Universal Utilities
GROUP

นโยบายธรรมาภิบาลข้อมูล
บริษัท ยูนิเวอร์แซล ยูทีลิตี้ส์ จำกัด (มหาชน) พ.ศ.2566

บริษัท ยูนิเวอร์แซล ยูทีลิตี้ส์ จำกัด (มหาชน) ให้ความสำคัญของการป้องกันรักษา ความปลอดภัยของข้อมูล รวมถึงวิธีการปฏิบัติในการรักษาความลับ การรักษาความน่าเชื่อถือ และความพร้อมใช้ของข้อมูล บริษัทจึงได้กำหนดนโยบายธรรมาภิบาลข้อมูล โดยมีวัตถุประสงค์ดังนี้

1. เพื่อเป็นแนวทางการปฏิบัติงานของพนักงานบริษัท ตลอดจนบุคคลที่เกี่ยวข้อง ให้ปฏิบัติตามนโยบายธรรมภิบาลข้อมูลได้อย่างถูกต้อง และสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง อาทิ กฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กฎหมายบริษัทมหาชนจำกัด และกฎหมายอื่นๆ ที่เกี่ยวข้อง เป็นต้น ตลอดจนหลักการกำกับดูแลกิจการที่ดี และจรรยาบรรณทางธุรกิจของกลุ่มบริษัท
2. เพื่อสร้างมาตรฐานวิธีการจัดเก็บ การทำลาย การจำแนกประเภทเอกสาร การใช้ข้อมูล การขอข้อมูล และการส่งต่อข้อมูล
3. เพื่อสื่อสารให้พนักงานรับทราบถึงนโยบายธรรมาภิบาลข้อมูลและการเผยแพร่บนเว็บไซต์บริษัทให้บุคคลภายนอกที่เกี่ยวข้องรับทราบด้วย

คำนิยาม

บริษัท หมายถึง บริษัท ยูนิเวอร์แซล ยูทีลิตี้ส์ จำกัด (มหาชน)

พนักงาน หมายถึง พนักงานประจำ พนักงานทดลองงาน พนักงานสัญญาจ้าง พนักงานชั่วคราว

ข้อมูล หมายถึง สิ่งที่สื่อความหมายไม่ว่าจะจัดทำไว้ในรูปของเอกสาร ข้อมูลอิเล็กทรอนิกส์ หรือรูปแบบอื่นใด ซึ่งอยู่ภายใต้การครอบครองของบริษัท

ข้อมูลลับ หมายถึง ข้อมูลซึ่งหากเปิดเผยทั้งหมดหรือบางส่วนจะก่อให้เกิดผลกระทบทางผลประโยชน์ด้านการค้า ความน่าเชื่อถือ หรือผลกระทบด้านอื่นๆ ของบริษัท

ข้อมูลปกปิด หมายถึง ข้อมูลที่ทราบได้เฉพาะกลุ่มบุคคลหากเปิดเผยมีผลกระทบต่อการบริหารจัดการภายในบริษัท

ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม รวมไปถึง ข้อมูลส่วนบุคคลของคู่ค้า ลูกค้า ผู้ใช้น้ำ และข้อมูลส่วนบุคคลที่ได้รับจากอุปกรณ์ที่เข้ามาในเครือข่ายของบริษัทและ/หรือบริษัทย่อย (Log data and device information) แต่ไม่รวมถึงข้อมูลผู้ถึงแก่กรรมโดยเฉพาะ

บริษัท ยูนิเวอร์แซล ยูทีลิตี้ส์ จำกัด (มหาชน)
ชั้น 18 อาคารอีสท์วอเตอร์ เลขที่ 1 ซอยวิภาวดีรังสิต 5
แขวงจอมพล เขตจตุจักร กรุงเทพฯ 10900
โทรศัพท์ +66 2272 1688 โทรสาร +66 2272 1691
www.uu.co.th

ข้อมูลส่วนบุคคลที่อ่อนไหว หมายถึง ข้อมูลที่เป็นเรื่องส่วนบุคคลโดยแท้ของบุคคล แต่มีความละเอียดอ่อนไหวและอาจสุ่มเสี่ยงในการเลือกปฏิบัติอย่างไม่เป็นธรรม เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่กฎหมายกำหนด

ข้อมูลภายใน หมายถึง ข้อมูลที่มีวัตถุประสงค์เพื่อใช้ภายในบริษัท รวมถึงข้อมูลที่มีการเปิดเผยแก่บุคคลเฉพาะ เช่น กรรมการบริษัท พนักงาน คู่ค้า ลูกค้า หน่วยงานราชการ เป็นต้น

ข้อมูลสาธารณะ หมายถึง ข้อมูลที่สาธารณชนสามารถเข้าถึงได้และมีวัตถุประสงค์เพื่อเผยแพร่ข้อมูลสู่ภายนอก ซึ่งในกรณีที่มีการเปิดเผยเอกสารดังกล่าวจะต้องไม่มีผลกระทบใดๆ ต่อบริษัท พนักงาน คู่ค้า ลูกค้า หรือบุคคลใดๆ ทั้งสิ้น เช่น ข่าว สื่อสิ่งพิมพ์ ข้อมูลบนเว็บไซต์ โฆษณาหรือประกาศรับสมัครงานของบริษัท เป็นต้น

การประมวลผล หมายถึง การดำเนินการใดๆ ที่เกี่ยวข้องกับข้อมูล เช่นการเก็บรวบรวม การบันทึก การถือครอง การใช้งาน การจัดการ การปรับเปลี่ยนหรือเปลี่ยนแปลง การเผยแพร่ เป็นต้น

แนวปฏิบัติตามนโยบายธรรมาภิบาลข้อมูล มีดังนี้

1. การจัดเก็บและการทำลายข้อมูล

1.1 ข้อมูลที่เก็บรวบรวมจะต้องเป็นข้อมูลที่มีความจำเป็นต่อการปฏิบัติงาน เป็นข้อมูลที่ถูกต้อง และหากเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของบริษัท

1.2 ให้จำแนกประเภทข้อมูลตามระดับชั้นความลับ ได้แก่ ข้อมูลลับ ข้อมูลปกปิด ข้อมูลส่วนบุคคล ข้อมูลภายใน และข้อมูลสาธารณะ โดยพิจารณาตาม**ภาคผนวก ก.** และจัดเก็บข้อมูลตามระดับชั้นความลับ โดยพิจารณาพื้นที่จัดเก็บให้มีความมั่นคงปลอดภัยที่เหมาะสม คำนึงถึงความเสี่ยงที่ข้อมูลอาจรั่วไหล และความเสี่ยงของอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลอาจเสื่อมสภาพ ทั้งนี้ การจัดเก็บข้อมูลต้องปฏิบัติไม่ต่ำกว่าคำแนะนำที่กำหนดไว้ใน **ภาคผนวก ข.**

1.3 จัดทำทะเบียนข้อมูลของแต่ละหน่วยงาน รวมทั้งพิจารณากำหนดในเรื่องดังต่อไปนี้

(1) กำหนดประเภทข้อมูลตามระดับชั้นความลับ ได้แก่ ข้อมูลลับ ข้อมูลปกปิด ข้อมูลส่วนบุคคล ข้อมูลภายใน และข้อมูลสาธารณะ

(2) กำหนดระยะเวลาในการจัดเก็บข้อมูล โดยพิจารณาตามความจำเป็นในการใช้ข้อมูล ระยะเวลาตามที่กฎหมายกำหนด และการเก็บเพื่อการตรวจสอบทั้งจากหน่วยงานภายในและภายนอก เช่น ฝ่ายกฎหมาย ฝ่ายตรวจสอบ กรมสรรพากร เป็นต้น รวมทั้งกำหนดวิธีการทำลายข้อมูล

(3) กำหนดพนักงานผู้รับผิดชอบในการจัดเก็บข้อมูล

(4) กำหนดสิทธิการเข้าถึง เฉพาะพนักงานที่มีความจำเป็นต้องใช้ข้อมูลในการปฏิบัติหน้าที่ รวมทั้งยกเลิกสิทธิการเข้าถึงโดยทันทีในกรณีที่ไม่มีความจำเป็นในการใช้ข้อมูลแล้ว เช่น พนักงานลาออก หรือมีการโอนย้ายพนักงาน หรือกรณีมีความจำเป็นต้องยกเลิกสิทธิ์เพื่อรักษาความมั่นคงปลอดภัยของข้อมูล

(5) กำหนดผู้มีอำนาจพิจารณาอนุญาตในกรณีมีผู้ร้องขอข้อมูล

ทั้งนี้ แต่ละหน่วยงานต้องทบทวนทะเบียนข้อมูลอย่างน้อยปีละ 1 ครั้ง

1.4 กรณีที่ครบกำหนดระยะเวลาการจัดเก็บข้อมูล ให้ทำลายข้อมูลตามที่กำหนดไว้ในภาคผนวก ข.

2. การใช้ข้อมูล

2.1 พนักงานจะต้องไม่ใช้ข้อมูลไปในทางที่อาจก่อให้เกิดความเสียหายต่อบริษัท

2.2 พนักงานจะต้องใช้ข้อมูลเพื่อการปฏิบัติงานเท่านั้น ห้ามใช้ข้อมูลเพื่อวัตถุประสงค์อื่นโดยเด็ดขาด

2.3 ข้อมูลส่วนบุคคลจะต้องใช้ตามวัตถุประสงค์ที่กำหนดไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) เท่านั้น จะนำไปใช้เพื่อวัตถุประสงค์อื่นไม่ได้ ทั้งนี้ หากมีความจำเป็นต้องใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่กำหนดไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ให้ขอคำแนะนำจากฝ่ายกฎหมาย หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพื่อปฏิบัติให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3. การให้ข้อมูล การส่งต่อข้อมูล และการเปิดเผยข้อมูล

3.1 ห้ามส่งต่อหรือเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าจะอยู่ในรูปแบบใดก็ตาม

3.2 พนักงานจะต้องไม่ส่งต่อหรือเปิดเผยข้อมูลลับ ข้อมูลปกปิด ข้อมูลส่วนบุคคล ข้อมูลภายใน เว้นแต่กรณีมีความจำเป็น เช่น เพื่อใช้ในการปฏิบัติงาน หรือเพื่อปฏิบัติตามกฎหมาย เป็นต้น

3.3 ในการส่งต่อหรือเปิดเผยข้อมูลลับ ข้อมูลปกปิด ข้อมูลส่วนบุคคล ข้อมูลภายใน หรือข้อมูลสาธารณะ ให้ปฏิบัติตาม**ภาคผนวก ค.**

3.4 การให้ข้อมูลข่าวสารต่อสาธารณชน จะต้องได้รับความเห็นชอบจากกรรมการผู้จัดการหรือผู้ที่ได้รับมอบหมายจากกรรมการผู้จัดการให้เป็นผู้ให้ข้อมูลข่าวสาร

4. หน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูล

4.1 พนักงานจะต้องป้องกันมิให้ข้อมูลต่างๆ เกิดความเสียหาย สูญหาย เปลี่ยนแปลง และ/หรือการแก้ไข รวมทั้งการเข้าถึง หรือเผยแพร่โดยมิได้รับอนุญาต

4.2 พนักงานจะต้องช่วยกันสอดส่องถึงความผิดปกติใดๆ ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล และรายงานต่อผู้บังคับบัญชาทันทีที่ทราบถึงความผิดปกติดังกล่าว

4.3 ในกรณีที่พบเหตุการรั่วไหลของข้อมูล หรือพบเหตุอื่นใดเกี่ยวกับข้อมูลที่อาจก่อให้เกิดความเสียหายต่อบริษัท ให้รายงานต่อผู้บังคับบัญชาทันทีที่พบเหตุดังกล่าว เพื่อดำเนินการแก้ไขทันที

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ 20 มิถุนายน 2566

ประกาศ ณ วันที่ 20 มิถุนายน 2566

(นางสาวสุณีวรรณ สุดสวัสดิ์วรกุล)
รักษาการกรรมการผู้จัดการ

ภาคผนวก ก. : แนวทางการจำแนกประเภทข้อมูลตามระดับชั้นความลับ

ระดับชั้นความลับของข้อมูล				
ข้อมูลลับ	**ข้อมูลปกปิด**	**ข้อมูลส่วนบุคคล**	**ข้อมูลภายใน**	**ข้อมูลสาธารณะ**
ข้อมูลซึ่งหากเปิดเผยทั้งหมดหรือบางส่วน จะก่อให้เกิดผลกระทบทางผลประโยชน์ทางการค้า ความน่าเชื่อถือ หรือผลกระทบด้านอื่นๆ ของบริษัท โดยจะต้องรักษาความปลอดภัยที่เข้มงวดและจำกัดการเข้าถึง เช่น งบการเงินที่ยังไม่เปิดเผย สัญญา แผนกลยุทธ์ ข้อมูล R&D ขั้นตอนการผลิตที่เป็นกรรมสิทธิ์ของบริษัท เทคโนโลยี ข้อมูลเกี่ยวกับการประมูล และข้อมูลความลับทางการค้าใดๆ ที่เกี่ยวข้องกับธุรกิจบริษัท และข้อมูลอื่นๆ ที่สามารถก่อให้เกิดผลกระทบต่อผลประโยชน์ทางการค้าหรือความน่าเชื่อถือของบริษัท เป็นต้น	**ข้อมูลที่ทราบได้เฉพาะกลุ่มบุคคลซึ่งหากเปิดเผยจะส่งผลกระทบต่อการบริหารจัดการภายในบริษัท โดยจะต้องรักษาความปลอดภัยที่เข้มงวด และจำกัดการเข้าถึง** เช่น ระเบียบวาระการประชุมที่เป็นเรื่องปกปิด เช่น การแต่งตั้งกรรมการ การปรับเงินเดือนพนักงาน การประเมินผลการปฏิบัติงานของกรรมการผู้จัดการ เป็นต้น	**ข้อมูลที่สามารถระบุตัวตนของบุคคลได้ ซึ่งหากมีการนำไปเผยแพร่หรือนำไปใช้โดยไม่ได้รับอนุญาตอาจก่อให้เกิดผลกระทบหรือความเสียหายต่อบริษัทตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งนี้ ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม โดยจะต้องรักษาความปลอดภัยที่เข้มงวด และจำกัดการเข้าถึง** เช่น ชื่อ-นามสกุล ข้อมูลการติดต่อ วันเกิด รูปถ่าย สัญชาติ ศาสนา ของกรรมการ ผู้ถือหุ้น ลูกค้า คู่ค้าซึ่งเป็นบุคคลธรรมดา ผู้แทนนิติบุคคลของคู่ค้า ลูกจ้างของคู่ค้า ผู้เช่า ลูกจ้างของผู้เช่า ผู้มาติดต่อ ผู้ใช้บริการอาคารหรือพื้นที่ปฏิบัติการ หรือพนักงาน เป็นต้น	**ข้อมูลที่มีวัตถุประสงค์เพื่อใช้ภายในบริษัท รวมถึงข้อมูลที่มีการเปิดเผยแก่บุคคลเฉพาะกลุ่ม เช่น กรรมการ พนักงาน คู่ค้า ลูกค้า หน่วยงานราชการ เป็นต้น โดยมีการรักษาความปลอดภัยและจำกัดการเข้าถึงตามความเหมาะสม หากมีการนำไปเผยแพร่อาจก่อให้เกิดผลกระทบต่อบริษัท** เช่น ข้อบังคับเกี่ยวกับการทำงาน เอกสารการอบรม สิทธิประโยชน์ประกันภัยกลุ่ม การนำส่งภาษีเงินได้บุคคลธรรมดา กองทุนสำรองเลี้ยงชีพ เอกสารที่ใช้ในการติดต่อหน่วยงานราชการ เป็นต้น	**ข้อมูลที่สาธารณชนสามารถเข้าถึงได้และมีวัตถุประสงค์เพื่อเผยแพร่สู่ภายนอก เช่น** ข้อมูลบนเว็บไซต์ของบริษัท เป็นต้น

ภาคผนวก ข. : แนวทางการจัดเก็บ รักษา และทำลายข้อมูล

1. ข้อมูลรูปแบบเอกสาร (Hard Copy) (ต้นฉบับและสำเนา)

การจัดการข้อมูล	ระดับชั้นความลับของข้อมูล				
	ข้อมูลลับ	ข้อมูลปกปิด	ข้อมูลส่วนบุคคล	ข้อมูลภายใน	ข้อมูลสาธารณะ
การจัดเก็บข้อมูลเอกสาร Hard Copy	1.ควรจัดเก็บในพื้นที่ที่เหมาะสมในตู้ที่มีกุญแจล็อค 2.ในกรณีที่มีการจัดเก็บภายนอกบริษัท จะต้องบรรจุในบรรจุภัณฑ์ที่มิดชิด	1.ควรจัดเก็บในพื้นที่ที่เหมาะสมในตู้ที่มีกุญแจล็อค 2.ในกรณีที่มีการจัดเก็บภายนอกบริษัท จะต้องบรรจุในบรรจุภัณฑ์ที่มิดชิด	1. ควรจัดเก็บในพื้นที่ที่เหมาะสมในตู้ที่มีกุญแจล็อค 2. ในกรณีที่มีการจัดเก็บภายนอกบริษัท จะต้องบรรจุในบรรจุภัณฑ์ที่มิดชิด	1.ควรจัดเก็บในพื้นที่ที่เหมาะสม 2.ในกรณีที่มีการจัดเก็บภายนอกบริษัท จะต้องบรรจุในบรรจุภัณฑ์ที่มิดชิด	พิจารณาตามความเหมาะสม
การทำสำเนาข้อมูลเอกสาร Hard Copy	ต้องได้รับอนุญาตจากผู้มีอำนาจอนุญาตตามข้อ 1.3 (5)	ต้องได้รับอนุญาตจากผู้มีอำนาจอนุญาตตามข้อ 1.3 (5)	ต้องได้รับอนุญาตจากผู้มีอำนาจอนุญาตตามข้อ 1.3 (5)	พิจารณาตามความเหมาะสม	พิจารณาตามความเหมาะสม
การทำลายเอกสาร Hard Copy	เมื่อครบระยะเวลาการจัดเก็บข้อมูล ให้ทำลายด้วยเครื่องทำลายเอกสาร	เมื่อครบระยะเวลาการจัดเก็บข้อมูล ให้ทำลายด้วยเครื่องทำลายเอกสาร	เมื่อครบระยะเวลาการจัดเก็บข้อมูล ให้ทำลายด้วยเครื่องทำลายเอกสาร พร้อมทั้งบันทึกรายการเอกสารและวันที่ที่ทำลายเอกสารในรายการประมวลผลข้อมูลส่วนบุคคล (ROPA)	เมื่อครบระยะเวลาการจัดเก็บข้อมูล ให้ทำลายด้วยเครื่องทำลายเอกสาร	เมื่อครบระยะเวลาการจัดเก็บข้อมูลให้ทำลายด้วยเครื่องทำลายเอกสาร

ภาคผนวก ข. : แนวทางการจัดเก็บ รักษา และทำลายข้อมูล

2. ข้อมูลรูปแบบไฟล์อิเล็กทรอนิกส์

การจัดการข้อมูล	ระดับชั้นความลับของข้อมูล				
	ข้อมูลลับ	ข้อมูลปกปิด	ข้อมูลส่วนบุคคล	ข้อมูลภายใน	ข้อมูลสาธารณะ
การจัดเก็บไฟล์อิเล็กทรอนิกส์	1. จัดเก็บในเครื่องคอมพิวเตอร์บริษัท 2. จัดเก็บใน SharePoint หรือระบบที่บริษัทจัดไว้ 3. จัดเก็บไฟล์อิเล็กทรอนิกส์ในอุปกรณ์จัดเก็บ ให้เป็นไปตามหลักปฏิบัติทางด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัท	1. จัดเก็บในเครื่องคอมพิวเตอร์บริษัท 2. จัดเก็บใน SharePoint หรือระบบที่บริษัทจัดไว้ 3. จัดเก็บไฟล์อิเล็กทรอนิกส์ในอุปกรณ์จัดเก็บ ให้เป็นไปตามหลักปฏิบัติทางด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัท	1. จัดเก็บในเครื่องคอมพิวเตอร์บริษัท 2. จัดเก็บใน SharePoint หรือระบบที่บริษัทจัดไว้ 3. จัดเก็บไฟล์อิเล็กทรอนิกส์ในอุปกรณ์จัดเก็บ ให้เป็นไปตามหลักปฏิบัติทางด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัท	1. จัดเก็บในเครื่องคอมพิวเตอร์บริษัท 2. จัดเก็บใน SharePoint หรือระบบที่บริษัทจัดไว้ 3. จัดเก็บไฟล์อิเล็กทรอนิกส์ในอุปกรณ์จัดเก็บ ให้เป็นไปตามหลักปฏิบัติทางด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัท	พิจารณาตามความเหมาะสม
การขอสิทธิ์เข้าถึงแหล่งจัดเก็บไฟล์อิเล็กทรอนิกส์	ต้องได้รับการอนุญาตจากผู้มีอำนาจ อนุญาตตามข้อ 1.3 (5) ทางอีเมล หรือรูปแบบใดรูปแบบหนึ่งที่สามารถยืนยันตัวผู้อนุญาตได้	ต้องได้รับการอนุญาตจากผู้มีอำนาจ อนุญาตตามข้อ 1.3 (5) ทางอีเมล หรือรูปแบบใดรูปแบบหนึ่งที่สามารถยืนยันตัวผู้อนุญาตได้	ต้องได้รับการอนุญาตจากผู้มีอำนาจ อนุญาตตามข้อ 1.3 (5) ทางอีเมล หรือรูปแบบใดรูปแบบหนึ่งที่สามารถยืนยันตัวผู้อนุญาตได้	ต้องได้รับการอนุญาตจากผู้มีอำนาจอนุญาตตามข้อ 1.3 (5) ทางอีเมล หรือรูปแบบใดรูปแบบหนึ่งที่สามารถยืนยันตัวผู้อนุญาตได้	พิจารณาตามความเหมาะสม
การทำสำเนาไฟล์อิเล็กทรอนิกส์	ต้องได้รับการอนุญาตจากผู้มีอำนาจอนุญาตตามข้อ 1.3 (5)	ต้องได้รับการอนุญาตจากผู้มีอำนาจอนุญาตตามข้อ 1.3 (5)	ต้องได้รับการอนุญาตจากผู้มีอำนาจอนุญาตตามข้อ 1.3 (5)	พิจารณาตามความเหมาะสม	พิจารณาตามความเหมาะสม
การลบไฟล์อิเล็กทรอนิกส์รวมถึง อีเมล	ให้ลบแบบถาวร ไม่สามารถกู้คืนได้	ให้ลบแบบถาวร ไม่สามารถกู้คืนได้	ให้ลบแบบถาวร ไม่สามารถกู้คืนได้	พิจารณาตามความเหมาะสม	พิจารณาตามความเหมาะสม

ภาคผนวก ค. : **การขอข้อมูล การส่งต่อข้อมูล และการเปิดเผยข้อมูล** (ข้อมูลในรูปแบบเอกสาร (Hard Copy) และรูปแบบไฟล์อิเล็กทรอนิกส์)

การจัดการข้อมูล	**ระดับชั้นความลับของข้อมูล**				
	ข้อมูลลับ	**ข้อมูลปกปิด**	**ข้อมูลส่วนบุคคล**	**ข้อมูลภายใน**	**ข้อมูลสาธารณะ**
การขอข้อมูล/การส่งต่อข้อมูล/การเปิดเผยข้อมูลต่อบุคคลภายนอก	1. ทำคำขอเป็นลายลักษณ์อักษร เช่น หนังสือ อีเมล เป็นต้น 2. ให้ผู้มีอำนาจอนุญาตตามข้อ 1.3 (5) เป็นผู้พิจารณาอนุญาต โดยคำนึงถึงความจำเป็นในการใช้ข้อมูล และอาจกำหนดเงื่อนไขอื่นๆ เช่น กำหนดวัตถุประสงค์ในการใช้ข้อมูล กำหนดระยะเวลาในการใช้ข้อมูล เป็นต้น 3. กรณีพนักงานเป็นผู้ได้รับข้อมูล จะต้องใช้ข้อมูลตามวัตถุประสงค์ที่ระบุไว้ในคำขอ และจะต้องไม่ส่งต่อหรือเปิดเผยข้อมูลแก่บุคคลอื่น รวมทั้งทำลายข้อมูลทันทีเมื่อไม่มีความจำเป็นต้องใช้ข้อมูลดังกล่าวแล้ว	1. ทำคำขอเป็นลายลักษณ์อักษร เช่น หนังสือ อีเมล เป็นต้น 2. ให้ผู้มีอำนาจอนุญาตตามข้อ 1.3 (5) เป็นผู้พิจารณาอนุญาต โดยคำนึงถึงความจำเป็นในการใช้ข้อมูล และอาจกำหนดเงื่อนไขอื่นๆ เช่น กำหนดวัตถุประสงค์ในการใช้ข้อมูล กำหนดระยะเวลาในการใช้ข้อมูล เป็นต้น 3. กรณีพนักงานเป็นผู้ได้รับข้อมูล จะต้องใช้ข้อมูลตามวัตถุประสงค์ที่ระบุไว้ในคำขอ และจะต้องไม่ส่งต่อหรือเปิดเผยข้อมูลแก่บุคคลอื่น รวมทั้งทำลายข้อมูลทันทีเมื่อไม่มีความจำเป็นต้องใช้ข้อมูลดังกล่าวแล้ว	1. ทำคำขอเป็นลายลักษณ์อักษร เช่น หนังสือ อีเมล เป็นต้น 2. ให้ผู้มีอำนาจอนุญาตตามข้อ 1.3 (5) เป็นผู้พิจารณาอนุญาต โดยคำนึงถึงความจำเป็นในการใช้ข้อมูล และอาจกำหนดเงื่อนไขอื่นๆ เช่น กำหนดวัตถุประสงค์ในการใช้ข้อมูล กำหนดระยะเวลาในการใช้ข้อมูล เป็นต้น 3. กรณีพนักงานเป็นผู้ได้รับข้อมูล จะต้องใช้ข้อมูลตามวัตถุประสงค์ที่ระบุไว้ในคำขอ และจะต้องไม่ส่งต่อหรือเปิดเผยข้อมูลแก่บุคคลอื่น รวมทั้งทำลายข้อมูลทันทีเมื่อไม่มีความจำเป็นต้องใช้ข้อมูลดังกล่าวแล้ว	พิจารณาตามความเหมาะสม	พิจารณาตามความเหมาะสม

การจัดการข้อมูล	ระดับชั้นความลับของข้อมูล				
	ข้อมูลลับ	ข้อมูลปกปิด	ข้อมูลส่วนบุคคล	ข้อมูลภายใน	ข้อมูลสาธารณะ
	4. กรณีบุคคลภายนอกเป็นผู้ได้รับข้อมูลต้องจัดให้มีข้อตกลงในการรักษาข้อมูลเป็นความลับระหว่างบริษัทและบุคคลภายนอก	4. กรณีบุคคลภายนอกเป็นผู้ได้รับข้อมูลต้องจัดให้มีข้อตกลงในการรักษาข้อมูลเป็นความลับระหว่างบริษัทและบุคคลภายนอก	4. กรณีบุคคลภายนอกเป็นผู้ได้รับข้อมูลต้องจัดให้มีข้อตกลงในการรักษาข้อมูลเป็นความลับระหว่างบริษัทและบุคคลภายนอก และข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement : DPA) ด้วย		
การส่งเอกสาร Hard Copy	ผู้ส่งต้องควบคุมดูแลความสำเร็จและครบถ้วนของการจัดส่ง	ผู้ส่งต้องควบคุมดูแลความสำเร็จและครบถ้วนของการจัดส่ง	ผู้ส่งต้องควบคุมดูแลความสำเร็จและครบถ้วนของการจัดส่ง	ผู้ส่งต้องควบคุมดูแลความสำเร็จและครบถ้วนของการจัดส่ง	พิจารณาตามความเหมาะสม
การส่งไฟล์อิเล็กทรอนิกส์ทางระบบอิเล็กทรอนิกส์ เช่น อีเมล เป็นต้น	1. ตั้งรหัสผ่านที่ปลอดภัย โดยรหัสควรมีความยาวอย่างน้อย 8 ตัวอักษร ซึ่งประกอบด้วยอักษรตัวใหญ่ อักษรตัวเล็ก ตัวเลข และสัญลักษณ์ผสมกัน หลีกเลี่ยงวันเดือนปีเกิดและชื่อของตัวเอง 2. รหัสที่ใช้เปิดข้อมูลต้องจัดส่งโดยแยกจากไฟล์ข้อมูลนั้นๆ	พิจารณาตามความเหมาะสม	พิจารณาตามความเหมาะสม	พิจารณาตามความเหมาะสม	พิจารณาตามความเหมาะสม

การจัดการข้อมูล	ระดับชั้นความลับของข้อมูล				
	ข้อมูลลับ	ข้อมูลปกปิด	ข้อมูลส่วนบุคคล	ข้อมูลภายใน	ข้อมูลสาธารณะ
	3. หากส่งให้ผู้รับหลายคนต้องส่งรหัสผ่านแต่ละรายไม่ซ้ำกัน หรืออาจจะใช้วิธีตั้งรหัสผ่านเป็นพวกเดียวกัน แต่เปลี่ยนตัวเลขที่ตามหลังเพื่อแยกความแตกต่าง				