สื่อสารนโยบาย และการทบทวนระเบียบปฏิบัติ การจัดระดับชั้นความลับ

วันที่ 28 สิงหาคม 2569

Agenda

สื่อสารนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

สื่อสารระเบียบปฏิบัติการจัดระดับชั้นความลับ

ตารางการจำแนกประเภทและการจัดการข้อมูลขององค์กร

รายงานผลการจัดระดับชั้นของข้อมูลและการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูล

01

สื่อสารนโยบายระบบบริหาร
จัดการความมั่นคงปลอดภัยสารสนเทศ

สื่อสารนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

1.1 องค์ประกอบของนโยบาย

ส่วนที่ 1 หน้าที่ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Responsibilities)
ส่วนที่ 2 หน้าที่ของผู้ดูแลระบบเทคโนโลยีสารสนเทศ (Administrator Responsibilities)
ส่วนที่ 3 การใช้อุปกรณ์สื่อสารประเภทพกพา (Mobile Device)
ส่วนที่ 4 การใช้คอมพิวเตอร์ทำงานจากระยะไกล (Teleworking)
ส่วนที่ 5 การกำหนดความปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security)
ส่วนที่ 6 การใช้รหัสผ่าน (Password)
ส่วนที่ 7 การใช้คอมพิวเตอร์พีซี/โน้ตบุ๊ค (Personal Computer/Notebook)
ส่วนที่ 8 การใช้งานซอฟต์แวร์ (Software Usage and Management)
ส่วนที่ 9 การใช้อินเทอร์เน็ต และบริการเครือข่าย (Internet and Network Service)
ส่วนที่ 10 การใช้บริการอีเมล (E-mail Service)
ส่วนที่ 11 การใช้เครือข่ายสังคมออนไลน์ (Online Social Networking)
ส่วนที่ 12 การเผยแพร่ข้อมูลในเว็บไซต์ (Publish Information on Website)
ส่วนที่ 13 การรักษา และป้องกันความลับของข้อมูล (Information Protection)
ส่วนที่ 14 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)
ส่วนที่ 15 การเข้ารหัสข้อมูล (Cryptography)
ส่วนที่ 16 การป้องกันไวรัสคอมพิวเตอร์ (Malware Protection)
ส่วนที่ 17 การไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น (Intellectual Property)
ส่วนที่ 18 การแลกเปลี่ยนสารสนเทศ (Information Sharing)
ส่วนที่ 19 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Incident Reporting)
ส่วนที่ 20 การบริหารความต่อเนื่องของธุรกิจ (Business Continuity Management)
ส่วนที่ 21 การรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Incident Management)
ส่วนที่ 22 การใช้งาน Cloud Computing อย่างปลอดภัย (Cloud Computing Security)
ส่วนที่ 23 การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในโครงการ (Information Security in Project Management)
ส่วนที่ 24 การควบคุมการเข้าถึง (Access Control)
ส่วนที่ 25 ความมั่นคงปลอดภัยสารสนเทศด้านการสื่อสาร(Communication Security)
ส่วนที่ 26 การบริหารจัดการความเสี่ยง (Risk Management)
ส่วนที่ 27 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)
ส่วนที่ 28 การนำเครื่องคอมพิวเตอร์ขององค์กรออกนอกพื้นที่ (Taking Company-Assigned Computers Outside Premises)
ส่วนที่ 29 การปิดบังข้อมูล (Data Masking)
ส่วนที่ 30 การป้องกันข้อมูลรั่วไหล (Data Leakage Prevention)
ส่วนที่ 31 การลบ ทำลายข้อมูล และการบริหารจัดการการบันทึกข้อมูล (Data Deletion and Record Management)
ส่วนที่ 32 การใช้งานทรัพย์สินอย่างเหมาะสม (Acceptable Use of Assets)
ส่วนที่ 33 การบริหารจัดการล็อก (Logging Management)
ส่วนที่ 34 การบริหารจัดการช่องโหว่ (Vulnerability Management)
ส่วนที่ 35 การใช้งานปัญญาประดิษฐ์อย่างปลอดภัย (Secure Use of Artificial Intelligence)
ส่วนที่ 36 การกำหนดชั้นความลับข้อมูลสารสนเทศ (Information Classification)

สื่อสารนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

1.2 เพิ่มเนื้อหาของนโยบายครั้งล่าสุด ส่วนที่ 36 การกำหนดชั้นความลับข้อมูลสารสนเทศ (Information Classification)

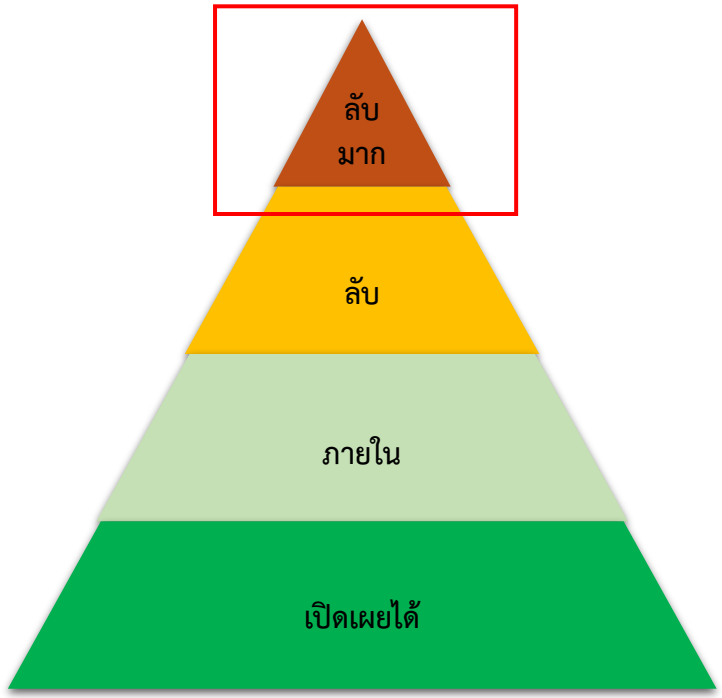
1. องค์กรกำหนดให้ข้อมูลสารสนเทศทุกประเภทต้องได้รับการจัดลำดับชั้นความลับของข้อมูลตามระดับความสำคัญ แหล่งที่มา และผลกระทบต่อองค์กร ก่อนนำไปใช้งาน จัดเก็บ ประมวลผล ส่งต่อ หรือทำลาย
2. เจ้าของข้อมูล (Data Owner) มีหน้าที่รับผิดชอบในการกำหนด ทบทวน และอนุมัติระดับการจัดลำดับชั้นความลับของข้อมูล รวมถึงกำหนดมาตรการคุ้มครองข้อมูลให้เหมาะสมกับระดับชั้นความลับของข้อมูล
3. บุคลากรทุกคน รวมถึงผู้รับจ้าง ผู้ให้บริการ และบุคคลภายนอกที่ได้รับสิทธิ์เข้าถึงข้อมูล ต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยโดยให้สอดคล้องตามลำดับชั้นความลับที่องค์กรกำหนด
4. องค์กรกำหนดให้มีมาตรการควบคุมการเข้าถึง การใช้งาน การจัดเก็บ การส่งต่อ การสำรองข้อมูล และการทำลายข้อมูล ให้สอดคล้องกับลำดับชั้นความลับของข้อมูล
5. การเปิดเผยหรือส่งต่อข้อมูลให้บุคคลภายนอกต้องได้รับการอนุมัติจากเจ้าของข้อมูล หรือผู้มีอำนาจตามที่องค์กรกำหนด และต้องมีมาตรการป้องกันข้อมูลที่เหมาะสม
6. องค์กรกำหนดให้มีการทบทวนลำดับชั้นความลับของข้อมูลเป็นระยะ หรือเมื่อมีการเปลี่ยนแปลงลักษณะของข้อมูล กระบวนการทางธุรกิจ ข้อกำหนดทางกฎหมาย หรือความเสี่ยงที่เกี่ยวข้อง
7. องค์กรกำหนดให้มีการสร้างความตระหนัก และสื่อสารให้บุคลากรทุกคนรับทราบและปฏิบัติตามนโยบายการกำหนดชั้นความลับข้อมูลสารสนเทศ (Information Classification) อย่างต่อเนื่อง
8. การไม่ปฏิบัติตามนโยบายนี้จะได้รับการพิจารณาดำเนินการตามระเบียบ ข้อบังคับ และมาตรการทางวินัยขององค์กร รวมถึงกฎหมาย และข้อกำหนดที่เกี่ยวข้อง

02

สื่อสารระเบียบปฏิบัติการจัดระดับชั้นความลับ

สื่อสารระเบียบปฏิบัติการจัดระดับชั้นความลับ

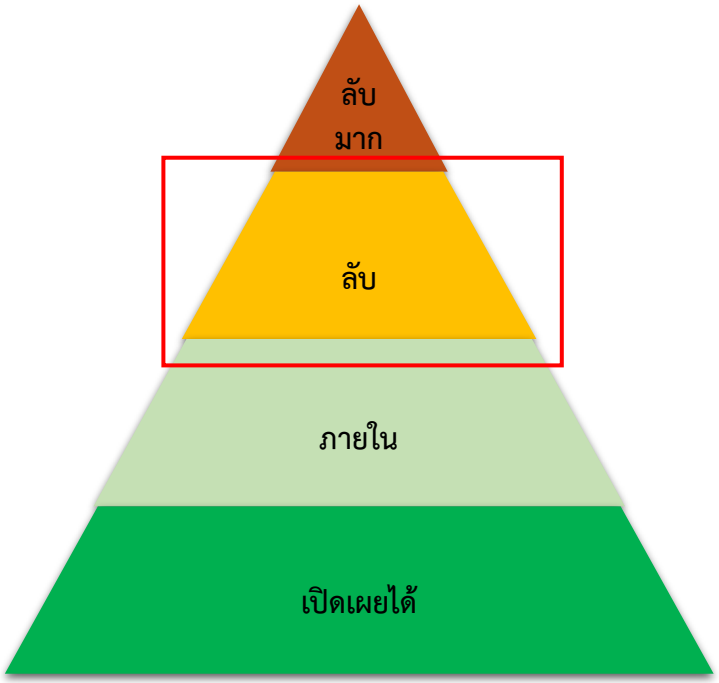
2.1 การบริหารจัดการชั้นความลับของข้อมูล



1. **ลับมาก (Top Secret)** หมายถึง ข้อมูลที่มีความสำคัญอย่างยิ่งต่อการดำเนินธุรกิจ การดำเนินงาน หรือผลประโยชน์ขององค์กร และกำหนดให้เฉพาะบุคคลหรือกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึง ใช้งาน หรือเปิดเผยข้อมูลดังกล่าวได้ การเปิดเผย การเข้าถึง การใช้ หรือการส่งต่อข้อมูลในระดับชั้นนี้โดยไม่ได้รับอนุญาต อาจก่อให้เกิดความเสียหายอย่างร้ายแรงต่อองค์กร ลูกค้า หรือคู่ค้า และอาจส่งผลกระทบอย่างมีนัยสำคัญต่อการดำเนินธุรกิจ ความสามารถในการแข่งขัน ชื่อเสียง หรือทรัพย์สินทางปัญญาขององค์กร อาทิเช่น ขั้นตอนและสูตรการผลิต, แผนกลยุทธ์ทางธุรกิจ, ข้อมูลส่วนบุคคลที่มีความอ่อนไหว, ความลับทางการค้า (Trade Secret), ข้อมูล Prototype หรือข้อมูลต้นแบบที่มีความสำคัญสูง ตลอดจนข้อมูลอื่นใดที่หากถูกเปิดเผยโดยไม่ได้รับอนุญาต อาจก่อให้เกิดความเสียหายร้ายแรงและยากต่อการแก้ไขหรือเยียวยาแก่องค์กร ลูกค้า หรือคู่ค้า เป็นต้น

สื่อสารระเบียบปฏิบัติการจัดระดับชั้นความลับ

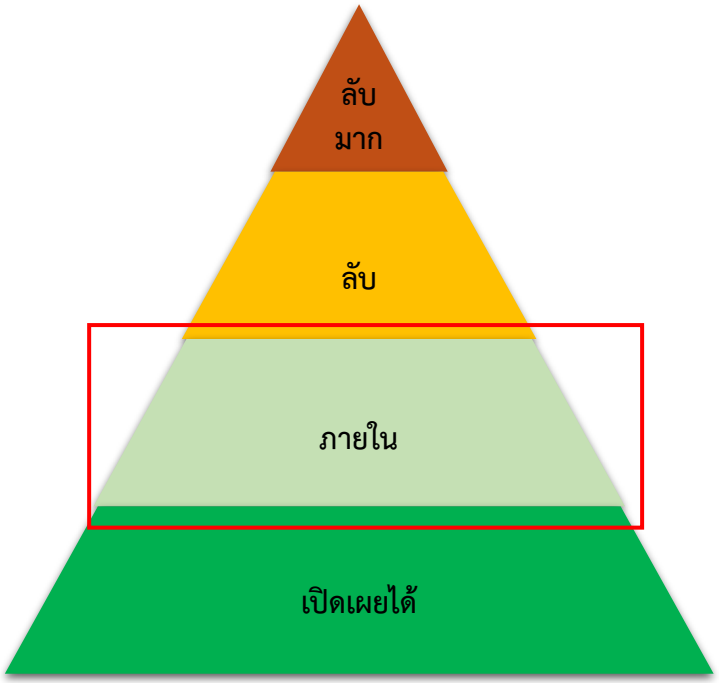
2.1 การบริหารจัดการชั้นความลับของข้อมูล (ต่อ)



2. **ลับ (Confidential)** หมายถึง เอกสาร ข้อมูล ข้อมูลทางอิเล็กทรอนิกส์ และสารสนเทศต่าง ๆ ที่มีความสำคัญต่อการดำเนินงานขององค์กร และกำหนดให้เข้าถึงหรือใช้งานได้เฉพาะบุคคลหรือหน่วยงานที่เกี่ยวข้องหรือได้รับอนุญาตเท่านั้น รวมถึงข้อมูลส่วนบุคคลทั่วไปที่ต้องได้รับการควบคุมและป้องกันการเปิดเผยต่อบุคคลที่ไม่มีสิทธิ์ การเปิดเผย การเข้าถึง การใช้ หรือการส่งต่อข้อมูลในระดับชั้นนี้โดยไม่ได้รับอนุญาต อาจก่อให้เกิดความเสียหายต่อองค์กร ลูกค้า หรือคู่ค้า รวมถึงอาจส่งผลกระทบต่อการดำเนินงาน ความปลอดภัยของระบบ หรือการปฏิบัติตามข้อกำหนดทางกฎหมายและข้อกำหนดที่เกี่ยวข้อง อาทิเช่น ข้อมูลส่วนบุคคลทั่วไป, Network Diagram, System Diagram, เอกสารสัญญา, Source Code ที่ไม่ได้จัดอยู่ในระดับลับมาก, รายงานการประเมินช่องโหว่และการทดสอบเจาะระบบ, ข้อมูลต้นทุน, ข้อมูลที่อยู่ภายใต้ข้อกำหนดทางกฎหมายหรือข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA), หรือข้อมูลอื่นใดที่หากถูกเปิดเผยโดยไม่ได้รับอนุญาต อาจก่อให้เกิดความเสียหายทางการเงิน การดำเนินงาน หรือชื่อเสียงขององค์กร เป็นต้น

02 สื่อสารระเบียบปฏิบัติการจัดระดับชั้นความลับ

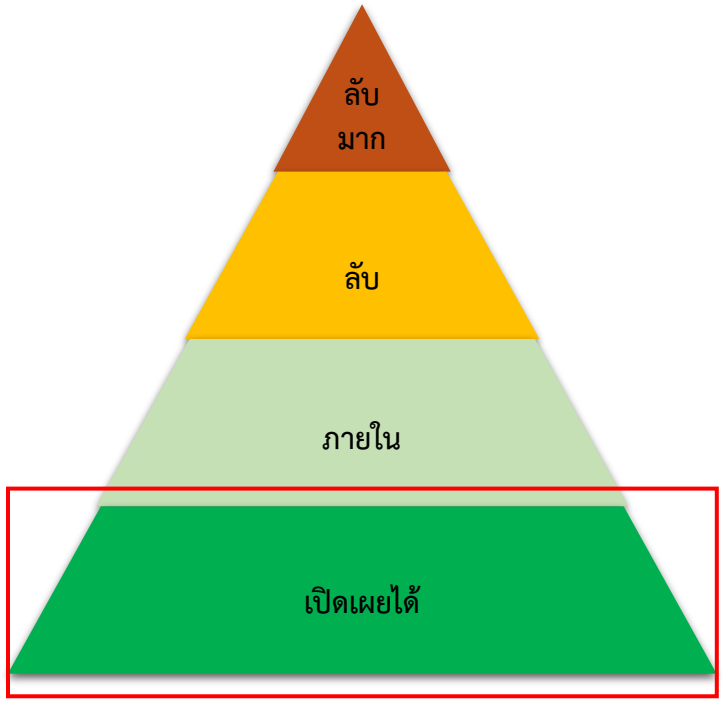
2.1 การบริหารจัดการชั้นความลับของข้อมูล (ต่อ)



3. **ภายใน (Internal)** หมายถึง เอกสาร ข้อมูล ข้อมูลทางอิเล็กทรอนิกส์ และสารสนเทศต่าง ๆ ที่องค์กรจัดทำหรือได้รับมาเพื่อใช้ในการดำเนินงานภายในองค์กร และไม่ควรเปิดเผยต่อบุคคลภายนอก เว้นแต่ได้รับอนุญาตจากผู้มีอำนาจหรือผู้รับผิดชอบตามที่องค์กรกำหนด การเปิดเผย การเข้าถึง การใช้ หรือการส่งต่อข้อมูลในระดับชั้นนี้โดยไม่ได้รับอนุญาต อาจก่อให้เกิดความเสียหายในระดับเล็กน้อยถึงปานกลางต่อองค์กร หรืออาจส่งผลกระทบต่อประสิทธิภาพในการดำเนินงาน การประสานงาน หรือความสัมพันธ์ทางธุรกิจขององค์กร อาทิเช่น ขั้นตอนปฏิบัติงานของแต่ละแผนก, แผนการปฏิบัติงาน, ข้อมูลราคาที่ไม่เป็นข้อมูลสำคัญทางธุรกิจ, แผนการผลิตทั่วไป, ข้อมูลการดำเนินงานภายใน, หรือข้อมูลอื่นใดที่หากถูกเปิดเผยอาจส่งผลกระทบต่อการดำเนินงาน ความสามารถในการแข่งขัน หรือความสัมพันธ์กับคู่ค้าในระดับที่ไม่รุนแรง เป็นต้น

02 สื่อสารระเบียบปฏิบัติการจัดระดับชั้นความลับ

2.1 การบริหารจัดการชั้นความลับของข้อมูล (ต่อ)



4. **เปิดเผยได้ (Public)** หมายถึง เอกสาร ข้อมูล ข้อมูลทางอิเล็กทรอนิกส์ และสารสนเทศต่าง ๆ ที่องค์กรจัดทำขึ้นหรือได้รับจากภายนอก และได้รับการพิจารณาอนุมัติให้สามารถเปิดเผยหรือเผยแพร่ต่อสาธารณะได้ โดยไม่มีข้อจำกัดในการเข้าถึงจากบุคคลภายนอก ทั้งนี้ การเผยแพร่ข้อมูลต้องเป็นไปตามวัตถุประสงค์ ขอบเขต และช่องทางที่องค์กรกำหนด อาทิ เช่น ข้อมูลที่เผยแพร่บนเว็บไซต์ขององค์กร, ข่าวประชาสัมพันธ์, โบรชัวร์ หรือเอกสารประชาสัมพันธ์, ข้อมูลผลิตภัณฑ์ที่ได้รับอนุมัติให้เผยแพร่, ข้อมูลการรับสมัครงานที่เผยแพร่ต่อสาธารณะ, ประกาศหรือข้อมูลที่องค์กรมีวัตถุประสงค์ให้ลูกค้า คู่ค้า หรือประชาชนทั่วไปได้รับทราบ เป็นต้น

สื่อสารระเบียบปฏิบัติการจัดระดับชั้นความลับ

2.1 การบริหารจัดการชั้นความลับของข้อมูล (ต่อ)

หลักเกณฑ์และวิธีการจำแนกชั้นความลับ

การจำแนกชั้นความลับของข้อมูลและสารสนเทศ ให้พิจารณาจากปัจจัยหลัก 3 ด้าน ดังต่อไปนี้

1. **ระดับผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต** พิจารณาถึงระดับความเสียหายที่อาจเกิดขึ้นต่อองค์กร โดยครอบคลุมด้านด้านการเงิน ด้านลูกค้า ด้านการปฏิบัติการ และด้านกฎระเบียบ
2. **ลักษณะและประเภทของข้อมูล** พิจารณาถึงลักษณะของข้อมูล เช่น ข้อมูลส่วนบุคคล, ข้อมูลส่วนบุคคลที่มีความอ่อนไหว ความลับทางการค้า ข้อมูลทางการเงิน ข้อมูลทางเทคนิค ข้อมูลด้านการผลิต ข้อมูลทางธุรกิจ หรือข้อมูลทั่วไป รวมถึงข้อกำหนดหรือข้อจำกัดในการใช้และเปิดเผยข้อมูล
3. **กลุ่มบุคคลหรือหน่วยงานที่มีสิทธิ์เข้าถึงข้อมูล** พิจารณาถึงขอบเขตของผู้ที่จำเป็นต้องเข้าถึงข้อมูลตามหน้าที่และความรับผิดชอบ ทั้งบุคลากรภายในองค์กร บุคคลภายนอก ลูกค้า คู่ค้า หรือหน่วยงานอื่นที่เกี่ยวข้อง

เจ้าของข้อมูล (Data Owner) ของแต่ละฝ่ายงานเป็นผู้รับผิดชอบในการประเมินและกำหนดชั้นความลับของข้อมูล โดยพิจารณาจากปัจจัยข้างต้น และสามารถขอคำปรึกษาหรือการสนับสนุนจากฝ่ายเทคโนโลยีสารสนเทศ ในด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและมาตรการควบคุมที่เหมาะสม ทั้งนี้ การจำแนกชั้นความลับของข้อมูลให้บันทึกไว้ใน เอกสาร *ISMS-FM-MIS-038_ตารางการจัดเก็บข้อมูลขององค์กรและกำหนดชั้นความลับ* ตามที่องค์กรกำหนด

สื่อสารระเบียบปฏิบัติการจัดระดับชั้นความลับ

2.1 การบริหารจัดการชั้นความลับของข้อมูล (ต่อ)

ขั้นตอนการจำแนกชั้นความลับมี 4 ขั้นตอน ดังนี้

1

ขั้นที่ 1 ระบุและบันทึกรายการข้อมูล (Data Identification)

- รวบรวมข้อมูลและสารสนเทศที่ฝ่ายงานจัดทำ สร้าง ได้รับ ใช้ หรือจัดเก็บ พร้อมระบุเจ้าของข้อมูล (Data Owner) และผู้ดูแลข้อมูล (Data Custodian)

2

ขั้นที่ 2 ประเมินความอ่อนไหวและผลกระทบ (Sensitivity and Impact Assessment)

- ประเมินระดับผลกระทบใน 4 มิติ ได้แก่ **ด้านการเงิน (F), ด้านลูกค้า (C), ด้านการปฏิบัติการ (O) และด้านกฎระเบียบ (L)** พร้อมตรวจสอบว่าข้อมูลเป็นข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลที่มีความอ่อนไหว ความลับทางการค้า หรือข้อมูลที่มีข้อจำกัดในการใช้และเปิดเผยหรือไม่

สื่อสารระเบียบปฏิบัติการจัดระดับชั้นความลับ

2.1 การบริหารจัดการชั้นความลับของข้อมูล (ต่อ)

ขั้นตอนการจำแนกชั้นความลับมี 4 ขั้นตอน ดังนี้ (ต่อ)

ขั้นที่ 3 กำหนดชั้นความลับ (Classification)

- กำหนดชั้นความลับ (Classification): กำหนดระดับชั้นความลับของข้อมูลตามเกณฑ์ที่องค์กรกำหนด โดยแบ่งออกเป็น 4 ระดับ ได้แก่ เปิดเผยได้ (Public), ภายใน (Internal), ลับ (Confidential) และลับมาก (Top Secret) ทั้งนี้ ให้พิจารณาและกำหนดชั้นความลับตามลักษณะของข้อมูล ระดับผลกระทบ และสิทธิ์ในการเข้าถึงข้อมูล เพื่อให้สอดคล้องกับเกณฑ์การจำแนกชั้นความลับขององค์กร

ขั้นที่ 4 สื่อสารและนำผลการจำแนกไปใช้ (Communication & Handling)

- สื่อสารและนำผลการจำแนกไปใช้ (Communication & Handling): สื่อสารผลการกำหนดระดับชั้นความลับให้ผู้ที่เกี่ยวข้องทราบ และดำเนินการจัดการข้อมูลให้สอดคล้องกับระดับชั้นความลับที่กำหนด เช่น การติดป้ายกำกับ (Label) บนไฟล์และเอกสาร การกำหนดสิทธิ์และควบคุมการเข้าถึงข้อมูลตามความเหมาะสม รวมถึงการกำหนดมาตรการในการจัดเก็บ การส่งต่อ การเผยแพร่ และการทำลายข้อมูลตามระดับชั้นความลับ

ทั้งนี้ ให้มีการทบทวนและปรับปรุงการจำแนกชั้นความลับ (Review & Update) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

02 สื่อสารระเบียบปฏิบัติการจัดระดับชั้นความลับ

2.1 การบริหารจัดการชั้นความลับของข้อมูล (ต่อ)

องค์ประกอบในการพิจารณา

องค์ประกอบการพิจารณา	เปิดเผยได้ (Public)	ภายใน (Internal)	ลับ (Confidential)	ลับมาก (Top Secret)
ความสำคัญของเนื้อหา	ไม่มีนัยสำคัญต่อองค์กร หรือสามารถเปิดเผยต่อสาธารณะได้	มีความสำคัญต่อการดำเนินงานภายในของหน่วยงานหรือกลุ่มงาน	มีความสำคัญต่อองค์กร และการดำเนินงานทางธุรกิจ	มีความสำคัญอย่างสูงต่อองค์กรและการดำเนินงานทางธุรกิจ
บุคคลที่ควรรับทราบ	สามารถเปิดเผย ต่อสาธารณะได้ เช่น บุคคลทั่วไป คู่ค้า ลูกค้า พนักงานทุกระดับ	บุคลากรภายในองค์กรหรือกลุ่มงานที่เกี่ยวข้องกับข้อมูลตามหน้าที่	จำกัดเฉพาะบุคคลหรือกลุ่มบุคคลที่ได้รับอนุญาตจาก Data Owner เท่านั้น	จำกัดเฉพาะผู้บริหารระดับสูง หรือบุคคลที่ได้รับอนุญาตหรือมอบหมายเป็นกรณีพิเศษเท่านั้น
ผลกระทบจากการเปิดเผยหรือเข้าถึงโดยไม่ได้รับอนุญาต	ไม่มีผลกระทบ หรือมีผลกระทบที่ไม่มีนัยสำคัญ	อาจส่งผลกระทบต่อการปฏิบัติงานประจำวันของหน่วยงาน แต่ไม่กระทบอย่างมีนัยสำคัญต่อการดำเนินธุรกิจ	อาจก่อให้เกิดความเสียหายอย่างมีนัยสำคัญต่อองค์กร การดำเนินธุรกิจ ลูกค้า หรือคู่ค้า	อาจก่อให้เกิดความเสียหายร้ายแรงอย่างยิ่งต่อองค์กร ลูกค้า หรือคู่ค้า และอาจส่งผลกระทบต่อความสามารถในการแข่งขัน ผลประโยชน์ทางธุรกิจ หรือทรัพย์สินทางปัญญาอย่างรุนแรง

สื่อสารระเบียบปฏิบัติการจัดระดับชั้นความลับ

2.1 การบริหารจัดการชั้นความลับของข้อมูล (ต่อ)

องค์ประกอบในการพิจารณา(ต่อ)

องค์ประกอบการพิจารณา	เปิดเผยได้ (Public)	ภายใน (Internal)	ลับ (Confidential)	ลับมาก (Top Secret)
ผลกระทบจากการแก้ไขหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต	อาจทำให้ข้อมูลคลาดเคลื่อนหรือเกิดความเข้าใจผิดแต่ไม่มีผลกระทบอย่างมีนัยสำคัญ	เอาจส่งผลกระทบต่อการปฏิบัติงานประจำวันของหน่วยงาน แต่ไม่กระทบอย่างมีนัยสำคัญต่อการดำเนินธุรกิจ	อาจก่อให้เกิดความเสียหายต่อการดำเนินงาน การเงิน ลูกค้า หรือคู่ค้า	อาจก่อให้เกิดความเสียหายร้ายแรงต่อองค์กร การดำเนินธุรกิจ ความสามารถในการแข่งขัน หรือผลประโยชน์สำคัญขององค์กร
ระดับการควบคุม	ไม่จำกัดการเข้าถึง	ควบคุมการเข้าถึงภายในองค์กรตามความเหมาะสม	จำกัดและควบคุมการเข้าถึงตามหน้าที่และความจำเป็นในการใช้งาน	ควบคุมอย่างเข้มงวด จำกัดเฉพาะผู้ที่ได้รับอนุญาตเป็นพิเศษ และต้องมีการติดตามการเข้าถึงตามความเหมาะสม

03

ตารางการจำแนกประเภทและการจัดการข้อมูลขององค์กร

ตารางการจำแนกประเภทและการจัดการข้อมูลขององค์กร

ตารางการจัดเก็บข้อมูลขององค์กรและการกำหนดชั้นความลับ

ลำดับ (No.)	ฝ่ายงาน (Department)	ชื่อข้อมูล / ชื่อไฟล์ข้อมูล / ชื่อเอกสาร (Data Name, Data File, Doc Name.)	คำอธิบายข้อมูล (Description of Data)	เจ้าของข้อมูล (Data Owner)	การประเมินความเสี่ยง						ความเสี่ยงอื่น ๆ							ชั้นความลับ (Classification Level)				ระยะเวลาการจัดเก็บข้อมูล (Retention Period)	หมายเหตุ	รูปแบบข้อมูลที่จัดเก็บ Softfile/ Hardcopy/ Both	การจัดเก็บข้อมูล									
					ระดับผลกระทบ (Impact)				โอกาสใช้งานข้อมูล	ระดับความเสี่ยง	เป็นข้อมูลที่สามารถเปิดเผยให้บุคคลภายนอกได้ (เช่น ข่าวทั่วไป)	เป็นข้อมูลที่สามารถเปิดเผยได้ภายในองค์กรเท่านั้น (เช่น คู่มือพนักงาน)	เป็นข้อมูลส่วนบุคคลที่สามารถเปิดเผยได้ภายในองค์กรเท่านั้น (เช่น Contact List)	เป็นข้อมูลส่วนบุคคลของพนักงาน (เช่น ชื่อ นามสกุล เบอร์โทร สัญญาจ้าง)	ข้อมูลส่วนบุคคลของบุคคลภายนอก (เช่น ที่อยู่ ชื่อ เบอร์โทร)	เป็นข้อมูลส่วนบุคคลอ่อนไหว (เช่น เชื้อชาติ ประวัติการรักษา)	ข้อมูลความลับทางการค้า (เช่น Trade Secret , ต้นทุนการผลิต เป็นต้น)	เปิดเผยได้ (Public)	ภายใน (Internal)	ลับ (Confidential)	ลับมาก (Top Secret)				Computer (PC / Notebook) พนักงาน	ผู้ดูแลข้อมูล (Custodian)	Share drive (Link / URL / Apex Drive)	ผู้ดูแลข้อมูล (Custodian)	Application (ระบบ) (ชื่อระบบ / ชื่อแอปพลิเคชัน)	ผู้ดูแลข้อมูล (Custodian)	ตู้เก็บเอกสาร (สถานที่ตั้งตู้เก็บเอกสาร)	ผู้ดูแลข้อมูล (Custodian)	อื่นๆ (NAS / External HDD / Thumb Drive)	ผู้ดูแลข้อมูล (Custodian)
					ผลกระทบด้านการเงิน	ผลกระทบด้านลูกค้า	ผลกระทบด้านการปฏิบัติการ	ผลกระทบด้านกฎระเบียบ																									
ตัวอย่าง	MIS		ระบบ EMIS - ข้อมูล Passport	MIS	2	2	1	2	5	10	No	Yes	No	No	No	Yes	No				✓	ตลอดไป		Softfile	No	MIS	-	-	VMS	MIS	-	-	-	-

04

รายงานผลการจัดระดับชั้นของข้อมูล และการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูล

04 รายงานผลการจัดระดับชั้นของข้อมูลและการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูล

4.1 ตารางการจัดเก็บข้อมูลขององค์กรและผลกระทบระดับความเสียหาย

ระดับผลกระทบ	เกณฑ์ระดับความเสียหาย (Consequence of Impact)			
	ผลกระทบด้านการเงิน	ผลกระทบด้านลูกค้า	ผลกระทบด้านการปฏิบัติการ	ผลกระทบด้านกฎระเบียบ
	F : Finacial	C : Customer	O : Operations	L : Legal & Regulations
5	ทำให้บริษัทเกิดความเสียหายทางการเงินอย่างรุนแรง รวมถึงการสูญเสียรายได้ การหยุดสายการผลิต ค่าใช้จ่ายในการกู้คืนระบบ ค่าใช้จ่ายจากการเรียกคืนสินค้า (Recall), ค่าปรับตามสัญญา หรือค่าปรับตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง เช่น PDPA, GDPR หรือกฎหมายทรัพย์สินทางปัญญา รวมมูลค่ามากกว่า 750 ล้านบาท	ข้อมูลเสียหายถาวร และทำให้ไม่สามารถกู้ข้อมูลกลับคืนได้ ส่งผลกระทบต่อการผลิตและส่งมอบสินค้า นานกว่า 48 ชั่วโมง หรือ ข้อมูลรั่วไหลส่งผลกระทบต่อความลับทางการค้าของผู้ว่าจ้าง (สูตรการผลิต , Prototype product data)ข้อมูลสำคัญของลูกค้า หรือข้อมูลที่เกี่ยวข้องกับกระบวนการผลิต เช่น สูตรการผลิต ข้อมูล Prototype, Drawing หรือ Specification เกิดความเสียหาย สูญหาย หรือรั่วไหล ซึ่งส่งผลให้ไม่สามารถกู้คืนข้อมูลหรือดำเนินกระบวนการผลิตได้ตามปกติ ส่งผลให้การผลิตหรือการส่งมอบสินค้าหยุดชะงักเกินกว่า 48 ชั่วโมง และกระทบต่อความเชื่อมั่นของลูกค้า ข้อผูกพันทางสัญญา หรือความสามารถในการแข่งขันทางธุรกิจ	ระบบสารสนเทศ ข้อมูลสำคัญ หรือระบบควบคุมการผลิตที่สำคัญของบริษัทไม่สามารถใช้งานได้ ทำงานผิดปกติ หรือถูกกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ส่งผลให้กระบวนการดำเนินธุรกิจหลักหรือสายการผลิตหยุดชะงัก รวมถึงอาจส่งผลกระทบต่อความต่อเนื่อง ความปลอดภัยของพนักงาน เครื่องจักร หรือสภาพแวดล้อมในการทำงาน เช่น ระบบ ERP, ระบบ Email, ระบบการเงิน, ศูนย์ Data Center, ระบบการผลิต, ระบบเครือข่าย หรือระบบขนส่ง และส่งผลกระทบต่อความต่อเนื่องทางธุรกิจหรือการส่งมอบสินค้าเกินกว่า 48 ชั่วโมง	ขัดต่อกฎหมาย ข้อกำหนด มาตรฐาน หรือเงื่อนไขทางสัญญาที่เกี่ยวข้องกับการดำเนินธุรกิจ ส่งผลให้บริษัทมีความเสี่ยงต่อการถูกดำเนินคดี ถูกปรับ ถูกระงับการดำเนินธุรกิจ สูญเสียสิทธิ์ทางการค้า หรือสูญเสียความเชื่อมั่นจากลูกค้าและหน่วยงานกำกับดูแลอย่างรุนแรง

รายงานผลการจัดระดับชั้นของข้อมูลและการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูล

4.1 ตารางการจัดเก็บข้อมูลขององค์กรและผลกระทบระดับความเสียหาย (ต่อ)

ระดับผลกระทบ	เกณฑ์ระดับความเสียหาย (Consequence of Impact)			
	ผลกระทบด้านการเงิน	ผลกระทบด้านลูกค้า	ผลกระทบด้านการปฏิบัติการ	ผลกระทบด้านกฎระเบียบ
	F : Finacial	C : Customer	O : Operations	L : Legal & Regulations
4	ทำให้บริษัทต้องชดใช้ค่าเสียหาย สูญเสียรายได้ หรือเกิดค่าใช้จ่ายในการกู้คืนระบบรวมมูลค่ามากกว่า 250 ล้านบาท แต่ไม่เกิน 750 ล้านบาท รวมถึงค่าปรับหรือค่าเสียหายที่เกี่ยวข้องกับ PDPA, GDPR หรือกฎหมายทรัพย์สินทางปัญญา	ระบบหรือบริการสำคัญเกิดข้อผิดพลาดส่งผลกระทบต่อการใช้งานของลูกค้าในบางส่วน หรือไม่สามารถใช้งานบางฟังก์ชันได้ รวมถึงใช้เวลาในการกู้คืนหรือแก้ไขปัญหาระหว่าง 24–48 ชั่วโมง หรือ ข้อมูลสำคัญได้รับความเสียหาย สูญหาย หรือรั่วไหล แต่ยังสามารถกู้คืนหรือควบคุมผลกระทบได้ ส่งผลกระทบต่อการผลิตหรือการส่งมอบสินค้าในบางส่วน โดยยังไม่กระทบต่อข้อมูลความลับทางการค้าระดับวิกฤตของผู้ว่าจ้าง	ระบบสารสนเทศ ข้อมูลสำคัญ หรือระบบควบคุมการผลิตบางส่วนไม่สามารถใช้งานได้ หรือการเชื่อมต่อระบบเกิดความล้มเหลว ส่งผลกระทบต่อการดำเนินงานหรือสายการผลิตบางส่วน รวมถึงอาจกระทบต่อความต่อเนื่องและความปลอดภัยในการดำเนินงานของพนักงาน เครื่องจักร หรือสภาพแวดล้อมในการทำงาน และใช้เวลาในการกู้คืนหรือแก้ไขปัญหาระหว่าง 24–48 ชั่วโมง	ขัดต่อกฎหมาย ข้อกำหนด หรือเงื่อนไขทางสัญญาบางประการ ส่งผลให้บริษัทอาจถูกแจ้งเตือน หรือเกิดค่าใช้จ่ายในการดำเนินการแก้ไข เพื่อให้เป็นไปตามข้อกำหนดของหน่วยงานกำกับดูแล ลูกค้า หรือข้อผูกพันตามสัญญา

รายงานผลการจัดระดับชั้นของข้อมูลและการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูล

4.1 ตารางการจัดเก็บข้อมูลขององค์กรและผลกระทบระดับความเสียหาย (ต่อ)

ระดับผลกระทบ	เกณฑ์ระดับความเสียหาย (Consequence of Impact)			
	ผลกระทบด้านการเงิน	ผลกระทบด้านลูกค้า	ผลกระทบด้านการปฏิบัติการ	ผลกระทบด้านกฎระเบียบ
	F : Finacial	C : Customer	O : Operations	L : Legal & Regulations
3	ทำให้บริษัทต้องชดใช้ค่าเสียหาย สูญเสียรายได้ หรือเกิดค่าใช้จ่ายในการกู้คืนระบบ รวมมูลค่ามากกว่า 50 ล้านบาท แต่ไม่เกิน 250 ล้านบาท รวมถึงค่าปรับหรือค่าเสียหายที่เกี่ยวข้องกับ PDPA, GDPR หรือกฎหมายทรัพย์สินทางปัญญา	ข้อมูลสำคัญได้รับความเสียหาย สูญหาย หรือรั่วไหลในระดับปานกลาง แต่ยังสามารถกู้คืนหรือควบคุมผลกระทบได้ ส่งผลกระทบต่อการผลิตหรือการส่งมอบสินค้าในบางส่วน หรือกระทบต่อข้อมูลทั่วไปของลูกค้า เช่น Contact Point หรือข้อมูลนิติบุคคล โดยใช้เวลาในการกู้คืนหรือแก้ไขปัญหาระหว่าง 12–24 ชั่วโมง	ระบบทำงานช้าหรือไม่สมบูรณ์ ส่งผลกระทบที่สำคัญต่อการดำเนินงานที่ลดลง เช่น ความล่าช้าในการประมวลผลข้อมูล, ฟังก์ชันบางอย่างไม่ทำงานตามปกติ และใช้เวลาในการกู้คืนหรือแก้ไขปัญหาระหว่าง 12-24 ชั่วโมง	การไม่ปฏิบัติตามกฎหมาย กฎระเบียบข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ หรือเงื่อนไขตามสัญญาบางประการ ส่งผลให้บริษัทต้องดำเนินการแก้ไขปรับปรุง รายงานต่อหน่วยงานกำกับดูแล ลูกค้า หรือผู้ตรวจประเมินที่เกี่ยวข้อง และอาจส่งผลกระทบต่อการดำเนินธุรกิจหรือความเชื่อมั่นของผู้เกี่ยวข้องในระดับปานกลาง

รายงานผลการจัดระดับชั้นของข้อมูลและการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูล

4.1 ตารางการจัดเก็บข้อมูลขององค์กรและผลกระทบระดับความเสียหาย (ต่อ)

ระดับผลกระทบ	เกณฑ์ระดับความเสียหาย (Consequence of Impact)			
	ผลกระทบด้านการเงิน	ผลกระทบด้านลูกค้า	ผลกระทบด้านการปฏิบัติการ	ผลกระทบด้านกฎระเบียบ
	F : Finacial	C : Customer	O : Operations	L : Legal & Regulations
2	ทำให้บริษัทต้องชดใช้ค่าเสียหาย สูญเสียรายได้ หรือเกิดค่าใช้จ่ายในการกู้คืนระบบ มากกว่า 5 ล้านบาท แต่ไม่เกิน 50 ล้านบาท รวมถึงค่าปรับหรือค่าเสียหายที่เกี่ยวข้องกับ PDPA, GDPR หรือกฎหมายทรัพย์สินทางปัญญา	ข้อมูลได้รับความเสียหายหรือเกิดข้อผิดพลาดเล็กน้อย แต่ไม่ส่งผลกระทบต่อการผลิต การส่งมอบสินค้า หรือข้อมูลสำคัญของลูกค้า	ระบบทำงานช้าหรือมีข้อผิดพลาดเล็กน้อยบางประการ ส่งผลกระทบเล็กน้อยต่อการดำเนินงาน และใช้เวลาในการกู้คืนหรือแก้ไขปัญหาระหว่าง 4–12 ชั่วโมง	อาจส่งผลกระทบต่อการปฏิบัติตามกฎหมาย ขัดต่อนโยบายหรือกฎระเบียบข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ โดยละเมิดเพียงวงจำกัดภายในและไม่ส่งผลต่อการดำเนินธุรกิจ
1	ทำให้บริษัทเกิดค่าใช้จ่ายหรือความเสียหายทางการเงินไม่เกิน 5 ล้านบาท รวมถึงค่าปรับหรือค่าเสียหายที่เกี่ยวข้องกับ PDPA, GDPR หรือกฎหมายทรัพย์สินทางปัญญา	ข้อมูลไม่เสียหาย ไม่สูญหาย และไม่ส่งผลกระทบต่อการผลิต การส่งมอบสินค้า หรือความเชื่อมั่นของลูกค้า	ไม่มีผลกระทบต่อการดำเนินงานหลักของบริษัท หรือสามารถกู้คืนและแก้ไขปัญหาได้ภายใน 4 ชั่วโมง	ไม่ส่งผลกระทบต่อกฎหมาย นโยบายหรือกฎระเบียบข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

04 รายงานผลการจัดระดับชั้นของข้อมูลและการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูล

4.2 โอกาสเกิด (Likelihood)

ระดับ	คะแนน	เกณฑ์การวัด
เกิดค่อนข้างแน่นอน	5	ใช้ข้อมูลทุกวัน หรือทุกสัปดาห์
น่าจะเกิด	4	ใช้ข้อมูลภายในระยะเวลา 1 เดือน
เป็นไปได้ที่จะเกิด	3	ใช้ข้อมูลภายในระยะเวลา 1 ปี
ไม่น่าจะเกิด	2	ใช้ข้อมูลภายในระยะเวลา 2-5 ปี
ยากที่จะเกิด	1	ใช้ข้อมูลภายในระยะเวลา 5 ปีขึ้นไป

4.3 ตารางความเสี่ยง (Risk Matrix)

ค่าความเสี่ยง = โอกาสเกิด (Likelihood) × ระดับผลกระทบสูงสุด (Max Impact)

โอกาส / ผลกระทบ	น้อยมาก (1)	น้อย (2)	ปานกลาง (3)	มาก (4)	มากมาก (5)
ค่อนข้างแน่นอน (5)	5	10	15	20	25
น่าจะเกิด (4)	4	8	12	16	20
เป็นไปได้ (3)	3	6	9	12	15
ไม่น่าจะเกิด (2)	2	4	6	8	10
ยากที่จะเกิด (1)	1	2	3	4	5

รายงานผลการจัดระดับชั้นของข้อมูลและการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูล

4.4 ผลการวิเคราะห์และจัดระดับชั้นของข้อมูล (Data Classification Level)

จากตารางแสดงผลสรุปการวิเคราะห์และจัดระดับชั้นของข้อมูล (Data Classification Level) ในภาพรวมตามฝ่ายงาน / แผนก ทั้งหมด 26 หน่วยงาน โดยพิจารณาจากชั้นความลับ 4 ประเภท เช่น เปิดเผยได้ (Public), ภายใน (Internal Use), ลับ (Confidential) และลับมาก (Top Secret)

ลำดับ	ฝ่ายงาน / แผนก	ชั้นความลับ			
		เปิดเผยได้ (Public)	ภายใน (Internal Use)	ลับ (Confidential)	ลับมาก (Top Secret)
1	BIZ	11	9	0	1
2	BOI	6	6	0	1
3	ED-G	0	16	0	9
4	DCC	0	25	0	1
5	F&A	1	5	1	1
6	FG	0	24	0	2
7	Film-G	N/A	N/A	N/A	N/A

ลำดับ	ฝ่ายงาน / แผนก	ชั้นความลับ			
		เปิดเผยได้ (Public)	ภายใน (Internal Use)	ลับ (Confidential)	ลับมาก (Top Secret)
8	GAG	0	32	0	0
9	HQS	50	4	3	1
10	ADM (HR)	0	19	5	3
11	ADM (HR-G Training)	0	18	0	0
12	IA	0	109	0	10
13	MIS	0	72	6	2

หมายเหตุ: *N/A หมายถึงไม่สามารถระบุข้อมูลได้*

รายงานผลการจัดระดับชั้นของข้อมูลและการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูล

4.5 ผลการวิเคราะห์และจัดระดับชั้นของข้อมูล (Data Classification Level) (ต่อ)

ลำดับ	ฝ่ายงาน / แผนก	ชั้นความลับ			
		เปิดเผยได้ (Public)	ภายใน (Internal Use)	ลับ (Confidential)	ลับมาก (Top Secret)
14	ADM (payroll)	0	6	1	4
15	PC-G	0	5	0	1
16	PE-G (Film-G)	0	27	0	0
17	Front2-G	N/A	N/A	N/A	N/A
18	MFG (Front, Middle, Back)	0	24	0	0
19	MFG (Front Scale)	0	8	0	0
20	PUR	1	23	3	0
21	QAA3	0	18	0	0
22	QCA3	0	65	0	0
23	R&D	0	71	6	0
24	SQE	3	4	0	0
25	ST-G	0	14	0	0
26	WMD	6	4	5	0

หมายเหตุ: *N/A หมายถึงไม่สามารถระบุข้อมูลได้*

04 รายงานผลการจัดระดับชั้นของข้อมูลและการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูล

4.6 รายละเอียดผลการวิเคราะห์ และจัดระดับชั้นของข้อมูล (Data Classification Level)

แยกตามฝ่ายงาน / แผนกโดยรายละเอียดประกอบด้วย ชื่อข้อมูล, ระดับชั้นความลับ, แหล่งที่จัดเก็บ และระยะเวลาเก็บรักษา

(ตัวอย่างข้อมูลของฝ่าย MIS)

ลำดับ	ชื่อข้อมูล	ชั้นความลับ	แหล่งจัดเก็บ	ระยะเวลาเก็บรักษา
1	ISMS-FM-01-MIS	ภายใน (Internal Use)	E-Drive	ย้อนหลัง 1 เวอร์ชัน
2	ISMS-PC-01-MIS	ภายใน (Internal Use)	E-Drive	ย้อนหลัง 1 เวอร์ชัน
3	ISMS-MG-01-MIS	ภายใน (Internal Use)	E-Drive	ย้อนหลัง 1 เวอร์ชัน
4	ISMS-MG-02-MIS	ภายใน (Internal Use)	E-Drive	ย้อนหลัง 1 เวอร์ชัน
5	ISMS-MG-03-MIS	ภายใน (Internal Use)	E-Drive	ย้อนหลัง 1 เวอร์ชัน

หมายเหตุ: *เนื้อหาที่แสดง เป็นเพียงตัวอย่าง 5 ข้อมูล โดยสามารถดูเนื้อหาฉบับเต็มได้ที่เอกสาร Data_Classification_Risk_Report_r6*

รายงานผลการจัดระดับชั้นของข้อมูลและการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูล

4.7 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูล

ตารางต่อไปนี้แสดงถึงผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูล ในภาพรวมตามฝ่ายงาน / แผนก โดยพิจารณาจากความสัมพันธ์ของผลกระทบ 4 ด้าน (*F=Financial, C=Customer, O=Operations, L=Legal & Regulations)* และความถี่ที่อาจจะเกิดขึ้น (Likelihood) โดยพิจารณามาตรการควบคุมด้านความมั่นคงปลอดภัยในการบริหารจัดการข้อมูลประกอบ และผลลัพธ์การประเมินสามารถสรุปได้ในรูปแบบความเสี่ยง 4 ระดับ (สูงมาก, สูง, ปานกลาง และต่ำ)

(ตัวอย่างข้อมูลของฝ่าย MIS)

ลำดับ	ชื่อข้อมูล	F	C	O	L	Likelihood	ระดับความเสี่ยง
1	ISMS-FM-01-MIS	1	1	1	1	3	3 — ต่ำ
2	ISMS-PC-01-MIS	1	1	1	1	3	3 — ต่ำ
3	Source code (Outsource)	2	2	2	1	5	10 — สูง
4	Database (Production)	2	2	3	3	5	15 — สูง
5	Database (Test)	1	1	1	1	5	5 — ต่ำ

หมายเหตุ: *เนื้อหาที่แสดง เป็นเพียงตัวอย่าง 5 ข้อมูล โดยสามารถดูเนื้อหาฉบับเต็มได้ที่เอกสาร Data_Classification_Risk_Report_r6*

รายงานผลการจัดระดับชั้นของข้อมูลและการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูล

4.8 การจัดการความเสี่ยงของข้อมูลแยกตามฝ่ายงาน (ตัวอย่างข้อมูลของฝ่าย MIS)

ลำดับ	ชื่อข้อมูล	ระดับ	มาตรการควบคุมที่แนะนำ
1	ISMS-FM-06-MIS	**สูง**	▪ กำหนดให้มีการเข้ารหัสข้อมูล (Data Encryption) ของระบบที่มีการจัดเก็บข้อมูล เพื่อป้องกันข้อมูลรั่วไหลจากการเข้าถึงโดยไม่ได้รับอนุญาต
2	Source code (Internal)	**สูง**	▪ กำหนดให้มีการจำกัดสิทธิ์การเข้าถึงเฉพาะผู้ที่เข้าถึงได้เท่านั้น ▪ ควบคุมการเข้าถึงพื้นที่ในการจัดเก็บเอกสารในรูปแบบ Hard copy โดยกำหนดให้เฉพาะผู้ที่มีสิทธิ์สามารถเข้าถึงได้เท่านั้น
3	Source code (Outsource)	**สูง**	▪ กำหนดให้มีการจำกัดสิทธิ์การเข้าถึงเฉพาะผู้ที่เข้าถึงได้เท่านั้น ▪ ควบคุมการเข้าถึงพื้นที่ในการจัดเก็บเอกสารในรูปแบบ Hard copy โดยกำหนดให้เฉพาะผู้ที่มีสิทธิ์สามารถเข้าถึงได้เท่านั้น
4	Database (Production)	**สูง**	▪ กำหนดให้มีการเข้ารหัสข้อมูล (Data Encryption) ของระบบที่มีการจัดเก็บข้อมูล เพื่อป้องกันข้อมูลรั่วไหลจากการเข้าถึงโดยไม่ได้รับอนุญาต
5	ระบบ EMIS - ข้อมูล Passport	**สูง**	▪ กำหนดให้มีการเข้ารหัสข้อมูล (Data Encryption) ของระบบที่มีการจัดเก็บข้อมูล เพื่อป้องกันข้อมูลรั่วไหลจากการเข้าถึงโดยไม่ได้รับอนุญาต
6	ระบบ VMS – ข้อมูลผู้ติดต่อ	**สูง**	▪ กำหนดให้มีการเข้ารหัสข้อมูล (Data Encryption) ของระบบที่มีการจัดเก็บข้อมูล เพื่อป้องกันข้อมูลรั่วไหลจากการเข้าถึงโดยไม่ได้รับอนุญาต

APEX

INSEC