแผนก และจำกัดสิทธิ์การเข้าถึงข้อมูลของแต่ละระดับ และเก็บไว้บนเซิร์ฟเวอร์ที่มีการป้องกันการโจมตี เพื่อป้องกันการถูกลักลอบเข้าถึงและการเปิดเผยข้อมูลโดยที่ไม่ได้รับอนุญาต
- ข้อมูลจะต้องไม่ถูกเปิดเผยออกสู่สาธารณะก่อนได้รับอนุญาตจากผู้บริหารระดับสูง คณะผู้บริหาร และ/หรือ ตามอำนาจดำเนินการของบริษัท
- พนักงานจะต้องป้องกันไม่ให้เอกสารเสียหายหรือสูญหาย
- ห้ามทำการโพสต์ข้อมูลบนเว็บไซต์ หรือส่งออกผ่านไปยังระบบเครือข่ายสาธารณะใด ๆ ก่อนได้รับอนุญาตจากผู้บริหารระดับสูง
- กรณีที่ยกเลิกใช้ข้อมูล หรือจำเป็นที่จะต้อง ลบ ทำลายทิ้ง สามารถดำเนินการโดยวิธีดังนี้
 - (1) กรณีเป็นเอกสารที่เป็นกระดาษ สำเนาต่าง ๆ ต้องถูกทำลายจากการย่อยหรือกระบวนการทำลายที่ไม่สามารถฟื้นฟูกลับไปได้หลังจากผ่านกระบวนการทำลายเรียบร้อยแล้วอาจทิ้งร่วมกับขยะปกติ
 - (2) กรณีเป็นข้อมูลอิเล็กทรอนิกส์ จะต้องแจ้งความประสงค์ต่อแผนกเทคโนโลยีดิจิทัล (DIT) เพื่อดำเนินการโดยวิธี ทำลายให้อุปกรณ์บันทึกข้อมูลเกิดความเสียหายทางกายภาพจนไม่สามารถกู้คืนข้อมูลได้ เช่น ฮาร์ดดิสก์ ทำลายโดยการทำให้แผ่นจานแม่เหล็กแตกออกหรือหักออกจากสภาพปกติ, โซลิตสเตตไดรฟ์ ทำลายโดยการทำให้ชิปหน่วยความจำแตกออกหรือหักออกจากสภาพปกติ

3. ข้อมูลที่เป็นความลับ (Confidential)

“ข้อมูลที่เป็นความลับ (Confidential)” เป็นข้อมูลที่มีความคุ้มครองทางกฎหมาย ระเบียบ นโยบายของบริษัท ข้อมูลความลับทางธุรกิจ หรือสัญญาต่างๆ ข้อมูลประเภทนี้อาจถูกเปิดเผยไปยังบุคคลจำเป็นที่จะต้องรู้ หรือเกี่ยวข้องเฉพาะกลุ่มเท่านั้น การเปิดเผยข้อมูลประเภทดังกล่าวแก่บุคคลหรือเผยแพร่สู่สาธารณะจะต้องได้รับอนุญาตจากผู้บริหารระดับสูง หรือคณะผู้บริหารระดับสูงเท่านั้น ตัวอย่างของข้อมูลที่เป็นความลับ เช่นข้อมูลที่เป็นประวัติพนักงาน ข้อมูลเงินเดือน หมายเลขบัญชีพนักงาน ข้อมูลทางการเงินของบริษัท หรือข้อมูลใด ๆ ที่ทางกฎหมายถือว่าเป็นข้อมูลลับ เป็นต้น โดยข้อมูลที่ถูกจัดอยู่ในประเภท “ข้อมูลที่เป็นความลับ (Confidential)” จะต้องมีการควบคุมข้อมูลดังต่อไปนี้

- ในกรณีที่เก็บข้อมูลในรูปแบบอิเล็กทรอนิกส์ จะถูกจัดเก็บไว้ใน Share Drive ของบริษัท โดยจำแนกตามแผนก และจำกัดสิทธิ์การเข้าถึงข้อมูลของแต่ละระดับ และเก็บไว้ในเซิร์ฟเวอร์ที่มีการป้องกันการโจมตี เพื่อป้องกันการถูกลักลอบเข้าถึงและการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
- ข้อมูลจะต้องไม่ถูกเปิดเผยก่อนได้รับอนุญาตจากผู้บริหารระดับสูงหรือคณะผู้บริหารระดับสูง
- ในกรณีที่ข้อมูลเป็นเอกสาร สำเนา ข้อมูลจะต้องเก็บในพื้นที่ที่เหมาะสม มีการควบคุมทางกายภาพ เพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาตเพียงพอต่อการรักษาข้อมูลความลับ เช่น เก็บในตู้เอกสารที่มีดิดล็อก มีกุญแจล็อก มีเจ้าหน้าที่รักษาความปลอดภัย เป็นต้น โดยข้อมูลจะต้องเข้าถึงหรือนำไปใช้ได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- ห้ามทำการโพสต์ข้อมูลบนเว็บไซต์ หรือส่งออกผ่านไปยังระบบเครือข่ายสาธารณะใด ๆ ก่อนได้รับอนุญาตจากผู้บริหารระดับสูง
- กรณีที่เลิกใช้ข้อมูล หรือจำเป็นที่จะต้อง ลบ ทำลายทิ้ง สามารถดำเนินการโดยวิธีดังนี้
 - (1) กรณีเป็นเอกสารที่เป็นกระดาษ สำเนาต่าง ๆ ต้องถูกทำลายจากการย่อยหรือกระบวนการทำลายที่สามารถฟื้นฟูนำกลับมาใช้ได้ อีก หลังจากกระบวนการทำลายเรียบร้อยแล้วอาจทิ้งรวมกับขยะปกติ
 - (2) กรณีเป็นข้อมูลอิเล็กทรอนิกส์ จะต้องแจ้งความประสงค์ต่อฝ่ายเทคโนโลยีดิจิทัล(DIT) เพื่อดำเนินการโดยใช้วิธีทำลายให้อุปกรณ์บันทึกข้อมูลเกิดความเสียหายทางกายภาพจนไม่สามารถกู้คืนข้อมูลได้ เช่น ฮาร์ดดิสก์ ทำลาย โดยการทำให้แผ่นจานแม่เหล็กแตกออกหรือหักออกจากสภาพปกติ, โซลิดสเตตไดรฟ์ ทำลายโดยการทำให้ชิปหน่วยความจำแตกออก หรือหักออกจากสภาพปกติ

ในกรณีที่มีการรั่วไหลของข้อมูลที่เป็นความลับสำคัญของบริษัท หรือถูกเปิดเผยออกไปสู่ที่สาธารณะหรือบุคคลที่ไม่เกี่ยวข้อง โดยไม่ได้รับอนุญาต พนักงานหรือหน่วยงานเจ้าของข้อมูลจะต้องแจ้งต่อแผนกเทคโนโลยีดิจิทัล (DIT) เพื่อทำการตรวจสอบและปรับปรุงแนวทางในการป้องกันที่เหมาะสม หรือ หากมีการรั่วไหลของข้อมูลเกิดขึ้นและเป็นข้อมูลส่วนบุคคลให้อ้างอิงตามนโยบายและระเบียบปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของบริษัทต่อไป

บทลงโทษ

กรรมการ ผู้บริหาร และพนักงานที่ฝ่าฝืนการปฏิบัติตามนโยบายฉบับนี้จะถูกลงโทษทางวินัยตามกฎหมายข้อบังคับของบริษัท และอาจมีความผิด ตามกฎหมาย หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง

นโยบายการจัดลำดับชั้นข้อมูลของบริษัทนี้ มีผลบังคับใช้ตั้งแต่วันที่ 24 กุมภาพันธ์ 2568 เป็นต้นไป



(นายปัญญา บุญญาภิวัฒน์)
ประธานกรรมการบริษัท