สพร./PRD
พฤษภาคม 2565

มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัลอยู่ระหว่างการจัดทำ
ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน

มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัลฉบับสมบูรณ์จะมีประกาศโดย
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ร่าง

มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
DGA Community Standard

ว่าด้วยร่างหลักเกณฑ์การจัดชั้นความลับและแบ่งปันข้อมูลภาครัฐ

(GOVERNMENT DATA CLASSIFICATION AND DATA SHARING FRAMEWORK)

สำหรับเสนอคณะกรรมการจัดทำร่างมาตรฐานพิจารณา

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ชั้น 17 อาคารบางกอกไทยทาวเวอร์ 108 ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ 10400
หมายเลขโทรศัพท์: 0 2612 6000 โทรสาร: 0 2612 6011 0 2612 6012

มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

DGA Community Standard

มสพร. X-2565

DGA X-2565

ว่าด้วยร่างหลักเกณฑ์การจัดชั้นความลับและแบ่งปันข้อมูลภาครัฐ

(GOVERNMENT DATA CLASSIFICATION AND DATA SHARING FRAMEWORK)

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักนายกรัฐมนตรี

มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ว่าด้วยร่างหลักเกณฑ์การจัดชั้นความลับและแบ่งปันข้อมูลภาครัฐ

มสพร. X-2565

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ชั้น 17 อาคารบางกอกไทยทาวเวอร์
108 ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ 10400
หมายเลขโทรศัพท์: (+66) 0 2612 6000 โทรสาร: (+66) 0 2612 6011

ประกาศโดย
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักนายกรัฐมนตรี

วันที่ ระบุวันที่ประกาศ

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย

กรรมการ

นายเฉลิมชัย ก๊กเกียรติกุล	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายมารุต บูรณรัช	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวปศิญา เชื้อดี	สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ
นายศุภโชค จันทรประทิน นางสาวพลอย เจริญสม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นางบุญยิ่ง ชั่งสัจจา	สำนักบริหารการทะเบียน กรมการปกครอง
นายณัฏฐา พาชัยยุทธ	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นายพัชโรดม ลิมปิษเฐียร นางสาวพัชรี ไชยเรืองกิตติ	สำนักงานคณะกรรมการกฤษฎีกา
นายกฤษณ์ โกวิทพัฒนา	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ และสังคมแห่งชาติ
นายสันติ สิทธิเลิศพิศาล	สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นายวีระ วีระกุล	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
นายวิทยา สุหฤทดำรง	วิศกรรมสถานแห่งประเทศไทย ในพระบรมราชูปถัมภ์

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการข้อมูลภาครัฐ

ที่ปรึกษา

นายสุพจน์ เธียรวุฒิ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	ประธานคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

ประธานคณะทำงาน

รองศาสตราจารย์ธีรณี อจลากุล	ผู้อำนวยการสถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ

รองประธานกรรมการ

ผู้ช่วยศาสตราจารย์โษฑศ์รัตต ธรรมบุษดี	มหาวิทยาลัยมหิดล

คณะทำงาน

นางสาวปศิญา เชื้อดี	สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ
นางสุนทรีย์ ส่งเสริม	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นายมารุต บูรณรัช	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวปริสุทธิ์ จิตต์ภักดี	สถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ
นางกาญจนา ภู่มาลี	สำนักงานสถิติแห่งชาติ
นายสารตรัย วัชราภรณ์	
นายพีรณัฐ แดงสกุล	สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ
นายณัฏฐา พาชัยยุทธ	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นางวณิสรา สุขวัฒน	
นางสาวธัญลักษณ กริตาคม	สำนักข่าวกรองแห่งชาติ
นายไผท สิทธิสุนทร	สำนักงานสภาความมั่นคงแห่งชาติ
นางสาวฐิติรัตน์ ทิพย์สัมฤทธิ์กุล	มหาวิทยาลัยธรรมศาสตร์
นายชรินทร์ ธีรฐิติยากูร	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายมนต์ศักดิ์ โซ่เจริญธรรม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาวนพจิตร เหลืองช่อสิริ	

ร่างหลักเกณฑ์การจัดชั้นความลับและแบ่งปันข้อมูลภาครัฐ (Government Data Classification and Data Sharing Framework) ฉบับนี้ขึ้น เพื่อใช้เป็นเกณฑ์พิจารณากำหนดชั้นความลับสำหรับทุกชุดข้อมูล (Dataset) ของหน่วยงานภาครัฐ และเพื่อลดการใช้ดุลพินิจของผู้มีอำนาจในการตัดสินใจกำหนดชั้นความลับของข้อมูล สามารถกำหนดการเข้าถึงและใช้งานข้อมูลและกำกับดูแลข้อมูลที่มีความอ่อนไหวหรือมีชั้นความลับอย่างเหมาะสมเพื่อรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล รวมทั้งกำหนดนโยบายการแบ่งปันข้อมูลระหว่างหน่วยงานภาครัฐโดยไม่ขัดต่อข้อกฎหมายที่เกี่ยวข้อง ทั้งนี้ เพื่อใช้ประโยชน์จากข้อมูลร่วมกันในการพัฒนาบริการและนวัตกรรมที่จะเป็นประโยชน์ต่อประเทศในด้านต่าง ๆ โดยหลักเกณฑ์ฉบับนี้ได้จัดทำตามมาตรฐานและแนวทางแห่ง

1. มาตรฐาน NIST 800-60 Volume 1. and 2. : Guide for Mapping Types of Information and Information Systems to Security Categories
2. มาตรฐาน FIPS PUB 199 : Standards for Security Categorization of Federal Information and Information Systems
3. มาตรฐาน ISO/IEC 27001: 2013 Information technology - Security techniques - Information security management systems – Requirements
4. Australian Government, Best Practice Guide to Applying Data Sharing Principles

และได้มีการจัดงานประชาพิจารณ์เพื่อเปิดรับฟังความคิดเห็นเป็นการทั่วไป และนำข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อให้ข้อเสนอแนะเกี่ยวกับมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วน และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ร่างหลักเกณฑ์การจัดชั้นความลับและแบ่งปันข้อมูลภาครัฐฉบับนี้จัดทำโดยฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สำนักนายกรัฐมนตรี

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ชั้น 17 อาคารบางกอกไทยทาวเวอร์
108 ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ 10400
หมายเลขโทรศัพท์: (+66) 0 2612 6000 โทรสาร: (+66) 0 2612 6011
E-mail: sd-g_division@dga.or.th
Website: www.dga.or.th

คำนำ

ปัจจุบันองค์กรทั่วโลกต่างให้ความสำคัญกับการรวบรวม จัดการ และใช้ประโยชน์จากข้อมูลเพิ่มมากขึ้นเรื่อย ๆ เพื่อปรับปรุงบริการหลักของตน อีกทั้งจำเป็นปฏิบัติตามข้อกฎหมาย กฎระเบียบและมาตรฐานการกำกับดูแลที่เพิ่มมากขึ้น เนื่องจากตระหนักดีว่าข้อมูลถือเป็นสินทรัพย์ที่สำคัญ (Data as Asset) ที่จะช่วยเพิ่มประสิทธิภาพในการทำงาน ช่วยในการวิเคราะห์ วางแผนและตัดสินใจเชิงนโยบาย และอำนวยความสะดวกในการให้บริการ ส่งผลให้องค์กรจำเป็นต้องมีกระบวนการป้องกันความปลอดภัยของข้อมูล โดยมีขั้นตอนสำคัญคือ การจำแนกหมวดหมู่และจัดชั้นความลับของข้อมูล เพื่อรับทราบการเข้าถึงและใช้ข้อมูล การลดความเสี่ยงภัยที่จะเกิดกับข้อมูล และการระบุชั้นความลับของข้อมูลจะช่วยให้หน่วยงานสามารถแบ่งปันข้อมูลทั้งภายในและภายนอกองค์กรได้ ดังนั้น การกำกับดูแลข้อมูลที่ดีต้องการให้องค์กรรักษาประสิทธิภาพการทำงานได้เพิ่มมากขึ้น ในขณะเดียวกันต้องมีการจัดการข้อมูลอ่อนไหว (Sensitive Data) อย่างเหมาะสมและเป็นไปตามข้อกฎหมายที่เกี่ยวข้อง

ประกอบกับหน่วยงานภาครัฐมีความจำเป็นต้องมีระบบบริหารและกระบวนการจัดการและคุ้มครองข้อมูลที่ครบถ้วน ตั้งแต่การจัดทำ การจัดเก็บ การจำแนกหมวดหมู่ การประมวลผลหรือใช้ข้อมูล การปกปิดหรือเปิดเผยข้อมูล การตรวจสอบ และการทำลาย ซึ่งเป็นไปตามมาตรา 8 แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 และประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ข้อ 4 (5) จำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ อันจะนำไปสู่การพัฒนาระบบข้อมูลที่สำคัญของภาครัฐเพื่อประโยชน์ในการกำหนดหลักเกณฑ์และวิธีการเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลของหน่วยงานของรัฐอย่างเป็นระบบ ตลอดจนการพัฒนาศูนย์กลางข้อมูลเปิดภาครัฐเพื่อให้ประชาชนสามารถเข้าถึงและใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

ในการนี้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) จึงได้จัดทำเอกสาร **ร่างหลักเกณฑ์การจัดชั้นความลับและแบ่งปันข้อมูลภาครัฐ (Government Data Classification and Data Sharing Framework)** ฉบับนี้ขึ้น เพื่อใช้เป็นเกณฑ์พิจารณากำหนดชั้นความลับสำหรับทุกชุดข้อมูล (Dataset) ของหน่วยงานภาครัฐ และเพื่อลดการใช้ดุลพินิจของผู้มีอำนาจในการตัดสินใจกำหนดชั้นความลับของข้อมูล สามารถกำหนดการเข้าถึงและใช้งานข้อมูลและกำกับดูแลข้อมูลที่มีความอ่อนไหวหรือมีชั้นความลับอย่างเหมาะสมเพื่อรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล รวมทั้งกำหนดนโยบายการแบ่งปันข้อมูลระหว่างหน่วยงานภาครัฐโดยไม่ขัดต่อข้อกฎหมายที่เกี่ยวข้อง ทั้งนี้ เพื่อใช้ประโยชน์จากข้อมูลร่วมกันในการพัฒนาบริการและนวัตกรรมที่จะเป็นประโยชน์ต่อประเทศในด้านต่าง ๆ

สารบัญ

สารบัญภาพ

มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยร่างหลักเกณฑ์การจัดชั้นความลับและแบ่งปันข้อมูลภาครัฐ (Government Data Classification and Data Sharing Framework)

1. บทนำ

1.1 ความเป็นมา

ปัจจุบันองค์กรทั่วโลกทั้งภาครัฐและภาคเอกชนต่างให้ความสำคัญกับการรวบรวม จัดการ และใช้ประโยชน์จากข้อมูลเพิ่มมากขึ้นเรื่อย ๆ เพื่อปรับปรุงบริการหลักของตน อีกทั้งจำเป็นต้องปฏิบัติตามข้อกฎหมาย กฎระเบียบและมาตรฐานการกำกับดูแลที่เพิ่มมากขึ้น เนื่องจากตระหนักดีว่าข้อมูลถือเป็นสินทรัพย์ที่สำคัญ (Data as Asset) ซึ่งการรวบรวมและการใช้ข้อมูลจะช่วยเพิ่มประสิทธิภาพในการทำงาน ช่วยในการวิเคราะห์ วางแผน ตัดสินใจเชิงนโยบาย และอำนวยความสะดวกในการให้บริการ ตลอดจนเป้าหมายอื่น ๆ ตามแผนการพัฒนาของประเทศ ทำให้องค์กรจำเป็นต้องมีกระบวนการป้องกันความปลอดภัยของข้อมูล โดยมีขั้นตอนสำคัญคือ การจำแนกหมวดหมู่และจัดชั้นความลับของข้อมูล เพื่อรับทราบการเข้าถึงและใช้ข้อมูล การลดความเสี่ยงภัยที่จะเกิดกับข้อมูล และการระบุชั้นความลับของข้อมูลจะช่วยให้หน่วยงานสามารถแบ่งปันข้อมูลทั้งภายในและภายนอกองค์กรได้ ในขณะที่หน่วยงานที่กำกับดูแลต้องคอยตรวจสอบวิธีการใช้ข้อมูลให้เป็นไปตามข้อกฎหมายที่เกี่ยวข้อง องค์กรยังต้องสามารถเข้าถึงและใช้ข้อมูลได้อย่างรวดเร็วเพื่อรักษาความสามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล จึงต้องการให้แน่ใจว่ากำลังรักษาความปลอดภัยข้อมูลเพื่อปกป้องผลประโยชน์ขององค์กรและคุ้มครองความเป็นส่วนตัวของผู้มีส่วนเกี่ยวข้อง ดังนั้น การกำกับดูแลข้อมูลที่ดีต้องการให้องค์กรรักษาประสิทธิภาพการทำงานได้เพิ่มมากขึ้น ในขณะเดียวกันต้องมีการจัดการข้อมูลที่มีความอ่อนไหว (Sensitive Data) อย่างเหมาะสมเพื่อรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการ การบูรณาการข้อมูลภาครัฐ การทำงานให้มีความสอดคล้องกัน การเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล และตามมาตรฐาน 8 ธรรมาภิบาลข้อมูลภาครัฐต้องประกอบด้วยอย่างน้อย (2) การมีระบบบริหารและกระบวนการจัดการและคุ้มครองข้อมูลที่ครบถ้วน ตั้งแต่การจัดทำ การจัดเก็บ การจำแนกหมวดหมู่ การประมวลผลหรือใช้ข้อมูล การปกปิดหรือเปิดเผยข้อมูล การตรวจสอบ และการทำลาย และประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ [1] ข้อ 4 (5) การจำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) จึงได้จัดทำเอกสาร ร่างหลักเกณฑ์การจัดชั้นความลับและการแบ่งปันข้อมูลภาครัฐ เพื่อให้หน่วยงานภาครัฐใช้เป็นเกณฑ์พิจารณาจำแนกและจัดชั้นความลับของข้อมูล (Data Classification) ระบุหมวดหมู่และชั้นความลับของข้อมูล กำหนดการเข้าถึงและใช้งานข้อมูล (Access Control) และกำกับดูแลข้อมูลที่มีคุณค่าขององค์กร เพื่อให้สามารถบรรลุเป้าหมายด้านความเป็นส่วนตัว (Privacy) และความปลอดภัย (Security) ของข้อมูล รวมทั้งสามารถใช้งานข้อมูลได้อย่างถูกต้องเหมาะสม ตลอดจนสามารถแบ่งปันข้อมูล (Data Sharing) ระหว่างหน่วยงานภาครัฐโดยไม่ขัดต่อข้อกฎหมายที่เกี่ยวข้อง ทั้งนี้ เพื่อใช้ประโยชน์จากข้อมูลร่วมกันในการพัฒนาบริการและนวัตกรรมที่จะเป็นประโยชน์ต่อประเทศในด้านต่าง ๆ

1.2 ขอบข่าย

ร่างหลักเกณฑ์การจัดชั้นความลับและการแบ่งปันข้อมูลภาครัฐฉบับนี้จัดทำขึ้นเพื่อให้หน่วยงานภาครัฐนำไปใช้เป็นเกณฑ์พิจารณาจำแนกและจัดชั้นความลับของข้อมูล ระบุหมวดหมู่และชั้นความลับของข้อมูล กำหนดการเข้าถึงและใช้งานข้อมูล กำกับดูแลและแบ่งปันข้อมูลของหน่วยงานให้สอดคล้องตามแนวทางในประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่อง ธรรมาภิบาลข้อมูลภาครัฐ โดยแนวทางฉบับนี้ได้จัดทำตามแนวมาตรฐานและแนวปฏิบัติที่ดีของ

1.2.1 มาตรฐาน NIST 800-60 Volume 1. and 2. : Guide for Mapping Types of Information and Information Systems to Security Categories [2]

1.2.2 มาตรฐาน FIPS PUB 199 : Standards for Security Categorization of Federal Information and Information Systems [3]

1.2.3 มาตรฐาน ISO/IEC 27001: 2013 Information technology - Security techniques - Information security management systems – Requirements [4]

1.2.4 Australian Government, Best Practice Guide to Applying Data Sharing Principles [5]

โดยร่างหลักเกณฑ์ฯ ที่จัดทำขึ้นนี้ แบ่งออกเป็น 2 ส่วนหลักได้แก่ กรอบแนวคิด และ หลักเกณฑ์การจัดชั้นความลับและการแบ่งปันข้อมูลภาครัฐ ประกอบด้วย เป้าประสงค์ ขอบเขต เกณฑ์การจัดชั้นความลับและการแบ่งปันข้อมูลภาครัฐ บทบาทและความรับผิดชอบ และแนวทางสู่การปฏิบัติ ซึ่งสามารถใช้เป็นเกณฑ์พิจารณากำหนดชั้นความลับสำหรับทุกชุด**ข้อมูลที่แลกเปลี่ยนกันได้ในรูปแบบอิเล็กทรอนิกส์ทุกประเภท ซึ่งรวมถึงข้อมูลลับในรูปแบบอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ โดยจะไม่ครอบคลุมเอกสารที่เป็นกระดาษทุกประเภท** เพื่อลดการใช้ดุลพินิจของผู้มีอำนาจในการตัดสินใจกำหนดชั้นความลับของข้อมูล เพื่อให้หน่วยงานสามารถกำหนดการเข้าถึงและใช้งานข้อมูลและกำกับดูแลข้อมูลที่มีความอ่อนไหวหรือมีชั้นความลับอย่างเหมาะสมเพื่อรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล **ซึ่งจะช่วยให้หน่วยงานของรัฐสามารถจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจของหน่วยงาน ได้อย่างมีประสิทธิภาพ** รวมทั้งกำหนดนโยบายการแบ่งปันข้อมูลระหว่างหน่วยงานภาครัฐโดยไม่ขัดต่อข้อกฎหมายที่เกี่ยวข้อง ทั้งนี้ หน่วยงานสามารถกำหนดเกณฑ์พิจารณาเพิ่มเติมให้สอดคล้องกับแนวนโยบายข้อมูลและระบบจัดเก็บข้อมูล (Legacy System) ของหน่วยงานได้ตามความเหมาะสม

ในกรณีของข้อมูลมั่นคงที่ส่งกระทบอย่างร้ายแรงต่อผลประโยชน์แห่งชาติหรือการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข หรือความปลอดภัยของประเทศ ให้หน่วยงานดำเนินการตามกฎหมายเฉพาะที่เกี่ยวข้อง เช่น พระราชบัญญัติข้อมูลข่าวสารของราชการฯ ระเบียบว่าด้วย การรักษาความลับของทางราชการ พ.ศ. 2544 ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 และระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552

1.3 บทนิยาม

จากการทบทวนนิยามศัพท์ที่เกี่ยวข้องจากประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2562-2565) รวมทั้งกรอบแนวคิดและมาตรฐานที่เกี่ยวข้องทั้งในและต่างประเทศ ได้ข้อสรุปความหมายของการจัดชั้นความลับและแบ่งปันข้อมูล และคำศัพท์อื่น ๆ ที่เกี่ยวข้องดังนี้

1.3.1 **การจัดชั้นความลับของข้อมูล (Data Classification)** หมายความว่า การจำแนกชั้นของข้อมูลในบริบทของการรักษาความปลอดภัยข้อมูลตามระดับของความอ่อนไหวและผลกระทบต่อบุคคล องค์กร และ

ประเทศ หากมีการเปิดเผย เปลี่ยนแปลง หรือทำลายข้อมูลโดยไม่ได้รับอนุญาต โดยการจัดชั้นความลับของข้อมูลช่วยกำหนดการควบคุมความปลอดภัยพื้นฐานที่เหมาะสมสำหรับการปกป้องข้อมูลนั้น ๆ ทั้งนี้ ข้อมูลสำคัญของบุคคล องค์กร และประเทศทั้งหมด ควรจัดชั้นตามระดับความอ่อนไหวหนึ่งในห้าระดับชั้นความลับของข้อมูลหรือตามที่หน่วยงานกำหนด เพื่อให้หน่วยงานของรัฐสามารถจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ

1.3.2 **ข้อมูลอ่อนไหว (Sensitive Data) หมายความว่า** ข้อมูลอ่อนไหวเป็นข้อมูลที่มีชั้นความลับและเป็นข้อมูลเกี่ยวข้องกับความมั่นคงที่ต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อคุ้มครองความเป็นส่วนตัว (privacy) หรือความปลอดภัย (security) ของบุคคลหรือองค์กร ซึ่งหากข้อมูลอ่อนไหวมีการเปิดเผยโดยไม่ได้รับอนุญาต จะมีแนวโน้มที่จะนำไปสู่ผลที่ไม่พึงประสงค์หรือส่งผลกระทบต่อ บุคคล หน่วยงาน องค์กร หรือ ประเทศ ตัวอย่างเช่น ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) ข้อมูลที่เกี่ยวข้องกับด้านความมั่นคง กฎหมาย เศรษฐกิจ การพาณิชย์

1.3.3 **ระดับชั้นความลับของข้อมูล (Data Classification Level)** หมายความว่า ระดับชั้นความลับของข้อมูลภาครัฐเพื่อจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจ โดยข้อมูลที่มีความอ่อนไหวแบ่งออกเป็น ชั้นเปิดเผย (Open) ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) ชั้นลับมาก (Secret) และ ชั้นลับที่สุด (Top Secret) **ซึ่งระดับชั้นความลับที่เป็น ชั้นลับ (Confidential) ชั้นลับมาก (Secret) และ ชั้นลับที่สุด (Top Secret) เป็นเพียงการจัดระดับชั้นข้อมูล ไม่ใช่การกำหนดให้ข้อมูลนั้นเป็นข้อมูลข่าวสารลับตามระเบียบการรักษาความลับทางราชการ**

1.3.4 **การแบ่งปันข้อมูล (Data sharing)** หมายความว่า การทำให้ข้อมูลพร้อมใช้งานสำหรับหน่วยงาน องค์กร หรือบุคคลอื่นภายใต้เงื่อนไขที่ตกลงกันไว้ หรือ การอ้างอิงสำหรับใช้ในการแบ่งปันข้อมูล (shared) แลกเปลี่ยนข้อมูล (exchangeable) และนำข้อมูลไปต่อยอด (extensible) เพื่อการสนับสนุนโครงสร้างพื้นฐานของกลุ่มผู้ใช้งานหรือผู้ใช้บริการแฟลตฟอร์ม (community infrastructure)

1.3.5 **ข้อมูลแบ่งปัน (Shared data)** หมายความว่า ข้อมูลสำคัญที่สอดคล้องกับยุทธศาสตร์ข้อมูล (Data Strategy) ภารกิจหลักและเป้าหมายของหน่วยงานและประเทศ รวมถึงข้อมูลอ่อนไหวที่ได้รับการจัดชั้นความลับในระดับ เผยแพร่ภายในองค์กร ลับ และลับมาก **ยกเว้นข้อมูลที่มีชั้นความลับมากที่สุด** ซึ่งสามารถแบ่งปันและแลกเปลี่ยนกันได้ระหว่างหน่วยงาน โดยจำเป็นต้องมีการกำหนดสิทธิในการเข้าถึงและใช้งาน รวมถึงการคุ้มครองข้อมูลให้มีความมั่นคงปลอดภัย

1.3.6 **นายทะเบียนข้อมูลข่าวสารลับ** หมายความว่า เจ้าหน้าที่ผู้ได้รับแต่งตั้งจากหัวหน้าหน่วยงานของรัฐเพื่อทำหน้าที่ควบคุมและรับผิดชอบการดำเนินการเกี่ยวกับข้อมูลข่าวสารลับขึ้นภายในหน่วยงานที่ตนรับผิดชอบ

1.3.7 **นายทะเบียนบัญชีข้อมูลหน่วยงาน** หมายความว่า หัวหน้าหน่วยงาน หรือผู้ที่ได้รับมอบหมาย ทำหน้าที่กำกับ ดูแล การลงทะเบียนบัญชีข้อมูลหน่วยงาน การตรวจสอบและแก้ไขบัญชีข้อมูลหน่วยงาน การเพิกถอนการลงทะเบียนบัญชีข้อมูลหน่วยงาน และอนุญาตใช้และเปิดเผยทะเบียนบัญชีข้อมูลของหน่วยงาน

สำหรับนิยามศัพท์ที่เกี่ยวข้องกับร่างหลักเกณฑ์ฯ ฉบับนี้ สามารถดูรายละเอียดได้ที่ ***อภิธานศัพท์***

1.4 กฎหมายและแนวทางที่เกี่ยวข้อง

1.4.1 พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540

1.4.2 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

1.4.3 ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และที่แก้ไขเพิ่มเติม

1.4.4 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มาตรา 7 และมาตรา 8 ธรรมาภิบาลข้อมูลภาครัฐ

1.4.5 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.4.6 นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2562-2565)

1.4.7 ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ข้อ 4 ธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน (5) การจำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ

2. กรอบแนวคิด

2.1 สถานการณ์ด้านการจัดชั้นความลับและการแบ่งปันข้อมูล

2.1.1 ความสำคัญ

การจัดชั้นความลับของข้อมูลมีการปรับปรุงอย่างมีนัยสำคัญ ซึ่งปัจจุบันมีการนำมาใช้เพื่อวัตถุประสงค์ที่หลากหลาย โดยปกติมักเพื่อสนับสนุนในการริเริ่มด้านความปลอดภัยของข้อมูล แต่ข้อมูลอาจถูกจัดชั้นความลับด้วยเหตุผลหลายประการ รวมถึงความสะดวกในการเข้าถึง การรักษาการปฏิบัติตามกฎระเบียบ และเพื่อให้เป็นไปตามวัตถุประสงค์ของการดำเนินภารกิจขององค์กรหรือส่วนบุคคลอื่น ๆ ซึ่งในบางกรณีการจัดชั้นความลับของข้อมูลถือเป็นข้อกำหนดด้านกฎระเบียบ เนื่องจากข้อมูลจะต้องสามารถค้นหาและเรียกค้นคืนได้ภายในกรอบเวลาที่กำหนดเพื่อวัตถุประสงค์ในการรักษาความปลอดภัยข้อมูล ดังนั้น การจัดชั้นความลับของข้อมูลจึงถือเป็นพื้นฐานสำคัญสำหรับกลยุทธ์ด้านความปลอดภัยของข้อมูล เนื่องจากช่วยระบุขอบเขตความเสี่ยงในการกำกับดูแลโครงสร้างพื้นฐานระบบเทคโนโลยีสารสนเทศ ทั้งภายในองค์กรและบนระบบคลาวด์ และเป็นประโยชน์ในการอำนวยความสะดวกเพื่อตอบสนองด้านความปลอดภัยที่เหมาะสมตามประเภทของข้อมูลที่ถูกเรียกดู ส่งต่อ หรือคัดลอก โดยกระบวนการจัดชั้นความลับของข้อมูลอาจมีความแตกต่างกันขึ้นอยู่กับวัตถุประสงค์ และจำเป็นต้องใช้ระบบอัตโนมัติเพื่อประมวลผลข้อมูลที่มีอยู่จำนวนมหาศาลที่ถูกสร้างขึ้นทุกวัน นอกเหนือจากข้อกังวลด้านความปลอดภัยของข้อมูลดังกล่าวแล้ว อาจมีสาเหตุสำคัญหลายประการสำหรับการนำกระบวนการจัดชั้นความลับของข้อมูลไปใช้ เช่น การระบุไฟล์ที่มีความอ่อนไหว ทรัพย์สินทางปัญญา และความลับทางการค้า การรักษาความปลอดภัย (และปกปิด) ของข้อมูลที่สำคัญ การติดตามข้อมูลที่ได้รับการควบคุมเพื่อให้เป็นไปตามข้อกฎหมายที่เกี่ยวข้อง อาทิ HIPAA PCI GDPR และ PDPA เพื่อเพิ่มประสิทธิภาพการค้นหาด้วยการสร้างดัชนีข้อมูล การค้นพบรูปแบบหรือแนวโน้มข้อมูลเชิงลึกที่มีนัยสำคัญทางสถิติ และเพื่อเพิ่มประสิทธิภาพการจัดเก็บโดยระบุข้อมูลที่ซ้ำกันหรือข้อมูลเก่า

กล่าวโดยสรุปได้ว่า การจัดชั้นความลับข้อมูลจึงเป็นกระบวนการจัดการข้อมูลตามหมวดหมู่และ/หรือชั้นความลับที่เกี่ยวข้อง ซึ่งมีการถูกนำไปใช้และคุ้มครองข้อมูลได้อย่างมีประสิทธิภาพมากขึ้น โดยหลักการพื้นฐานของการจัดชั้นความลับของข้อมูลจะช่วยให้ค้นหาแหล่งที่มาของข้อมูลและเรียกดูข้อมูลได้ง่ายขึ้น การจัดชั้นความลับของข้อมูลมีความสำคัญโดยเฉพาะอย่างยิ่งที่เกี่ยวข้องกับการจัดการความเสี่ยง และช่วยส่งเสริมจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจ การปฏิบัติตามกฎระเบียบและความปลอดภัยของข้อมูล การติดป้ายหรือแท็ก (Tag) ข้อมูลเพื่อให้ค้นหาและติดตามได้ง่าย นอกจากนี้ยังช่วยลดความซ้ำซ้อนของข้อมูลซึ่งสามารถลดค่าใช้จ่ายในการจัดเก็บและสำรองข้อมูล ในขณะที่ช่วยเร่งกระบวนการในการค้นหาแต่กระบวนการจัดชั้นความลับของข้อมูลอาจเป็นเทคนิคขั้นสูงที่ผู้นำองค์กรควรมีความเข้าใจและให้ความสำคัญเพิ่มมากขึ้น แม้ว่าการจัดชั้นความลับของข้อมูลเพื่อให้หน่วยงานของรัฐสามารถจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจได้อย่างมีประสิทธิภาพ อาจเป็นกระบวนการที่ซับซ้อนและยุ่งยากแต่ระบบอัตโนมัติสามารถช่วยปรับปรุงกระบวนการได้ โดยองค์กรต้องทำความเข้าใจและกำหนดประเภท/เกณฑ์ที่จะใช้ในการจำแนกระดับชั้นความลับของข้อมูล กำหนดวัตถุประสงค์ กำหนดบทบาทและความรับผิดชอบของเจ้าหน้าที่ในการ

กำกับดูแลมาตรการหรือโปรโตคอลในการจัดชั้นความลับของข้อมูลที่เหมาะสม รวมทั้งใช้มาตรฐานรักษาความปลอดภัยที่สอดคล้องกับหมวดหมู่/ระดับชั้นความลับของข้อมูลและการติดป้ายหรือแท็ก เมื่อดำเนินการจัดชั้นความลับของข้อมูลได้อย่างถูกต้องจะช่วยให้เจ้าหน้าที่และบุคคลที่สามที่เกี่ยวข้องกับการจัดเก็บ การส่ง หรือการเรียกดูข้อมูลมีกรอบในการทำงานได้อย่างมีประสิทธิภาพและไม่ขัดต่อข้อกฎหมายที่กำหนด ทั้งนี้ นโยบายและขั้นตอนการจัดชั้นความลับของข้อมูลควรมีการกำหนดไว้อย่างชัดเจน โดยคำนึงถึงข้อกำหนดด้านความปลอดภัยและการรักษาความลับของข้อมูล และตรงไปตรงมาเพียงพอที่จะช่วยให้เจ้าหน้าที่สามารถตีความได้ง่ายในการปฏิบัติตามข้อกำหนดอาทิ แต่ละหมวดหมู่หรือชั้นความลับอาจมีข้อมูลเกี่ยวกับประเภทของข้อมูลได้ ซึ่งรวมอยู่ในการจัดชั้นความลับและกฎระเบียบขององค์กรสำหรับการเรียกดู การส่ง และการจัดเก็บข้อมูล ควรพิจารณาด้านความปลอดภัยและความเสี่ยงที่อาจเกิดขึ้นจากการละเมิดนโยบายด้านความปลอดภัยขององค์กร

ในขณะที่ปัจจุบันมีความจำเป็นในการใช้ข้อมูลภาครัฐอย่างมีประสิทธิภาพเพิ่มมากขึ้นเพื่อปรับปรุงการให้บริการภาครัฐและแก้ปัญหาเชิงนโยบายที่มีความซับซ้อน ซึ่งยังไม่สามารถแก้ไขได้เมื่อข้อมูลยังคงกระจัดกระจายในลักษณะไซโลในแต่ละหน่วยงานของรัฐ อย่างไรก็ตาม สำหรับผู้ดูแลข้อมูลจำนวนมากอาจมีอุปสรรคในการแบ่งปันข้อมูลได้ ตัวอย่างเช่น อาจมีข้อกังวลบางประการเกี่ยวกับการแบ่งปันข้อมูลของหน่วยงานและการเปิดเผยข้อมูลต่อการตรวจสอบจากหน่วยงานภายนอกซึ่งอาจนำไปสู่การตัดสินใจที่จะไม่แบ่งปันข้อมูลหรือการประยุกต์ใช้การปกป้องคุ้มครองข้อมูลโดยไม่จำเป็น และอาจลดการใช้ประโยชน์ข้อมูลลงอย่างมีนัยสำคัญ

ข้อกังวลที่เรื่องการแบ่งปันข้อมูลหรือการประยุกต์ใช้ข้อมูลสามารถจัดการได้ด้วยการบริหารความเสี่ยงที่เหมาะสมและพิจารณาเปรียบเทียบกับผลประโยชน์ต่อส่วนรวมที่อาจเกิดขึ้นจากการแบ่งปันข้อมูล หลักการการแบ่งปันข้อมูลสนับสนุนความรับผิดชอบในการแบ่งปันของหน่วยงาน ด้วยการจัดให้มีวิธีการเพื่อการจัดการความเสี่ยงที่เกี่ยวข้องกับการแบ่งปันข้อมูลอย่างมีประสิทธิภาพ การใช้หลักการนี้สามารถทำให้เกิดการแบ่งปันข้อมูลของหน่วยงานภาครัฐถือครองอย่างปลอดภัยและมีประสิทธิภาพอันก่อให้เกิดประโยชน์ต่อสาธารณะ สามารถปกป้องความเป็นส่วนตัวและรักษาความลับของข้อมูลได้

ประกอบกับหน่วยงานภาครัฐมีการจัดเก็บข้อมูลจำนวนมหาศาลที่รวบรวมจากบุคคลและภาคธุรกิจต่าง ๆ หรือสร้างขึ้นผ่านอำนาจหน้าที่ในการให้บริหารของส่วนราชการ ข้อมูลเหล่านี้มีศักยภาพที่สำคัญในการกำหนดนโยบาย ประเมินแผนงาน/โครงการ และมีส่วนสนับสนุนการเติบโตทางเศรษฐกิจและส่งเสริมนวัตกรรมเพื่อประโยชน์ของประชาชนในประเทศ ด้วยตระหนักถึงคุณค่าของข้อมูลภาครัฐและความจำเป็นในการใช้งานอย่างมีประสิทธิภาพและเหมาะสม จึงจำเป็นต้องมีกรอบการแบ่งปันข้อมูลซึ่งปรับปรุงการเข้าถึงและนำข้อมูลภาครัฐกลับมาใช้ใหม่ ในขณะที่ยังคงรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล ซึ่งภายใต้บริบทนี้การแบ่งปันข้อมูลจึงเป็นข้อกำหนดในการเข้าถึงข้อมูลในลักษณะที่มีการควบคุม การเปิดเผยข้อมูล (Data release) หมายถึงการเปิดให้เข้าถึงข้อมูลได้ อาทิ การทำให้กลุ่มบุคคลหรือประชาคมเข้าถึงข้อมูลตามที่ตกลงกัน หรือ การทำให้ทุกคนสามารถใช้ข้อมูลได้แบบสาธารณะ ซึ่งข้อมูลภาครัฐสามารถถูกรับรู้ได้หลายวิธี โดยการแบ่งปันข้อมูลเป็นวิธีหนึ่งที่ทำให้สามารถนำข้อมูลที่มีอยู่กลับมาใช้ใหม่เพื่อก่อให้เกิดประโยชน์ต่อสาธารณะและสร้างชุดข้อมูลใหม่เพื่อให้ได้ข้อมูลเชิงลึกเกี่ยวกับชุมชน ครอบครัว เศรษฐกิจ อุตสาหกรรม และสิ่งแวดล้อม สำหรับการวิเคราะห์ วางแผนและตัดสินใจในเชิงนโยบายเพื่อเพิ่มประสิทธิภาพในการทำงาน อำนวยความสะดวกในการให้บริการภาครัฐ และพัฒนาประเทศต่อไป อย่างไรก็ตาม การแบ่งปันข้อมูลจะต้องจัดการอย่างระมัดระวังและปลอดภัยเพื่อให้ประชาชนเชื่อมั่นต่อการดำเนินงานของหน่วยงานของรัฐ

2.1.2 ปัญหาอุปสรรค

ด้วยการจัดหมวดหมู่และชั้นความลับของข้อมูลจำเป็นต้องดำเนินการให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม ซึ่งไม่สอดคล้องกับสถานการณ์ปัจจุบัน และได้กำหนดให้ผู้บริหารเป็นผู้มีอำนาจตัดสินใจในการ

กำหนดชั้นความลับและใช้ดุลพินิจของผู้บริหารในการตัดสินใจสั่ง **ให้/มิให้** เปิดเผยข้อมูล ประกอบกับยังขาดการกำหนดนิยามศัพท์และหลักเกณฑ์สำหรับการพิจารณากำหนดชั้นความลับที่ชัดเจน ส่งผลให้หน่วยงานของรัฐเลือกที่จะไม่เปิดเผยข้อมูลความลับทางราชการและข้อมูลความมั่นคงของหน่วยงานตน เนื่องจากขาดความมั่นใจและน่าจะมีความปลอดภัยมากกว่าการเปิดเผยข้อมูลดังกล่าว และทำให้การส่งเสริมให้มีการเปิดเผยข้อมูลภาครัฐโดยปกติวิสัย (Open by default) เป็นได้ด้วยความยากลำบาก ดังนั้น หน่วยงานของรัฐจึงต้องการแนวปฏิบัติในการพิจารณากำหนดชั้นความลับของข้อมูล เพื่อให้ผู้บริหารหรือผู้มีอำนาจตัดสินใจมีเกณฑ์ และแนวทางในการเปิดเผยและแบ่งปันข้อมูลภาครัฐเพื่อให้เกิดการใช้ประโยชน์จากข้อมูลร่วมกันและสร้างวัฒนธรรมการเปิดเผยข้อมูลภาครัฐโดยปกติวิสัยให้เกิดขึ้นได้จริง

โดยทั่วไปความพยายามในการจัดชั้นความลับของข้อมูลนั้นขอบเขตกว้างขวาง ซึ่งกระทบต่อการดำเนินงานเกือบทุกอย่างภายในองค์กร เนื่องจากขอบเขตกว้างและความซับซ้อนของการจัดการเนื้อหาในสภาพแวดล้อมดิจิทัลสมัยใหม่ องค์กรมักเผชิญกับความท้าทายในการรู้ว่าจะเริ่มต้นจากที่ใด วิธีจัดการการใช้งานที่ประสบความสำเร็จ และวิธีวัดผลความคืบหน้าในการดำเนินงาน

ปัญหาอุปสรรคที่พบบ่อยมักรวมถึง

- ปัญหาการออกแบบกรอบการจัดชั้นความลับข้อมูลที่ชัดเจนและเข้าใจง่าย รวมถึงการกำหนดระดับการจัดชั้นความลับและการควบคุมความปลอดภัยที่เกี่ยวข้อง
- ปัญหาการพัฒนาแผนการดำเนินงานซึ่งรวมถึงการใช้โซลูชันเทคโนโลยีที่เหมาะสม การปรับแผนให้สอดคล้องกับกระบวนการตามภารกิจที่มีอยู่ และการระบุผลกระทบต่อเจ้าหน้าที่
- ปัญหากรอบการจัดชั้นความลับของข้อมูลภายในโซลูชันเทคโนโลยีที่ใช้งานปัจจุบัน และระบุช่องว่างระหว่างขีดความสามารถด้านเทคโนโลยีของเครื่องมือและกรอบการจัดชั้นความลับของข้อมูล
- ปัญหาการกำหนดโครงสร้างธรรมาภิบาลข้อมูลระบบกำกับดูแลบำรุงรักษาอย่างต่อเนื่องและความสมบูรณ์ของความพยายามในการจัดชั้นความลับของข้อมูล
- ปัญหาการระบุตัวบ่งชี้ประสิทธิภาพหลัก (KPIs) เฉพาะเพื่อติดตามและวัดผลความคืบหน้าการดำเนินงาน
- ปัญหาความตระหนักและความเข้าใจในนโยบายการจัดชั้นความลับของข้อมูลว่าเหตุใดจึงมีความสำคัญและมีวิธีปฏิบัติการตามนโยบายอย่างไร
- ปัญหาการปฏิบัติตามการตรวจสอบภายในที่กำหนดเป้าหมายการสูญเสียข้อมูลและการควบคุมความปลอดภัยทางไซเบอร์
- ปัญหาการฝึกอบรมและสนับสนุนการมีส่วนร่วมกับผู้ใช้งานเพื่อสร้างความตระหนักถึงความจำเป็นในการจำแนกชั้นความลับของข้อมูลที่ถูกต้องในการดำเนินงานตามภารกิจของหน่วยงานและใช้มาตรการการจัดหมวดหมู่และชั้นความลับที่เหมาะสม

นอกจากนี้ หน่วยงานของรัฐมีความจำเป็นในการวิเคราะห์ข้อมูลขนาดใหญ่เพื่อช่วยให้การตัดสินใจวางแผนดำเนินงานในแต่ละเรื่องเป็นไปอย่างมีประสิทธิภาพ ส่งผลให้หน่วยงานภาครัฐต้องจัดเก็บรวบรวมและการจัดการข้อมูลมากขึ้น ซึ่งอาจมีอุปสรรคในการแบ่งปันข้อมูล เช่น อาจมีข้อกังวลเกี่ยวกับการแบ่งปันข้อมูลของหน่วยงาน และเปิดเผยข้อมูลต่อการตรวจสอบจากภายนอก ซึ่งอาจนำไปสู่การตัดสินใจที่จะไม่เปิดเผยข้อมูล หรือใช้การป้องกันที่ไม่จำเป็นกับข้อมูล ที่อาจลดการใช้ประโยชน์ของข้อมูลลง อย่างไรก็ตามข้อกังวลที่กล่าวมาข้างต้นนี้สามารถจัดการได้โดยหลักการแบ่งปันข้อมูลและพิจารณาตามความเสี่ยงที่ยอมรับได้ เพื่อให้เกิดการแบ่งปันข้อมูลที่ปลอดภัย มีประสิทธิภาพ และเป็นประโยชน์ต่อสาธารณะ

2.1.3 ประโยชน์

การจัดชั้นความลับของข้อมูลเพื่อจัดการข้อมูลในกระบวนงานที่เกี่ยวข้อง มีประโยชน์มากกว่าการช่วยให้ค้นหาข้อมูลได้ง่ายขึ้น และมีความจำเป็นเพื่อให้องค์กรสมัยใหม่สามารถเข้าใจข้อมูลจำนวนมหาศาลที่มี

อยู่ได้ทุกขณะ การจัดชั้นความลับของข้อมูลสะท้อนให้เห็นภาพที่ชัดเจนของข้อมูลทั้งหมดภายในการควบคุมขององค์กร รับรู้และความเข้าใจว่าข้อมูลถูกจัดเก็บไว้ที่ใด เป็นวิธีการเข้าถึงข้อมูลอย่างง่ายดาย และเป็นวิธีที่ดีที่สุดในการปกป้องและคุ้มครองข้อมูลจากความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้นเมื่อมีการนำข้อมูลไปใช้ อีกทั้งช่วยให้มีกรอบการทำงานที่เป็นระเบียบซึ่งเอื้อต่อมาตรการปกป้องและคุ้มครองข้อมูลที่เพียงพอมากขึ้น และส่งเสริมการปฏิบัติตามนโยบายด้านความปลอดภัยของเจ้าหน้าที่ และช่วยเพิ่มประสิทธิภาพการทำงานของระบบรักษาความปลอดภัยที่มีอยู่และเพิ่มความตระหนักด้านความปลอดภัยภายในองค์กร ตลอดจนเพิ่มบริบทและความหมายให้กับข้อมูล รู้ว่าข้อมูลอะไรคือข้อมูลที่สำคัญและจำเป็นที่ต้องมีการบริหารจัดการอย่างใกล้ชิด และรู้ว่าอะไรที่ไม่จำเป็นต่อองค์กร และในกรณีที่มีการแบ่งปันข้อมูลระหว่างหน่วยงานมากเท่าไร ยิ่งต้องมีการกำกับดูแลข้อมูลมากเท่านั้น

ดังนั้น การจัดชั้นความลับของข้อมูลเป็นวิธีการที่มีประสิทธิภาพในการปกป้องคุ้มครองข้อมูลที่มีคุณค่า โดยการระบุประเภทหรือชั้นความลับของข้อมูลที่จัดเก็บและระบุตำแหน่ง/แหล่งที่มาของข้อมูลที่ความอ่อนไหว จะช่วยให้สามารถจัดลำดับความสำคัญของมาตรการรักษาความปลอดภัย ปรับการควบคุมความปลอดภัยตามความอ่อนไหวของข้อมูล ทำความเข้าใจว่าใครสามารถเข้าถึง แก้ไข หรือลบข้อมูลได้ และประเมินความเสี่ยง เช่น ผลกระทบทางธุรกิจจากการละเมิด การโจมตีของแรนซัมแวร์ หรือภัยคุกคามอื่น ๆ ตลอดจนสร้างความสอดคล้องในการส่งข้อมูลที่สำคัญ แบ่งอำนาจหน้าที่และบทบาท (Authority and Responsibility) และความรับผิดชอบ (Accountability) ในการรักษาความปลอดภัยของข้อมูล สามารถมอบหมายผู้แทนดูแลข้อมูลได้อย่างเหมาะสม ลดความซับซ้อนของการตรวจสอบและการกำกับดูแล หลีกเลี่ยงข้อมูลรั่วไหลที่ไม่สามารถยอมรับได้ รวมทั้งป้องกันการลงโทษทางการเงินและกฎหมายที่รุนแรงอันเนื่องมาจากผลการปฏิบัติงานตามข้อกำหนด/ข้อกฎหมายที่เกี่ยวข้อง

นอกจากนี้ ผลของการปกป้องข้อมูลยังเป็นสิ่งสำคัญยิ่งเพื่อสร้างความได้เปรียบทางการแข่งขันอย่างยั่งยืน โดยการจัดชั้นความลับของข้อมูลสามารถช่วยขับเคลื่อนการเติบโตของรายได้ด้วยการสนับสนุนการมีส่วนร่วมด้านความปลอดภัยและริเริ่มการเติบโต ลดการใช้จ่ายได้โดยการจำกัดขอบเขตของข้อมูลที่ต้องการการป้องกันและเพิ่มประสิทธิภาพของการลงทุนที่มีอยู่ และลดความเสี่ยงโดยการเน้นที่ข้อมูลที่มีความอ่อนไหว ในขณะที่การมีหลักการแบ่งปันข้อมูลจะช่วยผู้ดูแลข้อมูลภายในหน่วยงานของรัฐที่จัดเก็บข้อมูลภาครัฐมีกรอบแนวทางในการแบ่งปันข้อมูลที่ถือครองได้อย่างปลอดภัยและมีประสิทธิภาพโดยใช้หลักการแบ่งปันข้อมูลในกรณีที่มีสาธารณประโยชน์ที่ชัดเจน ผู้ดูแลข้อมูลอาจพยายามแบ่งปันข้อมูลในลักษณะที่มีการควบคุมกับผู้ใช้ที่หลากหลาย เช่น หน่วยงานราชการ ชุมชนวิจัยทางวิชาการ และในกรณีภาคเอกชน หลักการแบ่งปันข้อมูลก็เพื่อช่วยให้ผู้ดูแลข้อมูลพิจารณาการป้องกันที่เหมาะสมก่อนแบ่งปันข้อมูลของรัฐบาล และเพื่อส่งเสริมการจัดการเพื่อเข้าถึงข้อมูลที่อ้างอิงตามหลักการที่มีความยืดหยุ่นมากขึ้น

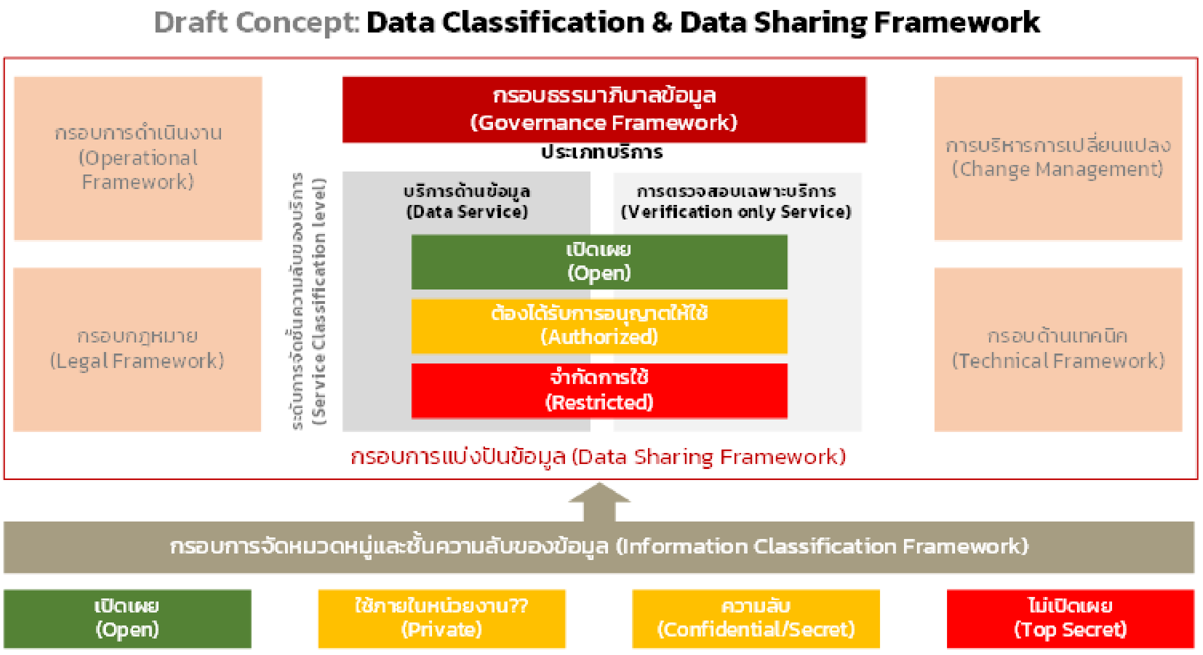
2.2 หลักการและแนวคิด

การจัดชั้นความลับของข้อมูลเป็นส่วนพื้นฐานในการรักษาความปลอดภัยข้อมูลขององค์กรและบุคคลที่สามารถเข้าถึงได้ เป็นกระบวนการในการระบุและกำหนดระดับความอ่อนไหวหรือการรักษาความลับที่กำหนดไว้ล่วงหน้าให้กับข้อมูลประเภทต่าง ๆ หากองค์กรไม่ได้จัดชั้นความลับของข้อมูลอย่างเหมาะสม จะไม่สามารถปกป้องข้อมูลได้อย่างถูกต้องหรือป้องกันไม่ให้มีการเข้าถึง การใช้ การหยุดชะงัก การแก้ไข หรือการทำลายโดยไม่ได้รับอนุญาตขณะอยู่ในที่จัดเก็บ โดยการจัดชั้นความลับของข้อมูลเป็นกระบวนการของการวิเคราะห์ข้อมูลที่มีโครงสร้างหรือไม่มีโครงสร้าง และจัดเป็นหมวดหมู่หรือชั้นความลับที่ขึ้นอยู่กับประเภทไฟล์และเนื้อหา ซึ่งช่วยให้องค์กรสามารถกำหนดและกำหนดและให้คุณค่ากับข้อมูลและเป็นจุดเริ่มต้นพื้นฐานสำหรับการกำกับดูแลหรือจัดทำธรรมาภิบาลข้อมูล กระบวนการจัดชั้นความลับข้อมูลจะจำแนกข้อมูลตามความอ่อนไหวและผลกระทบทางธุรกิจ/ในการดำเนินภารกิจของหน่วยงานเพื่อระบุความเสี่ยง เมื่อข้อมูลถูกจัด

ชั้นความลับแล้วจะสามารถจัดการเพื่อปกป้องข้อมูลที่มีความอ่อนไหวหรือสำคัญจากการโจรกรรมหรือการสูญหายได้ ทั้งนี้ การจัดชั้นความลับของข้อมูลจะแตกต่างกันไปตามบริบทหรือกฎหมายที่เกี่ยวข้องของหน่วยงานนั้นๆ

ทั้งนี้ การจัดชั้นความลับของข้อมูลช่วยให้องค์กรปรับปรุงความปลอดภัยของข้อมูลและรับรองการปฏิบัติตามกฎระเบียบและข้อกฎหมายที่เกี่ยวข้อง โดยมีเป้าหมายเพื่อกำหนดว่าหน่วยงานมีข้อมูลอะไรบ้างและใครต้องการข้อมูลนั้น เพื่อให้เกิดการจัดการข้อมูลอ่อนไหวและมีการกำหนดสิทธิในการเข้าถึง และกำหนดความรับผิดชอบต่อความปลอดภัยของข้อมูล ซึ่งข้อมูลที่มีการจัดชั้นความลับไม่ควรสามารถเข้าถึงได้โดยทุกคนเพราะจะแสดงให้เห็นว่าขาดความน่าเชื่อถืออันเนื่องมาจากความไม่ซื่อสัตย์ ขาดความถูกต้อง (Integrity) หรือผู้ที่อาจได้รับผลกระทบที่ไม่เหมาะสมอันเนื่องมาจากสถานการณ์ด้านข้อมูลส่วนบุคคล สำหรับข้อกังวลด้านการคุ้มครองข้อมูลส่วนบุคคลต้องกำหนดให้ผู้ประมวลผลข้อมูลดำเนินการตามข้อกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล สำหรับข้อมูลใช้ภายในองค์กรอาจกำหนดให้ฝ่ายบุคลากรดำเนินการตรวจสอบเพิ่มเติมเกี่ยวกับพนักงาน/เจ้าหน้าที่ อาทิ การตรวจสอบประวัติอาชญากรรม เพื่อการควบคุมการเข้าถึงข้อมูล ผู้ใช้จะต้องได้รับการระบุ ตรวจสอบสิทธิและได้รับอนุญาต ซึ่งจุดอ่อนที่สำคัญที่สุดในปัจจุบันในการพิสูจน์ตัวตนผู้ใช้คือการใช้รหัสผ่านอย่างต่อเนื่องเนื่องจากรหัสผ่านไม่แข็งแรงพอ ผู้ใช้/ผู้แบ่งปันข้อมูลมักเลือกสิ่งที่เดาหรือถอดรหัสได้ง่าย ดังนั้นการเข้าถึงข้อมูลที่เป็นความลับจำเป็นต้องควบคุมโดยใช้การพิสูจน์ตัวตนที่รัดกุมหรือแบบสองปัจจัย (Two Factor Authentication) โดยมีปัจจัยที่สองคือสิ่งที่ผู้ใช้มีหรือสิ่งที่ผู้ใช้เป็น และเป็นสิ่งจำเป็นนอกเหนือจากสิ่งที่ผู้ใช้รู้ อาทิ การเข้ารหัสผ่าน

ในขณะที่การแบ่งปันข้อมูลมีความสำคัญต่อกลยุทธ์ด้านเทคโนโลยีสมัยใหม่ และการจัดประเภทข้อมูลช่วยให้มั่นใจได้ว่าทั้งข้อกำหนดเกี่ยวกับข้อมูลและการปฏิบัติตามข้อกำหนดจะบรรลุผลอย่างมีประสิทธิผลและประสิทธิผล การจัดประเภทข้อมูลควรเป็นรากฐานที่สำคัญของกิจกรรมการจัดการข้อมูลและนโยบายการจัดการวงจรข้อมูล เพื่อให้มั่นใจว่ามีการจัดเก็บและใช้งานอย่างเหมาะสมและปลอดภัย ซึ่งกรอบการจัดชั้นความลับและแบ่งปันข้อมูลโดยทั่วไปมีองค์ประกอบที่หลากหลาย [6] อาทิ กรอบการดำเนินงาน (Operational Framework) กรอบกฎหมาย (Legal Framework) การบริหารการเปลี่ยนแปลง (Change Management) กรอบด้านเทคนิค (Technical Framework) และประเภทบริการ ที่ตอบสนองต่อข้อมูลที่มีความอ่อนไหว และมีการจัดชั้นความลับของข้อมูลเป็นรากฐานที่มั่นคงสำหรับกลยุทธ์ด้านความปลอดภัยของข้อมูล โดยกำหนดแนวทางและเงื่อนไขในการแบ่งปันข้อมูล ทั้งนี้ ข้อมูลที่ต้องได้รับอนุญาตให้ใช้นั้นจะต้องยอมรับข้อตกลงการใช้งานข้อมูล ใช้ข้อมูลตามวัตถุประสงค์และระยะเวลาที่ได้รับอนุญาตเท่านั้น และการทำลายข้อมูลหลังจากใช้งานแล้ว นอกจากนี้ ควรมีระบบรองรับในอนาคต เช่น กลไกการเข้ารหัสข้อมูลเพื่อความปลอดภัยในการจัดเก็บ การจัดการสิทธิการเข้าถึงข้อมูล การเก็บประวัติการเข้าถึงข้อมูล การยืนยันตัวตน (Authentication) การปรับปรุงข้อมูลที่จัดเก็บให้เป็นปัจจุบันและการประเมินคุณภาพข้อมูลอย่างกึ่งอัตโนมัติ อาทิ ความปรับปรุงให้เป็นปัจจุบัน ความครบถ้วน ปริมาณข้อมูล ประเภท และ Machine-readable เพื่อให้การจัดชั้นความลับและแบ่งปันข้อมูลได้อย่างมีประสิทธิภาพ



Source https://synergygrc.com/the-importance-of-implementing-data-classification-frameworks/

รูปที่ 1 กรอบการจัดชั้นความลับและแบ่งปันข้อมูล

2.2.1 หลักการจัดชั้นความลับของข้อมูล (Principle of data and information classification)

การดำเนินการจัดการข้อมูลโดยทั่วไปและการจำแนกชั้นความลับของข้อมูลโดยเฉพาะที่มีความแตกต่างกันไปตามประเภทองค์กรและอาจแตกต่างกันไปขึ้นอยู่กับแต่ละองค์กร อย่างไรก็ตาม มีหลักการพื้นฐานร่วมกันระหว่างองค์กรภาครัฐและภาคเอกชน 6 ประการ [7] ซึ่งแสดงโดยแหล่งข้อมูลทางกฎหมายระดับชาติ (และระดับภูมิภาค) และเป็นเครื่องมือขององค์กรระหว่างประเทศสำหรับการจัดการข้อมูลข่าวสาร โดยหลักการดังต่อไปนี้ควรใช้เป็นแนวทางมากกว่าเป็นเกณฑ์เทียบเคียง (Benchmark) อย่างเดียวในการสร้างและ/หรือการปรับปรุงการจัดการข้อมูลและกลยุทธ์การจัดชั้นความลับของข้อมูล

1) การเปิดกว้าง ความโปร่งใส และค่านิยมทางสังคม (Openness, Transparency, and Societal values) การจำแนกชั้นความลับควรใช้อย่างระมัดระวังและสอดคล้องกับความอ่อนไหว ค่านิยมและความสำคัญของข้อมูล การจำกัดการเข้าถึงควรเลือกพิจารณาเฉพาะในกรณีที่การเปิดเผยข้อมูลอาจเป็นอันตรายต่อผลประโยชน์ที่ชอบด้วยกฎหมายและภาระผูกพันทางกฎหมายขององค์กร เจ้าหน้าที่ หรือบุคคลที่สาม ซึ่งในกรณีดังกล่าวควรปฏิบัติตามขั้นตอนที่ระบุอย่างเคร่งครัดเพื่อให้แน่ใจว่าข้อมูลจะไม่ถูกรุกล้ำไม่ว่าจะโดยเจตนาหรือโดยไม่ได้ตั้งใจก็ตาม ความท้าทายคือการไม่จัดชั้นความลับมากเกินไปเพื่อความสะดวกหรือเพื่อความได้เปรียบอันจะเป็นการทำลายความโปร่งใสและความไว้วางใจจากสาธารณชน และกีดกันผู้มีส่วนได้ส่วนเสียในความเป็นเจ้าของสำหรับการตัดสินใจในการจัดการความเสี่ยงของตนเอง

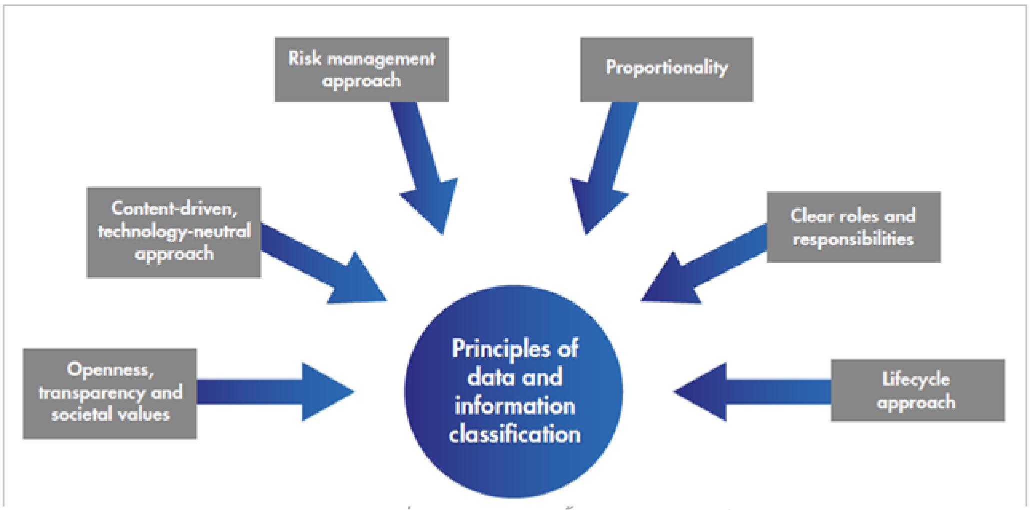
2) แนวทางการขับเคลื่อนด้วยเนื้อหาและเป็นกลางทางเทคโนโลยี (Content driven, technology neutral approach) ข้อมูลควรได้รับการจัดชั้นความลับตามเนื้อหาและความเสี่ยงที่เกี่ยวข้องกับความสอดคล้องของเนื้อหาในรูปแบบอิเล็กทรอนิกส์ โดยไม่คำนึงถึงรูปแบบ สื่อ หรือแหล่งที่มาของข้อมูล ไม่ควรมีการเลือกปฏิบัติตามรูปแบบหรือสื่อของข้อมูล ที่ถูกจัดเก็บไว้ในระบบข้อมูล บนสื่อบันทึกข้อมูล บนอุปกรณ์พกพาหรือในระบบคลาวด์ ในทำนองเดียวกันการตัดสินใจจัดชั้นความลับของข้อมูลควรขึ้นอยู่กับตัวเนื้อหาของข้อมูล และไม่จำเป็นต้องถูกได้รับมาโดยอัตโนมัติจากแหล่งข้อมูลที่อ้างอิงตาม ตอบสนอง หรืออ้างถึง ตัวอย่างเช่น การอ้างอิงแหล่งข้อมูลสาธารณะไม่ควรตัดสินใจโดยอัตโนมัติว่าการประมวลข้อมูลโดยรวมควรเปิดเผยต่อสาธารณะได้

3) แนวทางการบริหารความเสี่ยง (Risk management approach) ข้อมูลควรได้รับการคุ้มครองตามระดับของความอ่อนไหว คุณค่า และความสำคัญของข้อมูล ตามแนวทางนี้จะให้ค่าคะแนนขึ้นอยู่กับระดับที่สอดคล้องกับคุณค่าและความเสี่ยงของข้อมูล ระดับการป้องกันควรกำหนดขอบเขตของมาตรการเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ อาทิ ความรุนแรงและความเป็นไปได้ที่ข้อมูลจะถูกรุกล้ำหรือทำลาย ในการกำหนดระดับความอ่อนไหวและคุณค่าของข้อมูล ควรพิจารณาทั้งระดับของความเสียหายที่อาจเกิดขึ้นจากการถูกรุกล้ำหรือทำลาย (การเปิดเผยโดยไม่ได้รับอนุญาต การแก้ไข หรือการสูญเสีย) ตลอดจนคุณค่าที่เป็นไปได้ของข้อมูลที่ถูกจัดชั้น

4) สัดส่วนการจัดระดับชั้น (Proportionality) ข้อมูลต้องจัดระดับชั้นที่เหมาะสมซึ่งควรจะให้มีระดับต่ำที่สุด เพื่อส่งเสริมให้เกิดการใช้ประโยชน์จากข้อมูลให้ได้มากที่สุด ทั้งนี้ ควรมีแต่ข้อมูลที่สำคัญและจำเป็นต้องได้รับการปกป้องเท่านั้นจึงจะจัดให้อยู่ในระดับสูงเพื่อรักษาความปลอดภัยของข้อมูล

5) บทบาทและความรับผิดชอบที่ชัดเจน (Clear roles and responsibilities) ควรมีการกำหนดบทบาทหน้าที่ของผู้ที่มีส่วนเกี่ยวข้องกับข้อมูลที่ชัดเจน โดยคำนึงถึงการจัดชั้นความลับของข้อมูล นโยบายและกระบวนการควรได้รับการออกแบบสำหรับการรักษาความปลอดภัยข้อมูลภายในองค์กรและกฎหมายที่เกี่ยวข้อง [8] [9] และถือปฏิบัติด้วยการตระหนักรู้ในการบริหารจัดการและมุ่งมั่นในการรักษาความปลอดภัยของข้อมูล

6) แนวทางวงจรชีวิตของข้อมูล (Lifecycle approach) ในฐานะที่เป็นส่วนหนึ่งของระบบการจัดการข้อมูล ระบบการจำแนกชั้นความลับควรมีการพิจารณาตลอดวงจรชีวิตของข้อมูล ตั้งแต่การสร้าง การจัดเก็บ การเรียกดูข้อมูล การประมวลผลและใช้ข้อมูล การเผยแพร่ การจัดเก็บข้อมูลถาวร จนถึงการทำลาย นอกจากนี้ นโยบายการจัดการข้อมูลและประมวลผลข้อมูลขององค์กรไม่ควรเขียนไว้เป็นเป้าเพียงอย่างเดียวแต่ควรประเมินผลการดำเนินงานตามนโยบายอย่างสม่ำเสมอเพื่อให้มั่นใจว่าสอดคล้องกับความต้องการและความคาดหวังที่มีต่อองค์กร



รูปที่ 2 หลักการจัดชั้นความลับของข้อมูล

การตัดสินใจจำแนกชั้นความลับของข้อมูลที่ถูกต้อง เมื่อตัดสินใจว่าข้อมูลจะใช้การจัดชั้นความลับใด ควรทำการประเมินเพื่อพิจารณาผลกระทบที่อาจเกิดขึ้นหากข้อมูลถูกเปิดเผย/นำไปใช้โดยไม่ได้รับอนุญาต การจัดชั้นความลับที่ถูกต้องจะช่วยให้มั่นใจได้ว่าข้อมูลโดยเฉพาะข้อมูลที่มีความอ่อนไหวจะได้รับการควบคุมและดูแลเพิ่มเติม โดยใน**การประเมินเพื่อจำแนกชั้นความลับควรพิจารณา/คำนึงถึงประเด็น**ต่อไปนี้

- การจัดระดับชั้นความลับที่สูงเกินไปสามารถขัดขวางการเข้าถึงข้อมูล นำไปสู่การควบคุมเพื่อคุ้มครองที่ไม่จำเป็นและมีราคาแพง และทำให้ประสิทธิภาพในการดำเนินการขององค์กรลดลง
- การจัดระดับชั้นความลับต่ำเกินไปอาจนำไปสู่ผลเสียหายและเป็นอันตรายต่อผลประโยชน์ของข้อมูล

- การยอมให้เป็นอันตรายต่อผลประโยชน์กับชุดข้อมูลที่มีขนาดใหญ่กว่าในการจัดชั้นความลับระดับเดียวกันมีแนวโน้มที่จะส่งผลกระทบ (โดยเฉพาะอย่างยิ่งในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคล) มากกว่ากรณีเดียว โดยทั่วไปจะไม่ส่งผลให้มีการจัดชั้นความลับที่สูงขึ้น แต่อาจต้องมีการจัดการเพิ่มเติม อย่างไรก็ตาม หากการเก็บรวบรวมข้อมูลส่งผลให้มีการสร้างข้อมูลที่ความอ่อนไหวมากขึ้น ควรพิจารณาจัดชั้นความลับในระดับที่สูงที่สุด

- ความอ่อนไหวของข้อมูลอาจเปลี่ยนแปลงเมื่อเวลาผ่านไปตามวงรอบ และอาจจำเป็นต้องจัดชั้นความลับของข้อมูลใหม่ (Declassification) ตัวอย่างเช่น หากเอกสารถูกยกเลิกการจัดชั้นความลับหรือเปลี่ยนการติดป้าย หรือแท็ก ไฟล์ข้อมูลควรปรับเปลี่ยนเพื่อแสดงการติดป้ายสูงสุดภายในเอกสารด้วย

2.2.2 วิธีการจัดชั้นความลับของข้อมูล มักเกี่ยวข้องกับแท็กและป้ายกำกับจำนวนมากที่กำหนดประเภทของข้อมูล การรักษาความลับ ความสมบูรณ์ของข้อมูล และความพร้อมใช้งานอาจถูกนำมาพิจารณาในกระบวนการจัดชั้นของข้อมูล ระดับความอ่อนไหวของข้อมูลมักถูกจัดชั้นตามระดับความสำคัญหรือการรักษาความลับที่แตกต่างกัน ซึ่งสัมพันธ์กับมาตรการรักษาความปลอดภัยที่ใช้เพื่อปกป้องแต่ละระดับการจำแนกชั้นความลับของข้อมูล โดยพิจารณาตามมาตรฐานอุตสาหกรรม/สากลทั่วไปสามารถจำแนกชั้นความลับของข้อมูลออกเป็น 3 ประเภทหลักตาม

- **เนื้อหา (Content-based)** จะตรวจสอบและตีความไฟล์ของข้อมูลที่มีความอ่อนไหว
- **บริบท (Context-based)** จะพิจารณาแอปพลิเคชัน สถานที่ หรือผู้สร้างท่ามกลางตัวแปรอื่น ๆ เป็นตัวบ่งชี้ทางอ้อมของข้อมูลที่มีความอ่อนไหว
- **ผู้ใช้ (User-based)** ขึ้นอยู่กับคู่มือการเลือกผู้ใช้ปลายทางของแต่ละเอกสาร การจัดชั้นความลับของข้อมูลตามผู้ใช้ขึ้นอยู่กับความรู้ของผู้ใช้และดุลยพินิจในการสร้าง แก้ไข ตรวจสอบ หรือเผยแพร่เพื่อตั้งค่าสถานะเอกสารที่มีความอ่อนไหว

ทั้งนี้ วิธีการจัดชั้นความลับของข้อมูลเพื่อจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจ สามารถพิจารณาจากเนื้อหา บริบท และผู้ใช้อาจเป็นได้ทั้งถูกหรือผิด ขึ้นอยู่กับพันธกิจของหน่วยงาน และประเภทข้อมูล โดยข้อมูลข่าวสารลับอาจมีการปรับชั้นความลับได้ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 โดยสามารถจัดชั้นข้อมูลเป็นเปิดเผย (Open) เผยแพร่ภายในองค์กร (Private) ลับ (Confidential / Sensitive) ลับมาก (Secret / Medium Sensitive) ลับมากที่สุด ลับที่สุด (Top secret / Highly Sensitive) ในตัวอย่างนี้ ข้อมูลสาธารณะแสดงถึงข้อมูลที่มีความอ่อนไหวน้อยที่สุดโดยมีข้อกำหนดด้านความปลอดภัยต่ำสุด ในขณะที่ข้อมูลที่ถูกจำกัดการใช้อยู่ในประเภทความปลอดภัยสูงสุดและแสดงถึงข้อมูลที่มีความอ่อนไหวมากที่สุด การจัดชั้นความลับของข้อมูลนี้มักเป็นจุดเริ่มต้นสำหรับองค์กรหลายแห่งตามด้วยขั้นตอนการระบุและติดแท็กเพิ่มเติมโดยติดป้ายกำกับข้อมูลตามความเกี่ยวข้องกับองค์กร คุณภาพและการจัดชั้นข้อมูลอื่น ๆ ซึ่งกระบวนการจัดชั้นของข้อมูลที่ประสบความสำเร็จมากที่สุดถูกใช้ตามกระบวนการติดตามผลการดำเนินงานและกรอบแผนงานเพื่อจัดเก็บข้อมูลสำคัญไว้ในที่ที่เหมาะสม

โดยการจัดชั้นความลับของข้อมูลถือเป็นส่วนพื้นฐานในการรักษาความปลอดภัยข้อมูลขององค์กรและบุคคลที่สามารถเข้าถึงได้ เป็นกระบวนการในการระบุและกำหนดระดับความอ่อนไหวหรือการรักษาความลับที่กำหนดไว้ล่วงหน้าให้กับข้อมูลประเภทต่าง ๆ หากองค์กรไม่ได้จัดชั้นความลับข้อมูลอย่างเหมาะสมจะไม่สามารถปกป้องข้อมูลได้อย่างถูกต้องหรือป้องกันไม่ให้มีการเข้าถึง การใช้ การหยุดชะงัก การแก้ไข หรือการทำลายโดยไม่ได้รับอนุญาตขณะอยู่ในที่จัดเก็บ ซึ่งจากมุมมองของความปลอดภัยของข้อมูล CIA Triad Model (รูปที่ 3) ถูกใช้เพื่อเป็นแนวทางในนโยบายการรักษาความปลอดภัยข้อมูลและการจัดชั้นความลับของข้อมูลภายในองค์กร

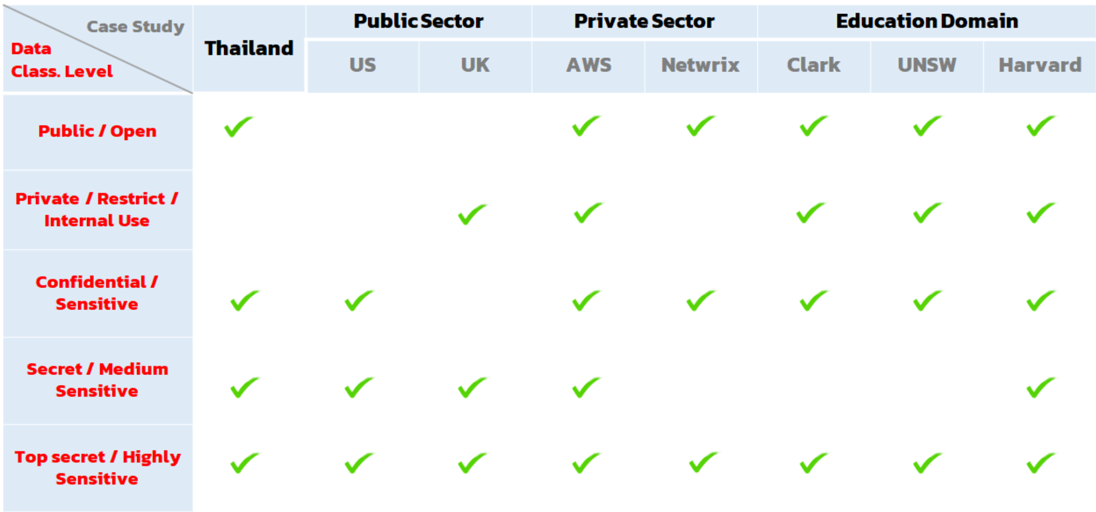
รูปที่ 3 CIA Triad Model

- **ด้านความลับ (Confidentiality)** การรักษาความลับนั้นเทียบเท่ากับความเป็นส่วนตัวโดยประมาณ ต้องจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้นเพื่อดูข้อมูลที่มีความอ่อนไหว
- **ด้านความถูกต้อง ครบถ้วนสมบูรณ์ ความคงสภาพ (Integrity)** ความสมบูรณ์เกี่ยวข้องกับการรักษาความสอดคล้องของข้อมูล ข้อมูลต้องไม่เปลี่ยนแปลงในระหว่างการส่ง และควรสอดคล้องกันตลอดวงจรชีวิตทั้งหมด
- **ด้านความพร้อมใช้งาน (Availability)** ความพร้อมใช้งานทำให้แน่ใจได้ว่าระบบทำงานและใช้งานได้ และไม่มีการสึกหรอเนื่องจากความล้มเหลวของฮาร์ดแวร์หรือซอฟต์แวร์

ดังนั้น การจัดชั้นความลับของข้อมูลจะพิจารณาร่วมกับวัตถุประสงค์ด้านความมั่นคงปลอดภัย (Security) ของระบบเทคโนโลยีสารสนเทศ และความเสี่ยง (Risks) ที่คาดว่าจะส่งผลกระทบ เช่น ข้อมูลสาธารณะก็มีความเสี่ยงหรือความอ่อนไหวในระดับต่ำ ส่วนข้อมูลที่ต้องการความคุ้มครองสูงก็จะมีระดับความเสี่ยงสูง ซึ่งภาครัฐหลายประเทศได้มีการจัดชั้นความลับของข้อมูลเป็น สาธารณะ ลับ ลับมาก และลับที่สุด

2.2.3 การศึกษาเปรียบเทียบการจัดชั้นความลับของข้อมูล (Data Classification Schemes)

จากการเปรียบเทียบระดับชั้นความลับข้อมูลของประเทศไทยและต่างประเทศทั้งหน่วยงานภาครัฐและภาคเอกชน [10] – [13] พบว่า ชั้นความลับข้อมูลสามารถแบ่งได้ 5 ระดับ ได้แก่ 1) ชั้นเปิดเผย (Open) 2) ชั้นเผยแพร่ภายในองค์กร (Private) 3) ชั้นลับ (Confidential / Sensitive) 4) ชั้นลับมาก (Secret / Medium Sensitive) และ 5) ชั้นลับที่สุด (Top secret / Highly Sensitive) โดยประเทศไทยและหน่วยงานในต่างประเทศมีระดับชั้นข้อมูลที่สอดคล้องและเป็นไปในทิศทางเดียวกัน แต่อาจมีความแตกต่างกันตามลักษณะการใช้งานของประเภทหน่วยงานดังภาพ



Case Study / Data Class. Level	Thailand	Public Sector		Private Sector		Education Domain		
		US	UK	AWS	Netwrix	Clark	UNSW	Harvard
Public / Open	✓			✓	✓	✓	✓	✓
Private / Restrict / Internal Use			✓	✓		✓	✓	✓
Confidential / Sensitive	✓	✓		✓	✓	✓	✓	✓
Secret / Medium Sensitive	✓	✓	✓	✓				✓
Top secret / Highly Sensitive	✓	✓	✓	✓	✓	✓	✓	✓

รูปที่ 4 การศึกษาเปรียบเทียบ Data Classification Schemes

2.2.4 หลักการแบ่งปันข้อมูล (Data Sharing Principles)

หลักการที่ออกแบบสำหรับการแบ่งปันข้อมูลอย่างปลอดภัยและเหมาะสม ผู้ดูแลข้อมูลจะต้องมีความยืดหยุ่นในการใช้หลักการโดยคำนึงถึงบริบทที่หน่วยงานตั้งใจจะแบ่งปันข้อมูลและอาจจำเป็นต้องพิจารณาคำถามอื่น ๆ ที่เกี่ยวข้องประกอบกัน หลักการแบ่งปันข้อมูลอ้างอิงตามกรอบงานด้านความปลอดภัย 5 ประการ (Five Safes Framework) ซึ่งพัฒนาขึ้นโดยสำนักงานสถิติแห่งชาติแห่งสหราชอาณาจักร Five Safes Framework ถือเป็นแนวมาตรฐานสากลที่เป็นที่ยอมรับในการเปิดเผยการบริหารความเสี่ยง และรัฐบาลประเทศออสเตรเลียได้ปรับเปลี่ยนเป็นหลักการในการทำงานที่เน้นเกณฑ์พิจารณาโดยกว้างที่เกี่ยวข้องกับการแบ่งปันข้อมูลระหว่างหน่วยงานภาครัฐ และจัดทำ Best Practice Guide to Applying Data Sharing Principles เพื่อเป็นคู่มือในการประยุกต์ใช้หลักการแบ่งปันข้อมูลภาครัฐ หลักการนี้สนับสนุนวิธีการการ

ออกแบบความเป็นส่วนตัวของข้อมูลในการแบ่งปันข้อมูลด้วยการสร้างสมดุลระหว่างประโยชน์ของการใช้ข้อมูลภาครัฐกับระดับการควบคุมและการจัดการความเสี่ยง โดยเฉพาะอย่างยิ่งการจัดการความเสี่ยงในการเปิดเผยข้อมูล โดยเน้นการควบคุมและผลประโยชน์ แทนที่จะลดระดับของรายละเอียดของข้อมูลที่จะแบ่งปันเพียงอย่างเดียว ซึ่งจะสามารถช่วยให้ใช้ประโยชน์ของข้อมูลได้อย่างเต็มที่สูงสุด

อย่างไรก็ดี หน่วยงานอาจยังขาดความมั่นใจที่จะแบ่งปันชุดข้อมูลต่อสาธารณะเนื่องจากความเสี่ยงในการระบุบุคคลที่จะให้ข้อมูล แต่ภายในหน่วยงานเดียวกันอาจสามารถแบ่งปันชุดข้อมูลโดยมีเพียงการป้องกันข้อมูลพื้นฐานที่มีอยู่ อาทิ การลบชื่อและที่อยู่ก่อนแบ่งปันกับเจ้าหน้าที่ที่ได้รับอนุญาตให้เข้าถึงได้ในสภาพแวดล้อมที่ปลอดภัย หรืออีกทางเลือกคือแบบฟอร์มการรวบรวมข้อมูลประเภทเดียวกันซึ่งไม่ได้ระบุตัวบุคคลหรือนิติบุคคลอาจเผยแพร่บนเว็บไซต์เพื่อการใช้งานสาธารณะ วิธีการที่ยืดหยุ่นนี้อาจเพิ่มโอกาสในการเข้าถึงข้อมูลได้และสามารถนำไปสู่ผลลัพธ์ที่ดีขึ้นสำหรับการวิจัยและการตัดสินใจ ในขณะที่ยังคงสร้างความเชื่อมั่นในการปกป้องคุ้มครองข้อมูลได้อย่างเหมาะสมและปลอดภัย

3. ร่างหลักเกณฑ์การจัดชั้นความลับและร่างหลักการและเงื่อนไขการแบ่งปันข้อมูล

3.1 เป้าประสงค์

ร่างหลักเกณฑ์การจัดชั้นความลับของข้อมูลและแบ่งปันข้อมูลภาครัฐจัดทำขึ้นเพื่อใช้เป็นเกณฑ์สำหรับการประเมินความอ่อนไหวของข้อมูล ด้วยการวัดจากผลกระทบต่อการดำเนินภารกิจและผลประโยชน์แห่งชาติที่ไม่พึงประสงค์ รวมทั้งความเสี่ยงที่อาจจะเกิดขึ้นกรณีเกิดการละเมิดข้อมูลหรือการรั่วไหลของข้อมูลโดยไม่ได้รับอนุญาตซึ่งจะส่งผลต่อหน่วยงานของรัฐ ซึ่งร่างหลักเกณฑ์นี้จะช่วยให้หน่วยงานของรัฐสามารถจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ โดยในการพิจารณาว่าจะปกป้องคุ้มครองและจัดการข้อมูลอย่างไรนั้นขึ้นอยู่กับการพิจารณาประเภท ความสำคัญ และการใช้งานของข้อมูล โดยเป็นการระบุระดับการคุ้มครองข้อมูลขั้นต่ำที่จำเป็นเมื่อดำเนินภารกิจขององค์กรและแบ่งปันข้อมูลระหว่างหน่วยงานภาครัฐโดยอ้างอิงจากการจัดชั้นความลับของข้อมูลที่ได้รับการจัดการ (Handled)

โดย**ร่างหลักเกณฑ์นี้จะใช้เพื่อพิจารณากำหนดชั้นความลับของข้อมูลภาครัฐ** และเพื่อลดการใช้ดุลพินิจของผู้มีอำนาจในการตัดสินใจกำหนดชั้นความลับของข้อมูล สามารถกำหนดการเข้าถึงและใช้งานข้อมูลและกำกับดูแลข้อมูลที่มีความอ่อนไหวหรือที่มีชั้นความลับอย่างเหมาะสมเพื่อรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล รวมทั้งกำหนดนโยบายการแบ่งปันข้อมูลระหว่างหน่วยงานภาครัฐโดยไม่ขัดต่อข้อกฎหมายที่เกี่ยวข้อง

3.2 ขอบเขต

ร่างหลักเกณฑ์การจัดชั้นความลับของข้อมูลและแบ่งปันข้อมูลภาครัฐ ประกอบด้วย การจัดหมวดหมู่และระดับชั้นความลับของข้อมูลภาครัฐ (Data Categories and Data Classification) เกณฑ์การแบ่งระดับชั้นความลับของข้อมูลภาครัฐ (Data Classification Level) เกณฑ์การประเมินความเสี่ยงและผลกระทบของการเปิดเผยข้อมูลภาครัฐ (Data Risk Assessment) โดยพิจารณาจากระดับผลกระทบตามวัตถุประสงค์ด้านความปลอดภัยของข้อมูล (CIA)[1] และเกณฑ์พิจารณาผลกระทบ (Impact) ทั้งด้านภาพลักษณ์/ชื่อเสียง (Reputation) ผู้ใช้บริการและการดำเนินงานตามภารกิจ (Users & Operations) การเงินและสินทรัพย์ (Financial & Assets) และความสอดคล้องกับกฎระเบียบและข้อบังคับ (Legal & Regulation) รวมทั้งเกณฑ์พิจารณาผลประโยชน์แห่งชาติ (National Interests) ร่วมกับการประเมินความเสี่ยงจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตหรือการรั่วไหลของข้อมูลอ่อนไหวหรือที่มีการจัดชั้นความลับ

---

[1] ความมั่นคงปลอดภัยของสารสนเทศมีองค์ประกอบด้วยกัน 3 ประการ ได้แก่ ด้านความลับ (Confidentiality) ด้านความถูกต้อง ครบถ้วนสมบูรณ์ ความคงสภาพ (Integrity) ด้านความพร้อมใช้งาน (Availability)

ร่างหลักเกณฑ์นี้สามารถใช้กับทุกข้อมูลที่แลกเปลี่ยนกันได้ในรูปแบบอิเล็กทรอนิกส์เท่านั้น ไม่ว่าจะเป็นข้อมูลประเภทใด ซึ่งรวมถึงข้อมูลลับในรูปแบบอิเล็กทรอนิกส์ ที่มีการสร้าง รวบรวม จัดเก็บ หรือประมวลผลโดยเจ้าหน้าที่ของหน่วยงานภาครัฐในรูปแบบอิเล็กทรอนิกส์ และใช้กับเจ้าหน้าที่รัฐและพนักงาน รวมทั้งบุคคลที่สามที่เกี่ยวข้องอื่น ๆ เช่น หน่วยงานเครือข่าย ที่ปรึกษา ผู้รับจ้าง (vendors) ผู้รับจ้างอิสระ ฯลฯ ซึ่งจัดการ/ดูแลข้อมูล ข้อมูลข่าวสารและระเบียนข้อมูลในรูปแบบต่าง ๆ เช่น ข้อความดิจิทัล รูปภาพ เสียง วิดีโอ เป็นต้น ระหว่างดำเนินงานของหน่วยงาน อาทิ การบริหาร การเงิน การวิจัย และ/หรือ การบริการ โดยใช้เป็นเกณฑ์พิจารณากำหนดประเภทของข้อมูลที่ต้องจัดชั้นความลับและระบุว่าผู้รับผิดชอบในการจำแนกชั้นความลับของข้อมูล การคุ้มครองและจัดการข้อมูลที่เหมาะสม

สำหรับทิศทางการจัดชั้นความลับและแบ่งปันข้อมูลภาครัฐ ควรกำหนด Data champion ซึ่งมีบทบาทเป็นบริกรข้อมูล (Data steward) ที่องค์กรควรให้ความสำคัญและลงทุนมากที่สุด และ Data champion ควรจะมีประสิทธิภาพในการสื่อสารข้อจำกัดของระบบเทคโนโลยีสารสนเทศกับผู้ใช้งานข้อมูล รวมทั้งส่งเสริมการกำกับดูแลและจัดการข้อมูล ทั้งนี้ เพื่อสร้างความเชื่อมั่นว่าเจ้าหน้าที่ของหน่วยงานเข้าใจว่าข้อมูลที่สร้างขึ้นมีคุณค่า และคุ้มค่าหรือควรค่าแก่การปกป้องคุ้มครองจากภัยคุกคามทั้งภายในและภายนอกองค์กร และเจ้าหน้าที่เหล่านั้นเป็นส่วนสำคัญของการจัดการและคุ้มครองข้อมูลของหน่วยงาน

3.3 ร่างหลักเกณฑ์การจัดชั้นความลับข้อมูลภาครัฐ

จากการศึกษาแนวทางจากต่างประเทศที่มีการประเมินผลกระทบและระดับความเสี่ยงเข้าด้วยกันว่าควรเปิดเผยข้อมูลข่าวสารลับหรือไม่ และเปิดเผยได้มากน้อยเพียงใด เพื่อให้ผู้บริหารมีแนวทางในการเปิดเผยข้อมูลความลับทางราชการ เพื่อให้เกิดการใช้ประโยชน์จากข้อมูลและสร้างวัฒนธรรม Open by default หน่วยงานของรัฐควรสำรวจและเลือกชุดข้อมูลสำคัญที่สอดคล้องตามภารกิจของหน่วยงานเพื่อนำมาจัดหมวดหมู่และชั้นความลับ เพื่อให้สามารถกำกับดูแล จัดการ และจัดเก็บข้อมูลได้อย่างปลอดภัยและใช้งานข้อมูลอย่างถูกต้องเหมาะสมในแต่ละระดับชั้นความลับ รวมทั้งสามารถแบ่งปันและใช้งานข้อมูลร่วมกันระหว่างหน่วยงานภาครัฐได้

3.3.1 การจัดหมวดหมู่และการจัดชั้นความลับของข้อมูลภาครัฐ (Data Classification Schemes)

จากหลักการและแนวคิดข้างต้นสามารถพิจารณาการจัดหมวดหมู่ของข้อมูลเป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ (DGF) ได้แก่ ข้อมูลสาธารณะ ข้อมูลส่วนบุคคล ข้อมูลความลับทางราชการ และข้อมูลความมั่นคง และพิจารณาการจัดระดับชั้นความลับของข้อมูลภาครัฐที่มีความอ่อนไหวให้สอดคล้องตามแนวมาตรฐานสากลและเป็นไปตามข้อกฎหมายที่เกี่ยวข้อง โดยการจัดชั้นความลับของข้อมูลเพื่อบริหารจัดการข้อมูลภายในหน่วยงานแบ่งออกเป็น ชั้นเปิดเผย (Open) สู่สาธารณะ เปิดเผยเมื่อได้รับอนุญาต ได้แก่ ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) และ ชั้นลับมาก (Secret) และเปิดเผยไม่ได้/ปกปิด ได้แก่ ชั้นลับที่สุด (Top Secret) ทั้งนี้ ข้อมูลใช้ภายในควรมีการจัดแบ่งหมวดหมู่ตาม DGF ก่อนจัดแบ่งระดับชั้นความลับของข้อมูลภาครัฐ ดังแสดงตามรูปที่ 4

Data Class. Level / Data Category	เปิดเผย (Open)	เผยแพร่ภายในองค์กร (Private)	ลับ (Confidential / sensitive)	ลับมาก (Secret / Medium Sensitive)	ลับที่สุด (Top secret / Highly Sensitive)
ข้อมูลสาธารณะ	▪ พ.ร.บ. ข้อมูลข่าวสารของทางราชการ 2540 (มาตรา 7 และมาตรา 9) ▪ มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลภาครัฐ				
ข้อมูลใช้ภายใน		**ISO 27001: 2013**			
ข้อมูลส่วนบุคคล		**พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562 (มาตรา 24 – มาตรา 27)**	**พ.ร.บ. ข้อมูลข่าวสารของทางราชการ 2540 (มาตรา 9 และมาตรา 15 ที่เปิดเผยได้)**		
ข้อมูลข่าวสารลับ			**ระเบียบว่าด้วยการรักษาความลับของทางราชการ 2544**		**▪ พ.ร.บ. ข้อมูลข่าวสารของทางราชการ 2540 (มาตรา 14 – มาตรา 15 อาจมีคำสั่งมิให้เปิดเผย)**
ข้อมูลความมั่นคง			**นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2562-2565)**		

รูปที่ 5 การจัดหมวดหมู่และระดับชั้นความลับของข้อมูลภาครัฐ

โดยมีแนวทางการจัดหมวดหมู่และชั้นความลับของข้อมูลภาครัฐดังนี้

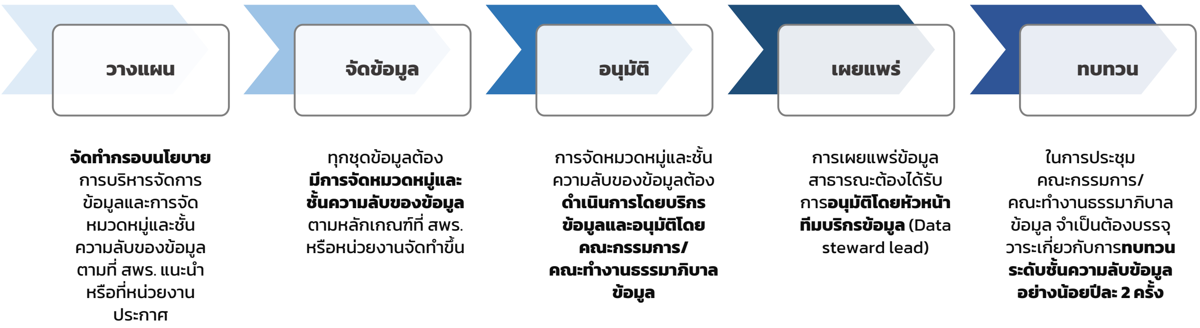
1) จัดทำกรอบนโยบายการบริหารจัดการข้อมูลและการจัดหมวดหมู่และชั้นความลับของข้อมูลตามที่ สพร. แนะนำ หรือที่หน่วยงานประกาศ

2) ทุกชุดข้อมูลต้องมีการจัดหมวดหมู่และชั้นความลับของข้อมูลตามหลักเกณฑ์ที่ สพร. หรือหน่วยงานจัดทำขึ้น

3) การจัดหมวดหมู่และชั้นความลับของข้อมูลต้องดำเนินการโดยบริกรข้อมูลและอนุมัติโดยคณะกรรมการ/คณะทำงานธรรมาภิบาลข้อมูล

4) การเผยแพร่ข้อมูลสาธารณะต้องได้รับการอนุมัติโดยหัวหน้าทีมบริกรข้อมูล (Data steward lead)

5) ในการประชุมคณะกรรมการ/คณะทำงานธรรมาภิบาลข้อมูล จำเป็นต้องบรรจุวาระเกี่ยวกับการทบทวนระดับชั้นความลับข้อมูลอย่างน้อยปีละ 2 ครั้ง



วางแผน	จัดข้อมูล	อนุมัติ	เผยแพร่	ทบทวน
จัดทำกรอบนโยบาย การบริหารจัดการข้อมูลและการจัดหมวดหมู่และชั้นความลับของข้อมูลตามที่ สพร. แนะนำหรือที่หน่วยงานประกาศ	ทุกชุดข้อมูลต้อง**มีการจัดหมวดหมู่และชั้นความลับของข้อมูล**ตามหลักเกณฑ์ที่ สพร. หรือหน่วยงานจัดทำขึ้น	การจัดหมวดหมู่และชั้นความลับของข้อมูลต้อง**ดำเนินการโดยบริกรข้อมูลและอนุมัติโดยคณะกรรมการ/คณะทำงานธรรมาภิบาลข้อมูล**	การเผยแพร่ข้อมูลสาธารณะต้องได้รับการ**อนุมัติโดยหัวหน้าทีมบริกรข้อมูล** (Data steward lead)	ในการประชุมคณะกรรมการ/คณะทำงานธรรมาภิบาลข้อมูล จำเป็นต้องบรรจุวาระเกี่ยวกับการ**ทบทวนระดับชั้นความลับข้อมูลอย่างน้อยปีละ 2 ครั้ง**

รูปที่ 6 แนวทางการจัดหมวดหมู่และชั้นความลับของข้อมูลภาครัฐ

สำหรับคำแนะนำในการดำเนินการจัดหมวดหมู่และชั้นความลับของข้อมูลของหน่วยงานภาครัฐเพื่อให้เป็นมาตรฐานเดียวกัน ดังต่อไปนี้

✓ การควบคุมและการดำเนินการเกี่ยวกับข้อมูลข่าวสารลับให้เป็นดุลพินิจของหัวหน้าหน่วยงานของรัฐนั้น ๆ ที่จะกำหนดแนวทางที่เหมาะสม ทั้งการมอบหมายหน้าที่หรือ แต่งตั้งเจ้าหน้าที่รับผิดชอบ โดยต้องคำนึงถึงการปฏิบัติในการเปิดเผยข้อมูลให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของราชการฯ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 และระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง

ทั้งนี้ ในกรณีของการลงทะเบียนบัญชีข้อมูลหน่วยงานที่เป็นข้อมูลข่าวสารลับ หัวหน้าหน่วยงานของรัฐสามารถแต่งตั้งให้นายทะเบียนข้อมูลข่าวสารลับเป็นนายทะเบียนบัญชีข้อมูลหน่วยงาน หรืออาจกำหนดให้นายทะเบียนบัญชีข้อมูลหน่วยงานให้เข้าถึงข้อมูลข่าวสารลับได้เฉพาะเรื่องที่ได้รับมอบหมายเท่านั้น ตามข้อ 8 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ตามที่ระเบียบฯ รปภ. 2552 และประกาศที่เกี่ยวข้อง กำหนดไว้

ผู้เกี่ยวข้องกับข้อมูลข่าวสารลับ (Role player) ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

หัวหน้าหน่วยงาน
มีอำนาจในการดำเนินการมอบหมายหน้าที่หรือ แต่งตั้งเจ้าหน้าที่รับผิดชอบเกี่ยวกับข้อมูลข่าวสารลับ

ผู้มีอำนาจกำหนดชั้นความลับ
(เจ้าของเรื่อง Data Owner)

ผู้มีอำนาจกำหนดชั้นความลับ (เจ้าของเรื่องที่ผ่านการรับรองความไว้วางใจ ตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552) เกี่ยวข้องกับข้อมูลข่าวสารลับ

หน้าที่เกี่ยวกับข้อมูลข่าวสารลับ

- จัดทำ
- สำนา/แปล
- จัดส่ง
- ตรวจสอบ
- (ปรับ/ยกเลิก Declassified)
- เปิดเผย
- ทำลาย

นายทะเบียนข้อมูลข่าวสารลับ
ผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับ

เป็นผู้ดำเนินการทางทะเบียน คือ การออกเลขที่หนังสือ การดำเนินการลงบันทึกข้อมูลในทะเบียนรับ ส่ง ทะเบียนควบคุมข้อมูลข่าวสารลับ การร่วมเป็นคณะกรรมการตรวจสอบ คณะกรรมการทำลาย การดำเนินการในขั้นตอนการขอทำลายข้อมูลข่าวสารลับ และการดำเนินการทางทะเบียนเมื่อเกิดเหตุละเมิด รั่วไหล

หน้าที่เกี่ยวกับข้อมูลข่าวสารลับ

- รับ-ส่ง /ออกเลขหนังสือ
- บรรจุซอง/ส่งทางระบบอิเล็กฯ
- สำเนา/แปล
- ตรวจสอบทางทะเบียน
- ลงบันทึกทางทะเบียน (ทุกกิจกรรม รับ ส่ง หาย ทำลาย เปิดเผย)
- ทำลาย/สอบสวน

คณะกรรมการฯ

เป็นผู้พิจาณาขั้นตอนต่าง ๆ ที่เกี่ยวกับวงจรชีวิตของข้อมูลข่าวสารลับ ประกอบด้วย 3 คณะ ได้แก่

1) คณะกรรมการตรวจสอบข้อมูลข่าวสารลับ
2) คณะกรรมการทำลายข้อมูลข่าวสารลับ
3) คณะกรรมการสอบสวน (กรณีมีการละเมิดข้อมูลข่าวสารลับ)

หน้าที่เกี่ยวกับข้อมูลข่าวสารลับ

- ตรวจสอบข้อมูลทำลายข้อมูล
- สอบสวนเมื่อข้อมูล
- ละเมิด/รั่วไหล

รูปที่ 7 ผู้ที่เกี่ยวข้องกับข้อมูลข่าวสารลับ

✓ ทุกฟิลด์ในแต่ละชุดข้อมูลถือว่ามีระดับชั้นความลับเท่ากัน

✓ ในกรณีชุดข้อมูลที่มีผลกระทบในเชิงพื้นที่ เช่น ประเทศ จังหวัด ท้องถิ่น เป็นต้น หน่วยงานสามารถกำหนดเกณฑ์ประกอบการพิจารณาเพิ่มเติมได้

✓ หากหน่วยงานมีการอ้างอิงหลักเกณฑ์และ/หรือมาตรฐานของต่างประเทศอยู่แล้วให้ดำเนินการตามมาตรฐานดังกล่าว

✓ สำหรับชุดข้อมูลที่มีการจัดระดับความลับในหมวดหมู่ข้อมูลส่วนบุคคล ข้อมูลความลับทางราชการ และข้อมูลความมั่นคง รวมถึงข้อมูลใช้ภายในองค์กร จำเป็นต้องระบุสิทธิ์ในการเข้าถึงและใช้งานข้อมูล

✓ หากชุดข้อมูลมีความอ่อนไหวทั้งด้านความเป็นส่วนตัว และความมั่นคง หน่วยงานสามารถพิจารณาแยกชุดข้อมูลและติดสินใจเผยแพร่หรือไม่เผยแพร่ข้อมูลให้สอดคล้องกับข้อกฎหมายที่เกี่ยวข้องและเกณฑ์การจัดชั้นความลับตามที่หน่วยงานกำหนด

✓ ข้อมูลอ่อนไหวที่ได้รับการจัดชั้นความลับจะต้องมีกระบวนการในการเข้าถึงข้อมูลตามกระบวนการและปฏิบัติตามข้อกฎหมายที่เกี่ยวข้องหรือตามข้อกำหนดของหน่วยงาน

✓ ข้อมูลที่อยู่ในชั้นความลับ “ลับที่สุด” จะไม่สามารถนำเข้าในระบบสารสนเทศได้ ต้องดำเนินการในรูปแบบเอกสาร (Hard Copy) เท่านั้น

✓ ในกรณีที่ผู้ร้องขอข้อมูลไม่ได้มีสิทธิ์ตามสิทธิ์การเข้าถึงข้อมูลจำเป็นต้องดำเนินการตามกระบวนการดังต่อไปนี้

- ข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคล (Data subject) จะต้องทำการร้องขอผ่านส่วนงานที่ถือครองข้อมูล และส่วนงานที่เป็นเจ้าของข้อมูล (Data owner) โดยแจ้งวัตถุประสงค์ให้ชัดเจน โดยส่วนงานที่เป็นเจ้าของข้อมูล และ ผู้ควบคุมข้อมูลส่วนบุคคล (Data controller) ต้องรับทราบและมีสิทธิ์ที่จะปฏิเสธ

การร้องขอนั้นเว้นแต่จะมีระเบียบหรือประกาศของหน่วยงานรองรับ และต้องเป็นไปตามแนวปฏิบัติตามข้อกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

- ข้อมูลความลับทางราชการ และ ข้อมูลความมั่นคง ต้องมีการร้องขอผ่านส่วนงานที่เป็นเจ้าของข้อมูล โดยหัวหน้าส่วนงานและบริกรข้อมูลต้องพิจารณาร่วมกัน หากเป็นข้อมูลที่มีความอ่อนไหวหรือมีความเสี่ยงต้องได้รับการอนุมัติ หัวหน้าหน่วยงานของรัฐหรือเจ้าหน้าที่รัฐที่ได้รับมอบหมายเป็นผู้มีอำนาจหน้าที่เปิดเผยข้อมูล โดยการเปิดเผยมีข้อยกเว้นความผิดทางละเมิดตามข้อ 49 และข้อ 50 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม
- ข้อมูลใช้ภายใน ต้องมีการร้องขอผ่านส่วนงานที่เป็นเจ้าของข้อมูล โดยต้องได้รับอนุญาตจากหัวหน้าส่วนงานและหัวหน้าทีมบริกรข้อมูล

1) เทคโนโลยีการจัดชั้นความลับของข้อมูล

- ระดับชั้นความลับข้อมูลจะต้องถูกระบุไว้ในเมทาดาตา ดังนั้นจึงจำเป็นต้องมีระบบในการจัดการเมทาดาตา (Metadata Management System) เพื่อกำหนดสิทธิการเข้าถึงและการนำข้อมูลไปใช้ได้อย่างเหมาะสม รักษาความปลอดภัยของข้อมูล และสอดคล้องกับกฎหมาย กฎระเบียบหน่วยงาน เพื่อส่งเสริมให้เกิดแลกเปลี่ยนหรือเปิดเผยข้อมูลของหน่วยงานรัฐได้
- การร้องขอข้อมูลต้องทำผ่านระบบและมีการเก็บบันทึก (Logging System) ด้วย

3.3.2 ร่างเกณฑ์การแบ่งระดับชั้นความลับของข้อมูลภาครัฐ (Data Classification Level)

หมวดหมู่ของข้อมูลแบ่ง ได้เป็น 1) ข้อมูลสาธารณะ 2) ข้อมูลส่วนบุคคล 3) ข้อมูลความลับทางราชการ และ 4) ข้อมูลความมั่นคง และพิจารณาการจัดระดับชั้นความลับของข้อมูลภาครัฐตามผลกระทบที่จะเกิดขึ้นตามแนวมาตรฐานสากลและเป็นไปตามข้อกฎหมายที่เกี่ยวข้อง **ทั้งนี้ นิยามการกำหนดชั้นความลับและแนวทางในการกำหนดชั้นความลับ (Classification) และปรับชั้นความลับ (Declassification) ให้อ้างอิงตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม** ซึ่งระดับชั้นความลับข้อมูลสามารถแบ่งได้ 5 ระดับ ได้แก่

1) ชั้นเปิดเผย (Open) สู่สาธารณะ เป็นข้อมูลข่าวสารของราชการที่หน่วยงานของรัฐต้องเปิดเผยให้ประชาชนได้รับรู้ รับทราบ หรือตรวจสอบได้โดยไม่จำเป็นต้องร้องขอ เช่น กฎ มติ ค.ร.ม. ข้อบังคับ รายงานผลการ ศึกษาทางวิชาการ และข้อมูลเปิดภาครัฐ ฯลฯ

2) ชั้นเผยแพร่ภายในองค์กร (Private) เปิดเผยเมื่อได้รับอนุญาต เป็นข้อมูลที่องค์กรไม่ได้เผยแพร่โดยอิสระ โดยทั่วไปจะเกี่ยวข้องกับข้อมูลที่มีลักษณะเป็นส่วนตัว (Private) ไม่ว่าจะกับข้อมูลบุคคลหรือองค์กร **และแม้ว่าการสูญเสียหรือการเปิดเผยข้อมูลอาจไม่ส่งผลให้เกิดผลกระทบที่สำคัญ แต่ก็ไม่พึงประสงค์ที่ให้เปิดเผยโดยไม่ได้รับอนุญาต** เช่น ข้อมูลระเบียน ข้อมูลพนักงาน เอกสารประกอบการปฏิบัติงาน และ วิธีปฏิบัติภายในหน่วยงาน ฯลฯ

3) ชั้นลับ (Confidential) เปิดเผยเมื่อได้รับอนุญาต เป็นข้อมูลที่มีระดับ Confidential หรือ Sensitive จะก่อให้เกิดความสูญเสีย หากมีการเปิดเผยต่อบุคคล/องค์กรที่ไม่ได้รับอนุญาตและส่งผลให้เกิดความอับอายอย่างมากต่อบุคคล/องค์กร และอาจเป็นผลทางกฎหมาย หรือจะก่อให้เกิดความเสียหายแก่**ผลประโยชน์แห่งรัฐ** เช่น ข้อมูลการฟ้องคดี และความเห็นภายในหน่วยงานที่ยังไม่ได้ข้อยุติ ฯลฯ

4) ชั้นลับมาก (Secret) เปิดเผยเมื่อได้รับอนุญาต เป็นข้อมูลที่จัดระดับ Secret หรือ Medium Sensitive สงวนไว้สำหรับข้อมูลที่จะก่อให้เกิดความสูญเสีย/ผลกระทบร้ายแรง อาจทำให้ชื่อเสียงและการสูญเสียทางการเงิน/ทรัพย์สิน ต่อความมั่นคงและ**ผลประโยชน์แห่งรัฐอย่างร้ายแรง หรือ ที่มีนัยสำคัญ (Importance)** หากสูญหายหรือเปิดเผยอย่างไม่ถูกต้องเหมาะสม เช่น รายงานการแพทย์ ข้อมูลความสัมพันธ์ระหว่างประเทศ และนโยบายสำคัญที่ใช้ปฏิบัติต่อรัฐต่างประเทศ ฯลฯ

5) ชั้นลับที่สุด (Top Secret) เปิดเผยไม่ได้ เป็นข้อมูลที่จัดระดับ Top Secret หรือ Highly Sensitive จำกัดการใช้/ไม่เปิดเผยสำหรับข้อมูลที่จะ**ก่อให้เกิดความสูญเสีย/ผลกระทบ ร้ายแรงที่สุด** อาจทำให้ชื่อเสียงและการสูญเสียทางการเงิน/ทรัพย์สิน ต่อความมั่นคงและ**ผลประโยชน์แห่งรัฐอย่างร้ายแรง หรือที่สำคัญยิ่งยวด (Vital)** หากสูญหายหรือเปิดเผยอย่างไม่ถูกต้องเหมาะสม **ซึ่งในกรณีข้อมูลที่อยู่ในชั้นความลับ "ลับที่สุด"จะไม่สามารถนำเข้าในระบบสารสนเทศได้ ต้องดำเนินการในรูปแบบเอกสาร (Hard Copy) เท่านั้น** เช่น ข้อมูลกำลังรบ ข้อมูลด้านการข่าวกรองยุทธศาสตร์ ข้อมูลความมั่นคงเชิงนโยบาย

สำหรับนิยามศัพท์ที่เกี่ยวข้องกับร่างหลักเกณฑ์ฯ ฉบับนี้ สามารถดูรายละเอียดได้ที่ ***อภิธานศัพท์***

หน่วยงานสามารถพิจารณาการจัดระดับชั้นความลับของข้อมูล โดยใช้เกณฑ์ดังต่อไปนี้ความลับของข้อมูล โดยใช้เกณฑ์ดังต่อไปนี้

Open	Private *(กระทบระดับบุคคล/องค์กร)*	Confidential / sensitive *(กระทบระดับบุคคล/องค์กร)*	Secret / Medium Sensitive *(กระทบระดับองค์กร/ประเทศ)*	Top secret / Highly Sensitive *(กระทบระดับองค์กร/ประเทศ)*
เกณฑ์การพิจารณาแบ่งระดับชั้นความลับ (Classification Criteria)*				
ตาม พ.ร.บ. ข้อมูลข่าวสารฯ **มาตรา 7** หน่วยงานของรัฐต้องส่งข้อมูลข่าวสาร ของราชการอย่างน้อยดังต่อไปนี้ลงพิมพ์ในราชกิจจานุเบกษา **มาตรา 9** ภายใต้บังคับมาตรา 14 และมาตรา 15 หน่วยงานของรัฐต้องจัดให้มีข้อมูลข่าวสารของราชการอย่างน้อยดังต่อไปนี้ไว้ให้ประชาชนเข้าตรวจดูได้ ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนด	**ข้อมูลจะถูกเป็นชั้น “Private” หรือไม่** รวมถึงการเปิดเผยโดยไม่ได้รับอนุญาตหรือไม่: ✓ สร้างความทุกข์ใจให้กับบุคคล ✓ ละเมิดการดำเนินการที่เหมาะสมเพื่อรักษาความเชื่อใจของข้อมูลที่ให้โดยบุคคลที่สาม ✓ ละเมิดข้อจำกัดทางกฎหมายในการเปิดเผยข้อมูล ✓ ทำให้เกิดการสูญเสียทางการเงินหรือสูญเสียศักยภาพในการหารายได้ หรือเพื่ออำนวยความสะดวกในการได้รับผลประโยชน์ที่ไม่เหมาะสม ✓ ให้ผลประโยชน์ที่ไม่เป็นธรรมแก่บุคคลหรือองค์กร ✓ สูญเสียความได้เปรียบขององค์กรเชิงพาณิชย์หรือนโยบายในการเจรจากับผู้อื่น	**ข้อมูลจะถูกจัดเป็นชั้น “Confidential” หรือไม่** รวมถึงการเปิดเผยโดยไม่ได้รับอนุญาตหรือไม่: ✓ ส่งผลกระทบต่อความสัมพันธ์กับองค์กร/ประเทศอื่นในทางลบ ✓ ก่อให้เกิดความทุกข์ใจอย่างมากต่อบุคคล ✓ ทำให้เกิดการสูญเสียทางการเงินหรือการสูญเสียศักยภาพในการหารายได้หรือเพื่ออำนวยความสะดวกในการได้รับผลประโยชน์หรือความได้เปรียบที่ไม่เหมาะสมสำหรับบุคคลหรือองค์กรหรือประเทศต่าง ๆ ✓ ฝ่าฝืนการดำเนินการที่เหมาะสมเพื่อรักษาความมั่นใจของข้อมูลที่ให้โดยบุคคลที่สาม ✓ ขัดขวางการพัฒนาที่มีประสิทธิภาพหรือการดำเนินงานตามนโยบายขององค์กร ✓ ฝ่าฝืนข้อจำกัดทางกฎหมายในการเปิดเผยข้อมูล ✓ สูญเสียความได้เปรียบขององค์กรเชิงพาณิชย์หรือนโยบายในการเจรจากับผู้อื่น ✓ บ่อนทำลายการจัดการที่เหมาะสมและการดำเนินงานขององค์กร	**ข้อมูลจะถูกจัดเป็นชั้น “Secret” หรือไม่** รวมถึงการเปิดเผยโดยไม่ได้รับอนุญาตหรือไม่: ✓ สร้างความเสียหายอย่างมีนัยสำคัญต่อความสัมพันธ์กับองค์กรอื่น ๆ (เช่น ก่อให้เกิดการประท้วงอย่างเป็นทางการหรือการลงโทษอื่น ๆ) ✓ สร้างความเสียหายต่อประสิทธิภาพการดำเนินงานหรือความปลอดภัยขององค์กร/ประเทศ ✓ ภารกิจงานสำคัญที่กระทบต่อด้านการเงินขององค์กร หรือผลประโยชน์ทางเศรษฐกิจและการค้าของประเทศ ✓ บ่อนทำลายศักยภาพทางการเงินส่วนใหญ่ขององค์กร/ประเทศ ✓ ขัดขวางการพัฒนาหรือการดำเนินงานของนโยบายองค์กร/ประเทศอย่างจริงจัง ✓ ปิดตัวลงหรือขัดขวางการดำเนินงาน/โครงการที่สำคัญขององค์กร/ประเทศ	ตาม พ.ร.บ. ข้อมูลข่าวสารฯ มาตรา 14 ข้อมูลข่าวสารของราชการที่อาจก่อให้ เกิดความเสียหายต่อสถาบันพระมหากษัตริย์จะเปิดเผยมิได้ มาตรา 15 ข้อมูลข่าวสารของราชการ... หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐอาจมีคำสั่งมิให้เปิดเผยก็ได้ โดยคำนึงถึงการปฏิบัติหน้าที่ตามกฎหมาย ประโยชน์สาธารณะ และประโยชน์ของเอกชนที่เกี่ยวข้องประกอบกัน ✓ ข้อมูลจะถูกจัดเป็นชั้น “Top Secret” หรือไม่ รวมถึงการเปิดเผยโดยไม่ได้รับอนุญาตหรือไม่: ✓ ก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศ และความมั่นคงในทางเศรษฐกิจหรือการคลังของประเทศ ✓ ทำให้การบังคับใช้กฎหมายเสื่อมประสิทธิภาพ หรือไม่อาจสำเร็จตามวัตถุประสงค์ได้ ไม่ว่าจะเกี่ยวกับการฟ้องคดี การป้องกัน การปราบปราม การทดสอบ การตรวจสอบ หรือการรู้แหล่งที่มาของข้อมูลข่าวสารหรือไม่ก็ตาม ✓ ความเห็นหรือคำแนะนำภายในหน่วยงานของรัฐในการดำเนินการเรื่องหนึ่งเรื่องใด แต่ทั้งนี้ไม่รวมถึงรายงานทางวิชาการ รายงานข้อ เท็จจริง หรือข้อมูลข่าวสารที่

Open	Private *(กระทบระดับบุคคล/องค์กร)*	Confidential / sensitive *(กระทบระดับบุคคล/องค์กร)*	Secret / Medium Sensitive *(กระทบระดับองค์กร/ประเทศ)*	Top secret / Highly Sensitive *(กระทบระดับองค์กร/ประเทศ)*
				นำมาใช้ในการทำความเห็นหรือคำแนะนำภายในดังกล่าว ✓ การเปิดเผยจะก่อให้เกิดอันตรายต่อชีวิตหรือความปลอดภัยของบุคคลหนึ่งบุคคลใด ✓ ข้อมูลข่าวสารของราชการที่มีกฎหมายคุ้มครองมิให้เปิดเผย หรือข้อมูลข่าวสารที่มีผู้ให้มาโดยไม่ประสงค์ให้ทางราชการนำไปเปิดเผยต่อผู้อื่น

หมายเหตุ * เกณฑ์การพิจารณาแบ่งระดับชั้นความลับ ได้พิจารณาจากผลกระทบ (Impact) ทั้งด้านภาพลักษณ์/ชื่อเสียง (Reputation) ผู้ใช้บริการและการดำเนินงานตามภารกิจ (Users & Operations) การเงินและสินทรัพย์ (Financial & Assets) ความสอดคล้องกับกฎระเบียบ ข้อบังคับ (Legal & Regulation) โดยไม่มีการจำกัดเงื่อนไขเกณฑ์การพิจารณาการจัดชั้นความลับ

การจัดระดับชั้นความลับของข้อมูลจะส่งผลให้ข้อมูลได้รับการดูแล โดยหน่วยงานสามารถกำหนดเงื่อนไขการเข้าถึงข้อมูลได้ดังตัวอย่างต่อไปนี้

Open	Private *(กระทบระดับบุคคล/องค์กร)*	Confidential / sensitive *(กระทบระดับบุคคล/องค์กร)*	Secret / Medium Sensitive *(กระทบระดับองค์กร/ประเทศ)*	Top secret / Highly Sensitive *(กระทบระดับองค์กร/ประเทศ)*
การเข้าถึง (Access Control)				
ไม่มีการจำกัดการเข้าถึงข้อมูล/เปิดเผยสู่สาธารณะ	**เจ้าหน้าที่ส่วนใหญ่ขององค์กร**มีแนวโน้มที่จะจัดการกับข้อมูล “Private" ในระหว่างการทำงาน/เปิดเผยเมื่อได้รับอนุญาต	มักจะได้รับการจัดการโดย**ผู้บริหารระดับกลางขึ้นไป** โดยที่เจ้าหน้าที่บางคนที่มีระดับต่ำกว่าจะได้รับการเข้าถึงเฉพาะในบางสถานการณ์เท่านั้น/เปิดเผยเมื่อได้รับอนุญาต	จะต้องได้รับการควบคุมอย่างเข้มงวดโดย**ผู้บริหารระดับสูง** และในหลายกรณีจะมีการแจกจ่ายสำเนาเอกสาร ตามระเบียบขั้นตอนเฉพาะขององค์กรและ/หรือประเทศ/เปิดเผยเมื่อได้รับอนุญาต	คำสั่งมิให้เปิดเผยข้อมูลข่าวสารของราชการจะกำหนดเงื่อนไขก็ได้ แต่**ต้องระบุว่าที่เปิดเผยไม่ได้/ปกปิดเพราะเป็นข้อมูลข่าวสารประเภทใดและเพราะเหตุใด** และให้ถือว่าการมีคำสั่งเปิดเผยข้อมูลข่าวสารของราชการ**เป็นดุลพินิจของเจ้าหน้าที่ของรัฐตามลำดับสายการบังคับบัญชา** แต่อาจอุทธรณ์ต่อ คกก. วินิจฉัยการเปิดเผยข้อมูลข่าวสารได้

3.3.3 ร่างเกณฑ์การประเมินความเสี่ยงและผลกระทบของการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (Data Risk Assessment)

1) ข้อควรคำนึงถึง

(1) วัตถุประสงค์ด้านความปลอดภัย (CIA) เทียบกับโอกาสที่จะเกิดผลกระทบ (Impact) ตามมาตรฐาน NIST 800-60 Volume 1. and 2. Guide for Mapping Types of Information and Information Systems to Security Categories ซึ่งสอดคล้องกับแนวการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรา 54 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

(2) องค์ประกอบการกำหนดชั้นความลับ ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ข้อ 19 การกำหนดให้ข้อมูลข่าวสารอยู่ในชั้นความลับใด ให้พิจารณาถึงองค์ประกอบอย่างน้อยดังต่อไปนี้ ความสำคัญของเนื้อหา แหล่งที่มาของข้อมูลข่าวสาร วิธีการนำไปใช้ประโยชน์ จำนวนบุคคลที่ควรรับทราบ ผลกระทบหากมีการเปิดเผย และ หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่องหรือผู้อนุมัติ

(3) ผลประโยชน์แห่งชาติ ตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

- การมีเอกราช อธิปไตย และบูรณภาพแห่งเขตอำนาจรัฐ
- การดำรงอยู่อย่างมั่นคงยั่งยืนของสถาบันหลักของชาติ
- การดำรงอยู่อย่างมั่นคงของชาติและประชาชนจากภัยคุกคามทุกรูปแบบ
- การอยู่ร่วมกันในชาติอย่างสันติสุข เป็นปึกแผ่น มั่นคงทางสังคม ท่ามกลางพหุสังคมและการมีเกียรติ และศักดิ์ศรีของความเป็นมนุษย์
- ความเจริญเติบโตของชาติ ความเป็นธรรม และความอยู่ดีมีสุขของประชาชน
- ความยั่งยืนของฐานทรัพยากรธรรมชาติ สิ่งแวดล้อม ความมั่นคงทางพลังงาน อาหาร
- ความสามารถในการรักษาผลประโยชน์ของชาติภายใต้การเปลี่ยนแปลงของสภาวะแวดล้อมระหว่างประเทศ
- การอยู่ร่วมกันอย่างสันติ มีเกียรติและศักดิ์ศรีในประชาคมอาเซียนและประชาคมโลก

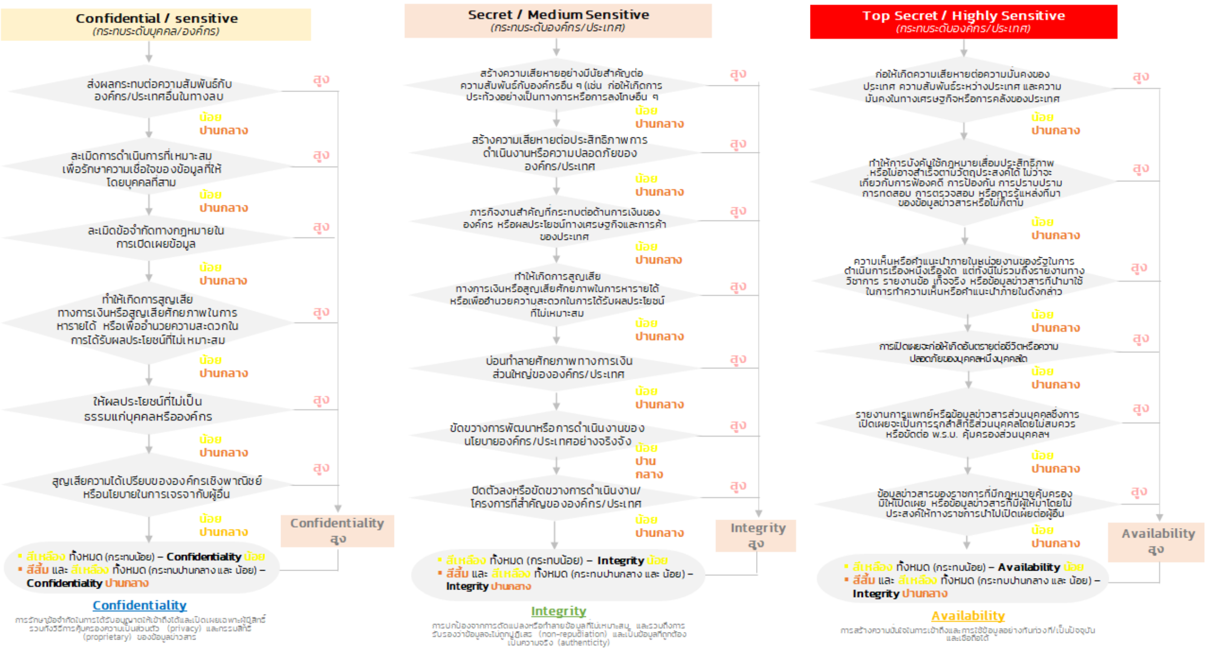
2) ระดับผลกระทบตามวัตถุประสงค์ด้านความปลอดภัยของข้อมูล (CIA)

วัตถุประสงค์ด้านความปลอดภัย (Security Objective)	ผลกระทบ (Impact)* และ ผลประโยชน์แห่งชาติ (National Interests)		
	น้อย (Low)	ปานกลาง (Moderate)	สูง (High)
ด้านความลับ (Confidentiality) การรักษาข้อจำกัดในการได้รับอนุญาตให้เข้าถึงได้และเปิดเผยเฉพาะผู้มีสิทธิ์ รวมทั้งวิธีการคุ้มครองความเป็นส่วนตัว (privacy) และกรรมสิทธิ์ (proprietary) ของข้อมูลข่าวสาร	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (severe or catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
ด้านความถูกต้อง ครบถ้วนสมบูรณ์ ความคงสภาพ (Integrity) การปกป้องจากการดัดแปลงหรือทำลายข้อมูลที่ไม่เหมาะสม และรวมถึงการรับรองว่าข้อมูลจะไม่ถูกปฏิเสธ (non-repudiation) และเป็นข้อมูลที่ถูกต้องเป็นความจริง (authenticity)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (severe or catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

วัตถุประสงค์ด้านความปลอดภัย (Security Objective)	ผลกระทบ (Impact)* และ ผลประโยชน์แห่งชาติ (National Interests)		
	น้อย (Low)	ปานกลาง (Moderate)	สูง (High)
ด้านความพร้อมใช้งาน (Availability) การสร้างความมั่นใจในการเข้าถึงและการใช้ข้อมูลอย่างทันท่วงที/เป็นปัจจุบันและเชื่อถือได้	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรง (serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรงมาก (severe or catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

หมายเหตุ * ผลกระทบ (Impact) แบ่งออกเป็น ด้านภาพลักษณ์/ชื่อเสียง (Reputation) ผู้ใช้บริการและการดำเนินงานตามภารกิจ (Users & Operations) การเงินและสินทรัพย์ (Financial & Assets) และ ความสอดคล้องกับกฎระเบียบข้อบังคับ (Legal & Regulation)

ในการประเมินผลกระทบโดยรวมในแต่ละระดับชั้นความลับให้พิจารณาตามเกณฑ์การแบ่งระดับชั้นความลับ (Classification Criteria) ของข้อมูลตามตามวัตถุประสงค์ด้านความปลอดภัยของข้อมูล (CIA) ซึ่งสามารถทำได้เป็นแผนผังการตัดสินใจจัดระดับชั้นความลับของข้อมูลเทียบกับผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ดังตัวอย่างในรูปที่ 6 [12]



รูปที่ 8 ตัวอย่างแผนผังการตัดสินใจจัดระดับชั้นความลับของข้อมูลเทียบกับผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

3) เกณฑ์พิจารณาระดับผลประโยชน์แห่งชาติ (National Interest)

ผลประโยชน์แห่งชาติที่สำคัญยิ่งยวด (Vital National Interests)	**ผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)**	**ผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)**	**ผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)**
คำอธิบาย (Description)			
เป็นเงื่อนไขที่จำเป็นอย่างยิ่งยวดต่อการปกป้องรักษาและการเพิ่มพูนความอยู่รอดปลอดภัยและการอยู่ดีกินดีภายใน ประเทศที่มีเสรีภาพและปลอดภัย ผลประโยชน์แห่งชาติของประเทศไทยที่มีความสำคัญยิ่งยวดที่นำเสนอในด้านทรัพยากร ที่ใช้ในการป้องกันผลประโยชน์แห่งชาติที่สำคัญยิ่งยวดนั้น จะต้องเพิ่มพูนและป้องกันโดยการสนับสนุนให้ประเทศไทยมีความเป็นผู้นำเพิ่มขึ้นในระดับภูมิภาค การเป็นผู้นำทางด้านการทหารในภูมิภาค ในด้านอำนาจกำลังรบที่เหนือกว่า ขีดความสามารถทางด้านการข่าวกรองที่เพียงพอ รวมถึงการสร้างชื่อเสียงและเกียรติภูมิของประเทศไทยในสังคมโลก นอกจากนั้นยังต้องมีการสร้างความเข้มแข็งที่วิกฤติในองค์การระหว่างประเทศที่ประเทศไทยเข้าไปมีส่วนร่วมด้วย โดยเฉพาะอย่างยิ่งความร่วมมือกับประเทศพันธมิตรที่เป็นมหาอำนาจที่มีพลังอำนาจในระดับโลกทั้งหลาย	สภาพเงื่อนไขซึ่งถ้าประนีประนอมแล้วอาจทำให้เกิดความเสียหายอย่างร้ายแรงแต่ไม่ทำให้ตกอยู่ในอันตรายอย่างร้ายแรงต่อรัฐบาลไทยในการที่จะปกป้องและส่งเสริมความเป็นกินอยู่ที่ดีในการเป็นประเทศที่มีความเสรีภาพและมีความปลอดภัย	สภาพที่ว่าถ้าประนีประนอมแล้วจะเกิดผลทางลบอย่างมากตามมาในภายหลังต่อความสามารถ ของรัฐบาลไทยในการที่จะปกป้องและเสริมสร้าง ความเป็นอยู่ที่ดีของคนไทยในฐานะที่เป็นประเทศ อิสระและมีความปลอดภัย	เป็นสภาพเงื่อนไขที่ต้องการเพียงแต่ว่ามีผลกระทบโดยตรงเพียงเล็กน้อยต่อความสามารถของรัฐบาลไทยในอันที่จะปกป้องและเพิ่มพูนความเป็นอยู่ที่ดีของคนไทยในประเทศที่มีเสรีภาพและมีความปลอดภัย ผลประโยชน์แห่งชาติสำคัญน้อยหรือสำคัญระดับรองของประเทศไทยที่นำเสนอ ซึ่งทรัพยากรที่มีอยู่ ผลประโยชน์แห่งชาติที่สำคัญจะเป็นไปเพื่อที่จะดำรงความแข็งแกร่งของประเทศไทยและประเทศที่เป็นพันธมิตรต่าง ๆ ในภูมิภาครวมถึงกลไกด้านความร่วมมือต่าง ๆ ด้วย
เกณฑ์การพิจารณาระดับผลประโยชน์แห่งชาติ			
- ป้องกันป้องปราม และลดภัยคุกคามของอาวุธนิวเคลียร์ ชีวะและเคมีหรืออาวุธอื่น ๆ ต่อประเทศไทยหรือต่อกองกำลังทหารใด ๆ ของประเทศไทยทั้งที่ตั้งอยู่ในประเทศ และนอกประเทศ - การทำให้เชื่อมั่นถึงความอยู่รอดของพันธมิตรตามสนธิสัญญาต่าง ๆ หรือตามข้อตกลงต่าง ๆ ในระดับ	- ป้องกันกีดขวาง และลดภัยคุกคามในอันที่จะใช้อาวุธนิวเคลียร์ ชีวะและเคมี ในทุก ๆ พื้นที่ของประเทศ - ป้องกันพื้นที่ของประเทศจากการถูกโจมตีจากอาวุธทำลายล้างสูง	- การขัดขวางต่อการละเมิดสิทธิมนุษยชนที่ร้ายแรงและที่มีจำนวนมากของประเทศเพื่อนบ้าน อันอาจจะ กระทบต่อความสงบเรียบร้อยของประเทศไทย - ส่งเสริมพหุนิยม เสรีภาพ และประชาธิปไตยในประเทศที่มีความสำคัญทางยุทธศาสตร์ต่อประเทศไทยให้มากที่สุด	- การทำให้เกิดความสมดุลด้านการค้าในลักษณะทวิภาคี - ขยายขอบเขตของการปกครองในระบอบประชาธิปไตยไปทุกแห่งหนเท่าที่เป็นประโยชน์ต่อประเทศชาติ - สนับสนุนความเป็นเอกภาพแห่งดินแดน - ขยายการส่งออกของสินค้าเฉพาะบางประเภท

ผลประโยชน์แห่งชาติที่สำคัญยิ่งยวด (Vital National Interests)	**ผลประโยชน์แห่งชาติสำคัญยิ่ง** (Extremely Important National Interests)	**ผลประโยชน์แห่งชาติที่สำคัญ** (Important National Interests)	**ผลประโยชน์แห่งชาติสำคัญน้อย** (Less Important or Secondary National Interests)
นานาชาติที่ประเทศไทยได้กระทำไว้อันเป็นการรักษาไว้ซึ่งประโยชน์ของไทย - ทำให้มั่นใจในความอยู่รอดและเสถียรภาพของระบบต่าง ๆ ทั้งในประเทศและอยู่นอกประเทศ (เช่น ระบบการค้า ระบบตลาดเงิน ระบบการขนส่งพลังงาน หรือ ระบบการรักษาสิ่งแวดล้อมของประเทศ เป็นต้น) - การสถาปนาความสัมพันธ์อย่างเป็นผลและเข้ากันได้กับผลประโยชน์ของประเทศไทยกับประเทศซึ่งอาจจะเป็นคู่แข่งทางยุทธศาสตร์ใด ๆ - การสถาปนาความสัมพันธ์อย่างเป็นผลและเข้ากันได้กับผลประโยชน์ของประเทศไทยกับประเทศซึ่งอาจจะเป็นคู่แข่งทางยุทธศาสตร์ใด ๆ	- ส่งเสริมการยอมรับการบังคับใช้กฎหมายของนานาชาติรวมทั้งกลไกที่ใช้ในการแก้ไขความขัดแย้งอย่างสันติร่วมกับนานาชาติ - ป้องกันการเกิดขึ้นของระบบการครอบงำที่จะเกิดขึ้นในประเทศ - การส่งเสริมประชาธิปไตย ความมั่งคั่งและความมีเสถียรภาพของประเทศ - ป้องกันจัดการ ความขัดแย้งที่เกิดขึ้นในภูมิภาคอันจะกระทบต่อความสงบเรียบร้อยของประเทศ - การดำรงรักษาความเป็นผู้นำ ทางด้านเกี่ยวกับการทหาร เทคโนโลยี โดยเฉพาะอย่างยิ่งระบบงานด้านการข่าวกรอง ข่าวกรองยุทธศาสตร์ - ป้องกันการอพยพของผู้อพยพเข้ามายังชายแดนของประเทศที่มีขนาดใหญ่ที่ไม่สามารถควบคุมได้ - การปราบปรามการก่อการร้าย (โดยเฉพาะการก่อการร้ายที่ได้รับการสนับสนุนจากรัฐใด ๆ) อาชญากรรมข้ามชาติ และการค้ายาเสพติดข้ามชาติ - ป้องกันการฆ่าล้างเผ่าพันธุ์	เท่าที่จะกระทำได้ โดยปราศจากการทำให้เกิดการเสียเสถียรภาพ - ป้องกันหรือลดความรุนแรงของความขัดแย้งในประเทศที่มีความสำคัญทางยุทธศาสตร์ต่อประเทศไทย - ปกป้องชีวิตและความเป็นอยู่ของคนสัญชาติไทย ผู้ซึ่งเป็นเป้าหมายของการถูกลักพาตัวของขบวนการก่อการร้าย - ป้องกันทรัพย์สินของชาติซึ่งอยู่ในต่างแดน - ร่วมกับนานาชาติในการส่งเสริมนโยบายด้านสิ่งแวดล้อมในระยะยาว	

ที่มา ผลงานวิจัย “ตัวแบบในการกำหนดยุทธศาสตร์และยุทธศาสตร์ชาติในศตวรรษที่ 21” โดย พันเอก โสภณ ศิริงาม หลักสูตร วปอ. รุ่นที่ 59 ผู้อำนวยการกองยุทธศาสตร์ และความมั่นคงวิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ [13]

4) เกณฑ์การประเมินความเสี่ยงและผลกระทบของการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

การวิเคราะห์ความเสี่ยงเป็นข้อมูลในการตัดสินใจเพื่อจัดการกับความเสี่ยง โดยพิจารณาเงื่อนไขในการกำหนดเกณฑ์การประเมินความเสี่ยงใน 2 มิติ คือ โอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) เพื่อกำหนดระดับความเสี่ยง (Level of Risk) การวิเคราะห์ความเสี่ยงสามารถเป็นได้ทั้งการวิเคราะห์เชิงคุณภาพ (Qualitative) กึ่งปริมาณ (Semi-Quantitative) เชิงปริมาณ (Quantitative) หรือผสมผสานกันไปกระบวนการประเมินความเสี่ยงของหน่วยงาน จะทำการวิเคราะห์โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงและผลกระทบอันเนื่องมาจากความเสี่ยง ซึ่งในที่นี้

ผลกระทบ (Impact) หมายถึง ความเสียหายที่จะเกิดขึ้นหากความเสี่ยงนั้นเกิดขึ้น เป็นการพิจารณาระดับความรุนแรงและมูลค่าความเสียหายจากความเสี่ยงที่คาดว่าจะได้รับ โดยมีระดับคะแนน และตัวอย่างเกณฑ์การพิจารณาระดับผลกระทบและผลประโยชน์แห่งชาติ ดังนี้

ระดับคะแนน	ความหมาย
3	ความรุนแรงของผลกระทบระดับสูง
2	ความรุนแรงของผลกระทบระดับปานกลาง
1	ความรุนแรงของผลกระทบระดับน้อย

ตัวอย่างเกณฑ์การพิจารณาระดับผลกระทบและผลประโยชน์แห่งชาติ

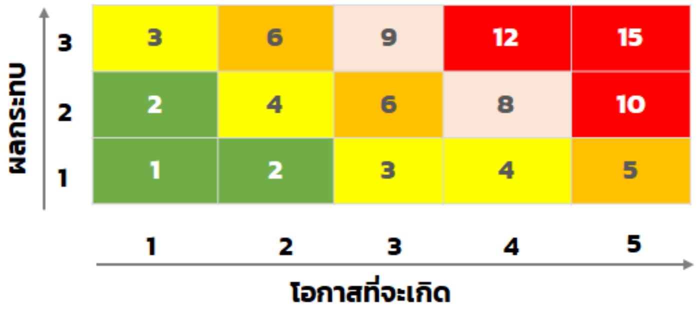
เกณฑ์	ค่าคะแนนระดับความรุนแรงของระดับผลกระทบและผลประโยชน์แห่งชาติ		
	1 = น้อย	2 = ปานกลาง	3 = สูง
Reputation	*น้อย/อย่างจำกัด*	*อย่างร้ายแรง*	*อย่างร้ายแรงมาก*
Users & Operations	*รายบริการ/ การดำเนินงานขององค์กร*	*ราย กลุ่มบริการ/ การดำเนินของกระทรวง/ระหว่างองค์กร/จังหวัด*	*ข้ามกลุ่มบริการ/ภูมิภาค การดำเนินงานตามแผนบูรณาการ/กลุ่มจังหวัด*
Financial & Assets	*ตั้งแต่ 5 แสน แต่ไม่เกิน 5 ล้าน/ Small project*	*ตั้งแต่ 5 ล้าน แต่ไม่เกิน 50 ล้าน/ Medium project*	*ตั้งแต่ 50 ล้าน แต่ไม่เกิน 100 ล้าน/ Large Project*
Legal and Regulation	*ละเว้นการปฏิบัติตามระเบียบข้อบังคับขององค์กร ซึ่งเกิดผลกระทบน้อย*	*ละเว้นการปฏิบัติตามระเบียบข้อบังคับและกฎกระทรวง ซึ่งเกิดผลกระทบที่มีนัยสำคัญ และไม่เป็นไปตามเป้าของ ก.พ.ร.*	*ละเว้นการปฏิบัติตามกฎหมาย มติ ครม. หรือระเบียบข้อบังคับ ซึ่งเกิดผลกระทบที่มีนัยสำคัญ และไม่เป็นไปตามเป้าของแผนบูรณาการ/กลุ่มจังหวัด*
National Interests	*ผลประโยชน์แห่งชาติสำคัญน้อย*	*ผลประโยชน์แห่งชาติที่สำคัญ*	*ผลประโยชน์แห่งชาติที่สำคัญยิ่ง*

หมายเหตุ หน่วยงานของรัฐควรกำหนดเกณฑ์การพิจารณาระดับผลกระทบและผลประโยชน์แห่งชาติให้สอดคล้องกับนโยบายและกฎระเบียบที่เกี่ยวข้อง และเหมาะสมกับบริบทขององค์กร

โอกาสที่จะเกิด (Likelihood) หมายถึง การประเมินโอกาสของเสี่ยงจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตหรือการรั่วไหลของข้อมูลที่มีชั้นความลับที่จะเกิดขึ้น โดยการพิจารณาจากสถิติการเกิดเหตุการณ์ในอดีต ปัจจุบัน หรือการคาดการณ์ล่วงหน้าของโอกาสที่จะเกิดในอนาคต ทั้งนี้ ให้ผู้ดูแลข้อมูลและเจ้าของข้อมูลร่วมกันประเมินโอกาสที่จะเกิดขึ้น โดยมีระดับคะแนนและระดับความเสี่ยงดังนี้

ระดับคะแนน	ความหมาย
5	มีโอกาสเกิดขึ้นสูงมาก/เป็นประจำ
4	มีโอกาสเกิดขึ้นสูง/บ่อยครั้ง
3	มีโอกาสเกิดขึ้นบ้าง/บางครั้ง
2	มีโอกาสเกิดขึ้นน้อยครั้ง
1	มีโอกาสเกิดขึ้นยาก

ระดับความเสี่ยง (Risk Level) กำหนดค่าเท่ากับผลคูณของระดับโอกาสที่ความเสี่ยงอาจเกิดขึ้น (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) อันเนื่องมาจากความเสี่ยง ซึ่งระดับความเสี่ยงแบ่งตามความสำคัญและการจัดการความเสี่ยงได้ดังนี้



ผลกระทบ					
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
	โอกาสที่จะเกิด				

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1-2	ต่ำมาก	*ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ โดยไม่ต้องมีมาตรการควบคุมก็ได้*
3-4	ต่ำ	*ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้ แต่อาจต้องมีการติดตามเป็นระยะ ๆ*
5-6	ปานกลาง	*ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น*
7-9	สูง	*ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย*
10 ขึ้นไป	สูงมาก	*ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยงโดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย*

สำหรับการประยุกต์ใช้ร่างหลักเกณฑ์การจัดชั้นความลับของข้อมูลภาครัฐ สามารถดูรายละเอียดได้ที่ *ตัวอย่างการจัดชั้นความลับของข้อมูลภาครัฐ*

3.3.4 ร่างข้อเสนอแนะการจัดการข้อมูลภาครัฐ (Data Handling) ที่มีการจัดชั้นความลับของข้อมูล

ข้อมูลทั้งหมดไม่ได้ถูกสร้างขึ้นอย่างเท่าเทียมกันนับตั้งแต่เวลาที่ข้อมูลถูกสร้างขึ้นจนกระทั่งถูกทำลาย การจัดชั้นความลับข้อมูลสามารถช่วยให้องค์กรมั่นใจได้ว่าจะได้รับการป้องกัน จัดเก็บ และจัดการข้อมูลอย่างมีประสิทธิภาพ การจัดชั้นความลับข้อมูลเป็นหัวใจสำคัญของกลยุทธ์การปกป้องคุ้มครองข้อมูลขององค์กรซึ่งช่วยลดความเสี่ยงต่อข้อมูลที่มีความอ่อนไหว สนับสนุนการตัดสินใจและเพิ่มประสิทธิภาพของการป้องกันข้อมูลสูญหาย การเข้ารหัส และการควบคุมความปลอดภัยอื่น ๆ ด้วยการกำหนดรูปแบบการจัดชั้นความลับที่ชัดเจนตรงไปตรงมา การประเมินและกำหนดตำแหน่ง/แหล่งที่มาของข้อมูลอย่างครอบคลุมและประยุกต์ใช้โซลูชันที่เหมาะสม องค์กรสามารถมั่นใจได้ว่าข้อมูลที่มีความอ่อนไหวจะได้รับการจัดการ (Handling) อย่างเหมาะสมและลดภัยคุกคามต่อการดำเนินงานขององค์กร โดยมีข้อเสนอแนะการจัดการข้อมูลภาครัฐ (Data Handling) ที่มีการจัดชั้นความลับของข้อมูลดังต่อไปนี้

ระดับชั้นความลับ การบริหารจัดการ	เปิดเผย (Open)	เผยแพร่ภายในองค์กร (Private)	ลับ (Confidential / Sensitive)	ลับมาก (Secret / Medium sensitive)	ลับที่สุด (Top secret / Highly sensitive)
ตัวอย่างชุดข้อมูล	- กฎ มติ ค.ร.ม. ข้อบังคับ - รายงานผลการศึกษาทางวิชาการ - ข้อมูลเปิดภาครัฐ	- ข้อมูลระเบียน - ข้อมูลพนักงาน - เอกสารประกอบการปฏิบัติงาน - วิธีปฏิบัติภายในหน่วยงาน	- ข้อมูลการฟ้องคดี - ความเห็นภายในหน่วยงานที่ยังไม่ได้ข้อยุติ	- รายงานการแพทย์ - ข้อมูลความสัมพันธ์ระหว่างประเทศ - นโยบายสำคัญที่ใช้ปฏิบัติต่อรัฐต่างประเทศ	- ข่าวสารที่อาจก่อความเสียหายต่อสถาบันพระมหากษัตริย์ - ข้อมูลที่กระทบต่อความมั่นคงทางทหาร เช่น คลังอาวุธ และความมั่นคงทางทรัพยากร เช่น ตำแหน่งของชนิดพันธุ์ที่ใกล้สูญพันธุ์/ถูกคุกคาม
การควบคุมการเข้าถึง (Access Control)	- ไม่มีการจำกัดการเข้าถึงข้อมูล/เปิดเผยสู่สาธารณะ	- จำกัดการเข้าถึงข้อมูลเฉพาะบุคคลภายในหน่วยงาน	- จำกัดการเข้าถึงเฉพาะบุคคลที่จำเป็นต้องรู้หรือมีสิทธิ์รู้โดยและลงนามข้อตกลงไม่เปิดเผยข้อมูล (non-disclosure agreements) - สามารถตรวจสอบคำขอการเข้าถึงข้อมูล การทบทวน การอนุมัติ และกระบวนการยกเลิกได้	- จำกัดการเข้าถึงเฉพาะบุคคลที่จำเป็นต้องรู้หรือมีสิทธิ์รู้โดยและลงนามข้อตกลงไม่เปิดเผยข้อมูล (non-disclosure agreements) - ต้องได้รับการอนุญาตจากเจ้าของข้อมูล - สามารถตรวจสอบคำขอการเข้าถึงข้อมูล การทบทวน การอนุมัติ และกระบวนการยกเลิกได้	- ไม่เปิดเผย/ปกปิด

ระดับชั้นความลับ / การบริหารจัดการ	เปิดเผย (Open)	เผยแพร่ภายในองค์กร (Private)	ลับ (Confidential / Sensitive)	ลับมาก (Secret / Medium sensitive)	ลับที่สุด (Top secret / Highly sensitive)
การเข้ารหัส (Encryption)	- ไม่มีการเข้ารหัส	- ไม่มีการเข้ารหัสการสร้าง การจัดเก็บ การประมวลผล และการส่งข้อมูล - มีการเข้ารหัสสำหรับบุคคลที่สาม	- การเข้ารหัสระหว่างการสร้างการจัดเก็บ การประมวลผล และการส่งข้อมูล - มีการเข้ารหัสสำหรับบุคคลที่สาม	- มีการเข้ารหัสที่ซับซ้อนระหว่างการสร้าง การจัดเก็บ การประมวลผล และการส่งข้อมูล - มีการเข้ารหัสที่ซับซ้อนสำหรับบุคคลที่สาม	- ไม่เปิดเผย/ปกปิด
การจัดเก็บ (Storage)	- ไม่มีข้อจำกัดการจัดเก็บข้อมูล	- การจัดเก็บข้อมูลเป็นไปตามนโยบายองค์กรหรือดุลยพินิจของผู้จัดการหรือผู้คุ้มครองข้อมูล	- ห้ามจัดเก็บข้อมูลที่ลับมากในเครื่องและอุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต	- ห้ามจัดเก็บข้อมูลที่ลับมากในเครื่องและอุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต เว้นแต่จะได้รับอนุมัติจากเจ้าหน้าที่รักษาความปลอดภัยข้อมูล และต้องมีการเข้ารหัส - จัดเก็บที่ปลอดภัยเมื่อไม่ใช้งาน	- ไม่เปิดเผย/ปกปิด

ทั้งนี้ หน่วยงานของรัฐสามารถกำหนดรูปแบบการจัดการข้อมูล (Data Handling) ในแต่ละระดับชั้นความลับได้ตามความเหมาะสมกับสอดคล้องกับนโยบายการบริหารจัดการข้อมูลและจัดชั้นความลับของข้อมูลของหน่วยงาน

3.4 ร่างหลักการและเงื่อนไขการแบ่งปันข้อมูล (Data Sharing Criteria)

หลักการแบ่งปันข้อมูลเป็นกรอบในการปรับปรุงการเข้าถึงและการนำข้อมูลภาครัฐที่แลกเปลี่ยนกันได้ในรูปแบบอิเล็กทรอนิกส์ เพื่อรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล ซึ่งร่างหลักการฯ นี้ เป็นหลักการให้หน่วยงานนำไปพิจารณาก่อนการแบ่งปันข้อมูลของหน่วยงานภาครัฐ โดยการแบ่งปันข้อมูลควรคำนึงถึงกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติข้อมูลข่าวสารของราชการฯ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 และระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ทั้งนี้ การแบ่งปันข้อมูลจะช่วยจัดเตรียมการเข้าถึงข้อมูลในลักษณะที่มีการควบคุมการเปิดเผยข้อมูล ซึ่งการแบ่งปันข้อมูลช่วยให้นำข้อมูลที่มีอยู่กลับมาใช้ใหม่เพื่อก่อให้เกิดประโยชน์ต่อสาธารณะและการสร้างชุดข้อมูลใหม่เพื่อให้ข้อมูลเชิงลึกเกี่ยวกับภาคประชาสังคม (ชุมชน ครอบครัว และประชาชน) ระบบเศรษฐกิจและภาคการผลิต (ภาคอุตสาหกรรม การค้าและบริการ) ตลอดจนทรัพยากรและสิ่งแวดล้อม อย่างไรก็ตาม การแบ่งปันข้อมูลจะต้องได้รับการจัดการอย่างระมัดระวังและปลอดภัย เพื่อให้ประชาชนไว้วางใจว่าหน่วยงานของรัฐมีการจัดการกับข้อมูลที่ถือครองอย่างเหมาะสม ทั้งนี้ สพร. ได้อ้างอิงหลักการตาม Best Practice Guide to Applying Data Sharing Principles จัดทำโดยรัฐบาลประเทศออสเตรเลีย ซึ่งมีหลักการและเงื่อนไขการแบ่งปันข้อมูล การประยุกต์ใช้หลักการ และข้อเสนอแนะแนวทางการแบ่งปันข้อมูลภาครัฐ ดังต่อไปนี้

1) **หลักการและการประยุกต์ใช้แบ่งปันข้อมูลภาครัฐ** แบ่งออกเป็น 3 ระยะดังนี้

ระยะที่ 1 ก่อนการประยุกต์ใช้หลักการแบ่งปันข้อมูล

(1) **จัดทำคำขอแบ่งปันข้อมูล (Data Sharing Request)** ก่อนจะมีการแบ่งปันข้อมูลต้องมีการจัดทำคำขอแบ่งปันข้อมูลไปยังผู้ดูแลข้อมูล ซึ่งอาจมาจากหน่วยงานของรัฐอื่น ภาคเอกชน หรือภาคการศึกษา เพื่อเริ่มต้นการพิจารณาโครงการ/แผนงาน/กิจกรรมที่จะแบ่งปันข้อมูล ซึ่งควรมีเนื้อหาระบุอย่างชัดเจนถึงข้อตกลง ข้อกำหนดและเงื่อนไขของโครงการ/แผนงาน/กิจกรรม วัตถุประสงค์ในการใช้ข้อมูล และการนำไปใช้ในประโยชน์ เพื่อประเมินความเหมาะสมของการแบ่งปันข้อมูลในเบื้องต้นได้ โดยมีเกณฑ์พิจารณาดังนี้

- **ข้อมูลเป็นข้อมูลที่มีอยู่และเหมาะสมหรือไม่** ผู้ดูแลข้อมูลควรดำเนินการประเมินคำขอและระบุแหล่งที่มาหลักของข้อมูลที่สามารถแบ่งปันตามคำขอ โดยผู้ดูแลข้อมูลจะต้องมีความเข้าใจที่ดีที่สุดเกี่ยวกับขอบเขตการใช้ข้อมูลว่า เป็นข้อมูลของหน่วยงานหรือไม่ สามารถแบ่งปันหรือเปิดเผยข้อมูลได้มากน้อยเพียงใด
- **ข้อมูลสามารถแบ่งปันได้ตามกฎหมายหรือไม่** ผู้ดูแลข้อมูลควรรับรองว่า การแบ่งปันข้อมูลเป็นไปตามที่กฎหมายกำหนด ซึ่งผู้ดูแลข้อมูลจำเป็นต้องตระหนักถึงข้อจำกัดทางกฎหมายและมีการสื่อสารไปยังผู้ร้องขอได้อย่างชัดเจน ทั้งนี้ สำหรับหน่วยงานภาครัฐ การเปิดเผยข้อมูลที่ชั้นความลับควรพิจารณาพระราชบัญญัติข้อมูลข่าวสารของราชการฯ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 2564 และระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552
- **ข้อมูลมีความอ่อนไหวหรือไม่** ผู้ดูแลข้อมูลควรพิจารณาว่า ข้อมูลมีความอ่อนไหว และมีระดับอ่อนไหวเป็นอย่างไร เช่น ข้อมูลส่วนบุคคล ข้อมูลความมั่นคงของประเทศ สิ่งที่สำคัญคือต้องพิจารณาว่าความอ่อนไหวของข้อมูลอาจเปลี่ยนแปลงไปตามสถานการณ์ หากต้องการเข้าถึงข้อมูลอ่อนไหวสามารถทำได้โดยการจำกัดการเข้าถึงเฉพาะผู้ใช้ที่ได้รับอนุญาต แต่ข้อมูลเดียวกันนี้จำเป็นต้องลบข้อมูลที่สามารถระบุตัวตนได้หากเปิดเผยต่อสาธารณะ

(2) **จัดทำข้อตกลงการแบ่งปันข้อมูล** (Data Sharing Agreement) ซึ่งข้อตกลงการแบ่งปันข้อมูล จัดทำขึ้นระหว่างผู้ดูแลข้อมูลและหน่วยงานที่ได้รับหรือเข้าถึงข้อมูล เช่น หน่วยงานภาครัฐอื่น ๆ สถาบัน การศึกษาและวิจัย องค์กรภาคเอกชน เป็นต้น โดยเนื้อหาในข้อตกลงอาจรวมถึงวัตถุประสงค์เงื่อนไข

และรายละเอียดของโครงการ/แผนงาน/กิจกรรมที่จะแบ่งปันข้อมูล ทั้งนี้ เจ้าหน้าที่ที่รับผิดชอบของหน่วยงานที่ได้รับหรือเข้าถึงข้อมูลจะยินยอมให้ผู้ใช้งานข้อมูลทั้งหมดภายในหน่วยงานต้องปฏิบัติตามข้อกำหนดและเงื่อนไขการเข้าถึงข้อมูลภายในข้อตกลง ทั้งนี้ ในกรณีของข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล โดยมีการแบ่งปันเมื่อต้นทางกับปลายทางมีสถานะเป็นผู้ควบคุมข้อมูล (Data Controller) ทั้ง 2 ฝ่าย โดยข้อกำหนดขั้นที่ต้องระบุในข้อตกลง ต้องสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(3) **พิจารณาความต้องการของผู้ใช้ข้อมูล** ผู้ดูแลข้อมูลต้องพิจารณาความต้องการเฉพาะของบุคคลหรือหน่วยงานที่ร้องขอ เพื่อพิจารณาแนวทางการสนับสนุนการแบ่งปันข้อมูลและช่วยให้เกิดการประโยชน์สูงสุดจากการใช้ข้อมูล ทั้งนี้ เมื่อได้รับคำขอแล้วผู้ดูแลข้อมูลจะต้องกำหนดข้อตกลงการแบ่งปันที่เหมาะสม อาทิ การแบ่งปันข้อมูลให้แก่ผู้ร้องขอ หรือ ให้ผู้ร้องขอเข้าถึงข้อมูล โดยผู้ดูแลข้อมูลมีหน้าที่ตรวจสอบว่าความเหมาะสมเพื่อให้การแบ่งปันข้อมูลเป็นไปตามที่กฎหมายกำหนดและมีความปลอดภัยของข้อมูลแบ่งปัน

(4) **ขีดความสามารถและวัฒนธรรมองค์กร** ผู้ดูแลข้อมูลจำเป็นต้องมีทำการประเมินทักษะและขีดความสามารถที่มีอยู่ภายในหน่วยงานก่อนการแบ่งปันข้อมูล และพัฒนาความเชี่ยวชาญของตนเอง เพื่อให้จัดการเตรียมการแบ่งปันข้อมูลเป็นไปอย่างมีประสิทธิภาพ นอกจากนี้ ควรปรับทัศนคติด้านวัฒนธรรมภายในองค์กร โดยผู้ดูแลข้อมูลต้องเปลี่ยนจาก *“การหลีกเลี่ยงความเสี่ยง”* ไปเป็น *“การจัดการความเสี่ยง”* ที่เกี่ยวข้องเพื่อให้เกิดการแบ่งปันข้อมูลและใช้ประโยชน์จากข้อมูลร่วมกัน

ส่วนที่ 2 การประยุกต์ใช้หลักการแบ่งปันข้อมูล

หลักการแบ่งปันข้อมูลจะต้องพิจารณาการจัดการความเสี่ยงในการเปิดเผยข้อมูลและประโยชน์สาธารณะ เพื่อให้มีการควบคุมความเสี่ยงที่จะเกิดขึ้นในการแบ่งปันข้อมูล ประกอบด้วย 5 หลักการดังนี้

(1) **หลักการด้านโครงการ (Project Principle) : ข้อมูลจะถูกแบ่งปันเพื่อวัตถุประสงค์ที่เหมาะสมอันก่อให้เกิดประโยชน์สาธารณะ** ผู้ดูแลข้อมูลต้องพิจารณาวัตถุประสงค์ของโครงการ/แผนงาน/กิจกรรม หรือการใช้ข้อมูลในคำขอข้อมูลว่ามีความเหมาะสมหรือไม่ และตอบสนองวัตถุประสงค์ในการแบ่งปันข้อมูลของหน่วยงาน ซึ่งหน่วยงานของรัฐหลายแห่งจะมีนโยบายหรือข้อกำหนดทางกฎหมายให้แบ่งปันข้อมูลได้หากเป็นไปตามวัตถุประสงค์ เช่น นโยบายของรัฐบาล การวิจัยและพัฒนาโดยสาธารณประโยชน์ การออกแบบโปรแกรม การนำไปปฏิบัติ และการประเมินผล หรือ การส่งมอบบริการภาครัฐ เป็นต้น และควรมีการประเมินโครงการที่จะแบ่งปันข้อมูลทั้งด้านกฎหมาย ด้านจริยธรรม/หลักจรรยาบรรณ และสาธารณประโยชน์ ทั้งนี้ขอให้คำนึงถึงประโยชน์ต่อสาธารณะเป็นสำคัญ ซึ่งโครงการเหล่านั้นควรได้รับการจัดการผ่านกระบวนการกำกับดูแลอย่างเป็นทางการ โดยอาจให้คณะกรรมการ/คณะทำงานด้านธรรมาภิบาลข้อมูลพิจารณาประเมินข้อเสนอโครงการทั้งหมดเพื่อการแบ่งปันข้อมูล และผู้ดูแลข้อมูลสามารถขอรวมประเด็นสำคัญบางประการไว้ในข้อเสนอโครงการ เช่น ข้อกำหนดสำหรับการอนุมัติจริยธรรมหรือความยินยอมจากต้นฉบับ ซึ่งกระบวนการอนุมัติของคณะกรรมการจะแสดงให้ทั้งผู้ขอและผู้ดูแลข้อมูลทราบว่าโครงการไม่มีอุปสรรคทางจริยธรรมที่สำคัญ ในทำนองเดียวกัน หากมีการแจ้งความยินยอมจากผู้ให้บริการด้านข้อมูลอาจลดความกังวลของผู้ดูแลข้อมูลเกี่ยวกับข้อพิจารณาอื่น ๆ ที่อาจส่งผลต่อกระบวนการประเมินโครงการ เช่น ต้นทุนของการแบ่งปันข้อมูล หรือ การแบ่งปันข้อมูลอาจส่งผลกระทบต่อองค์กร เป็นต้น

(2) **หลักการด้านบุคคล (People Principle) : ผู้มีสิทธิ์ที่เหมาะสมในการเข้าถึงข้อมูล** ผู้ใช้งานข้อมูลอาจต้องผ่านกระบวนการอนุมัติเพื่อประเมินความรู้ ทักษะ และแรงจูงใจของผู้ใช้ในการพิจารณาว่าสามารถใช้งาน (และในบางกรณีจัดเก็บ) ข้อมูลแบ่งปันได้อย่างเหมาะสมหรือไม่ สำหรับการให้สิทธิ์ผู้ใช้งานข้อมูล เกณฑ์การอนุญาตแก่ผู้ใช้อาจมีพื้นฐานทางกฎหมาย เช่น กฎหมายอาจอนุญาตให้ผู้ใช้งานเฉพาะในการเข้าถึงข้อมูล หรืออาจตอบสนองต่อผู้ดูแลข้อมูลซึ่งผู้ใช้เข้าใจความคาดหวังเมื่อเข้าถึงข้อมูลที่แชร์ ในบางกรณีผู้ดูแลข้อมูลอาจใช้งานข้อมูลทั้งหมดหรือบางส่วนของกระบวนการที่ได้รับอนุญาตโดยหน่วยงานอื่นที่สร้างข้อมูลเพื่อจำกัดการทำซ้ำ ทั้งนี้ ผู้ใช้งานข้อมูลอาจได้รับอนุญาตให้เข้าถึงข้อมูลที่แชร์สำหรับโครงการใด

โครงการหนึ่ง หรือได้รับสิทธิ์ในการเข้าถึงข้อมูลสำหรับหลายโครงการเพิ่มเติม อาจรวมถึงสิทธิ์ในการเข้าถึงข้อมูลอย่างต่อเนื่อง อาทิ การเข้าถึงชุดข้อมูลที่มีการอัพเดทเป็นระยะโดยผู้ดูแลข้อมูล ซึ่งผู้ดูแลข้อมูลจะต้องพิจารณาขอบเขตของการอนุญาตในบริบทของการร้องขอเพื่อการเข้าถึงในแต่ละครั้ง

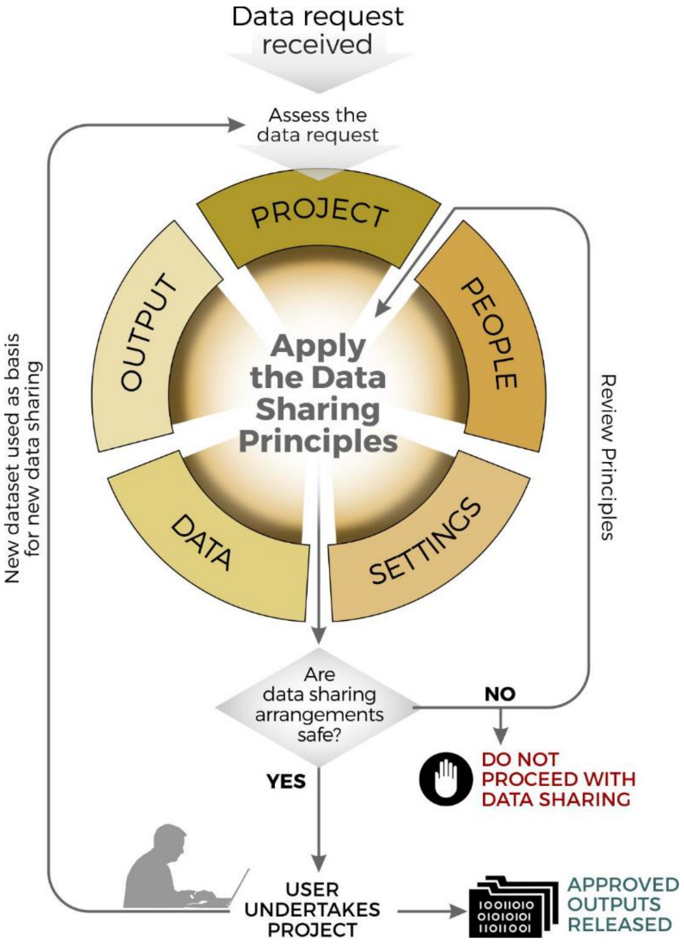
(3) **หลักการด้านสภาพแวดล้อม (Setting Principle) : สภาพแวดล้อมที่มีการแบ่งปันข้อมูลช่วยลดความเสี่ยงของการใช้หรือการเปิดเผยโดยไม่ได้รับอนุญาต** ผู้ดูแลข้อมูลจำเป็นต้องพิจารณาความเสี่ยงที่จะเกิดขึ้นทั้งในสภาพแวดล้อมทางกายภาพและระบบเทคโนโลยีสารสนเทศเพื่อควบคุมวิธีการจัดเก็บ ถ่ายโอน และเข้าถึงข้อมูลได้ รวมไปถึงการพิจารณาว่าทุกฝ่ายที่เกี่ยวข้องได้ดำเนินการตามขั้นตอนที่เหมาะสมหรือไม่ เพื่อลดการใช้งานและเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือการสูญหายของข้อมูล เพื่อให้มั่นใจได้ว่าข้อมูลจะถูกใช้ในสภาพแวดล้อมที่ปลอดภัยและมีเสถียรภาพ นอกจากนี้ ลักษณะสำคัญของหลักการนี้เกี่ยวข้องกับการฝึกอบรม (มักเป็นส่วนหนึ่งของการให้สิทธิ์ผู้ใช้งานข้อมูล) เพื่อช่วยให้ผู้ใช้งานข้อมูลหลีกเลี่ยงข้อผิดพลาด และเพื่อตอบสนองผู้ดูแลข้อมูลที่ผู้ใช้สามารถคาดหวังได้อย่างสมเหตุสมผลว่าจะใช้และจัดเก็บข้อมูลอย่างเหมาะสม

(4) **หลักการด้านข้อมูล (Data Principle) : มีการปกป้องคุ้มครองข้อมูลที่นำไปใช้งานอย่างเหมาะสม** ผู้ดูแลข้อมูลต้องควบคุมข้อมูลที่แบ่งปันให้แก่ผู้ใช้งานข้อมูล โดยมุ่งเน้นไปที่การจัดการข้อมูล อาทิ การลดขนาดข้อมูล การรวมข้อมูล การลบข้อมูลที่ระบุตัวตนโดยตรง หรือการระงับการบันทึกข้อมูลส่วนบุคคล ซึ่งเป็นสิ่งจำเป็นในการควบคุมความเสี่ยงที่ไม่สามารถแก้ไขได้ด้วยหลักการด้านโครงการ บุคลากร และสภาพแวดล้อม ทั้งนี้ ผู้ดูแลข้อมูลอาจจำกัดการเข้าถึงข้อมูลโดยเฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่จะสามารถเข้าถึงและเห็นรายละเอียดของข้อมูลนั้น อย่างไรก็ตาม หลักการนี้มีข้อจำกัดคือต้องเข้าใจความแตกต่างระหว่างหลักการด้านข้อมูล และหลักการด้านผลลัพธ์ โดยหลักการด้านข้อมูลใช้ในการควบคุม เช่น การลบข้อมูลที่ระบุตัวตนโดยตรง และการรักษาความลับอื่น ๆ การรักษา กับชุดข้อมูลทั้งหมดที่มีให้กับผู้ใช้ ในขณะที่หลักการด้านผลลัพธ์จะใช้ควบคุมผลลัพธ์ที่จะเปิดเผยต่อสาธารณะหรือพร้อมสำหรับการแบ่งปันเพิ่มเติมโดยผู้ใช้ที่ได้รับอนุญาต กล่าวคือ หลักการด้านข้อมูลจะปกป้องข้อมูลที่ไปจากผู้ดูแลข้อมูลไปยังผู้ใช้ข้อมูล และหลักการด้านผลลัพธ์จะปกป้องข้อมูลภายหลังออกจากผู้ใช้งานข้อมูล

(5) **หลักการด้านผลลัพธ์: การจัดเตรียมการแบ่งปันข้อมูลได้รับการคุ้มครองอย่างเหมาะสมก่อนที่จะแบ่งปันหรือเผยแพร่ต่อไป** หากผู้ใช้งานข้อมูลต้องการแบ่งปันข้อมูลที่ผ่านการวิเคราะห์แล้ว ผู้ใช้ข้อมูลต้องดำเนินการประเมินตามหลักการแบ่งปันข้อมูลใหม่อีกครั้ง ก่อนจะแบ่งปันชุดข้อมูลใหม่ เพื่อสร้างสมดุลระหว่างความเสี่ยงในการเปิดเผยข้อมูลกับผลประโยชน์ หลักการนี้เกี่ยวข้องกับสิ่งที่จะเกิดขึ้นกับข้อมูลหรือข้อมูลที่ถูกสร้างขึ้นตามมาจากการแบ่งปันข้อมูล ในหลายกรณี ผลลัพธ์นี้จะเป็นสิ่งพิมพ์ รายงาน หรืออื่น ๆ ที่เผยแพร่สู่สาธารณะ หรือแม้ว่าผลงานจะไม่ถูกเปิดเผยต่อสาธารณะ อาทิ โครงการของรัฐบาล รายงานการประเมิน จำเป็นต้องได้รับการคุ้มครอง ในการแบ่งปันข้อมูลอาจส่งผลให้เกิดการสร้างชุดข้อมูลใหม่ซึ่งอาจถูกแบ่งปันต่อ ตัวอย่างเช่น ผู้ดูแลข้อมูลจัดเตรียมชุดข้อมูลให้กับหน่วยงานข้อมูลที่ความเชี่ยวชาญซึ่งปรับปรุงหรือแก้ไขข้อมูลและให้ผู้ใช้งานที่ได้รับอนุญาตเข้าถึงข้อมูลเพื่อการวิเคราะห์นั้น หน่วยงานข้อมูลที่ความเชี่ยวชาญจำเป็นต้องดำเนินการประเมินตามหลักการแบ่งปันข้อมูลใหม่อีกครั้งร่วมกับผู้ดูแลข้อมูลเดิม ก่อนที่ชุดข้อมูลใหม่จะถูกแชร์ต่อไป

โดยมีกระบวนการประยุกต์ใช้หลักการแบ่งปันข้อมูล เริ่มจากหน่วยงานรับคำร้องขอข้อมูล และประเมินคำร้องขอข้อมูลด้วยการประยุกต์ใช้หลักการแบ่งปันข้อมูล 5 ประการ (โครงการ บุคคล สภาพแวดล้อม ข้อมูล และผลลัพธ์) เพื่อให้มีการควบคุมความเสี่ยงที่จะเกิดขึ้นในการแบ่งปันข้อมูลและสร้างความมั่นใจได้ว่ามีการจัดเตรียมการแบ่งปันข้อมูลได้อย่างปลอดภัย กรณีที่การแบ่งปันข้อมูลมีความปลอดภัย สามารถแบ่งปันข้อมูลให้ผู้ใช้ดำเนินการโครงการต่อไป ทั้งนี้ เมื่อดำเนินโครงการจะเกิดชุดข้อมูลใหม่ที่ถูกใช้งานและจำเป็นต้องทำการร้องขอข้อมูลตามกระบวนการประยุกต์ใช้หลักการแบ่งปันข้อมูลใหม่ และในกรณีที่การแบ่งปันข้อมูล

ไม่มีความปลอดภัยจะไม่อนุญาตให้แบ่งปันข้อมูลและกลับไปทบทวนตามหลักการใหม่อีกครั้ง ดังแสดงตามรูปที่ 6 ทั้งนี้ สามารถดูรายละเอียดได้ที่ *ตัวอย่างการประยุกต์ใช้หลักการแบ่งปันข้อมูล*



ที่มา: Best Practice Guide to Applying Data Sharing Principles Version 15 March 2019, Department of the Prime Miniter and Cabinet, Australian Government.

รูปที่ 9 การประยุกต์ใช้หลักการแบ่งปันข้อมูล

ส่วนที่ 3: ภายหลังการประยุกต์หลักการแบ่งปันข้อมูล

เมื่อนำหลักการไปใช้แล้ว ผู้ดูแลข้อมูลจะต้องพิจารณาว่าการควบคุมนั้นปกป้องข้อมูลที่จะแบ่งปันอย่างเหมาะสม ผู้ดูแลข้อมูลต้องถามว่า “มีหลักการลดความเสี่ยงของการแบ่งปันให้อยู่ในระดับที่ยอมรับได้หรือไม่” และ “สามารถแชร์ข้อมูลอย่างปลอดภัยได้หรือไม่” หากคำตอบคือ “ไม่” ผู้ดูแลข้อมูลสามารถกลับไปพิจารณาหลักการแต่ละข้อซ้ำเพื่อปรับระดับการควบคุมและการเข้าถึงข้อมูลใหม่อีกครั้ง หากไม่สามารถลดความเสี่ยงของการแบ่งปันให้อยู่ในระดับที่ยอมรับได้ ข้อมูลนั้นก็ไม่ควรแบ่งปัน ทั้งนี้ ผู้ดูแลข้อมูลควรมีการกำหนดกระบวนการตรวจสอบในการกำกับดูแล การรายงาน และการประกันเพื่อให้เกิดการควบคุมความเสี่ยงที่เหมาะสมกับข้อมูลแบ่งปัน (Shared data) และมั่นใจได้ว่าผู้ใช้งานข้อมูลปฏิบัติตามเงื่อนไขที่กำหนดภายในข้อตกลงการแบ่งปันข้อมูลเพื่อให้การแบ่งปันข้อมูลมีความเหมาะสมกับการใช้งานและมีความปลอดภัย

2) ข้อเสนอแนะแนวทางการแบ่งปันข้อมูลภาครัฐ

(1) กำหนดนโยบายและหลักการการแบ่งปันข้อมูล (Data Sharing Policy & Principle) ด้วยการกำหนดเงื่อนไขให้สอดคล้องตาม “5 Data Sharing Principles” พร้อมระบุเหตุผลที่ยอมรับได้ในการไม่แบ่งปันข้อมูล ข้อมูลจะพร้อมใช้งานหรือเปิดเผยข้อมูลเมื่อใด หน่วยงานอื่นจะเข้าถึงข้อมูลได้อย่างไร มีข้อจำกัดใด ๆ เกี่ยวกับข้อมูลหรือไม่ ข้อมูลมีเอกสารเพียงพอที่จะเป็นประโยชน์หรือไม่

(2) กำหนดข้อมูลแบ่งปัน และ คำขอการแบ่งปันข้อมูล (Shared Data and Data Sharing Request) โดย

- ข้อมูลแบ่งปัน (Shared Data) ในที่นี้ได้แก่ ข้อมูลสำคัญที่สอดคล้องกับ Data Strategy ภารกิจและเป้าหมายของหน่วยงาน/ประเทศ และ ข้อมูลที่มีความอ่อนไหวหรือมีการจัดชั้นความลับในระดับชั้น “Private” “Confidential” และ “Secret”

ข้อควรคำนึงถึงในการแบ่งปันข้อมูล :

✓ ข้อมูล**ไม่สามารถเปิดเผย**ต่อสาธารณะได้ เนื่องจากเป็นข้อมูลข่าวสารที่ไม่ต้องเปิดเผย ตาม พ.ร.บ. ข้อมูลข่าวสารฯ มาตรา 14 และ มาตรา 15 ที่อาจมีคำสั่งมิให้เปิดเผยก็ได้ และเป็นข้อมูลที่สามารถระบุตัวตนของบุคคลได้ ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ[2]

✓ **ข้อมูลประกอบด้วยตำแหน่งของชนิดพันธุ์ที่ใกล้สูญพันธุ์/ถูกคุกคาม หรือสิ่งประดิษฐ์ที่มีคุณค่า** และจะ**ถูกแบ่งปันกับหน่วยงาน/ฝ่ายที่เชื่อถือได้เท่านั้นที่ตกลงตามเงื่อนไข**หรือเกณฑ์ในการใช้ซ้ำ (Reuse Criteria)

✓ **ไม่สามารถเปิดเผยข้อมูล**ได้จนกว่าจะมีการออกสิทธิบัตร (Patents) ที่เกี่ยวข้องกับการวิจัยและนวัตกรรมนั้น

- คำขอการแบ่งปันข้อมูล (Data Sharing Request) ควรต้อง

  - แสดงให้เห็น*จุดมุ่งหมาย/เป้าหมายที่เหมาะสม* สอดคล้องกับการตรวจสอบเป้าประสงค์เกี่ยวข้อง (หากมี)
  - แสดงให้เห็นถึงประโยชน์ต่อสาธารณะ หรือ ผลประโยชน์แห่งชาติ รวมทั้งความสอดคล้องกับข้อกฎหมายที่กำหนด เพื่อนำไปสู่การเปิดเผยข้อมูลภาครัฐ
  - ระบุถึงข้อมูลที่ต้องการร้องขอ/เหตุผลที่ร้องขอ กรอบเวลาที่ต้องการใช้ข้อมูลและผลลัพธ์ที่คาดหวัง
  - ระบุถึงตัวบุคคล/หน่วยงานจะร่วมงานในโครงการ/ข้อตกลงในการแบ่งปันข้อมูล
  - แสดงให้เห็นถึงความเป็นไปได้ในการแบ่งปันข้อมูล อาทิ ข้อมูลเหมาะสมสำหรับการตอบสนองคำขอข้อมูลแบ่งปัน

(3) กำหนดข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement)

- ทำขึ้นระหว่างผู้ดูแลข้อมูลและหน่วยงานที่ได้รับชุดข้อมูลที่ร้องข้อหรือข้อมูลแบ่งปัน
- อาจรวมถึงผลการตรวจสอบตามเป้าประสงค์และรายละเอียดของโครงการที่ครอบคลุมโดยข้อตกลง
- ควรระบุถึงข้อมูลใดบ้างที่ใช้ได้และใช้ไม่ได้ภายใต้ข้อตกลง
- ควรให้ข้อมูลเกี่ยวกับบทลงโทษใด ๆ ที่อาจถูกกำหนดไว้หากไม่ปฏิบัติตามข้อกำหนดและเงื่อนไขในข้อตกลง (ซึ่งอาจรวมถึงการอ้างอิงถึงบทลงโทษที่มีการบังคับใช้ตามกฎหมายที่เกี่ยวข้อง)

3.5 บทบาทและความรับผิดชอบ

หน่วยงานของรัฐควรกำหนดบุคลากรที่จะรับผิดชอบในการปฏิบัติตามหน้าที่ที่เกี่ยวข้องกับแต่ละบทบาท ตามนโยบายการจัดชั้นความลับของข้อมูลขององค์กรซึ่งใช้กับข้อมูลข้อมูลที่แลกเปลี่ยนกันได้ในรูปแบบอิเล็กทรอนิกส์ทุกประเภท รวมถึงข้อมูลดิจิทัลที่จัดเก็บไว้ในสื่อประเภทใดก็ได้ โดยมีผลกับเจ้าหน้าที่ทุกคนในองค์กร รวมถึงบุคคลที่สามที่ได้รับอนุญาตให้เข้าถึงข้อมูล ทีมจัดชั้นความลับของข้อมูลบทบาทและความรับผิดชอบในการตัดสินใจจัดชั้นความลับของข้อมูลของหน่วยงาน [14] ดังต่อไปนี้

---

[2] ในกรณีที่หน่วยงานรัฐมีความจำเป็นตามเงื่อนไขข้อยกเว้นในมาตรฐาน 24 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หน่วยงานรัฐสามารถเปิดเผยข้อมูลได้

บทบาทด้านข้อมูล	หน้าที่และความรับผิดชอบในการจัดชั้นความลับของข้อมูล
เจ้าของข้อมูล (Data Owner) ได้รับมอบหมายจากผู้บริหารด้านข้อมูล มีหน้าที่รับผิดชอบต่อสินทรัพย์ข้อมูลด้วยการ - ตรวจสอบให้แน่ใจว่ามีการใช้ local protocol ที่มีประสิทธิภาพเพื่อเป็นแนวทางในการใช้งานข้อมูลอย่างเหมาะสม - บริหารการเข้าถึงและการใช้ข้อมูล - ตรวจสอบให้แน่ใจว่าเป็นไปตามข้อกำหนดทางกฎหมาย กฎระเบียบ และนโยบายที่เกี่ยวข้องกับข้อมูลหรือทรัพย์สิน - ตรวจสอบให้แน่ใจว่าข้อมูลเป็นไปตามมาตรฐานด้านกฎหมาย ระเบียบข้อบังคับการแลกเปลี่ยน และการปฏิบัติงาน	เจ้าของข้อมูลมีหน้าที่รับผิดชอบในการตรวจสอบให้แน่ใจว่าข้อมูลของตนได้รับการจัดชั้นความลับตามมาตรฐานและหลักเกณฑ์ที่กำหนด และยังมีหน้าที่รับผิดชอบในการตรวจสอบให้แน่ใจว่าข้อมูลถูกเก็บไว้ในระบบที่ได้รับการจัดชั้นความลับในระดับเดียวกันหรือสูงกว่าชั้นข้อมูล ดังนี้ - ทบทวนและจัดหมวดหมู่: ตรวจทานและจัดหมวดหมู่ชุดข้อมูลที่รวบรวมโดยส่วนงาน/ฝ่าย - กำหนดป้ายกำกับการจัดชั้นความลับข้อมูล: กำหนดป้ายกำกับการจัดประเภทข้อมูลตามระดับความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต - รวบรวมข้อมูล: เพื่อตรวจสอบให้แน่ใจว่าข้อมูลที่รวบรวมจากหลายแหล่งมีการจัดชั้นความลับอย่างน้อยมีการจัดระดับชั้นความปลอดภัยสูงสุดของแต่ละระดับการชั้นของข้อมูล - ประสานงานการจัดชั้นความลับของข้อมูล: เพื่อตรวจสอบให้แน่ใจว่าข้อมูลที่มีการแบ่งปันทั้งภายในหน่วยงานและระหว่างหน่วยงานมีการจัดชั้นความลับและป้องกันข้อมูลอย่างสม่ำเสมอ - ปฏิบัติตามข้อกำหนดการจัดชั้นความลับของข้อมูล (ร่วมกับผู้ดูแลข้อมูล): เพื่อตรวจสอบให้แน่ใจว่าข้อมูลที่มีผลกระทบในระดับสูงและปานกลางมีความปลอดภัยตามมาตรฐานและนโยบายรัฐส่วนกลาง รวมทั้งกฎระเบียบและแนวทางปฏิบัติของหน่วยงาน - เข้าถึงข้อมูล (ร่วมกับผู้ดูแลข้อมูล): เพื่อพัฒนาแนวทางการเข้าถึงข้อมูลสำหรับแต่ละระดับชั้นความลับของข้อมูล
ผู้ดูแลข้อมูล (Data Custodian) หรือช่างเทคนิคจากฝ่ายเทคโนโลยีสารสนเทศหรือสำนักงานรักษาความปลอดภัยข้อมูลในองค์กรขนาดใหญ่ มีหน้าที่รับผิดชอบในการบำรุงรักษาและสำรองข้อมูลระบบ ฐานข้อมูลและเซิร์ฟเวอร์ที่เก็บข้อมูลขององค์กร และยังรับผิดชอบในการปรับใช้ทางเทคนิคของกฎระเบียบทั้งหมดที่กำหนดโดยเจ้าของข้อมูลและตรวจสอบให้แน่ใจว่ากฎระเบียบถูกบังคับใช้ภายในระบบทำงาน	รวมถึงความรับผิดชอบในการ - ควบคุมการเข้าถึง: ตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมการเข้าถึงที่เหมาะสม กำกับติดตามและตรวจสอบตามป้ายกำกับการจัดชั้นความลับของข้อมูลที่กำหนดโดยเจ้าของข้อมูล - ปฏิบัติตามข้อกำหนดการจัดชั้นความลับของข้อมูล (ร่วมกับเจ้าของข้อมูล): ตรวจสอบให้แน่ใจว่าข้อมูลที่มีผลกระทบในระดับสูงและปานกลางมีความปลอดภัยตามมาตรฐานและนโยบายรัฐส่วนกลาง รวมทั้งกฎระเบียบและแนวทางปฏิบัติของหน่วยงาน - เข้าถึงข้อมูล (ร่วมกับเจ้าของข้อมูล) : พัฒนาแนวทางการเข้าถึงข้อมูลสำหรับแต่ละระดับชั้นความลับของข้อมูล
บริกรข้อมูล (Data Steward) มีหน้าที่รับผิดชอบด้านคุณภาพและความสมบูรณ์ การดำเนินการและการบังคับใช้การจัดการข้อมูลภายในส่วนงาน/ฝ่าย หรือโครงการวิจัยของตน	มีหน้าที่ในการจำแนก/จัดระดับชั้นความลับของข้อมูล และระบุชั้นข้อมูลในเมทาดาตา (Metadata)[3] เพื่อกำหนดสิทธิการเข้าถึงและการนำข้อมูลไปใช้ได้อย่างเหมาะสม และอนุมัติการเข้าถึงภายใต้การมอบหมายจากเจ้าของข้อมูล โดยพิจารณาจากความเหมาะสมตามบทบาทของผู้ใช้ข้อมูลและการใช้งานตามวัตถุประสงค์ ในกรณีที่จำเป็น อาจต้องได้รับการอนุมัติจากผู้บริหารข้อมูล/เจ้าของข้อมูลก่อนที่จะให้สิทธิ์ในการเข้าถึง - อนุมัติการร้องขอข้อมูลร่วมกับเจ้าของข้อมูลและตรวจสอบ ทบทวนการจัดลำดับชั้นความลับข้อมูล - ร่วมกับหัวหน้าทีมบริกรข้อมูล ตรวจสอบการใช้งานข้อมูลสาธารณะและประเมินผลกระทบจากการเปิดเผยข้อมูล

---

[3] เมทาดาตา (Metadata) หรือข้อมูลที่ใช้อธิบายข้อมูล

บทบาทด้านข้อมูล	หน้าที่และความรับผิดชอบในการจัดชั้นความลับของข้อมูล
ผู้ใช้งานข้อมูล (Data User) หมายถึง บุคคล องค์กร หรือหน่วยงานที่เข้าถึง ป้อนข้อมูล แก้ไข ลบ ดึงข้อมูล หรือวิเคราะห์ข้อมูลในระบบข้อมูลเพื่อวัตถุประสงค์ในการปฏิบัติงานที่ได้รับอนุญาตจากเจ้าของข้อมูล ผู้ใช้งานข้อมูลต้องใช้ข้อมูลในลักษณะที่สอดคล้องกับวัตถุประสงค์ที่ตั้งใจไว้ และปฏิบัติตามนโยบายที่เกี่ยวข้องกับการใช้ข้อมูล	ผู้ใช้งานข้อมูลไม่ได้เกี่ยวข้องกับกระบวนการกำกับดูแล แต่มีหน้าที่ในการปฏิบัติตามข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement) และรับผิดชอบในการประกันคุณภาพของข้อมูล การรักษาความปลอดภัยที่เหมาะสมและการอนุมัติเป็นสิ่งจำเป็นจากบริกรข้อมูลเพื่อรักษาคุณภาพและความสมบูรณ์ของข้อมูล สร้างความไว้วางใจให้ปกป้องข้อมูล ผู้ใช้งานข้อมูลมีหน้าที่รับผิดชอบในการปฏิบัติตามนโยบายการกำกับดูแลข้อมูล นโยบายการกำกับดูแลข้อมูลการวิจัยและการจัดการวัสดุ และมาตรฐานและแนวทางที่เกี่ยวข้อง
คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ทำหน้าที่ตัดสินใจเชิงนโยบาย กฎเกณฑ์และแนวทางต่างๆ ต่อการจัดชั้นข้อมูลและการแบ่งปันข้อมูล	กำหนดแนวทาง ให้ข้อเสนอแนะ และอนุมัตินโยบายการจัดชั้นข้อมูล และการแบ่งปันข้อมูล และข้อบังคับอื่น ๆ ที่เกี่ยวข้องกับข้อมูลอ่อนไหว
ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) รับผิดชอบด้านการนำข้อมูลมาวิเคราะห์ข้อมูล และส่งเสริมให้เกิดการแลกเปลี่ยน เชื่อมโยงข้อมูล ระหว่างหน่วยงานภาครัฐ	ให้การสนับสนุนและพิจารณาการจัดชั้นความลับของข้อมูล และการจัดการความเสี่ยงที่อาจเกิดจากข้อมูลของหน่วยงานภาครัฐ รวมถึงการสร้างความร่วมมือในการแบ่งปันข้อมูลระหว่างหน่วยงาน
ผู้บริหารด้านความปลอดภัยและเทคโนโลยีสารสนเทศ (CIO & CISO) ความรับผิดชอบทางเทคนิคขั้นสูงสุดสำหรับการปกป้องคุ้มครองข้อมูลเป็นบทบาทใดบทบาทหนึ่งหรือทั้งสองอย่างของ CIO ที่ดำเนินการด้านระบบเทคโนโลยีสารสนเทศ (IT) ในขณะที่ CISO จะรักษาความปลอดภัยกับการดำเนินงานด้านไอทีให้มีประสิทธิภาพ	ทั้งคู่จำเป็นต้องเข้าใจแนวทางการจัดการข้อมูลที่มีความอ่อนไหว - CIO แนวทางการจัดหมวดหมู่/ชั้นความลับของข้อมูลและลดความยุ่งยากในการตัดสินใจลงทุนโครงสร้างพื้นฐานด้านไอทีโดยการทำรายการ ปริมาณ ตำแหน่ง และชั้นความลับของข้อมูลที่มีความอ่อนไหว - CISO การจัดชั้นความลับมุ่งเน้นว่าควรจัดสรรทรัพยากรการรักษาความปลอดภัยไว้ที่ใด และสามารถจัดการกับความเสี่ยง (Risk Management) ที่อาจทำให้ระบบเกิดปัญหากระทบกับการดำเนินธุรกิจขององค์กร โดยการระบุช่องว่างด้านความปลอดภัยก่อนที่จะกลายเป็นการละเมิด ทั้งนี้ ในกรณีของการจัดการข้อมูลส่วนบุคคล จะมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ร่วมตรวจสอบการดำเนินงานและการรักษาความปลอดภัยข้อมูลด้วย
ผู้นำองค์กร (CEO)	ให้การสนับสนุนการจัดชั้นความลับของข้อมูล เนื่องจากการสูญหายของข้อมูลภายในองค์กรอาจส่งผลให้เกิดผลกระทบต่อผลการดำเนินงาน ค่าปรับ/ค่าเสียหาย หรือทั้งสองอย่าง การจัดชั้นความลับช่วยผลักดันการมองเห็นและการปกป้องทั้งข้อมูลลูกค้า (PII) และข้อมูลการพัฒนาผลิตภัณฑ์ (IP) หรือบริการของภาครัฐ

3.6 ข้อเสนอแนะสู่การปฏิบัติ

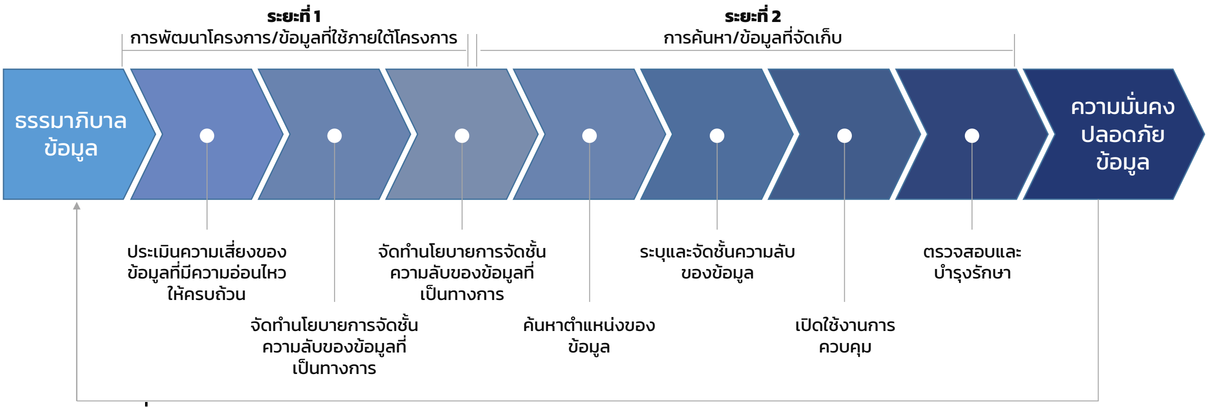
3.6.1 การจัดชั้นความลับของข้อมูลที่มีประสิทธิภาพ

การจัดชั้นความลับของข้อมูลควรประกอบไปด้วย 3 ส่วน ได้แก่ 1) การทำความเข้าใจกับสถานการณ์ด้านข้อมูลปัจจุบัน 2) กำหนดนโยบายการจัดชั้นความลับของข้อมูล และ 3) การจัดลำดับความสำคัญและจัดระเบียบข้อมูล โดยรายละเอียดจะกล่าวในข้อ 3.5.2

3.6.2 ขั้นตอนการจัดชั้นความลับของข้อมูล

สำหรับการดำเนินการจัดชั้นความลับของข้อมูลเป็นพื้นฐานของการบริหารจัดการข้อมูลอ่อนไหว เพื่อให้มั่นใจได้ว่าข้อมูลอ่อนไหวได้รับการดูแลอย่างเหมาะสม และเป็นส่วนสำคัญของกลยุทธ์การรักษาความปลอดภัยข้อมูลที่มีประสิทธิภาพ เพื่อคุ้มครองข้อมูลภายในหน่วยงานให้มีความมั่นคงปลอดภัย แบ่งปันและ

แลกเปลี่ยนข้อมูลระหว่างหน่วยงานได้ รวมทั้งสามารถใช้ประโยชน์จากข้อมูลร่วมกันได้ ควรดำเนินการตามขั้นตอนการจัดชั้นความลับของข้อมูล [15] แบ่งออกเป็น 2 ระยะ ได้แก่ ระยะที่ 1 การพัฒนาโครงการ/ข้อมูลที่ใช้ภายใต้โครงการ และ ระยะที่ 2 การค้นหา/ข้อมูลที่จัดเก็บ ดังขั้นตอนต่อไปนี้



ที่มา: 7 Steps to Effective Data Classification Version 15 August 2019, Thomas Eck.

รูปที่ 10 ขั้นตอนการจัดชั้นความลับของข้อมูล

1) ทำการประเมินความเสี่ยงของข้อมูลที่มีความอ่อนไหวให้ครบถ้วน ตรวจสอบให้แน่ใจว่ามีความเข้าใจที่ชัดเจนเกี่ยวกับข้อกำหนดด้านความเป็นส่วนตัวและการรักษาความลับ ตามกฎระเบียบและข้อกำหนดขององค์กร และกำหนดวัตถุประสงค์การจัดชั้นความลับของข้อมูลด้วยการสัมภาษณ์ที่เกี่ยวข้องกับผู้มีส่วนได้ส่วนเสียหลัก รวมถึงผู้นำองค์กรในการปฏิบัติตามข้อกฎหมาย

2) จัดทำนโยบายการจัดชั้นความลับของข้อมูลที่เป็นทางการ เพื่อป้องกันการจำแนกระดับชั้นความลับที่ละเอียดมากเกินไปซึ่งจะทำให้เกิดความสับสนและไม่สามารถจัดการได้ และเสริมสร้างบทบาทและความรับผิดชอบของเจ้าหน้าที่ นโยบายและขั้นตอนควรมีการกำหนดไว้อย่างชัดเจน และสอดคล้องกับความอ่อนไหวของข้อมูลที่สำคัญและให้เจ้าหน้าที่สามารถตีความให้เข้าใจได้ง่าย แต่ละระดับชั้นความลับควรมีรายละเอียดเกี่ยวกับประเภทของข้อมูล พร้อมด้วยแนวทางในการจัดการข้อมูล (handling data) และความเสี่ยงที่อาจเกิดขึ้น ทั้งนี้ เมื่อประกาศใช้นโยบายและสื่อสารให้ผู้ปฏิบัติงานได้รับทราบแล้ว ผู้ปฏิบัติงานควรดำเนินการจัดชั้นข้อมูลที่สร้างขึ้นใหม่และเข้าถึงข้อมูลล่าสุดทั้งหมดนับตั้งแต่วันที่ประกาศนโยบายก่อนที่จะจัดชั้นความลับของข้อมูลเดิมที่เหลืออยู่

3) จำแนกประเภทของข้อมูล การกำหนดประเภทความอ่อนไหวของข้อมูลที่มีอยู่ภายในองค์กรถือเป็นความท้าทายในปัจจุบัน ซึ่งควรมีการจัดระเบียบตามกระบวนงานตามภารกิจและขับเคลื่อนโดยเจ้าของข้อมูล และติดตามการไหลของข้อมูลจะให้ข้อมูลเชิงลึกว่าข้อมูลใดจำเป็นต้องได้รับการปกป้องและควรป้องกันอย่างไร อาจพิจารณาคำถามต่อไปนี้ องค์กรมีการเก็บรวบรวมข้อมูลอะไรบ้าง ข้อมูลเป็นข้อมูลข่าวสารลับหรือข้อมูลความมั่นคง องค์กรมีแนวทางการรักษาความปลอดภัยข้อมูลอย่างไร สามารถแบ่งปันข้อมูลนั้นได้หรือไม่

4) ค้นหาตำแหน่งของข้อมูล ภายหลังจำแนกประเภทข้อมูลในองค์กรแล้ว สถานที่จัดเก็บข้อมูลทั้งหมดจะถูกจัดเก็บแบบอิเล็กทรอนิกส์เป็นสิ่งสำคัญ การไหลของข้อมูลเข้าและออกจากองค์กร จึงเป็นข้อพิจารณาที่สำคัญว่า องค์กรจัดเก็บและแบ่งปันข้อมูลภายในและภายนอกอย่างไร มีการใช้บริการบนระบบคลาวด์หรือไม่ รวมถึงบนอุปกรณ์มือถือ ทั้งนี้ เครื่องมือค้นหาข้อมูลสามารถช่วยสร้างคลังข้อมูลที่ไม่มีโครงสร้างและช่วยให้เข้าใจอย่างชัดเจนว่าข้อมูลขององค์กรถูกจัดเก็บไว้ที่ใด โดยไม่คำนึงถึงรูปแบบหรือตำแหน่ง เพื่อช่วยแก้ปัญหาเกี่ยวกับการระบุเจ้าของข้อมูลด้วยการให้ข้อมูลเชิงลึกเกี่ยวกับผู้ใช้ที่จัดการข้อมูล ซึ่งการค้นหาสามารถรวมคำสำคัญ หรือประเภท หรือรูปแบบข้อมูลเฉพาะ เช่น หมายเลขเวชระเบียน หมายเลขประกันสังคม หรือหมายเลขบัตรเครดิต

5) ระบุและจัดชั้นความลับของข้อมูล เมื่อทราบตำแหน่งที่จัดเก็บข้อมูลแล้ว จะสามารถระบุและจัดชั้นความลับของข้อมูลได้และพิจารณาบทลงโทษที่เกี่ยวข้องกับการสูญเสียหรือการละเมิดข้อมูล ทั้งนี้ เครื่องมือการจำแนกชั้นความลับเชิงพาณิชย์สนับสนุนการริเริ่มการจัดชั้นความลับด้วยการอำนวยความสะดวกในการกำหนดการจัดชั้นความลับที่เหมาะสม จากการใช้ป้ายกำกับการจัดชั้นความลับของข้อมูลรวมถึงติดแท็กในเมทาดาตาของชุดข้อมูล ทั้งนี้ ระบบการจำแนกชั้นความลับที่ดีขึ้นอยู่กับผู้ใช้ ระบบที่สามารถแนะนำ การชั้นจัดข้อมูลได้แบบอัตโนมัติ

- จัดเตรียมเมนูตัวเลือกการจัดประเภทข้อมูลที่เหมาะกับองค์กร
- การตรวจหาเนื้อหาภายในรายการข้อมูล ตามด้วยการนำเสนอตัวเลือกการจัดหมวดหมู่/ชั้นความลับสำหรับการเลือกโดยผู้ใช้
- ระบบอัตโนมัติโดยที่ระบบเลือกการจำแนกประเภทชั้นความลับที่เหมาะสมโดยพิจารณาจากเครื่องมือวิเคราะห์ที่มีการป้อนข้อมูลของผู้ใช้อย่างจำกัด (ถ้ามี)

6) เปิดใช้งานการควบคุม กำหนดมาตรการความปลอดภัยทางไซเบอร์พื้นฐานและกำหนดการควบคุมตามนโยบายการจัดชั้นความลับของข้อมูลสำหรับการติดป้ายกำกับแต่ละระดับชั้นความลับ เพื่อให้แน่ใจว่ามีโซลูชันที่เหมาะสม ข้อมูลที่มีความเสี่ยงสูงต้องการการป้องกันขั้นสูง ในขณะที่ข้อมูลที่มีความเสี่ยงต่ำต้องการการป้องกันน้อยกว่า ด้วยการทำความเข้าใจว่าข้อมูลอยู่ที่ไหนและคุณค่าขององค์กรของข้อมูลสามารถนำการควบคุมความปลอดภัยที่เหมาะสมมาใช้โดยพิจารณาจากความเสี่ยงที่เกี่ยวข้อง เมทาดาตาการจำแนกชั้นความลับสามารถใช้โดยการป้องกันข้อมูลรั่วไหล (DLP) การเข้ารหัส และโซลูชันการรักษาความปลอดภัยอื่น ๆ เพื่อกำหนดว่าข้อมูลใดมีความอ่อนไหวและควรได้รับการปกป้องอย่างไร

7) ตรวจสอบและบำรุงรักษา เตรียมติดตามและดูแลระบบการจัดชั้นความลับของข้อมูลขององค์กร โดยปรับปรุงตามความจำเป็น นโยบายการจัดชั้นความลับควรเป็นแบบพลวัต ต้องสร้างกระบวนการที่เกี่ยวข้องกับการตรวจสอบและการปรับปรุงให้เป็นปัจจุบัน

3.6.3 การจัดการความเสี่ยงในการแบ่งปันข้อมูล

เพื่อส่งเสริมการแบ่งปันข้อมูลอย่างปลอดภัย หลักการทั้งห้าได้จัดทำกรอบการจัดการความเสี่ยงในการเปิดเผยข้อมูล ซึ่งสร้างสมดุลระหว่างความเสี่ยงที่จะเกิดขึ้นกับผลประโยชน์สาธารณะ หลักการแต่ละข้อถือได้ว่าเป็นกลไกการควบคุมที่ปรับได้ (เช่น ระดับการควบคุมที่สูงขึ้นหรือต่ำกว่าตามสัดส่วนในสภาพแวดล้อมที่มีการเข้าถึงข้อมูล) แม้ว่าหลักการแต่ละข้อสามารถพิจารณาแยกกันได้ แต่หลักการทั้ง 5 ประการควรได้รับการพิจารณาร่วมกันเพื่อประเมินว่าการแบ่งปันข้อมูลแบบใดแบบหนึ่งเป็นการจัดเตรียม การแบ่งปันข้อมูลที่ปลอดภัยหรือไม่ ในกรณีที่การประยุกต์ใช้หลักการไม่สามารถจัดให้มีการแบ่งปันข้อมูลได้อย่างปลอดภัย ผู้ดูแลข้อมูลไม่ควรเปิดเผยข้อมูลนั้น ทั้งนี้ การควบคุมควรอยู่บนพื้นฐานของการประเมินความเป็นไปได้และผลที่ตามมาของความเสี่ยงที่อาจจะเกิดขึ้นตามความเป็นจริง และจัดทำขึ้นในบริบทของการยอมรับความเสี่ยงขององค์กร มากกว่าที่จะอิงจากสถานการณ์ตามสมมุติฐานกรณีในกรณีที่เลวร้ายที่สุด

บรรณานุกรม

[1] ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล. (2563) เรื่องธรรมาภิบาลข้อมูลภาครัฐ ประกาศ ณ วันที่ 12 มีนาคม 2563 คัดจากราชกิจจานุเบกษา เล่มที่ 137 ตอนพิเศษ 74 ง วันที่ 31 มีนาคม 2563.

[2] The National Institute of Standards and Technology. (2008) Guide for Mapping Types of Information and Information Systems to Security Categories (NIST 800-60 Volume 1. and 2.)

[3] Federal Information Processing Standards Publication. (2004) Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199) (Url: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf)

[4] International Organization for Standardization. (2013) Information technology - Security techniques - Information security management systems – Requirements (ISO/IEC 27001)

[5] Australian Government. (2019) Best Practice Guide to Applying Data Sharing Principles. Retrieved from https://www.pmc.gov.au/sites/default/files/publications/data-sharing-principles-best-practice-guide-15-mar-2019.pdf

[6] Steve Simmonds. (2020, April). The Importance of Implementing Data Classification Frameworks. Retrieved from https://synergygrc.com/the-importance-of-implementing-data-classification-frameworks/

[7] Organization of American States and AWS. (2019) Data Classification. Retrieved from https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf

[8] ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม ประกาศ ณ วันที่ 30 พฤษภาคม พ.ศ. 2561 คัดจากราชกิจจานุเบกษา 135 ตอนพิเศษ 148 ง วันที่ 26 มิถุนายน 2561.

[9] ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และที่แก้ไขเพิ่มเติม ประกาศ ณ วันที่ 31 ตุลาคม พ.ศ. 2560 คัดจากราชกิจจานุเบกษา 134 ตอนพิเศษ 285 ง วันที่ 22 พฤศจิกายน 2560.

[10] Netwrix (2018) Data Classification Policy Example. Retrieved from https://www.netwrix.com/data_classification_policy_template.html

[11] Clark University. (2018) Data Classification Policies. Retrieved from https://www2.clarku.edu/offices/its/policies/pdf/data-classification-policy.pdf

[12] University of New South Wales. (2021) Data Classification Standard. Retrieved from https://www.unsw.edu.au/content/dam/pdfs/governance/policy/2022-01-policies/datastandard.pdf

[13] Harvard. (2017) Information Security Quick Reference Guide. Retrieved from https://security.harvard.edu/files/it-security/files/infosecquickguide20170920.pdf?m=1583529266

[12] Hamilton College. (2016) Procedure: Data Classification Handling Retrieved from https://www.hamilton.edu/documents/HCDataClassificationProcedure_20160808forwebsite.pdf

[13] พันเอก โสภณ ศิริงาม. (2549-2560). ตัวแบบในการกำหนดยุทธศาสตร์และยุทธศาสตร์ชาติ ในศตวรรษที่ 21 Retrieved from http://www.dsdw2016.dsdw.go.th/doc_pr/ndc_2559-2560/PDF/wpa_8293/ALL.pdf

[14] Carnegie Mellon University. (2019) Guidelines for Data Classification. Retrieved from https://www.cmu.edu/iso/governance/guidelines/data-classification.html

[15] Thomas Eck. (2019) 7 Steps to Effective Data Classification. Retrieved from https://edge.siriuscom.com/security/7-steps-to-effective-data-classification