เรื่อง : นโยบายการกำหนดชั้นข้อมูลอันเป็นความลับ

เลขที่เอกสาร : P-COM-024

นโยบายบริษัทเรื่อง นโยบายการกำหนดชั้นข้อมูลอันเป็นความลับ ของบริษัทฉบับนี้ผ่านการอนุมัติ
โดยมติที่ประชุมคณะกรรมการบริษัทให้มีผลบังคับใช้ตั้งแต่วันที่ 1 กรกฎาคม 2568 เป็นต้นไป

สารบัญ

ส่วนที่ เรื่อง หน้าที่

ส่วนที่ 1 วัตถุประสงค์

บริษัทคินคอร์ปอเรชั่นจำกัด(“บริษัท”)จัดทำนโยบายฉบับนี้ขึ้นเพื่อเป็นแนวทางในการบริหารจัดการข้อมูลสารสนเทศขององค์กรอย่างเป็นระบบโดยมีวัตถุประสงค์เพื่อกำหนดหลักเกณฑ์ในการจัดชั้นความลับของข้อมูลและมาตรฐานในการทำลายสื่อบันทึกข้อมูลและข้อมูลบนสื่อบันทึกข้อมูลที่ไม่จำเป็นต้องใช้งานหรือล้าสมัยแล้ว ทั้งนี้เพื่อ

- ลดความเสี่ยงจากการใช้ดุลพินิจส่วนบุคคลในการกำหนดชั้นความลับของข้อมูล
- ป้องกันการเข้าถึงหรือใช้งานข้อมูลโดยไม่ได้รับอนุญาต
- ป้องกันการรั่วไหลของข้อมูลสำคัญสู่บุคคลภายนอก
- ส่งเสริมให้มีระบบการบริหารจัดการและควบคุมการเข้าถึงข้อมูลที่เหมาะสมตามระดับความลับ
- สนับสนุนการดำเนินการตามกฎหมายด้วยมาตรการด้านความปลอดภัยและความรับผิดชอบที่ชัดเจนในการดูแลรักษาและทำลายข้อมูล

ส่วนที่ 2 คำนิยามที่เกี่ยวข้อง

“การกำหนดชั้นความลับของข้อมูล”	หมายถึง การจำแนกชั้นของข้อมูลในบริบทของการรักษาความปลอดภัยข้อมูลตามระดับของความอ่อนไหวและผลกระทบต่อบุคคลและองค์กรหากมีการเปิดเผยเปลี่ยนแปลงหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตโดยการจัดชั้นความลับของข้อมูลช่วยกำหนดการควบคุมความปลอดภัยพื้นฐานที่เหมาะสมสำหรับการปกป้องข้อมูลนั้น ๆ
“ข้อมูลอ่อนไหว”	หมายถึง ข้อมูลอ่อนไหวเป็นข้อมูลที่มีชั้นความลับและเป็นข้อมูลที่ต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาตเพื่อคุ้มครองความเป็นส่วนตัวหรือความปลอดภัยของบุคคลหรือองค์กรและให้หมายรวมถึงข้อมูลส่วนบุคคลชนิดพิเศษตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลด้วย
“ข้อมูลส่วนบุคคล”	หมายถึง ข้อมูลที่เกี่ยวกับบุคคลธรรมดาทำให้สามารถระบุตัวตนของบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ-นามสกุล อีเมล ที่อยู่ เบอร์โทรศัพท์ ที่อยู่จดหมายอิเล็กทรอนิกส์ที่ระบุตัวบุคคลธรรมดา IP Address รูปภาพบุคคล ซึ่งเกี่ยวข้องกับการดำเนินการต่าง ๆ ของบริษัท เช่น ข้อมูลที่เกี่ยวข้องกับการจัดซื้อ จัดจ้าง และบริการอื่น ๆ เป็นต้น

“ข้อมูลอันเป็นความลับ” หมายถึง
ข้อมูลข่าวสารลับที่มีคำสั่งไม่ให้เปิดเผยและอยู่ในความครอบครองหรือควบคุมดูแลของบริษัทซึ่งมีการกำหนดให้มีชั้นความลับตามแนวปฏิบัติฉบับนี้โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานของบริษัทและประโยชน์ของบริษัทประกอบกัน

“ข้อมูลลับ” หมายถึง
ข้อมูลที่ยังมิได้มีการเปิดเผยต่อสาธารณชนหรือผ่านระบบของตลาดหลักทรัพย์เป็นการทั่วไปซึ่งเป็นสาระสำคัญต่อการเปลี่ยนแปลงของราคาหรือมูลค่าของหลักทรัพย์และการตัดสินใจซื้อขายหลักทรัพย์ ตัวอย่างของข้อมูลภายใน ได้แก่
1)ฐานะทางการเงินและผลประกอบการทางการเงิน
2)การจ่ายหรือไม่จ่ายเงินปันผล
3)การเปลี่ยนแปลงมูลค่าที่ตราไว้ของหลักทรัพย์
4)แผนธุรกิจและแผนการระดมทุนการเพิ่ม/ลดทุนโดยใช้เครื่องมือทางการเงินต่าง ๆ
5)การเปลี่ยนแปลงที่สำคัญในแผนการลงทุน หรือโครงการลงทุน
6)การร่วมทุน การควบรวมกิจการ หรือการขายกิจการ
7)การซื้อขายหลักทรัพย์ที่สำคัญ และการไถ่ถอนหลักทรัพย์
8)การได้มา หรือสูญเสียสัญญาทางการค้าที่สำคัญของธุรกิจ
9)ข้อพิพาททางกฎหมายที่สำคัญ
10)การเปลี่ยนแปลงวัตถุประสงค์ของบริษัท
11)การเปลี่ยนแปลงนโยบายการบัญชีที่สำคัญ
12)การเปลี่ยนแปลงอำนาจควบคุมหรือการเปลี่ยนแปลงที่สำคัญในคณะกรรมการบริษัท หรือผู้บริหารระดับสูง

“ข้อมูล” หมายถึง
ข้อมูล ข้อความสารสนเทศคำสั่ง ชุดคำสั่ง
หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์และข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลด้วย

“ข้อมูลสารสนเทศ” หมายถึง
ข้อมูลที่ผ่านการประมวลผลแล้วการจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปตัวเลขข้อความหรือกราฟิกให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผนการตัดสินใจ และ อื่น ๆ ได้ รวมถึงข้อมูลส่วนบุคคล

“ความลับทางการค้า”	หมายถึง ข้อมูลการค้าซึ่งยังไม่รู้จักกันโดยทั่วไปหรือยังเข้าถึงไม่ได้ในหมู่บุคคลซึ่งโดยปกติแล้วต้องเกี่ยวข้องกับข้อมูลดังกล่าวโดยเป็นข้อมูลที่มีประโยชน์ในเชิงพาณิชย์เนื่องจากการเป็นความลับและเป็นข้อมูลที่ผู้ควบคุมความลับทางการค้าได้ใช้มาตรการที่เหมาะสมเพื่อรักษาไว้เป็นความลับ
“ข้อมูลการค้า”	หมายถึง สิ่งที่สื่อความหมายให้รู้ข้อความ เรื่องราวข้อเท็จจริง หรือสิ่งใดไม่ว่าการสื่อความหมายนั้นและผ่านวิธีการใดๆและไม่ว่าจะจัดไว้ในรูปใดๆและให้หมายความรวมถึงสูตรรูปแบบงานที่ได้รวบรวมหรือประกอบขึ้นโปรแกรม วิธีการ เทคนิค หรือกรรมวิธีด้วย (พรบ.ความลับทางการค้า พ.ศ.2545
“การเปิดเผยข้อมูลความลับ”	หมายถึง การเผยแพร่ การขาย การให้เช่าซื้อ การแจกจ่าย การทำซ้ำ การดัดแปลง และการให้เช่าต้นฉบับหรือสำเนางาน ที่เกี่ยวข้องกับ “ข้อมูลอันเป็นความลับ”ไม่ว่าทั้งหมดหรือบางส่วนไม่ว่าจะอยู่ในลักษณะที่อาจก่อให้เกิดความเสียหายแก่ผู้ให้ข้อมูลหรือไม่ก็ตาม
“การปรับชั้นความลับ”	หมายถึง การลดหรือเพิ่มชั้นความลับของข้อมูลข่าวสารลับและให้หมายความรวมถึงการยกเลิกชั้นความลับของข้อมูลข่าวสารลับนั้นด้วย
“การทำลาย”	หมายถึง ระบวนการทำลายข้อมูลในรูปแบบเอกสารไม่ว่าจะเป็นเอกสารกระดาษหรือเอกสารในรูปแบบอิเล็กทรอนิกส์ให้ไม่สามารถอ่านหรือกู้คืนได้อีกเพื่อป้องกันการเข้าถึงการเปิดเผยหรือการนำข้อมูลไปใช้งานโดยไม่ได้รับอนุญาตทั้งนี้รวมถึงการทำลายสื่อบันทึกข้อมูลที่บรรจุเอกสารดังกล่าวด้วย

ส่วนที่ 3 หลักการกำหนดชั้นความลับของข้อมูล

3.1บริษัทใช้ความระมัดระวังในการจำแนกชั้นความลับความสอดคล้องกับความอ่อนไหวและความสำคัญของข้อมูลในการจำกัดการเข้าถึงข้อมูลจะพิจารณาในกรณีที่เป็นการเปิดเผยข้อมูลที่อาจส่งผลกระทบต่อกฎหมาย ชื่อเสียงและผลประโยชน์ของบริษัท

3.2 การกำหนดชั้นความลับของข้อมูลจะพิจารณาตามเนื้อหา และความเสี่ยงที่ส่งผลกระทบทางกฎหมาย ชื่อเสียง และผลประโยชน์ของบริษัท หรือ อื่นๆ ที่เกี่ยวข้องโดยไม่คำนึงถึงรูปแบบหรือแหล่งที่มาของข้อมูลที่มีจัดเก็บไว้ในระบบฐานข้อมูลของบริษัทไม่ว่าเป็นการจัดเก็บในรูปแบบ Hard Copy หรือ Electronic file ก็ตาม

3.3 บริษัทจัดให้มีแนวทางการบริหารความเสี่ยงของข้อมูล ที่ควรได้รับความคุ้มครองตามระดับความอ่อนไหวและความสำคัญของข้อมูลเพื่อกำหนดขอบเขตของมาตรการในการลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้อาทิความรุนแรงและ ความเป็นไปได้ที่ข้อมูลจะถูกรุกล้ำหรือถูกทำลาย หรือระดับความเสียหายที่อาจเกิดขึ้น เป็นต้น

3.4 การกำหนดระดับชั้นของข้อมูลต้องมีความเหมาะสมเพื่อให้ผู้เกี่ยวข้องได้ใช้ประโยชน์จากข้อมูลให้ได้มากที่สุดโดยมีตั้งแต่ระดับต่ำที่สุดไปจนถึงระดับข้อมูลที่สำคัญสูงซึ่งระดับที่สำคัญสูงจะต้องได้รับการปกป้องเพื่อรักษาความปลอภัยของข้อมูล

3.5 ในการบริหารจัดการระบบควบคุมภายในให้เป็นไปอย่างเหมาะสมบริษัทได้กำหนดบทบาทหน้าที่ของผู้มีส่วนเกี่ยวข้องและข้อมูลที่ชัดเจนตลอดจนสร้างความตระหนักรู้ในการบริหารจัดการและมุ่งมั่นในการรักษาความปลอดภัยของข้อมูล

ส่วนที่ 4 ประเภทของชั้นความลับ

1) ชั้นเปิดเผย (Open/Public) หมายถึง	ข้อมูลที่สามารถเปิดเผย หรือเผยแพร่ทั่วไปได้ทั้งภายใน - ภายนอกโดยไม่จำกัดการเข้าถึง
2) ชั้นความลับถูกจำกัด&ชั้นเผยแพร่ภายในองค์กร (Private) หมายถึง	ข้อมูลที่จำกัดการเข้าถึงหรือ ต้องได้รับการอนุญาติจากเจ้าของข้อมูลก่อน มีการเข้ารหัส และแยกอีเมลรหัสกับอีเมลข้อมูล หรือข้อมูลที่ไม่ได้เผยแพร่โดยอิสระ
3) ชั้นความลับที่มีระดับสูง & ข้อมูลอ่อนไหวและมีผลกระทบต่อสิทธิเสรีภาพ หมายถึง	ข้อมูลลับที่มีระดับสูงสุดซึ่งหากเปิดเผยอาจก่อให้เกิดความเสียหายต่อบริษัทได้ต้องมีการจำกัดการเข้าถึงอย่างเข้มงวดต้องได้รับอนุญาตจากเจ้าของข้อมูล มีการเข้ารหัส และแยกอีเมลรหัสกับอีเมลข้อมูล และมีแผนปฏิบัติการฉุกเฉิน รองรับความเสี่ยงเพื่อความปลอดภัยของข้อมูล ซึ่งรวมถึงข้อมูลอ่อนไหว ข้อมูลส่วนบุคคลชนิดพิเศษตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ 5 การปกป้องข้อมูลองค์กรมิให้รั่วไหลโดยแบ่งชั้นข้อมูล (DATA CLASSIFICATION)

หัวข้อ / ลำดับชั้นความลับ	ชั้นความลับที่มีระดับสูง & ข้อมูลอ่อนไหว และมีผลกระทบต่อสิทธิเสรีภาพ	ชั้นถูกจำกัด & ชั้นเผยแพร่ภายในองค์กร (Private)	ชั้นเปิดเผย (Open/Public)
คำอธิบาย	ข้อมูลที่ได้รับความคุ้มครองตามกฎหมายและข้อมูลที่ต้องกำหนดสิทธิ์ในการเข้าถึง หรือข้อมูลที่ถูกจำกัด	ข้อมูลที่ผู้จัดการหน่วยงานไม่มีอำนาจตัดสินใจให้เผยแพร่หรือเปิดเผยต่อสาธารณะหรือข้อมูลที่ได้รับการคุ้มครองตามข้อผูกพันตามสัญญาหรือข้อมูลที่เผยแพร่ภายในองค์กรเท่านั้น	ข้อมูลที่ไม่มีความเป็นส่วนตัวหรือเป็นความลับ
ข้อบังคับทางกฎหมาย	มีกฎหมายกำหนดให้ต้องมีการคุ้มครองข้อมูล	การคุ้มครองข้อมูลในระดับชั้นนี้ ขึ้นอยู่กับดุลยพินิจของผู้จัดการหรือผู้ดูแลข้อมูล	
ความเสี่ยงที่ส่งผลกระทบต่อชื่อเสียง / ผลประโยชน์ของบริษัท	มีความเสี่ยงสูง (High)	ปานกลาง (Medium)	ต่ำ (Low)
การแสดงระดับชั้นความลับข้อมูลสารสนเทศ (Information Labeling)			
เอกสารหรือรายงาน	แสดงชั้นความลับด้วยตัวอักษร ระบุชั้นความลับบน หัวกระดาษของเอกสารหรือ บนเอกสารหากเอกสารดังกล่าวไม่มีหัวกระดาษ		
ภาพเขียน ภาพถ่าย แผนที่ แผนภูมิ	แสดงชั้นความลับด้วยตัวอักษรตามลำดับชั้นความลับ		
การนำเสนอหรือการพูดถึงข้อมูลสารสนเทศที่มีชั้นความลับ	ผู้แสดงหรือผู้พูดจะต้องแจ้งให้ผู้ฟังทราบถึงระดับชั้นความลับของสารสนเทศนั้น ๆ หากแสดงภาพฉายบนจอภาพ ให้แสดงชั้นความลับด้วยอักษรทั้งก่อนและเมื่อเสร็จสิ้นการนำเสนอ		
การจัดการข้อมูลสารสนเทศ			
การทำซ้ำและการสำเนาข้อมูลสารสนเทศ			
จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากระดับผู้บริหาร	✓		
การส่งข้อมูลสารสนเทศ			
การส่งข้อมูลข่าวสารเจ้าหน้าที่ที่ได้รับมอบหมายออกนอกบริเวณบริษัท คิน คอร์ปอเรชั่น จำกัด ต้องบรรจุซองหรือภาชนะหีบห่อทึบแสง 2 ชั้น โดยซองหรือภาชนะชั้นในให้ระบุ ชื่อหรือตำแหน่งผู้รับหน่วยงานผู้ส่ง	✓		

และทำเครื่องหมายแสดงชั้นความลับทั้งด้านหน้าและด้านหลัง ส่วนซองหรือภาชนะชั้นนอกให้ทำเหมือนซองหรือภาชนะชั้นใน แต่ไม่ต้องแสดงชั้นความลับ			
การส่งข้อมูลข่าวสารทางโทรคมนาคม ไปรษณีย์ลงทะเบียน หรือวิธีอื่นต้องได้รับอนุญาตจากระดับผู้บริหารหรือผู้ที่ได้รับมอบหมาย	✓		
การจัดส่งข้อมูลโดยใช้จดหมายอิเล็กทรอนิกส์			✓
ใช้กุญแจเข้ารหัสในการป้องกันข้อมูล เมื่อมีการส่งข้อมูลผ่านระบบเครือข่าย และจดหมายอิเล็กทรอนิกส์	✓	✓	
การควบคุมการเข้าถึงระบบสารสนเทศ	ข้อจำกัดด้านกฎหมายจริยธรรมหรืออื่น ๆทำให้ไม่สามารถเข้าถึงข้อมูลได้โดยไม่ได้รับอนุญาตเป็นการเฉพาะหรือข้อมูลที่สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุมัติการเข้าถึงและลงนามในข้อตกลงว่าจะไม่เปิดเผยข้อมูล	การเข้าถึงได้เฉพาะพนักงานที่มีหน้าที่เกี่ยวข้องเท่านั้น	ไม่มีจำกัดการเข้าถึงข้อมูลสามารถเข้าถึงได้โดยอิสระ
กลไกการรับ-ส่งข้อมูล	ห้ามมิให้ส่งข้อมูลที่เป็นความลับในระดับนี้ผ่านเครือข่ายหลักที่ไม่ใช่ของของบริษัทและ/หรือห้ามส่งผ่านระบบอิเล็กทรอนิกส์ใด ๆ (เช่น อีเมลที่ไม่ใช่ของบริษัท การส่งข้อความโต้ตอบแบบทันที การส่งข้อความตัวอักษร (Line))	ไม่แนะนำให้มีการส่งข้อมูลที่ถูกจำกัดผ่านเครือข่ายไร้สายใดๆหรือเครือข่ายแบบใช้สาย(LAN)ที่ไม่ใช่ของบริษัทหากมีความจำเป็นให้ใช้ VPN ของบริษัทเท่านั้นและ/หรือห้ามส่งผ่านระบบอิเล็กทรอนิกส์ใด ๆ (เช่น อีเมลที่ไม่ใช่ของบริษัท การส่งข้อความโต้ตอบแบบทันทีการส่งข้อความตัวอักษร(Line))ก็ไม่ควรทำเช่นกัน	ไม่จำเป็นต้องมีการป้องกันสำหรับข้อมูลเปิดเผย/สาธารณะ อย่างไรก็ตามควรระมัดระวังในการใช้ข้อมูลทั้งหมดของบริษัทให้เป็นไปอย่างเหมาะสม

หัวข้อ / ลำดับชั้นความลับ	ชั้นความลับที่มีระดับสูง & ข้อมูลอ่อนไหว และมีผลกระทบต่อสิทธิเสรีภาพ	ชั้นถูกจำกัด & ชั้นเผยแพร่ภายในองค์กร (Private)	ชั้นเปิดเผย (Open/Public)
การจัดเก็บข้อมูลสารสนเทศ			
กำหนดรหัสผ่าน (Password) ในการเข้าถึงข้อมูล	✓		
ควบคุมการเข้าถึงข้อมูลตามความเหมาะสม	✓		
การจัดเก็บข้อมูล	- ห้ามจัดเก็บข้อมูลที่เป็นความลับในระดับชั้นนี้ไว้ในเครื่อง/อุปกรณ์คอมพิวเตอร์ที่ไม่ได้รับการอนุญาตจากบริษัท - ต้องมีการเข้ารหัสที่ได้รับการอนุมัติบนอุปกรณ์คอมพิวเตอร์พกพา - มีระบบรักษาความปลอดภัยในการจัดเก็บข้อมูลโดยเฉพาะการรับ – ส่ง ทางอีเมล ทั้งภายใน - ภายนอกต้องได้รับอนุญาตจากเจ้าของข้อมูลมีเข้ารหัสและแยกอีเมล รหัส กับอีเมลข้อมูล	- ให้ปฏิบัติตามแนวปฏิบัติเรื่องการควบคุมการเข้าถึงระบบสารสนเทศ (Access Control) กล่าวคือมีการกำหนดสิทธิเข้าถึงข้อมูลซึ่งจะต้องได้รับการพิจารณาอนุญาตจากผู้มีอำนาจ หรือเจ้าของข้อมูลหรือผู้ดูแลระบบที่ได้รับมอบหมายเป็นลายลักษณ์อักษร - มีระบบรักษาความปลอดภัยในการจัดเก็บข้อมูล - ข้อมูลที่ยังไม่เปิดเผยต่อสาธารณะต้องปฏิบัติตามขั้นตอนการรักษาความปลอดภัยโดยเคร่งครัด	- ไม่จำเป็นต้องมีการป้องกันใด ๆ สำหรับข้อมูลสาธารณะ อย่างไรก็ตาม ควรระมัดระวังในการใช้ข้อมูลทั้งหมดของบริษัทให้เป็นไปอย่างเหมาะสม
การสำรองและการกู้คืนเอกสาร	จำเป็นต้องมีขั้นตอนการปฏิบัติงานในการสำรองและการกู้คืนเอกสาร	ไม่จำเป็นต้องมีขั้นตอนการปฏิบัติงานในการสำรองและการกู้คืนเอกสารแต่ควรระบุวิธีการจัดเก็บเอกสารอย่างเป็นระบบ	
การเก็บรักษาข้อมูลที่เป็นเอกสาร	จำเป็นต้องมีแนวปฏิบัติในการเก็บรักษาข้อมูลที่เป็นเอกสาร		ไม่จำเป็นจำเป็นต้องมีแนวปฏิบัติในการเก็บรักษาข้อมูลที่เป็นเอกสารแต่ควรระบุวิธีการจัดเก็บเอกสารอย่างเป็นระบบ
การควบคุมการเข้าถึงระบบสารสนเทศ			
ระดับผู้บริหาร	✓	✓	✓
ระดับหัวหน้าส่วน /ฝ่ายงาน	✓	✓	✓
ระดับเจ้าหน้าที่ปฏิบัติงาน	-	✓	✓
บุคคลภายนอก	-	-	✓

ระบบควบคุมภายใน	ผู้จัดการ/ผู้ดูแลข้อมูลที่มีหน้าที่รับผิดชอบข้อมูลที่เป็นความลับต้องตรวจสอบและทบทวนระบบและขั้นตอนสำหรับการใช้ข้อมูลในทางที่ผิดและ/หรือการเข้าถึงโดยไม่ได้รับอนุญาต พร้อมรายงานความผิดปกติให้กับเจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศเพื่อวิเคราะห์ หาแนวทางแก้ไขหรือกำหนดแนวทางปฏิบัติด้านความปลอดภัยของหน่วยงาน	ผู้จัดการ/ผู้ดูแลข้อมูลซึ่งรับผิดชอบข้อมูลที่ถูกจำกัดจะต้องตรวจสอบและทบทวนระบบและขั้นตอนของตนเป็นระยะ ๆ สำหรับการใช้ในทางที่ผิดและ/หรือการเข้าถึงโดยไม่ได้รับอนุญาต	ไม่จำเป็นต้องมีการตรวจสอบโดยผู้ควบคุมข้อมูล
การทำลายข้อมูลสารสนเทศ			
ทำลายข้อมูลด้วยวิธีที่ไม่สามารถกู้คืนข้อมูลได้ในภายหลัง	✓	✓	

หัวข้อ / ลำดับชั้นความลับ	ชั้นความลับที่มีระดับสูง & ข้อมูลอ่อนไหว และมีผลกระทบต่อสิทธิเสรีภาพ	ชั้นถูกจำกัด & ชั้นเผยแพร่ภายในองค์กร (Private)	ชั้นเปิดเผย (Open/Public)
ตัวอย่างข้อมูล / *** ข้อมูลที่ได้รับการยกเว้น**	ข้อมูลที่ได้รับการควบคุมตามกฎหมาย และข้อมูลที่จะให้การเข้าถึงข้อมูลลับ หรือข้อมูลที่จำกัด คือทรัพยากรข้อมูลที่สามารถเข้าถึงข้อมูลที่เป็นความลับหรือถูกจำกัด (ชื่อผู้ใช้และรหัสผ่าน) ข้อมูลที่สามารถระบุตัวบุคคลที่เข้าถึงได้ กำหนดสิทธิ์การเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น เช่น - หมายเลขประกันสังคม ใบขับขี่ บัตรประจำตัวประชาชน และหมายเลขหนังสือเดินทาง ฯ - ข้อมูลทางบัญชีการเงิน เช่น เช็คบัญชีออมทรัพย์ หมายเลขบัตรเครดิตหรือบัตรเดบิต ฯ - ข้อมูลสุขภาพ* เช่น สถานะสุขภาพ การรักษาพยาบาล ค่ารักษาพยาบาล - ข้อมูลส่วนบุคคลเฉพาะพนักงาน และ/หรือผู้มีส่วนได้เสีย - การเรียกร้องค่าชดเชยหรือความทุพพลภาพของพนักงาน - ข้อมูลทางธุรกิจ /การเงิน เช่น ข้อมูลสินเชื่อ เป็นต้น	ข้อมูลที่ผู้จัดการตัดสินใจว่าจะไม่เผยแพร่หรือเปิดเผยต่อสาธารณะ และข้อมูลได้รับการคุ้มครองตามข้อผูกพันตามสัญญา คือ ทรัพยากรข้อมูลที่สามารถเข้าถึงข้อมูลที่ถูกจำกัด หรือข้อมูลที่เผยแพร่เฉพาะภายในองค์กร ต้องระบุตัวบุคคลที่เข้าถึงข้อมูลได้โดยการกำหนดสิทธิ์ผู้ใช้/รหัสผ่าน เช่น - ข้อมูลส่วนตัว/พนักงาน เชื้อชาติ เผ่าพันธุ์ สัญชาติ เพศ วันที่และสถานที่เกิด รูปถ่ายติดบัตรพนักงาน - ข้อมูลรายได้และข้อมูลเงินเดือน - ขั้นตอนการปฏิบัติงาน - ข้อมูลติดต่อที่กำหนดโดยเจ้าของข้อมูล - ข้อมูลธุรกิจ/การเงิน เช่น การทำธุรกรรมทางการเงินที่ไม่มีข้อมูลที่เป็นความลับ -ข้อมูลทางธุรกิจที่ครอบคลุมและมีข้อตกลงที่จะต้องไม่เปิดเผยข้อมูล - บันทึกการใช้จ่าย การกู้ยืม มูลค่าสุทธิ	ข้อมูลที่ไม่คาดว่าจะมีความเป็นส่วนตัวหรือเป็นความลับ หรือข้อมูลติดต่อที่ได้รับความยินยอมจากเจ้าของข้อมูลแล้ว /ข้อมูลของบริษัทที่เปิดเผยแล้ว - ชื่อ ที่อยู่ ที่อยู่อีเมล -หมายเลขโทรศัพท์ที่แสดงในบริษัท ปริญญาเกียรตินิยมและรางวัลสถาบันการศึกษา สาขาวิชาที่เรียน - วันที่ทำงาน ตำแหน่งปัจจุบัน ข้อมูลธุรกิจ - แผนที่บริษัท - ประกาศรับสมัครงาน - สิ่งพิมพ์/ประชาสัมพันธ์ของบริษัท

หัวข้อ / ลำดับชั้นความลับ	ชั้นความลับที่มีระดับสูง & ข้อมูลอ่อนไหว และมีผลกระทบต่อสิทธิเสรีภาพ	ชั้นถูกจำกัด & ชั้นเผยแพร่ภายในองค์กร (Private)	ชั้นเปิดเผย (Open/Public)
		- งานวิจัยที่ไม่ได้ตีพิมพ์หรือรายละเอียดงานวิจัย/ผลงาน/นวัตกรรมที่ไม่ใช่ข้อมูลลับ - ข้อมูลส่วนบุคคลที่ได้รับความยินยอมและฐาน ตามกฎหมาย เช่น การจ้างงาน , การประเมินผลงาน ข้อมูลครอบครัว (คู่สมรส คู่ครอง บุตรฯลฯ) ข้อมูลทางการแพทย์ - ข้อมูลผู้บริจาคที่ไม่ระบุชื่อ (และ/หรือชื่อองค์กร ถ้ามี) พร้อมข้อมูลของขวัญประเภทใดก็ได้ (เช่น จำนวนเงินและวัตถุประสงค์ของข้อผูกมัด) ข้อมูลผู้บริจาคอื่น ๆ เช่น นามสกุล ชื่อจริง หรือชื่อย่อ (และ/หรือชื่อองค์กร ถ้ามี) หมายเลขโทรศัพท์/โทรสาร อีเมล และ -ข้อมูลเกี่ยวกับการบริหารจัดการภายในองค์กร - รายละเอียดข้อมูลงบประมาณประจำปี - การเปิดเผยความขัดแย้งทางผลประโยชน์ - ข้อมูลการลงทุนของบริษัท	

หมายเหตุ :
ประเภทข้อมูลได้รับการคุ้มครองตามกฎหมายและหรือได้รับการยกเว้นหรือได้รับความยินยอมเป็นการเฉพาะเพื่อประโยชน์สูงสุดของเจ้าของข้อมูล

ส่วนที่ 6 การทำลายสื่อบันทึกข้อมูลและข้อมูลบนสื่อบันทึกข้อมูล (Disposal of Media Procedure)

6.1ผู้มีหน้าที่รับผิดชอบ

ผู้จัดการฝ่ายเทคโนโลยีสารเสนเทศ

มีหน้าที่รับผิดชอบดูแลระบบสารสนเทศและอุปกรณ์ไอทีทั้งหมดขององค์กรจึงมีอำนาจในการพิจรณาอนุมัติการทำลายสื่อบันทึกข้อมูลที่หมดอายุการใช้งานหรือไม่สามารถนำกับ มาใช่ใหม่ได้ เช่น ฮาร์ดดิสก์ (**HDD USB Drive Server Storage)**รวมถึงการทำลายข้อมูลในระบบต่างๆ ขององค์กร

หน้าที่หลัก

- ตรวจสอบความจำเป็นในการทำลาย
- ประเมินวิธีการทำลายที่เหมาะสม (เช่น Secure Erase, Physical Destruction)
- อนุมัติหรือไม่อนุมัติคำร้องขอทำลาย
- ตรวจสอบให้มั่นใจว่ามีการบันทึกหลักฐานการทำลายอย่างครบถ้วน

ผู้จัดการแผนกหรือเจ้าของข้อมูล (Data Owner / Department Manager)

ในกรณีที่มีข้อมูลหรือสื่อบันทึกข้อมูลเป็นของแผนกอื่น เช่น ฝ่ายบัญชี ฝ่ายบุคคล หรือฝ่ายจัดซื้อหัวหน้าแผนกของข้อมูลนั้นจะต้องร่วมอนุมัติหรือรับทราบการทำลายข้อมูลเพื่อให้มั่นใจว่าไม่มีการทำลายข้อมูลโดยไม่ได้รับอนุญาต

หน้าที่หลัก

- ตรวจสอบความถูกต้องของข้อมูลที่ร้องขอทำลาย
- ประเมินผลกระทบหากข้อมูลถูกทำลาย
- อนุมัติหรือให้ความเห็นชอบร่วมกับฝ่าย IT
- ตรวจสอบให้แน่ใจว่าไม่มีข้อกำหนดทางกฎหมายหรือภาษีที่ต้องเก็บรักษาข้อมูลนั้นไว้

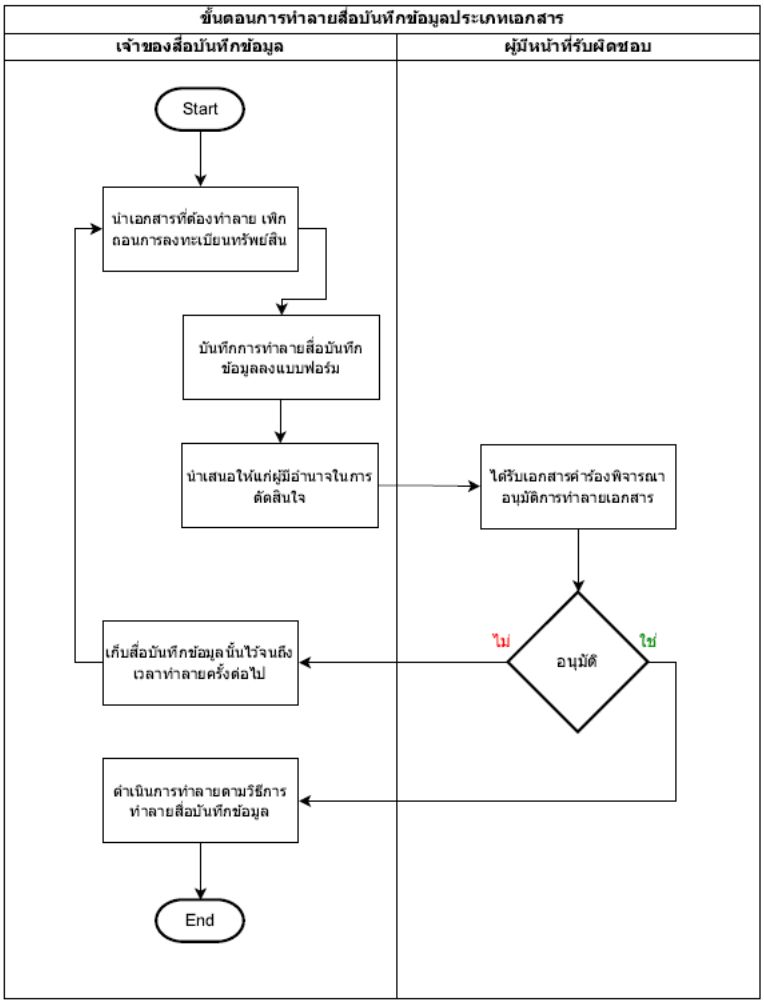
ผู้บริหารระดับสูง หรือกรรมการผู้จัดการ (Managing Director / CEO)

6.2 แนวทางปฏิบัติ

- เจ้าของ/ผู้ใช้/ผู้ดูแลสื่อบันทึกข้อมูล ควรลบหรือทำลายข้อมูล ภายในสื่อบันทึกก่อนที่จะดำเนินการเสนอเรื่องขอทำลายสื่อบันทึกข้อมูลนั้น
- วิธีการทำลายสื่อบันทึกข้อมูลแต่ละประเภท ต้องกำหนดให้เหมาะสม เพื่อป้องกันการกู้คืนข้อมูลกลับมาใช้ใหม่
- วิธีการทำลายสื่อบันทึกข้อมูล ขึ้นอยู่กับระดับความสำคัญของข้อมูลในสื่อบันทึกดังกล่าว โดยอ้างอิงถึงขั้นตอนการกำหนดระดับชั้นความลับ (Information Classification, Labelling and Handling Procedure)

- การลบหรือทำลายสื่อบันทึกข้อมูล จะกระทำได้หลังจากพ้นระยะเวลาจัดเก็บตามที่ระบุไว้ตามขั้นตอนการควบคุมเอกสารและบันทึกการใช้งาน (Record Control Procedure)

6.3 ขั้นตอนปฏิบัติ



6.3.1กระบวนการเริ่มต้น

เมื่อเจ้าของสื่อบันทึกข้อมูลมีความต้องการที่จะทำลายเอกสารหรือสื่อบันทึกข้อมูลที่จะทำลายเอกสารหรือสื่อบันทึกข้อมูลที่ไม่ใช้งานแล้วโดยเริ่มจากการนำเอกสารที่ต้องการทำลายมาเพิกถอนออกจากทะเบียนทรัพย์สินหรือบัญชีรายการที่เกี่ยวข้องเพื่อให้แน่ใจว่าสื่อนั้นไม่อยู่ในระบบการจัดการทรัพย์สินขององค์กรอีกต่อไปหลังจากนั้นเจ้าของข้อมูลจะต้องบันทึกการทำลายสื่อบันทึกข้อมูลลงในแบบฟอร์มที่กำหนด เช่น แบบฟอร์ม Disposal of Media Record เพื่อให้เป็นหลักฐานและรองรับในการดำเนินการตามขั้นตอนถัดไป

เมื่อกรอกเอกสารแบบฟอร์มเรียบร้อยแล้ว ขั้นตอนต่อไปคือการนำเสนอแบบฟอร์มและเอกสารที่เกี่ยวข้องให้กับผู้มีอำนาจในการตัดสินใจซึ่งเป็นชั้นความลับชั้นเปิดผยหรือชั้นที่ถูกจำกัดให้ถูกเผยแพร่ภายในองค์กรจะให้ หัวหน้าแผนกเทคโนโลยีสารสนเทศ ร่วมกับหัวหน้าแผนกเจ้าของข้อมูล

เพื่อพิจารณาเบื้องต้น หรือหากเป็นเอกสารชั้นความลับระดับสูงถึงจะเสนอเรื่องต่อไปยัง ผู้บริหารระดับสูง เพื่อทำการพิจรณาอนุมัติการทำลายเอกสารอย่างเป็นทางการ

หากผู้บริหารพิจารณาแล้ว “อนุมัติ” ให้ดำเนินการทำลาย เจ้าของสื่อบันทึกข้อมูลตามวิธีการที่ได้รับการอนุมัติ โดยวิธีการทำลายต้องเหมาะสม กับประเภทของข้อมูล เช่น การย่อยทำลาย การเผา การฉีก การลบข้อมูลอย่างถาวร เป็นต้น ทั้งนี้เพื่อให้มั่นใจว่าไม่สามารถนำข้อมูลนั้นกลับมาใช้ซ้ำได้อีกและป้องกันการรั่วไหลของข้อมูลสำคัญ

ในกรณีที่ “ไม่ได้รับอนุมัติ” ให้ดำเนินการทำลาย เจ้าของสื่อบันทึกข้อมูลจะต้องเก็บรักษาสื่อหรือเอกสารนั้นไว้ ในพื้นที่ที่ปลอดภัยและเหมาะสมเพื่อรอการพิจารณาใหม่ในรอบการทำลายครั้งถัดไป ทั้งนี้ควรบันทึกสถานะของเอกสารนั้นไว้ในระบบหรือลงในทะเบียนเอกสารอย่างชัดเจน

เมื่อการดำเนินการทำลายเสร็จสิ้นครบถ้วน
กระบวนการทั้งหมดจะสิ้นสุดลงโดยมีการจัดเก็บหลักฐานหรือรายงานการทำลายไว้
เพื่อใช้ในการตรวจสอบย้อนหลัง

6.3.2วิธีการทำลายสื่อบันทึกข้อมูล และข้อมมูลบนสื่อบันทึกข้อมูล สามารถปฏิบัติได้โดยแบ่งตามกรณีและประเภทของสื่อ ดังนี้

- ทรัพย์สินที่พ้นระยะเวลาจัดเก็บ และไม่มีความจำเป็นต้องใช้งานหรือล้าสมัย ให้ดำเนิการทำลายตามประเภทของสื่อบันทึกข้อมูลในตารางที่ 1
- ทรัพย์สินตามสัญญา MA(Maintence Agreement) เช่น เครื่องคอมพิวเตอร์แม่ข่ายอุปกรณ์เครือข่าย สื่อบันทึกข้อมูลต่างๆ วิธีการทำลายแบ่งเป็น 2 กรณี ดังนี้
    - กรณีทรัพย์สินที่นำออก เกิดการชำรุดเสียหาย จนไม่สามารถเปิดอุปกรณ์ขึ้นมาเพื่อทำลายข้อมูลภายในได้ ให้เจ้าหน้าที่ผู้นำออก ลงนามในข้อตกลงการรักษาความลับทางราชการ (Non-Disclosure Agreement) เพื่อป้องกันไม่ให้ข้อมูลที่มีความสำคัญรั่วไหล
    - กรณีทรัพย์สินที่นำออก สามารถเปิดใช้งานได้ปกติให้ดำเนินการทำลายข้อมูลโดยจัดสร้างของดิสก์ใหม่ทั้งหมด (Format แบบ Low Level Format) ตามตารางที่ 1

- ทรัพย์สินที่เปลี่ยนผู้ครอบครอง เช่นการเปลี่ยนตำแหน่งหน้าที่ และนำทรัพย์สินนั้นไปให้ผู้อื่นใช้งานซึ่งมีข้อมูลสำคัญอยู่ภายใน ให้ดำเนิการทำลายข้อมูลโดยจัดสร้างโครงสร้างของดิสก์ใหม่ทั้งหมด (Format แบบ Low Level Format) ตามตารางที่ 1

ประเภทของสื่อบันทึกข้อมูล	การทำลายข้อมูลบนสื่อบันทึกข้อมูล	การทำลายสื่อบันทึกข้อมูล
เอกสารกระดาษ (ด้านระบบ/อุปกรณ์คอมพิวเตอร์)	● ไม่มี	● แยกชิ้นส่วน ● เผา (ถ้าทำได้)
Hard Drives	● ทำการ Format แบบ Low LevelFormat ถ้าหาก Format ไม่ได้ให้นำไปทำลายได้เลย	● แยกชิ้นส่วน ● ทุบทำลาย
USB Removable Media	● ทำการ Format แบบ Low Level Format ถ้าหาก Format ไม่ได้ ให้นำไป ทำลายได้เลย	● แยกชิ้นส่วน ● ทุบทำลาย
เทปแม่เหล็ก เป็นม้วนและคาสเซท	● ลบข้อมูล	● แยกชิ้นส่วน ● ทุบทำลายให้แตกหัก
CD, DVD	● ลบข้อมูล (ถ้าทำได้)	● ใช้วิธีการตัดหรือหักแผ่น ● ทุบทำลายให้แตกหัก
CD/RW และ DVD/RW	● ต้องมีการ Format ก่อนนำไปทำลายถ้าหาก Format ไม่ได้ให้นำไปทำลายได้เลย	● ใช้วิธีการตัดหรือหักแผ่น ● ทุบทำลายให้แตกหัก
อุปกรณ์เก็บข้อมูลอื่น ๆ	● ลบข้อมูล (ถ้าทำได้)	● แยกชิ้นส่วน ● ทุบทำลาย

ตารางที่ 1: ประเภทของสื่อบันทึกข้อมูล

6.3.4 การเก็บรักษา

- ระยะเวลาการเก็บรักษา แบ่งออกเป็น 2 ประเภท ตามลักษณะของเอกสาร/บันทึกการใช้งาน ดังนี้
  - เอกสาร/บันทึกการใช้งาน ที่อยู่ในรูปแบบเอกสารที่เป็นกระดาษ
  - เอกสารที่เป็นไฟล์อิเล็กทรอนิกส์ระยะเวลาในการจัดเก็บจัดเก็บภายหลังจากที่ไม่ได้ใช้งานแล้วโดยมีระยะเวลา ตามตารางในหัวข้อที่ 6.3.4
- บันทึกการใช้งานที่เป็น System Log, Application Log, Security Device Log ระยะเวลาในการจัดเก็บจัดเก็[ไว้ไม่น้อยกว่า 90 วัน (หากระบบรองรับ)

6.3.4 การกำหนดระยะเวลาในการจัดเก็บ

ประเภทของบันทึก	ตัวอย่างของบันทึก	ระยะเวลาในการจัดเก็บ
เอกสารการปฏิบัติงาน (Operational Record)	▪ Change Request Form	ไม่น้อยกว่า 3 ปี
ข้อมูลการจราจรบนระบบเครือข่าย (Traffic Log)	▪ Traffic log	ไม่น้อยกว่า 90 วัน
ข้อมูลกิจกรรมต่าง ๆ ของทุกระบบ (System Log)	▪ Audit log	

ประเภทของบันทึก	ตัวอย่างของบันทึก	ระยะเวลาในการจัดเก็บ
เอกสารสัญญาที่เกี่ยวข้องกับงานบริหารงานสารสนเทศ	▪ เอกสาร SLA ▪ สัญญารักษาความลับ (Non-disclosure Agreements) ▪ สัญญา MA ▪ รายงานผลการ MA ▪ รายงานผลการตรวจรับระบบ / อุปกรณ์	ไม่น้อยกว่า 3 ปี หรือตามเงื่อนไขสัญญา

ส่วนที่ 7 แนวปฏิบัติในการดำเนินการกำหนดชั้นข้อมูลอันเป็นความลับและการทำสัญญาปกปิดความลับ (Non Disclosure Agreement)

7.1.บุคลากรพนักงานที่สามารถเข้าถึงข้อมูลอันเป็นความลับในชั้นความลับใดก็ตามจะต้องเป็นบุคคลที่ผู้บังคับบัญชามอบหมายความไว้วางใจ และให้เข้าถึงข้อมูลอันเป็นความลับ ได้เฉพาะเรื่องที่ได้รับมอบหมายเท่านั้น และมีหน้าที่รักษาความลับและความปลอดภัยของข้อมูล เพื่อปกป้องข้อมูลอันเป็นความลับและเพื่อไม่ให้ข้อมูลอันเป็นความลับถูกเปิดเผย

7.2. ข้อมูลที่เป็นความลับและข้อมูลที่ถูกจำกัดต้องได้รับการเก็บรักษาอย่างปลอดภัย ถูกต้อง และเชื่อถือได้ และพร้อมสำหรับการใช้งาน โดยผู้ที่ได้รับอนุญาตมีมาตรการรักษาความปลอดภัยที่แตกต่างกันไปตามความเหมาะสมกับระดับที่ข้อมูลจะสูญหายหรือเสียหาย หรือทำให้ธุรกิจเสื่อมเสีย เสียหาย หรือละเมิดกฎหมาย นโยบาย หรือสัญญา มาตรการรักษาความปลอดภัยของข้อมูลกำหนดโดยเจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศและผู้จัดการหน่วยงานที่ดูแลข้อมูล

7.3. การกำหนดมาตรการรักษาความปลอดภัยของข้อมูล ต้องมีการประเมินความเสี่ยงด้านมูลค่าของข้อมูล ความละเอียดอ่อน ชื่อเสียง หรือผลประโยชน์ของบริษัท เพื่อใช้การรักษาความปลอดภัยในระดับที่เหมาะสม

7.4. กำหนดให้ผู้จัดการหน่วยงาน มีหน้าที่รักษาดูแลข้อมูลอันเป็นความลับ โดยจัดทำ**ตารางควบคุมรายการเอกสารข้อมูลอันเป็นความลับในหน่วยงานของตน (ตามแบบฟอร์ม)** โดยจะต้องรักษาข้อมูล อันเป็นความลับให้ปลอดภัยการจำกัดบุคคลเข้าถึงข้อมูลอันเป็นความลับ หรือหากมีการเปิดเผยข้อมูลอันเป็นความลับแก่ผู้ใด ต้องกระทำโดยระมัดระวัง พร้อมจัดทำแผนปฏิบัติการฉุกเฉินกรณีที่ข้อมูลอันเป็นความลับที่มีความเสี่ยงสูง เกิดการรั่วไหล หรือถูกโจรกรรมข้อมูล หรือข้อมูลสูญหายให้สอดคล้องตามนโยบายของบริษัท

7.5. จัดให้มีการตรวจสอบข้อมูลที่ได้รับการจัดชั้นความลับเพื่อให้แน่ใจว่าข้อมูลอันเป็นความลับได้ และถูกจัดเก็บอย่างเหมาะสมปลอดภัยและมี**แผนรองรับความเสี่ยงของข้อมูลความลับที่มีความเสี่ยงสูงนั้น ๆ หากพบว่ามีการจัดการข้อมูลไม่ถูกต้องหรือไม่เหมาะสม** ให้แจ้งผู้เกี่ยวข้องรีบดำเนินการแก้ไขทันที

7.6. กำหนดให้ เจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศ มีหน้าที่**การกำหนดสิทธิ์การเข้าถึงและการนำข้อมูลไปใช้อย่างเหมาะสม** โดยได้รับการอนุมัติจากผู้จัดการหน่วยงานก่อนที่จะให้สิทธิ์ในการเข้าถึง และ**ทบทวนสิทธิ์การเข้าถึงอย่างน้อยปีละ 1 ครั้ง** รวมถึงรับผิดชอบทางเทคนิคขั้นสูงสำหรับการปกป้องคุ้มครองข้อมูล เพื่อให้การดำเนินงานด้านเทคโนโลยีมีประสิทธิภาพ

7.7. หากพบว่าข้อมูลสูญหาย ถูกลบหรือถูกละเมิดข้อมูล ให้ผู้ทราบข้อเท็จจริงรายงานข้อเท็จจริงที่เกี่ยวข้องให้ผู้จัดการทราบ เพื่อพิจารณารายงานการละเมิดกรณีข้อมูลที่จัดอยู่ในรูปแบบ Electronic file และอยู่ในระบบคลาว์ของบริษัท

ให้แจ้งไปยังเจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศดำเนินการตรวจสอบการกระทำที่เกี่ยวกับข้อมูลที่ถูกละเมิดนั้น ประเมินผลกระทบที่เกิดขึ้นและรายงานไปยังผู้บริหารสูงสุดสายงานเทคโนโลยีสารสนเทศ เพื่อรายงานต่อคณะกรรมการบริหารทั้งนี้ให้ปฏิบัติตามนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกรณีข้อมูลที่อยู่ในประเภท Hard Copy หากพบว่าข้อมูลสูญหาย ถูกลบหรือถูกทำลาย โดยไม่ชอบให้ผู้พบเห็นแจ้งเหตุไปยังหน่วยงานตรวจสอบภายใน เพื่อดำเนินการสอบสวนหาข้อเท็จจริงและรายงานผลต่อคณะกรรมการบริหาร และคณะกรรมการตรวจสอบทราบ

7.8. จัดให้มีการสื่อสารและฝึกอบรมอย่างต่อเนื่องแก่พนักงาน เพื่อให้เกิดความรู้ความเข้าใจอย่างแท้จริงเกี่ยวกับมาตรการและความรับผิดชอบที่จำเป็นสำหรับการรักษาความปลอดภัยของข้อมูลความคาดหวังและบทลงโทษหากไม่ปฏิบัติตามนโยบายฉบับนี้

7.9 หน่วยงานที่รับผิดชอบจัดทำสัญญาโดยใช้แบบฟอร์มสัญญากลางที่ทางหน่วยงานกำกับและควบคุมได้จัดทำขึ้นโดยระบุวัตถุประสงค์และรายละเอียดต่างๆให้ชัดเจนรวมทั้งให้ดำเนินการโดยคำนึงถึงผลประโยชน์ของบริษัทมากที่สุด

7.10 มอบหมายให้หน่วยงานที่เกี่ยวข้องดำเนินการจัดทำสัญญาให้เก็บข้อมูลเป็นความลับกับคู่ค้า ที่ปรึกษาหรือบุคคลที่เกี่ยวข้องซึ่งทราบข้อมูลขององค์กรทุกครั้งเมื่อมีการทำสัญญาหรือเจรจาธุรกิจทั้งนี้ต้องจัดทำสัญญาดังกล่าวให้แล้วเสร็จโดยเร็วที่สุดภายใน 7 วันทำการนับแต่วันเริ่มสัญญาโดยก่อนทำสัญญาต้องแจ้งและขอเลขที่สัญญาจากหน่วยงานกำกับและควบคุมเมื่อดำเนินการเรียบร้อยให้หน่วยงานที่รับผิดชอบในเรื่องนั้นจัดเก็บสำเนาเอกสารสัญญารักษาความลับไว้และให้ส่งมอบต้นฉบับเอกสารสัญญาให้หน่วยงานกำกับและควบคุมจัดเก็บเข้าสาระบบและจัดทำทะเบียนเอกสารสัญญา

ส่วนที่ 8 การติดตามผล การทบทวนและการปรับปรุง

กำหนดให้หน่วยงานตรวจสอบภายในมีหน้าที่สอบทานความเพียงพอเหมาะสมและประสิทธิภาพของระบบควบคุมภายในและการปฏิบัติตามนโยบายฉบับนี้หากพบว่ามีบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องกับข้อมูลอันเป็นความลับได้รู้หรืออาจรู้ถึงข้อมูลอันเป็นความลับหรือเมื่อสงสัยว่ามีการละเมิดการรักษาความลับของข้อมูลข่าวสารของบริษัทให้ดำเนินการสอบสวนโดยไม่ชักช้าและรายงายผลต่อคณะกรรมการตรวจสอบทราบ

ส่วนที่ 9 บทลงโทษ

หากพบว่าพนักงานหรือผู้ที่เกี่ยวข้องมีการละเมิดหรือไม่ปฏิบัติตามมาตรการตามนโยบายฉบับนี้และนโยบายที่เกี่ยวข้องกับนโยบายนี้พนักงานหรือผู้เกี่ยวข้องนั้นอาจถูกระงับหรือการยุติการเข้าถึงและอาจมีการลงโทษทางวินัยตามระเบียบข้อบังคับ หรือตามที่กำหนดไว้ในนโยบายที่เกี่ยวข้องอื่น ๆ หรือมีโทษทางแพ่งหรือทางอาญา ตามแต่กรณี

ส่วนที่ 10 ทะเบียนควบคุมเอกสาร

ลำดับ	วันที่จัดทำ	รายละเอียดการดำเนินการ	วันที่บังคับใช้
00	1 ธันวาคม 2567	จัดทำเอกสารและอนุมัติประกาศใช้ครั้งแรก	1 มกราคม 2568
01	1 มิถุนายน 2568	ทบทวนเอกสารเพิ่มหัวข้อการจัดเก็บและการทำลายข้อมูล	1 กรกฎาคม 2568