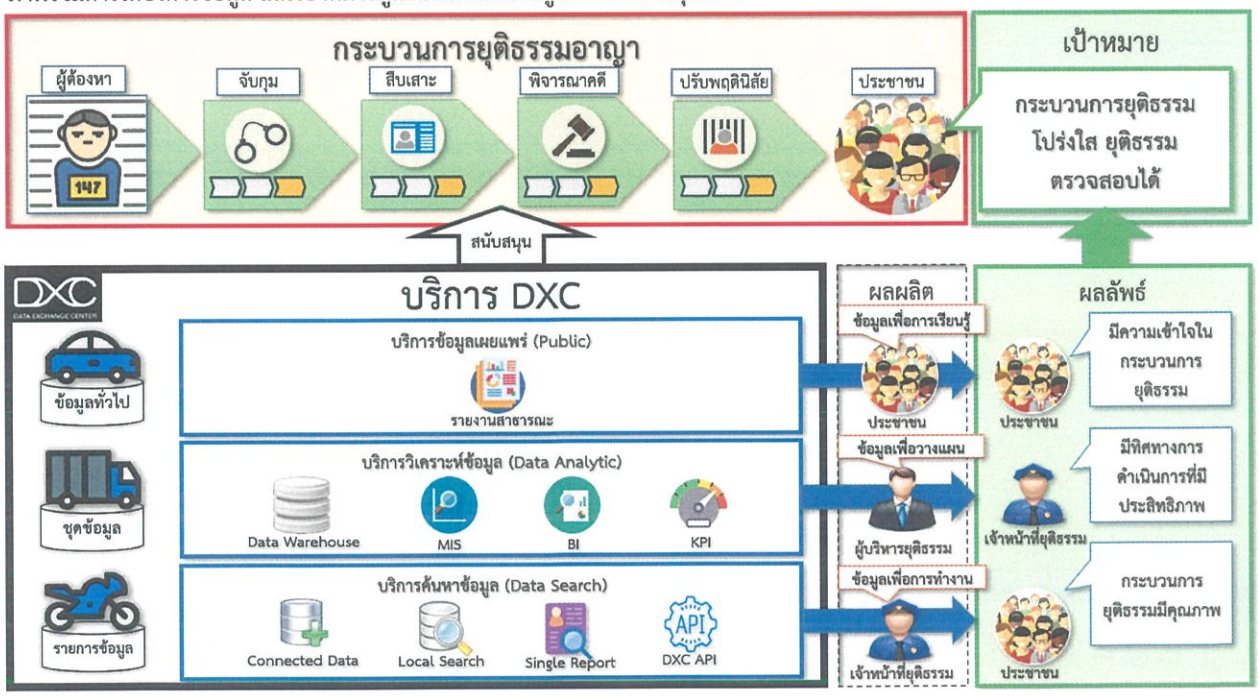
(ร่าง) ขอบเขตของงาน (Terms of Reference : TOR)
โครงการปรับปรุงด้านความปลอดภัยระบบ DXC ตามมาตรฐาน ISO 27001:2022

.....

๑. ความเป็นมา

ศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (Data Exchange Center : DXC) จัดตั้งขึ้นเพื่อส่งเสริมให้การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมให้เกิดผลสัมฤทธิ์ สามารถลดขั้นตอนการทำงานและเพิ่มประสิทธิภาพกระบวนงานในกระบวนการยุติธรรมได้อย่างเป็นรูปธรรม ในรูปแบบอิเล็กทรอนิกส์ที่เป็นมาตรฐาน โดยการค้นหา รวบรวม ประมวลผล รวมทั้งการเชื่อมโยงข้อมูลที่เป็นประโยชน์ระหว่างหน่วยงานในกระบวนการยุติธรรมและหน่วยงานที่เกี่ยวข้อง ให้สามารถรองรับการทำงานในรูปแบบดิจิทัลได้อย่างเหมาะสมต่อการรับและให้บริการหน่วยงานภาครัฐ ตลอดจนประชาชนที่เกี่ยวข้องด้วยความสะดวก รวดเร็ว โปร่งใส และปลอดภัยอย่างมั่นคงต่อเนื่อง ปัจจุบันนโยบายของรัฐบาลมีเป้าหมายอย่างชัดเจนในการส่งเสริมให้มีการแลกเปลี่ยนข้อมูลกระบวนการยุติธรรมระหว่างหน่วยงานให้เกิดผลสัมฤทธิ์และใช้ขั้นตอนน้อยที่สุดเพื่อความสะดวกรวดเร็วลดขั้นตอนกระบวนงานยุติธรรม ซึ่งตรงกับหน้าที่หลักและเป้าประสงค์ของการจัดตั้งศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม และเพื่อให้เป็นการเพิ่มประสิทธิภาพ โดยที่ผ่านมาในปีงบประมาณ พ.ศ. ๒๕๖๑ – ๒๕๖๕ ศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรมได้รับงบประมาณในการพัฒนาเชื่อมต่อข้อมูลหน่วยงานกระบวนการยุติธรรมกระแสหลัก สำนักงานศาลยุติธรรม สำนักงานอัยการสูงสุด และข้อมูลที่สำคัญในการให้บริการจากบริการข้อมูล Linkage Center กระทรวงมหาดไทย ในการสนับสนุนข้อมูลให้กับเจ้าหน้าที่ของรัฐที่เกี่ยวข้องในการบริการประชาชนด้านกระบวนการยุติธรรมที่มีข้อมูลสำคัญ ให้เกิดความเชื่อมั่นในระบบความมั่นคงปลอดภัย ตาม Roadmap การพัฒนาศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม

ภาพรวมการให้บริการข้อมูล และเป้าหมายศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม



ปัจจุบันศูนย์ DXC มีหน่วยงานในเครือข่ายจำนวน ๒๗ หน่วยงาน ได้แก่

๑. สำนักงานศาลยุติธรรม ๒. สำนักงานตำรวจแห่งชาติ ๓. สำนักงานอัยการสูงสุด ๔. กรมราชทัณฑ์ ๕. กรมพินิจและคุ้มครองเด็กและเยาวชน ๖. กรมคุมประพฤติ ๗. กรมสอบสวนคดีพิเศษ ๘. สำนักงาน ป.ป.ส. ๙. สำนักงาน ปปง. ๑๐. กรมการปกครอง ๑๑. กรมการขนส่งทางบก ๑๒. สำนักงานปลัดกระทรวงยุติธรรม ๑๓. สำนักงานกิจการยุติธรรม ๑๔. กองอำนวยการรักษาความมั่นคงภายในภาค ๔ ส่วนหน้า ๑๕. ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ ๑๖. กรมบังคับคดี ๑๗. สถาบันนิติวิทยาศาสตร์ ๑๘. กรมคุ้มครองสิทธิและเสรีภาพ ๑๙. สำนักงาน ป.ป.ท. ๒๐. สำนักงานประกันสังคม ๒๑. สำนักข่าวกรองแห่งชาติ ๒๒. หน่วยข่าวกรองทางทหาร ๒๓. สำนักงานคณะกรรมการการเลือกตั้ง ๒๔. กรมประมง ๒๕. สำนักงานผู้ตรวจการแผ่นดิน ๒๖. สำนักงาน ป.ป.ช. และ ๒๗. ธนาคารแห่งประเทศไทย

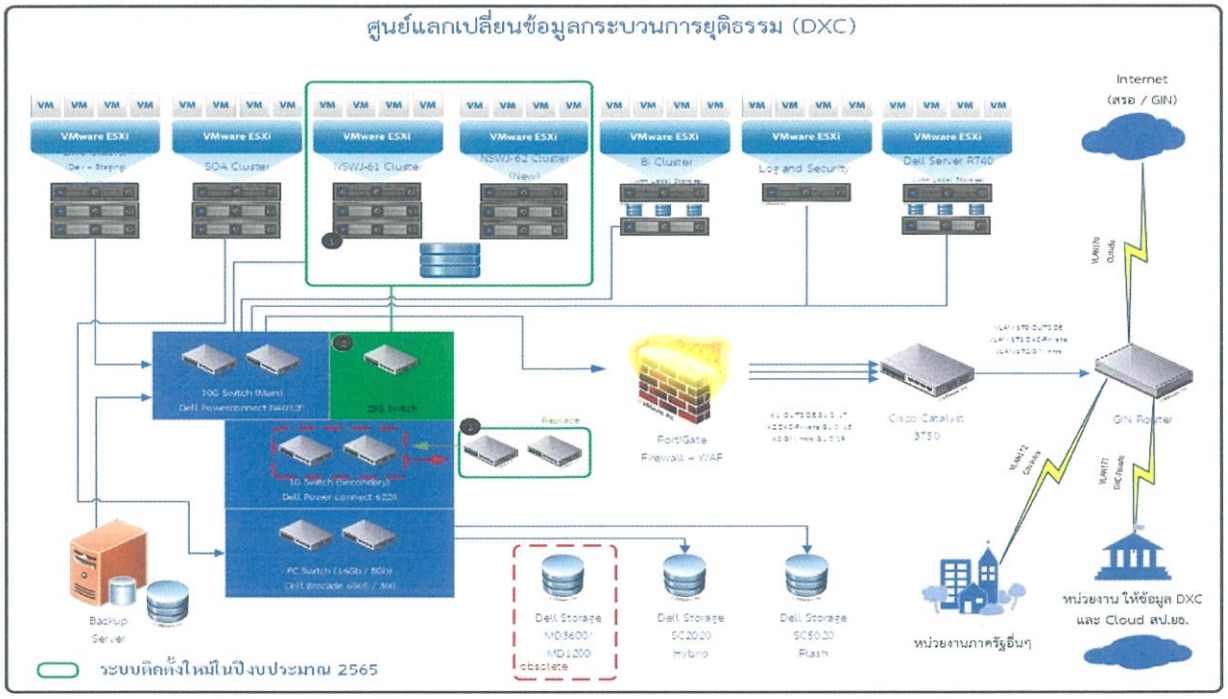
ศูนย์ DXC มีการเชื่อมโยงแลกเปลี่ยนข้อมูลจำนวน ๕๙ ฐานข้อมูล โดยจะมีการดำเนินการตามตารางนี้

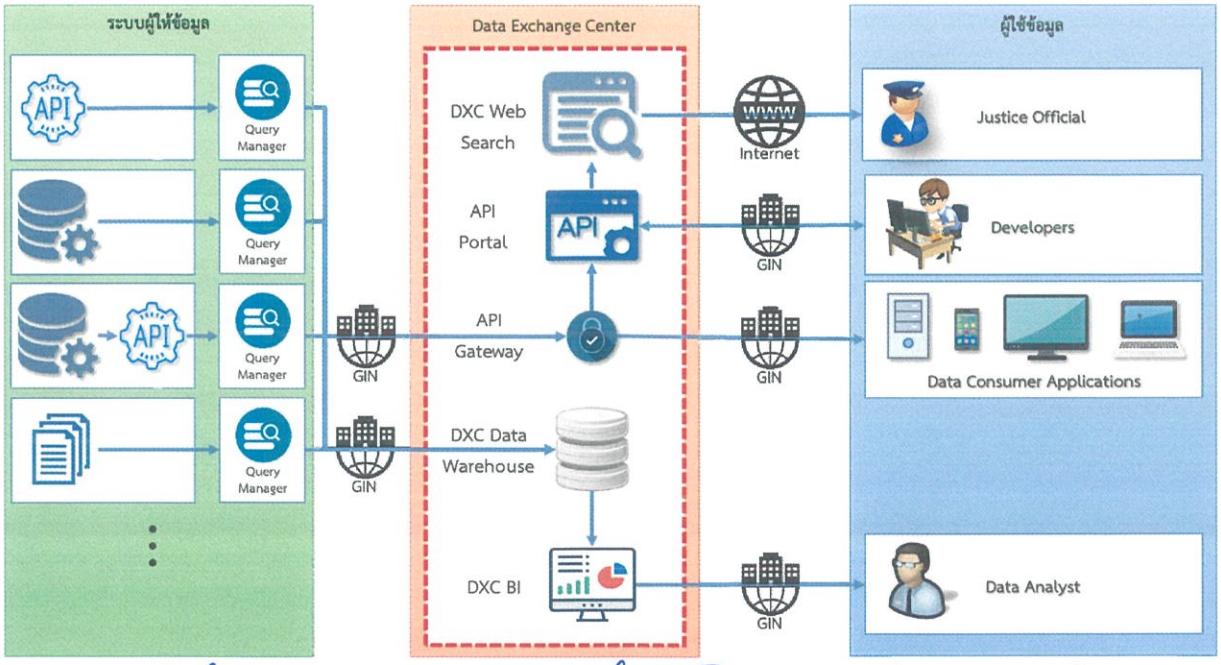
ที่	หน่วยงานเจ้าของข้อมูล	ที่	ฐานข้อมูล
๑	กรมการปกครอง	๑	ฐานข้อมูลทะเบียนราษฎร (Linkage Center)
		๒	ฐานข้อมูลบัตรประจำตัวประชาชน (Linkage Center)
		๓	ฐานข้อมูลที่อยู่บุคคลทุกประเภท (Linkage Center)
		๔	ฐานข้อมูลผู้ขอออกหนังสือผ่านแดนทั้งหมด (Linkage Center)
		๕	ฐานข้อมูลทะเบียนบุคคลต่างด้าว (Linkage Center)
		๖	ฐานข้อมูลใบอนุญาต ป.๔ ครอบครองอาวุธปืน (Linkage Center)
		๗	ฐานข้อมูลใบสูติบัตร (Linkage Center)
		๘	ฐานข้อมูลภาพใบหน้า (Linkage Center)
		๙	ข้อมูลทะเบียนสมรส (Linkage Center)
		๑๐	ข้อมูลทะเบียนหย่า (Linkage Center)
		๑๑	ฐานข้อมูลการจดทะเบียนเปลี่ยนชื่อตัว(Linkage Center)
		๑๒	ฐานข้อมูลการจดทะเบียนเปลี่ยนชื่อสกุล (Linkage)
		๑๓	ฐานข้อมูลทะเบียนราษฎร (ค้นหาด้วยชื่อตัว-ชื่อสกุล) (Linkage)
๒	สำนักงานประกันสังคม	๑๔	ฐานข้อมูลผู้ประกันตน
		๑๕	ฐานข้อมูลเลือกสถานพยาบาล
		๑๖	ฐานข้อมูลประวัติการจ้างงาน
๓	กรมการขนส่งทางบก	๑๗	ฐานข้อมูลทะเบียนยานพาหนะ
		๑๘	ฐานข้อมูลใบอนุญาตขับขี่
๔	สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด	๑๙	ฐานข้อมูลประวัติคดียาเสพติด
๕	กรมคุมประพฤติ	๒๐	ฐานข้อมูลผู้ถูกคุมประพฤติ
		๒๑	ฐานข้อมูลผู้ถูกคุมประพฤติในคดียาเสพติดและผลการเข้าร่วมกิจกรรมแก้ไขฟื้นฟู
๖	กรมพินิจและคุ้มครองเด็กและเยาวชน	๒๒	ฐานข้อมูลเด็กหรือเยาวชนผู้กระทำผิด

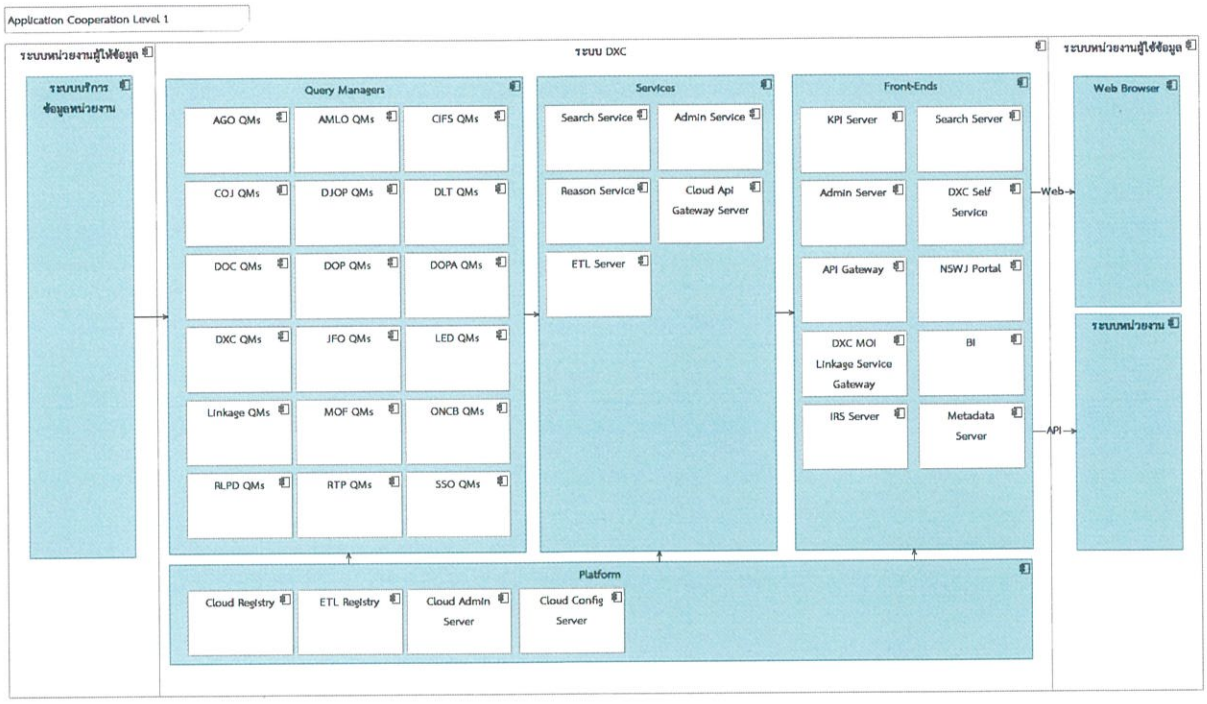
ที่	หน่วยงานเจ้าของข้อมูล	ที่	ฐานข้อมูล
๗	กรมบังคับคดี	๒๓	ฐานข้อมูลบุคคลล้มละลาย
๘	กรมราชทัณฑ์	๒๔	ฐานข้อมูลผู้ต้องขัง(ที่พิพากษาแล้ว)
		๒๕	ฐานข้อมูลผู้ต้องขัง(ที่ยังไม่พิพากษา)
		๒๖	ฐานข้อมูลอายัดตัวผู้ต้องขัง
		๒๗	ฐานข้อมูลผู้ต้องขัง(บุคคลล้มละลาย)
๙	สถาบันนิติวิทยาศาสตร์	๒๘	ฐานข้อมูลศพนิรนาม
		๒๙	ฐานข้อมูลศพไร้ญาติ
		๓๐	ฐานข้อมูลคนหาย
๑๐	กรมคุ้มครองสิทธิและเสรีภาพ	๓๑	ฐานข้อมูลความช่วยเหลือทางด้านการเงิน แก่ผู้เสียหายในคดีอาญา
		๓๒	ฐานข้อมูลความช่วยเหลือทางด้านการเงิน แก่จำเลยในคดีอาญา
		๓๓	ฐานข้อมูลผู้ร้องทุกข์
๑๑	กรมสอบสวนคดีพิเศษ	๓๔	ฐานข้อมูลหมายจับคดีพิเศษ
๑๒	สำนักงานปลัดกระทรวงยุติธรรม	๓๕	ฐานข้อมูลกองทุนยุติธรรม
		๓๖	ฐานข้อมูลกองทุนยุติธรรม(๒๕๖๔)
๑๓	กระทรวงการคลัง	๓๗	ฐานข้อมูลผู้มีรายได้น้อย
๑๔	กรมที่ดิน	๓๘	ฐานข้อมูลการครอบครองกรรมสิทธิ์ที่ดินและห้องชุด (Linkage Center)
๑๕	กรมพัฒนาฝีมือแรงงาน	๓๙	ฐานข้อมูลการพัฒนาฝีมือแรงงาน (Linkage Center)
๑๖	สำนักงานหลักประกันสุขภาพแห่งชาติ	๔๐	ข้อมูลสิทธิประกันสุขภาพและการลงทะเบียนกับหน่วยบริการ (Linkage Center)
๑๗	คณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ (ป.ป.ช.)	๔๑	ฐานข้อมูลผู้ถูกกล่าวหาคดีด้านการทุจริต (Linkage Center)
๑๘	สำนักงานอัยการสูงสุด	๔๒	ฐานข้อมูลผู้ต้องหา/จำเลย
		๔๓	ฐานข้อมูลข้อหาในตัวผู้ต้องหา/จำเลย
		๔๔	ฐานข้อมูลสถานที่เกิดเหตุ
		๔๕	ฐานข้อมูลผู้เสียหาย
		๔๖	ฐานข้อมูลคำพิพากษาในตัวผู้ต้องหา/จำเลย
		๔๗	ฐานข้อมูลสำนวนหลัก
		๔๘	ฐานข้อมูลสำนวนย่อย
		๔๙	ฐานข้อมูลคำสั่งอัยการ
		๕๐	ฐานข้อมูลอัยการแต่ละสำนวน
		๕๑	ฐานข้อมูลสารบบคดี (รายละเอียดข้อมูลคดี)
		๕๒	ฐานข้อมูลสารบบคดี (รายละเอียดข้อมูลส่วนบุคคล)
๑๙	กรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ	๕๓	ฐานข้อมูลคนพิการ (Linkage)

ที่	หน่วยงานเจ้าของข้อมูล	ที่	ฐานข้อมูล
๒๐	กรมการกงสุล	๕๔	ฐานข้อมูลหนังสือเดินทางประเทศไทย (Linkage)
๒๑	กรมสรรพากร	๕๕	ฐานข้อมูลทะเบียนผู้เสียภาษี (Linkage)
๒๒	สำนักงานศาลยุติธรรม	๕๖	ฐานข้อมูลหมายจับศาล
		๕๗	ฐานข้อมูลคำพิพากษาอย่างย่อ
		๕๘	ฐานข้อมูลคำพิพากษาฉบับเต็ม
*	ข้อมูลบูรณาการ ๓ หน่วยงาน (กรมพินิจฯ กรมคุมประพฤติ กรมราชทัณฑ์)	๕๙	ฐานข้อมูลคำบุคคลพ้นโทษ

แผนผัง Infrastructure และ Application







ศูนย์ DXC มี ๓ บริการหลักสำหรับเจ้าหน้าที่ผู้ปฏิบัติงานด้านงานยุติธรรม ดังนี้

๑. ระบบสืบค้นและจัดทำรายงานผู้กระทำผิด เป็นบริการสืบค้นข้อมูลและจัดทำรายงานประวัติบุคคลของผู้กระทำผิด โดยสามารถค้นหาได้ทั้งแบบค้นหารายฐานข้อมูล (Local Search) และรูปแบบสรุปจากทุกฐานข้อมูล (Single Report)

๒. ระบบรับส่งข้อมูลที่อยู่ในระบบ DXC ผ่าน API Portal เป็นบริการรับส่งข้อมูลที่ต้องการในระบบ DXC ไปยังระบบของหน่วยงานอย่างอัตโนมัติผ่าน API Portal

๓. ระบบรายงานข้อมูลสำหรับผู้บริหาร เป็นบริการข้อมูลในภาพรวมกระบวนการยุติธรรม เช่น รายงานอัตราการกระทำผิดซ้ำ รายงานปริมาณการใช้งานระบบ DXC เป็นต้น

ทั้งนี้ ศูนย์ DXC ได้ตรวจประเมินและได้รับการรับรองตามมาตรฐาน ISO/IEC 27001:2013 เมื่อวันที่ ๑๘ กันยายน ๒๕๖๓ และดำเนินการติดตามและทบทวนความสอดคล้องตามมาตรฐาน หรือเรียกว่า Surveillance Audit มาอย่างต่อเนื่อง ต่อมาในปี ๒๕๖๕ มาตรฐาน ISO/IEC 27001 ได้มีการเปลี่ยนเวอร์ชั่นในการตรวจสอบมาตรฐานจาก ISO/IEC 27001:2013 เป็น ISO/IEC 27001:2022 โดยสรุปสาระสำคัญได้ ดังนี้

๑) การเปลี่ยนแปลงด้านบทบรรณาธิการได้แก่ : คำว่า “มาตรฐานสากล” แทนที่ด้วยคำว่า “เอกสาร” ทั้งหมด การจัดเรียงวลีภาษาอังกฤษบางส่วนใหม่เพื่อให้เข้าใจง่ายขึ้น

๒) การเปลี่ยนแปลงเพื่อให้สอดคล้องกับแนวทาง ISO ได้แก่ : การจัดโครงสร้างตัวเลขใหม่ ข้อกำหนดในการกำหนดกระบวนการที่จำเป็นสำหรับการนำ ISMS ไปปฏิบัติและปฏิสัมพันธ์ของกระบวนการเหล่านั้น ข้อกำหนดที่ชัดเจนในการสื่อสารบทบาทองค์กรที่เกี่ยวข้องกับความปลอดภัยของข้อมูลภายในองค์กร

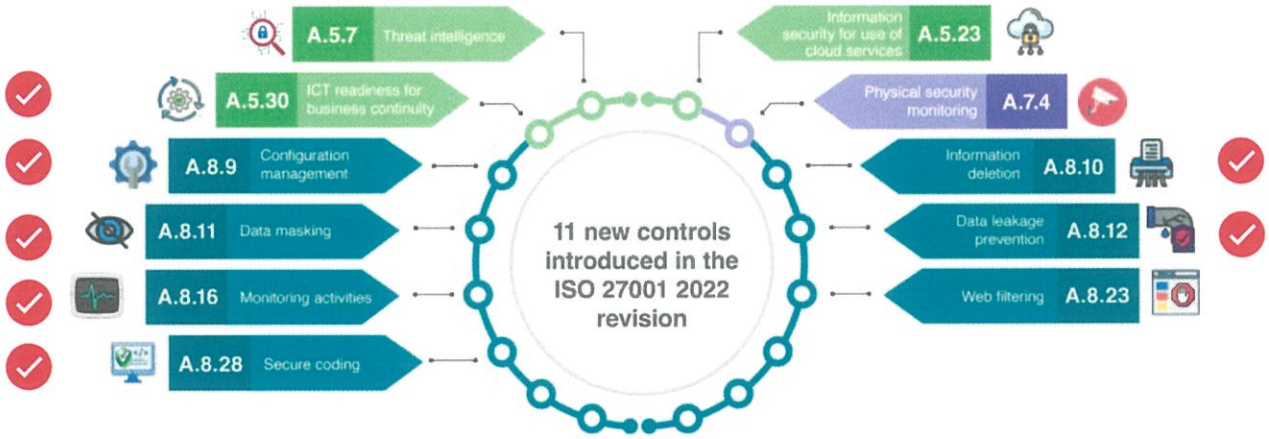
๓) การวางแผนการเปลี่ยนแปลง : ข้อกำหนดใหม่เพื่อให้มั่นใจว่าองค์กรกำหนดวิธีการสื่อสารเป็นส่วนหนึ่งของข้อ ๗.๔ ข้อกำหนดใหม่ในการสร้างเกณฑ์สำหรับกระบวนการปฏิบัติงานและการดำเนินการควบคุมกระบวนการ

๔) การเปลี่ยนแปลงที่สำคัญในการแก้ไขนี้มีอยู่ใน Annex A ซึ่งสะท้อนถึงการเปลี่ยนแปลงที่อยู่ใน ISO/IEC 27001:2022 การเปลี่ยนแปลงเหล่านี้คือ : โครงสร้างโดยรวมได้รับการปรับปรุงเป็น ๔ ส่วนหลัก คือองค์การ บุคคล กายภาพ และเทคโนโลยี แทน ๑๔ ส่วนในฉบับก่อนหน้านี้ มาตรการควบคุม (Controls) ลดลงจาก ๑๑๔ เหลือ ๙๓ รายการ มีการรวมมาตรการควบคุมบางตัว และบางตัวถูกลบออก มีการแนะนำ

มาตรการควบคุมใหม่ และส่วนอื่นๆ ที่อัปเดต แนวคิดของแอททริบิวต์ได้รับการแนะนำ มีความสอดคล้องกับคำศัพท์เฉพาะที่ใช้ทั่วไปในระบบความปลอดภัยในโลกดิจิทัล แอททริบิวต์ทั้ง ๕ นี้ ได้แก่ ประเภทการควบคุม คุณสมบัติด้านการรักษาความปลอดภัยของสารสนเทศ แนวคิดหลักด้านการรักษาความปลอดภัยทางไซเบอร์ ความสามารถในการปฏิบัติงาน และกลุ่มการรักษาความปลอดภัย

๕) การเพิ่มเติมและเปลี่ยนแปลงเกณฑ์การตรวจสอบมาตรฐานความปลอดภัยของข้อมูลมากยิ่งขึ้น

ดังนั้นในปีงบประมาณ พ.ศ. ๒๕๖๗ ศูนย์ DXC จึงจำเป็นต้องมีการปรับปรุงระบบต่างๆ ให้สอดคล้องกับการเพิ่มเติมและเปลี่ยนแปลงเกณฑ์การตรวจสอบมาตรฐานความปลอดภัยของข้อมูลมากยิ่งขึ้น จำนวน ๘ ประเด็น ได้แก่ A.5.7) Threat Intelligence A.5.30) ICT Readiness for business continuity A.8.9) Configuration management A.8.10) Information deletion A.8.11) Data masking A.8.12) Data leakage prevention A.8.16) Monitoring Activity และ A.8.28) Secure coding ดังแสดงตามภาพ



๒. วัตถุประสงค์

๒.๑ เพื่อปรับปรุงระบบศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) ให้มีความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001:2022

๒.๒ เพื่อให้ระบบศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) สามารถให้บริการได้อย่างมีมาตราฐานแบบสากล

๒.๓ เพื่อสร้างความเชื่อมั่นด้านความปลอดภัยของข้อมูลกับหน่วยงานเชื่อมโยงข้อมูล รวมถึงผู้ใช้งานระบบศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC)

๓. เป้าหมาย

ศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม เป็นศูนย์บริการด้านการแลกเปลี่ยนข้อมูลมีระบบการให้บริการที่มีมาตรฐานความปลอดภัยในระดับ สากล ISO/IEC 27001:2022

๔. ประโยชน์ที่คาดว่าจะได้รับ

๔.๑ ด้านผลผลิต ระบบศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) ที่มีมาตรฐานความปลอดภัยในระดับสากล ISO/IEC 27001:2022

๔.๒ ด้านผลลัพธ์ ศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม เป็นศูนย์บริการด้านการแลกเปลี่ยนข้อมูลที่มีระบบการให้บริการที่มีมาตรฐานความปลอดภัยในระดับสากล ISO/IEC 27001:2022

๔.๓ ด้านผลสัมฤทธิ์ ยกระดับศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) สร้างความเชื่อมั่นด้านปลอดภัยของข้อมูล

๕. <u>คุณสมบัติของผู้ยื่นข้อเสนอ</u>

๕.๑ มีความสามารถตามกฎหมาย

๕.๒ ไม่เป็นบุคคลล้มละลาย

๕.๓ ไม่อยู่ระหว่างเลิกกิจการ

๕.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๕.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๕.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๕.๗ เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๕.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอราคารายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานกิจการยุติธรรม ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๕.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

๕.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงานสิ่งของหรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

๕.๑๑ ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง

๕.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิ ที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า ๒ ล้านบาท

(๓) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา โดยพิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(๔) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณที่ยื่นข้อเสนอในครั้งนั้น (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน)

(๕) กรณีตาม (๑) - (๔) ยกเว้นสำหรับกรณีดังต่อไปนี้

(๕.๑) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(๕.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑

๕.๑๓ ผู้ยื่นข้อเสนอจะต้องมีประสบการณ์หรือผลงานในการพัฒนาระบบสารสนเทศที่มีลักษณะการเชื่อมโยงข้อมูลระหว่างหน่วยงานภาครัฐหรือภาคเอกชน อย่างน้อย ๑ โครงการ โดยต้องเป็นโครงการที่มีการเชื่อมโยงข้อมูลแบบเว็บเซอร์วิสไม่น้อยกว่า ๒ หน่วยงาน โดยผู้ยื่นข้อเสนอต้องแนบเอกสารหลักฐานสัญญาจ้างงานดังกล่าวมายื่นพร้อมเอกสารประกวดราคาครั้งนี้ด้วย โดยแต่ละสัญญาต้องมีมูลค่าไม่น้อยกว่า ๒,๐๐๐,๐๐๐ บาท (สองล้านบาทถ้วน) และเป็นผลงานย้อนหลังไม่เกิน ๕ ปี นับจากวันที่ยื่นข้อเสนอ

๕.๑๔ ผู้ยื่นข้อเสนอจะต้องจัดทำรูปแบบและแนวทางการพัฒนาและปรับปรุงระบบด้านความปลอดภัยการให้บริการของศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) ตามมาตรฐาน ISO/IEC 27001:2022 เพื่อแสดงความเข้าใจในการพัฒนาปรับปรุงระบบตามโครงการฯ โดยผู้ยื่นข้อเสนอต้องแนบเอกสารดังกล่าวมายื่นพร้อมเอกสารประกวดราคาครั้งนี้ด้วย

๕.๑๕ ผู้ยื่นข้อเสนอต้องมีทีมงานในการดำเนินโครงการนี้ ไม่น้อยกว่า ๓ คน โดยต้องแนบเอกสารหลักฐานคุณสมบัติและรายละเอียดการติดต่อ (เบอร์โทรศัพท์และไปรษณีย์อิเล็กทรอนิกส์) ซึ่งประกอบด้วย

๕.๑๕.๑ ผู้บริหารโครงการ หรือ Project Manager มีคุณสมบัติ ดังนี้

มีวุฒิทางการศึกษาอย่างน้อยปริญญาโท สาขาวิศวกรรมศาสตร์คอมพิวเตอร์ หรือสาขาวิศวกรรมศาสตร์ในสาขาที่เกี่ยวข้อง หรือสาขาวิทยาการคอมพิวเตอร์ หรือสาขาวิทยาศาสตร์คอมพิวเตอร์ หรือสาขาสารสนเทศศาสตร์ หรือสาขาอื่นๆ ที่เกี่ยวข้อง และมีประสบการณ์ในการทำงานที่เกี่ยวข้องกับการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ ไม่น้อยกว่า ๕ ปี จำนวนไม่น้อยกว่า ๑ คน

๕.๑๕.๒ หัวหน้าทีมงานด้านพัฒนาและปรับปรุงระบบโครงสร้างระบบสารสนเทศ มีคุณสมบัติ ดังนี้

มีวุฒิทางการศึกษาอย่างน้อยปริญญาโท สาขาวิศวกรรมศาสตร์คอมพิวเตอร์ หรือสาขาวิศวกรรมศาสตร์ในสาขาที่เกี่ยวข้อง หรือสาขาวิทยาการคอมพิวเตอร์ หรือสาขาวิทยาศาสตร์คอมพิวเตอร์ หรือสาขาสารสนเทศศาสตร์ หรือสาขาอื่นๆ ที่เกี่ยวข้อง และมีประสบการณ์ไม่น้อยกว่า ๕ ปี ในการพัฒนาระบบหรือปรับปรุงโครงสร้างระบบสารสนเทศ ในหน่วยงานภาครัฐหรือเอกชน จำนวนไม่น้อยกว่า ๑ คน

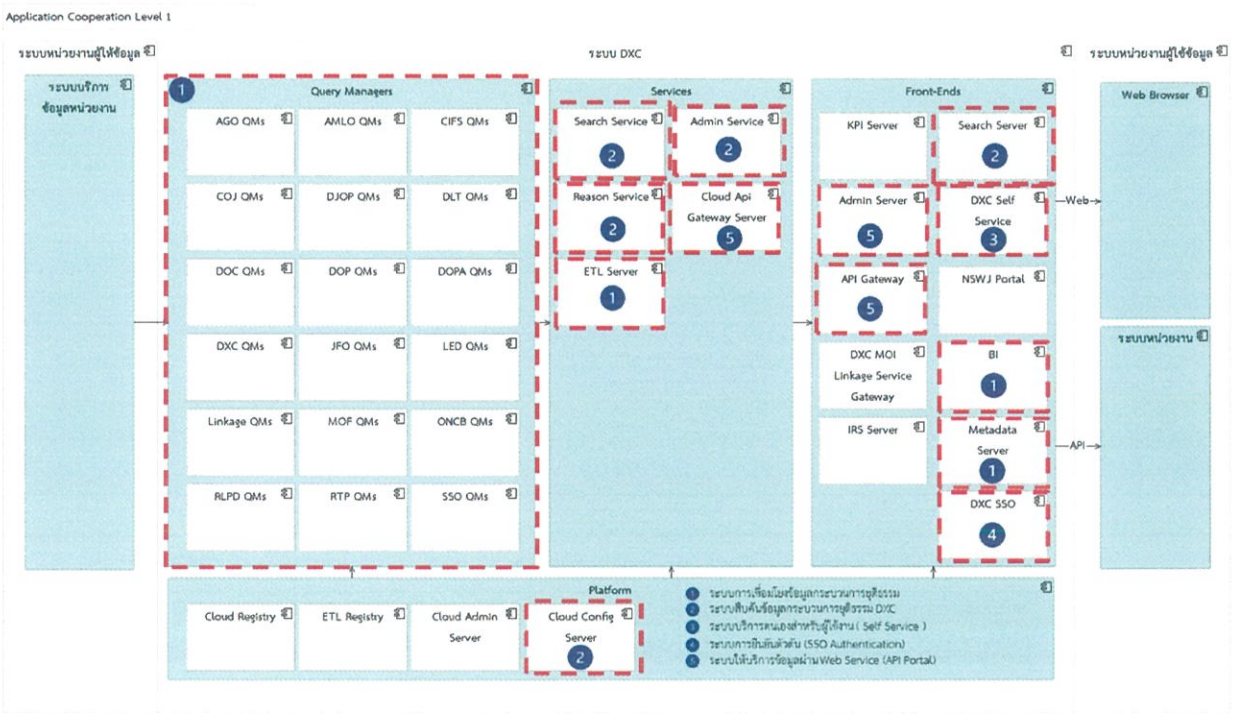
๕.๑๕.๓ หัวหน้าทีมงานพัฒนาและปรับปรุงระบบสารสนเทศ มีคุณสมบัติ ดังนี้

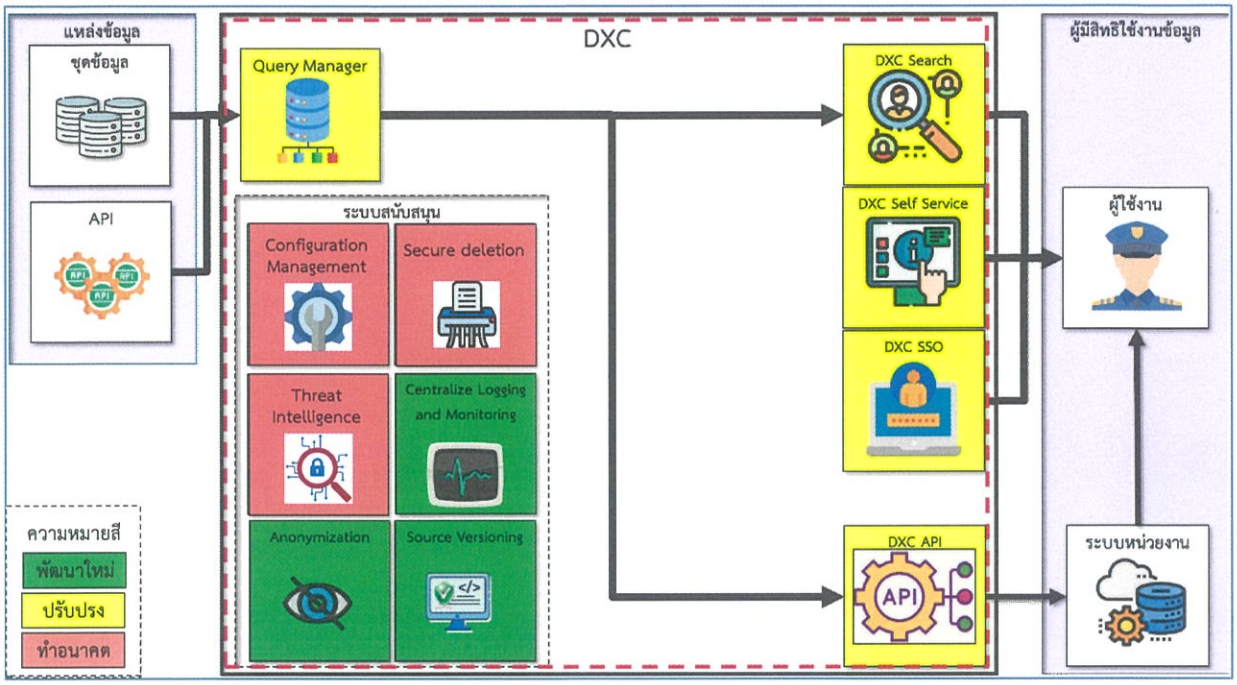
มีวุฒิทางการศึกษาอย่างน้อยปริญญาตรี สาขาวิศวกรรมศาสตร์คอมพิวเตอร์ หรือสาขาวิศวกรรมศาสตร์ในสาขาที่เกี่ยวข้อง หรือสาขาวิทยาการคอมพิวเตอร์ หรือสาขาวิทยาศาสตร์คอมพิวเตอร์ หรือสาขาสารสนเทศศาสตร์ หรือสาขาอื่นๆ ที่เกี่ยวข้อง และมีประสบการณ์ในการพัฒนาระบบ Web Service และเชื่อมโยงข้อมูล ในหน่วยงานภาครัฐหรือเอกชนไม่น้อยกว่า ๕ ปี จำนวนไม่น้อยกว่า ๑ คน

๖. ขอบเขตของงานที่จะดำเนินการจัดจ้าง

การจ้างเหมาบริการปรับปรุงด้านความปลอดภัยระบบ DXC ตามมาตรฐาน ISO/IEC 27001:2022 เป็นการดำเนินการทบทวนและปรับปรุงระบบให้มีความสอดคล้องกับประเด็นต่างๆ ข้างต้น เพื่อให้ระบบสามารถให้บริการได้อย่างมีมาตราฐานแบบสากล มีทั้งสิ้น ๕ ระบบ ดังนี้

๑. ระบบการเชื่อมโยงข้อมูลกระบวนการยุติธรรมจำนวน ๕๙ ฐานข้อมูล จาก ๒๓ หน่วยงานเจ้าของข้อมูล
๒. ระบบสืบค้นข้อมูลกระบวนการยุติธรรม DXC
๓. ระบบบริการตนเองสำหรับผู้ใช้งาน (Self Service)
๔. ระบบการยืนยันตัวตน (SSO Authentication)
๕. ระบบให้บริการข้อมูลผ่าน Web Service (API Portal)





ISO 27001 VERSION 2022 GAP

ดำเนินการในอนาคต | ไม่ต้องดำเนินการ | ดำเนินการภายใต้โครงการ | ดำเนินการเองโดย สกธ.

Type	Title	People	Process	Technology	Documentation
Organization	5.7 Threat Intelligence	อบรมความตระหนักในความสำคัญของการแจ้งเตือนภัยคุกคาม และ ให้ทราบถึงบุคลากรที่เกี่ยวข้องในการประสานงาน	กระบวนการรวบรวม และใช้ข้อมูลภัยคุกคามเพื่อจัดทำกระบวนการป้องกัน	จัดหาและติดตั้งระบบข่าวกรองด้านภัยคุกคามไซเบอร์ (Threat Intelligence Platform)	ไม่บังคับ - Supplier Security Policy - Incident Management Procedure - Security Operating Procedures
Organization	5.23 Information Security for use of cloud services	- อบรมความตระหนักในด้านความปลอดภัยบน Cloud - อบรมการใช้งานความปลอดภัยของผู้ให้บริการ Cloud	- กระบวนการจัดทำข้อกำหนดความปลอดภัยของผู้ให้บริการ Cloud เพื่อใช้ในการคัดเลือก	ไม่มี (หมายเหตุ ไม่มีการใช้งาน Cloud)	ไม่บังคับ - Supplier Security Policy
Organization	5.30 ICT Readiness for business continuity	- อบรมสร้างความตระหนักต่อการขาดช่วงของการทำงานที่อาจจะเกิดขึ้น - อบรมการดูแลรักษาระบบในกรณีเกิดเหตุขัดข้อง	- กระบวนการจัดทำแผนความเสี่ยง และ การกู้คืนระบบ - กระบวนการจัดทำแผนดูแลรักษาระบบ - กระบวนการจัดทำแผนทดสอบการกู้คืนจากภัยพิบัติ	ปรับปรุงระบบเชื่อมโยงข้อมูลให้รองรับการทำงานที่ Resilience และ Redundancy โดยให้มีบริการหลายชุดเพื่อรองรับกรณีระบบชุดใดชุดหนึ่งมีปัญหาโดยรองรับการกระจายการทำงาน (Load Balancing)	ไม่บังคับ - Disaster Recovery Plan - Internal Audit Report – readiness testing
Physical	7.4 Physical Security Monitoring	- อบรมสร้างความตระหนักให้เจ้าหน้าที่เห็นถึงภัยในการให้เข้าไปในสถานที่ที่ไม่ได้รับสิทธิ - อบรมการใช้งานระบบความปลอดภัย	- กระบวนการดูแลความปลอดภัย และผู้รับผิดชอบ	Video and Alarm System	ไม่บังคับ - Procedures that Regulate Physical Security - Incident Management Procedure

Type	Title	People	Process	Technology	Documentation
Technological 	8.9 Configuration Management	อบรมความตระหนักต่อความจำเป็นในการควบคุมการเปลี่ยนแปลง ค่าความปลอดภัย และ วิธีการแก้ค่าความปลอดภัย	กระบวนการบริหารจัดการการตั้งค่าความปลอดภัย และจัดทำทะเบียน Configuration Management (CMDB)	จัดหาและติดตั้งระบบ Configuration Management (CMDB)	จำเป็น Security Operation Procedures – Configuration Rules
Technological 	8.10 Information deletion	อบรมความตระหนักต่อความจำเป็นในการลบข้อมูลอ่อนไหว	กระบวนการกำหนดแนวทางการลบข้อมูล	จัดหาและติดตั้งระบบ Secure Deletion Tools	ไม่จำเป็น Disposal and Destruction Policy, Acceptable Use Policy, Security Operating Procedures Data Retention Policy (Enterprise)
Technological 	8.11 Data masking	อบรมความตระหนักต่อความจำเป็นในการปกปิดข้อมูล และวิธีการปกปิดข้อมูล	กระบวนการพิจารณาข้อมูลที่ต้องทำการ ปกปิด สิทธิ ประเภทข้อมูล และวิธีในการปกปิดข้อมูล	- จัดหาและติดตั้งโปรแกรมทำ Anonymization ให้กับข้อมูลที่มีการจัดเก็บ - ปรับปรุง API ที่มีอยู่ให้มีการจัดทำ JSON Masking - ปรับปรุงระบบให้บริการให้มีการจัดทำ UI Masking	ไม่จำเป็น Information Classification Policy, Access Control Policy, Secure Development Policy ENT -Privacy Policy / Personal Data Protection Policy, Anonymization and Pseudonymization Policy
Technological 	8.12 Data leakage prevention	อบรมสร้างความตระหนักต่อข้อมูลอ่อนไหวที่มี และความสำคัญของการป้องกัน	กระบวนการพิจารณาข้อมูลอ่อนไหว ประเมินความเสี่ยง และ ช่องทางข้อมูล เพื่อหาจุดที่มีโอกาสให้ข้อมูลรั่วไหล	- เข้ารหัสข้อมูลระหว่าง ระบบภายในและภายนอก - เข้ารหัสข้อมูลอ่อนไหวใน Configuration - ควบคุมสิทธิการเข้าถึงข้อมูลการตั้งค่า	ไม่จำเป็น Information Classification Policy, Security Operating Procedures, Policy on Acceptable Use
Technological 	8.16 Monitoring activities	อบรมสร้างความตระหนักในการติดตามตรวจสอบการทำงานของระบบ กรณีผิดปกติ และ วิธีการตรวจสอบ	กระบวนการพิจารณาระบบที่ควร ติดตาม ตรวจสอบ ความรับผิดชอบ วิธีการ เกณฑ์เหตุผิดปกติ	จัดหาและติดตั้ง ระบบติดตามตรวจสอบการทำงานของระบบ (SystemObservability Platform)	ไม่จำเป็น Security Operating Procedures
Technological 	8.23 Web filtering	อบรมสร้างความตระหนักในภัยของการใช้ Internet ข้อแนะนำการใช้ Internet อย่างปลอดภัย และ อบรมผู้ดูแลระบบในการใช้งาน Web Filtering	กระบวนการพิจารณาประเภท เว็บที่ไม่ควรให้เข้าถึง และการดูแลระบบคัดครอง	- Web Application Firewall (WAF) - Network Firewall - Antivirus	ไม่จำเป็น Security Operating Procedures, Acceptable Use Policy
Technological 	8.28 Secure coding	อบรมทีมพัฒนาให้ตระหนักถึงความสำคัญในการเขียนโปรแกรมให้ปลอดภัย	กระบวนการตั้งเกณฑ์การเขียนโปรแกรมอย่างปลอดภัย กระบวนการตรวจสอบ	ระบบบริหารจัดการและ ตรวจสอบความปลอดภัยของ Source Code (Version Control System and Source Code Scanning)	ไม่จำเป็น Secure Development Policy

โดยผู้รับจ้างจะต้องดำเนินการตามขอบเขตงาน ดังนี้

๖.๑ ข้อกำหนดทั่วไป

๖.๑.๑ ผู้รับจ้างจะต้องจัดทำแผนการดำเนินงานโครงการ โดยระบุระยะเวลาการดำเนินงานและผู้รับผิดชอบอย่างชัดเจน และจัดทำแนวคิดสถาปัตยกรรมการเชื่อมโยงข้อมูล (Conceptual Information Integration Architecture) ในการพัฒนาระบบ

๖.๑.๒ ผู้รับจ้างมีหน้าที่ในการนำเสนอผลงานการขับเคลื่อนโครงการ ต่อคณะกรรมการ คณะอนุกรรมการ คณะทำงาน หรือหน่วยงานอื่นๆ ที่เกี่ยวข้อง

๖.๑.๓ ผู้รับจ้างต้องดำเนินการพัฒนาระบบภายใต้โครงการนี้ โดยไม่ส่งผลกระทบกับการทำงานของระบบเดิม (Application DXC Core และ Application DXC QM และส่วนอื่นๆ ที่เกี่ยวข้อง)

๖.๑.๔ ผู้รับจ้างจะต้องติดตั้งระบบที่พัฒนาขึ้นในโครงการนี้ให้สามารถใช้งานได้อย่างมีประสิทธิภาพภายใต้กระบวนการและขั้นตอนการใช้งานที่มีอยู่เดิม หรือตามที่สำนักงานกิจการยุติธรรมกำหนด

๖.๑.๕ ผู้รับจ้างจะต้องรับผิดต่อสำนักงาน ดังนี้

๖.๑.๕.๑ ในกรณีที่ผู้รับจ้าง ผู้แทน ช่าง หรือลูกจ้างของผู้รับจ้างจงใจหรือประมาทเลินเล่อ หรือไม่มีความรู้ความชำนาญพอ กระทำหรืองดเว้นการกระทำใดๆ เป็นเหตุให้ระบบเทคโนโลยีสารสนเทศของสำนักงาน เสียหาย หรือไม่อยู่ในสภาพที่ใช้การได้ดี ผู้รับจ้างจะต้องดำเนินการจัดหาระบบเทคโนโลยีสารสนเทศที่มีคุณภาพและความสามารถในการใช้งานไม่ต่ำกว่าของเดิมชดใช้แทน หรือชดใช้ราคาระบบเทคโนโลยีสารสนเทศในขณะที่เกิดความเสียหาย ในกรณีที่ไม่อาจจัดหาระบบเทคโนโลยีสารสนเทศดังกล่าวชดใช้แทนได้ ให้แก่สำนักงาน ภายในระยะเวลาที่สำนักงานกำหนด และผู้รับจ้างต้องรับผิดตามกฎหมายพร้อมชดเชยค่าเสียหายที่เกิดขึ้น

๖.๑.๕.๒ ในกรณีนำข้อมูลของระบบแลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) หรือข้อมูลของหน่วยงานที่เกี่ยวข้องไปเผยแพร่หรือนำไปใช้ในทางมิชอบ โดยทั้งเจตนาและไม่เจตนา ผู้รับจ้างต้องรับผิดตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นๆ ที่เกี่ยวข้อง พร้อมชดเชยค่าเสียหายที่เกิดขึ้น

๖.๑.๖ ในการพัฒนาระบบงานต่างๆ เมื่อการพัฒนาระบบเสร็จสิ้น ผู้รับจ้างจะต้องจัดส่ง Source Code ให้กับสำนักงานกิจการยุติธรรม และระบบที่พัฒนาขึ้นภายใต้โครงการนี้ถือเป็นลิขสิทธิ์ของสำนักงานกิจการยุติธรรมอย่างถูกต้องตามกฎหมาย ทั้งนี้ สำนักงานกิจการยุติธรรมจะเปิดเผย Source Code ที่เป็นลิขสิทธิ์ของสำนักงานกิจการยุติธรรมให้กับผู้รับจ้าง เพื่อให้สามารถดำเนินการพัฒนาระบบงาน

๖.๒ ข้อกำหนดการพัฒนาและปรับปรุงระบบสารสนเทศศูนย์ DXC

๖.๒.๑ พัฒนาและปรับปรุงมาตรฐานความปลอดภัยระบบการเชื่อมโยงข้อมูลกระบวนการยุติธรรมจำนวน ๕๙ ฐานข้อมูล

ออกแบบและพัฒนาระบบให้บริการข้อมูลให้รองรับมาตรฐานตาม ISO/IEC 27001:2022 โดยมีการดำเนินการดังต่อไปนี้

๖.๒.๑.๑ ตรวจสอบระบบ และจัดทำ Gap Analysis ของระบบเทียบกับมาตรฐานความปลอดภัย ISO/IEC 27001:2022 ใน ๘ ประเด็น ดังนี้ A.5.7) Threat Intelligence A.5.30) ICT Readiness for business continuity A.8.9) Configuration management A.8.10) Information deletion A.8.11) Data masking A.8.12) Data leakage prevention A.8.16) Monitoring Activity A.8.28) Secure coding

๖.๒.๑.๒ ออกแบบและนำเสนอแนวคิดสถาปัตยกรรมการเชื่อมโยงข้อมูล (Conceptual Information Integration Architecture) เพื่อกำหนดแนวทางทางด้านเทคนิคของการแลกเปลี่ยนข้อมูลที่เหมาะสมจากแต่ละหน่วยงาน ให้รองรับมาตรฐานตาม ISO/IEC 27001:2022

๖.๒.๑.๓ พัฒนาระบบตามแนวคิดสถาปัตยกรรมการเชื่อมโยงข้อมูล (Conceptual Information Integration Architecture) และตั้งค่า/ปรับปรุง/จัดการ ระบบให้รองรับตามมาตรฐานตาม ISO/IEC 27001:2022 และการใช้งานในระบบศูนย์แลกเปลี่ยนข้อมูลที่มีอยู่

๖.๒.๑.๔ ปรับปรุงระบบศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรมที่เกี่ยวข้องให้รองรับการแสดงผลตามข้อกำหนด

(๑) พัฒนาและปรับปรุงระบบเชื่อมโยงข้อมูล ที่มีอยู่และระบบโครงสร้างพื้นฐานที่เกี่ยวข้อง

(๒) ปรับปรุงระบบให้สามารถปิดบัง (Masking) ข้อมูลผลลัพธ์ที่ต้องการปกปิดในรูปแบบบางส่วน หรือ ทั้งหมด เพื่อให้ผลลัพธ์แสดงให้เห็นตามสิทธิ์ หรือ นโยบายที่กำหนดไว้

(๓) ปรับปรุงระบบให้มีการตรวจสอบ และควบคุมสิทธิ์ตามผลการตรวจสอบความปลอดภัยที่พบ

(๔) ปรับปรุงให้ระบบมีการส่งข้อมูลผ่านช่องทางเข้ารหัส

(๕) ปรับปรุงระบบเชื่อมโยงข้อมูลให้รองรับการทำงานที่ Resilience และ Redundancy โดยให้มีบริการหลายชุด เพื่อรองรับกรณีระบบชุดใดชุดหนึ่งมีปัญหา โดยรองรับการกระจายการทำงาน (Load Balancing)

(๖) ปรับปรุงระบบบริการที่เกี่ยวข้องให้รองรับการให้บริการข้อมูลการใช้งาน ไปยังฐานข้อมูลจัดเก็บประวัติการใช้งานกลาง

(๗) พัฒนา หรือปรับปรุง ระบบติดตามตรวจสอบการทำงานของระบบ (System Observability Platform)

(๘) พัฒนา หรือปรับปรุง ระบบบริหารจัดการและตรวจสอบความปลอดภัยของ Source Code (Version Control System and Source Code Scanning)

๖.๒.๑.๕ ดำเนินการแก้ไขปรับปรุงระบบ กรณีตรวจพบข้อผิดพลาดของระบบและกรณีตรวจพบภัยคุกคาม ช่องโหว่หรือการโจมตีต่าง ๆ เป็นระยะเวลาไม่น้อยกว่า ๑ ปี หลังจากส่งงานงวดที่ ๔ และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

๖.๒.๒ พัฒนาและปรับปรุงมาตรฐานความปลอดภัยระบบสืบค้นข้อมูลกระบวนการยุติธรรม DXC

๖.๒.๒.๑ ตรวจสอบระบบ และจัดทำ Gap Analysis ของระบบเทียบกับมาตรฐานความปลอดภัย ISO/IEC 27001:2022 ใน ๘ ประเด็น ดังนี้ A.5.7) Threat Intelligence A.5.30) ICT Readiness for business continuity A.8.9) Configuration management A.8.10) Information deletion A.8.11) Data masking A.8.12) Data leakage prevention A.8.16) Monitoring Activity A.8.28) Secure coding

๖.๒.๒.๒ ออกแบบและนำเสนอแนวคิดสถาปัตยกรรมการเชื่อมโยงข้อมูล (Conceptual Information Integration Architecture) เพื่อกำหนดแนวทางทางด้านเทคนิคของการแลกเปลี่ยนข้อมูลที่เหมาะสมจากแต่ละหน่วยงาน ให้รองรับมาตรฐานตาม ISO/IEC 27001:2022

๖.๒.๒.๓ พัฒนาระบบตามแนวคิดสถาปัตยกรรมการเชื่อมโยงข้อมูล (Conceptual Information Integration Architecture) และตั้งค่า/ปรับปรุง/จัดการ ระบบให้รองรับตามมาตรฐานตาม ISO/IEC 27001:2022 และการใช้งานในระบบศูนย์แลกเปลี่ยนข้อมูลที่มีอยู่

๖.๒.๒.๔ ปรับปรุงระบบศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรมที่เกี่ยวข้อง ให้รองรับการแสดงผลตามข้อกำหนด มาตรฐานตาม ISO/IEC 27001:2022

(๑) พัฒนาและปรับปรุงระบบเชื่อมโยงข้อมูล ที่มีอยู่และระบบโครงสร้างพื้นฐานที่เกี่ยวข้อง

(๒) ปรับปรุงระบบให้สามารถปิดบัง (Masking) ข้อมูลผลลัพธ์ที่ต้องการปกปิดในรูปแบบบางส่วน หรือ ทั้งหมด เพื่อให้ผลลัพธ์แสดงให้เห็นตามสิทธิ์ หรือ นโยบายที่กำหนดไว้

(๓) ปรับปรุงระบบให้มีการตรวจสอบ และควบคุมสิทธิ์ตามผลการตรวจสอบความปลอดภัยที่พบ

(๔) ปรับปรุงให้ระบบมีการส่งข้อมูลผ่านช่องทางเข้ารหัส

(๕) ปรับปรุงระบบเชื่อมโยงข้อมูลให้รองรับการทำงานที่ Resilience และ Redundancy โดยให้มีบริการหลายชุด เพื่อรองรับกรณีระบบชุดใดชุดหนึ่งมีปัญหา โดยรองรับการกระจายการทำงาน (Load Balancing)

(๖) ปรับปรุงระบบบริการที่เกี่ยวข้องให้รองรับการให้บริการข้อมูลการใช้งาน ไปยังฐานข้อมูลจัดเก็บประวัติการใช้งานกลาง

(๗) พัฒนา หรือปรับปรุง ระบบติดตามตรวจสอบการทำงานของระบบ (System Observability Platform)

(๘) พัฒนา หรือปรับปรุง ระบบบริหารจัดการและตรวจสอบความปลอดภัยของ Source Code (Version Control System and Source Code Scanning)

๖.๒.๒.๕ ดำเนินการแก้ไขปรับปรุงระบบ กรณีตรวจพบข้อผิดพลาดของระบบและกรณีตรวจพบภัยคุกคาม ช่องโหว่หรือการโจมตีต่าง ๆ เป็นระยะเวลาไม่น้อยกว่า ๑ ปี หลังจากส่งงานงวดที่ ๔ และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

๖.๒.๓ พัฒนาและปรับปรุงมาตรฐานความปลอดภัยระบบบริการตนเองสำหรับผู้ใช้งาน DXC (Self Service)

๖.๒.๓.๑ ตรวจสอบระบบ และจัดทำ Gap Analysis ของระบบเทียบกับมาตรฐานความปลอดภัย ISO/IEC 27001:2022 ใน ๘ ประเด็น ดังนี้ A.5.7) Threat Intelligence A.5.30) ICT Readiness for business continuity A.8.9) Configuration management A.8.10) Information deletion A.8.11) Data masking A.8.12) Data leakage prevention A.8.16) Monitoring Activity A.8.28) Secure coding

๖.๒.๓.๒ ออกแบบและนำเสนอแนวคิดสถาปัตยกรรมการเชื่อมโยงข้อมูล (Conceptual Information Integration Architecture) เพื่อกำหนดแนวทางทางด้านเทคนิคของการแลกเปลี่ยนข้อมูลที่เหมาะสมจากแต่ละหน่วยงาน ให้รองรับมาตรฐานตาม ISO/IEC 27001:2022

๖.๒.๓.๓ พัฒนาระบบตามแนวคิดสถาปัตยกรรมการเชื่อมโยงข้อมูล (Conceptual Information Integration Architecture) และตั้งค่า/ปรับปรุง/จัดการ ระบบให้รองรับตามมาตรฐานตาม ISO/IEC 27001:2022 และการใช้งานในระบบศูนย์แลกเปลี่ยนข้อมูลที่มีอยู่

๖.๒.๓.๔ ปรับปรุงระบบศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรมที่เกี่ยวข้อง ให้รองรับการแสดงผลตามข้อกำหนด มาตรฐานตาม ISO/IEC 27001:2022

(๑) พัฒนาและปรับปรุงระบบเชื่อมโยงข้อมูล ที่มีอยู่และระบบโครงสร้างพื้นฐานที่เกี่ยวข้อง

(๒) ปรับปรุงระบบให้สามารถปิดบัง (Masking) ข้อมูลผลลัพธ์ที่ต้องการปกปิดในรูปแบบบางส่วน หรือ ทั้งหมด เพื่อให้ผลลัพธ์แสดงให้เห็นตามสิทธิ์ หรือ นโยบายที่กำหนดไว้

(๓) ปรับปรุงระบบให้มีการตรวจสอบ และควบคุมสิทธิ์ตามผลการตรวจสอบความปลอดภัยที่พบ

(๔) ปรับปรุงให้ระบบมีการส่งข้อมูลผ่านช่องทางเข้ารหัส

(๕) ปรับปรุงระบบบริการตนเองสำหรับผู้ใช้งาน DXC (Self Service) ให้รองรับการทำงานที่ Resilience และ Redundancy โดยให้มีบริการหลายชุดเพื่อรองรับกรณีระบบชุดใดชุดหนึ่งมีปัญหา โดยรองรับการกระจายการทำงาน (Load Balancing)

(๖) ปรับปรุงระบบบริการที่เกี่ยวข้องให้รองรับการให้บริการข้อมูลการใช้งาน ไปยังฐานข้อมูลจัดเก็บประวัติการใช้งานกลาง

(๗) พัฒนา หรือปรับปรุง ระบบติดตามตรวจสอบการทำงานของระบบ (System Observability Platform)

(๘) พัฒนา หรือปรับปรุง ระบบบริหารจัดการและตรวจสอบความปลอดภัยของ Source Code (Version Control System and Source Code Scanning)

๖.๒.๓.๕ ดำเนินการแก้ไขปรับปรุงระบบ กรณีตรวจพบข้อผิดพลาดของระบบและกรณีตรวจพบภัยคุกคาม ช่องโหว่หรือการโจมตีต่าง ๆ เป็นระยะเวลาไม่น้อยกว่า ๑ ปี หลังจากส่งงานงวดที่ ๔ และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

๖.๒.๔ พัฒนาและปรับปรุงมาตรฐานความปลอดภัยระบบการยืนยันตัวตน (SSO Authentication)

๖.๒.๔.๑ ตรวจสอบระบบ และจัดทำ Gap Analysis ของระบบเทียบกับมาตรฐานความปลอดภัย ISO/IEC 27001:2022 ใน ๘ ประเด็น ดังนี้ A.5.7) Threat Intelligence A.5.30) ICT Readiness for business continuity A.8.9) Configuration management A.8.10) Information deletion A.8.11) Data masking A.8.12) Data leakage prevention A.8.16) Monitoring Activity A.8.28) Secure coding

๖.๒.๔.๒ ออกแบบและนำเสนอแนวคิดสถาปัตยกรรมการเชื่อมโยงข้อมูล (Conceptual Information Integration Architecture) เพื่อกำหนดแนวทางทางด้านเทคนิคของการแลกเปลี่ยนข้อมูลที่เหมาะสมจากแต่ละหน่วยงาน ให้รองรับมาตรฐานตาม ISO/IEC 27001:2022

๖.๒.๔.๓ พัฒนาระบบตามแนวคิดสถาปัตยกรรมการเชื่อมโยงข้อมูล (Conceptual Information Integration Architecture) และตั้งค่า/ปรับปรุง/จัดการ ระบบให้รองรับตามมาตรฐานตาม ISO/IEC 27001:2022 และการใช้งานในระบบศูนย์แลกเปลี่ยนข้อมูลที่มีอยู่

๖.๒.๔.๔ ปรับปรุงระบบศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรมที่เกี่ยวข้องให้รองรับการแสดงผลตามข้อกำหนด มาตรฐานตาม ISO/IEC 27001:2022

(๑) พัฒนาและปรับปรุงระบบเชื่อมโยงข้อมูล ที่มีอยู่และระบบโครงสร้างพื้นฐานที่เกี่ยวข้อง

(๒) ปรับปรุงระบบให้สามารถปิดบัง (Masking) ข้อมูลผลลัพธ์ที่ต้องการปกปิดในรูปแบบบางส่วน หรือ ทั้งหมด เพื่อให้ผลลัพธ์แสดงให้เห็นตามสิทธิ์ หรือ นโยบายที่กำหนดไว้

(๓) ปรับปรุงระบบให้มีการตรวจสอบ และควบคุมสิทธิ์ตามผลการตรวจสอบความปลอดภัยที่พบ

(๔) ปรับปรุงให้ระบบมีการส่งข้อมูลผ่านช่องทางเข้ารหัส

(๕) ปรับปรุงระบบการยืนยันตัวตน ให้รองรับการทำงานที่ Resilience และ Redundancy โดยปรับปรุงให้ บริการ Microservice API ที่เกี่ยวข้อง มีการทำงานร่วมกันมากกว่า ๑ ชุด เพื่อรองรับกรณีระบบชุดใดชุดหนึ่งมีปัญหา โดยรองรับการกระจายการทำงาน (Load Balancing)

(๖) ปรับปรุงระบบบริการที่เกี่ยวข้องให้รองรับการให้บริการข้อมูลการใช้งาน ไปยังฐานข้อมูลจัดเก็บประวัติการใช้งานกลาง

(๗) พัฒนา หรือปรับปรุง ระบบติดตามตรวจสอบการทำงานของระบบ (System Observability Platform)

(๘) พัฒนา หรือปรับปรุง ระบบบริหารจัดการและตรวจสอบความปลอดภัยของ Source Code (Version Control System and Source Code Scanning)

๖.๒.๔.๕ ดำเนินการแก้ไขปรับปรุงระบบ กรณีตรวจพบข้อผิดพลาดของระบบและกรณีตรวจพบภัยคุกคาม ช่องโหว่หรือการโจมตีต่าง ๆ เป็นระยะเวลาไม่น้อยกว่า ๑ ปี หลังจากส่งงานงวดที่ ๔ และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

๖.๒.๕ พัฒนาและปรับปรุงมาตรฐานความปลอดภัยระบบให้บริการข้อมูลผ่าน WebService (API Portal)

๖.๒.๕.๑ ตรวจสอบระบบ และจัดทำ Gap Analysis ของระบบเทียบกับมาตรฐานความปลอดภัย ISO/IEC 27001:2022 ใน ๘ ประเด็น ดังนี้ A.5.7) Threat Intelligence A.5.30) ICT Readiness for business continuity A.8.9) Configuration management A.8.10) Information deletion A.8.11) Data masking A.8.12) Data leakage prevention A.8.16) Monitoring Activity A.8.28) Secure coding

๖.๒.๕.๒ ออกแบบและนำเสนอแนวคิดสถาปัตยกรรมการเชื่อมโยงข้อมูล (Conceptual Information Integration Architecture) เพื่อกำหนดแนวทางทางด้านเทคนิคของการแลกเปลี่ยนข้อมูลที่เหมาะสมจากแต่ละหน่วยงาน ให้รองรับมาตรฐานตาม ISO/IEC 27001:2022

๖.๒.๕.๓ พัฒนาระบบตามแนวคิดสถาปัตยกรรมการเชื่อมโยงข้อมูล (Conceptual Information Integration Architecture) และตั้งค่า/ปรับปรุง/จัดการ ระบบให้รองรับตามมาตรฐานตาม ISO/IEC 27001:2022 และการใช้งานในระบบศูนย์แลกเปลี่ยนข้อมูลที่มีอยู่

๖.๒.๕.๔ ปรับปรุงระบบศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรมที่เกี่ยวข้องให้รองรับการแสดงผลตามข้อกำหนด มาตรฐานตาม ISO/IEC 27001:2022

(๑) พัฒนาและปรับปรุงระบบเชื่อมโยงข้อมูล ที่มีอยู่และระบบโครงสร้างพื้นฐานที่เกี่ยวข้อง

(๒) ปรับปรุงระบบให้สามารถปิดบัง (Masking) ข้อมูลผลลัพธ์ที่ต้องการปกปิดในรูปแบบบางส่วน หรือ ทั้งหมด เพื่อให้ผลลัพธ์แสดงให้เห็นตามสิทธิ์ หรือ นโยบายที่กำหนดไว้

(๓) ปรับปรุงระบบให้มีการตรวจสอบ และควบคุมสิทธิ์ตามผลการตรวจสอบความปลอดภัยที่พบ

(๔) ปรับปรุงให้ระบบมีการส่งข้อมูลผ่านช่องทางเข้ารหัส

(๕) ปรับปรุงระบบให้บริการข้อมูลผ่าน WebService (API Portal) ให้รองรับการทำงานที่ Resilience และ Redundancy โดยปรับปรุงให้ บริการ Microservice API ที่เกี่ยวข้อง มีการทำงานร่วมกันมากกว่า ๑ ชุด เพื่อรองรับกรณีระบบชุดใดชุดหนึ่งมีปัญหา โดยรองรับการกระจายการทำงาน (Load Balancing)

(๖) ปรับปรุงระบบบริการที่เกี่ยวข้องให้รองรับการให้บริการข้อมูลการใช้งานไปยังฐานข้อมูลจัดเก็บประวัติการใช้งานกลาง

(๗) พัฒนา หรือปรับปรุง ระบบติดตามตรวจสอบการทำงานของระบบ (System Observability Platform)

(๘) พัฒนา หรือปรับปรุง ระบบบริหารจัดการและตรวจสอบความปลอดภัยของ Source Code (Version Control System and Source Code Scanning)

๖.๒.๕.๕ ดำเนินการแก้ไขปรับปรุงระบบ กรณีตรวจพบข้อผิดพลาดของระบบและกรณีตรวจพบภัยคุกคาม ช่องโหว่หรือการโจมตีต่าง ๆ เป็นระยะเวลาไม่น้อยกว่า ๑ ปี หลังจากส่งงานงวดที่ ๔ และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

๖.๒.๖ จัดฝึกอบรมโดยจัดหาวิทยากร สถานที่พร้อมเอกสารการฝึกอบรมให้กับเจ้าหน้าที่ของหน่วยงานที่เกี่ยวข้อง ทั้งนี้ รายชื่อวิทยากรจะต้องได้รับความเห็นชอบจากสำนักงานกิจการยุติธรรมโดยผู้รับจ้างเป็นผู้รับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งสิ้น พร้อมจัดทำรายงานสรุปการจัดฝึกอบรม โดยมีการอบรมอย่างน้อย ๕ ครั้ง หัวข้อการอบรม ดังนี้

(๑) การแจ้งเตือนภัยคุกคาม อย่างน้อย ๑ ครั้ง

(๒) การควบคุมการเปลี่ยนแปลง ค่าความปลอดภัย และวิธีการแก้ค่าความปลอดภัย อย่างน้อย ๑ ครั้ง

(๓) การบริหารจัดการข้อมูลอ่อนไหว อย่างน้อย ๑ ครั้ง

(๔) การติดตามตรวจสอบการทำงานของระบบ กรณีผิดปกติ และวิธีการตรวจสอบ อย่างน้อย ๑ ครั้ง

(๕) การเขียนโปรแกรมให้ปลอดภัย อย่างน้อย ๑ ครั้ง

๗. <u>กำหนดเวลาส่งมอบงาน</u>

๑๘๐ วัน นับถัดจากวันลงนามในสัญญา

๘. <u>พื้นที่การดำเนินการ</u>

สำนักงานกิจการยุติธรรม อาคารรัฐประศาสนภักดี ชั้น ๙ ศูนย์ราชการเฉลิมพระเกียรติฯ ๘๐ พรรษา ถนนแจ้งวัฒนะ หลักสี่ กรุงเทพมหานคร และหน่วยงานที่เกี่ยวข้อง

๙. <u>หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ</u>

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สำนักงานกิจการยุติธรรมจะพิจารณาตัดสินโดยใช้เกณฑ์ราคาโดยพิจารณาจากราคารวม ตัดสินโดยใช้หลักเกณฑ์ราคาต่ำสุด หากปรากฏว่ามีผู้เสนอราคาต่ำสุดเท่ากันหลายราย จะพิจารณาราคาต่ำสุดของผู้ที่เสนอราคาในลำดับแรกเป็นผู้ชนะการยื่นข้อเสนอ

๑๐. <u>วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร</u>

๕,๕๐๐,๐๐๐.- บาท (ห้าล้านห้าแสนบาทถ้วน)

๑๑. งวดงานและการจ่ายเงิน

สำนักงานจะจ่ายค่าจ้างซึ่งได้รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงด้วยแล้วให้แก่ ผู้รับจ้าง โดยแบ่งออกเป็น ๔ งวด ดังนี้

งวดที่ ๑ ร้อยละ ๒๐ ของวงเงินตามสัญญา เมื่อผู้รับจ้างดำเนินการส่งมอบงาน ภายใน ๔๕ วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบเอกสารรูปแบบของเอกสาร (Hard Copy) จำนวน ๕ ชุด และรูปแบบของไฟล์เอกสาร (Soft Copy) ทั้งในรูปแบบของ File Word และ PDF ลงใน Flash Drive จำนวน ๒ ชุด และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว ดังรายการต่อไปนี้

๑. แผนการดำเนินงานโครงการด้านความปลอดภัยระบบ DXC ตามมาตรฐาน ISO/IEC 27001:2022 ของศูนย์ DXC ประจำปีงบประมาณ พ.ศ. ๒๕๖๗
๒. แผนประเมินความเสี่ยงการดำเนินโครงการ
๓. ข้อมูลเจ้าหน้าที่ที่เกี่ยวข้อง พร้อมหมายเลขโทรศัพท์ อีเมล์ ประวัติการศึกษา ประวัติการทำงาน ความรู้ความเชี่ยวชาญ
๔. สัญญารักษาความลับ (NDA)
๕. แนวคิดสถาปัตยกรรมการเชื่อมโยงข้อมูล (Conceptual Information Integration Architecture)

งวดที่ ๒ ร้อยละ ๔๕ ของวงเงินตามสัญญา เมื่อผู้รับจ้างดำเนินการส่งมอบงาน ภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบเอกสารรูปแบบของเอกสาร (Hard Copy) จำนวน ๕ ชุด และรูปแบบของไฟล์เอกสาร (Soft Copy) ทั้งในรูปแบบของ File Word และ PDF ลงใน Flash Drive จำนวน ๒ ชุด และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว ดังรายการต่อไปนี้

๑. การพัฒนาและปรับปรุงมาตรฐานความปลอดภัยระบบการยืนยันตัวตน (SSO Authentication) โดยจัดทำรายงานผลการดำเนินงาน ตาม TOR ข้อ ๖.๒.๔
๒. การพัฒนาและปรับปรุงมาตรฐานความปลอดภัยระบบให้บริการข้อมูลผ่าน Web Service (API Portal) โดยจัดทำรายงานผลการดำเนินงาน ตาม TOR ข้อ ๖.๒.๕

งวดที่ ๓ ร้อยละ ๓๐ ของวงเงินตามสัญญา เมื่อผู้รับจ้างดำเนินการส่งมอบงาน ภายใน ๑๕๐ วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบเอกสารรูปแบบของเอกสาร (Hard Copy) จำนวน ๕ ชุด และรูปแบบของไฟล์เอกสาร (Soft Copy) ทั้งในรูปแบบของ File Word และ PDF ลงใน Flash Drive จำนวน ๒ ชุด และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว ดังรายการต่อไปนี้

๑. การพัฒนาและปรับปรุงมาตรฐานความปลอดภัยระบบการเชื่อมโยงข้อมูลกระบวนการยุติธรรมจำนวน ๕๙ ฐานข้อมูล โดยจัดทำรายงานผลการดำเนินงาน ตาม TOR ข้อ ๖.๒.๑
๒. การพัฒนาและปรับปรุงมาตรฐานความปลอดภัยระบบสืบค้นข้อมูลกระบวนการยุติธรรม DXC โดยจัดทำรายงานผลการดำเนินงาน ตาม TOR ข้อ ๖.๒.๒
๓. ผลการจัดฝึกอบรม ตาม TOR ข้อ ๖.๒.๖

งวดที่ ๔ ร้อยละ ๕ ของวงเงินตามสัญญา เมื่อผู้รับจ้างดำเนินการส่งมอบงาน ภายใน ๑๘๐ วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบเอกสารรูปแบบของเอกสาร (Hard Copy) จำนวน ๕ ชุด และรูปแบบของไฟล์เอกสาร (Soft Copy) ทั้งในรูปแบบของ File Word และ PDF ลงใน Flash Drive จำนวน ๒ ชุด และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว ดังรายการต่อไปนี้

๑. การพัฒนาและปรับปรุงมาตรฐานความปลอดภัยระบบบริการตนเองสำหรับผู้ใช้งาน (Self Service) โดยจัดทำรายงานผลการดำเนินงาน ตาม TOR ข้อ ๖.๒.๓
๒. รายงานสรุปผลการดำเนินงานโครงการ

๑๒. อัตราค่าปรับ

๑๒.๑ กรณีที่ผู้รับจ้างนำงานที่รับจ้างไปจ้างช่วงให้ผู้อื่นทำอีกทอดหนึ่งโดยไม่ได้รับอนุญาตจากสำนักงานจะกำหนดค่าปรับสำหรับการฝ่าฝืนดังกล่าวเป็นจำนวนร้อยละ ๑๐ ของวงเงินของงานจ้างช่วงนั้น

๑๒.๒ กรณีที่ผู้รับจ้างปฏิบัติผิดสัญญาจ้างนอกเหนือจากข้อ ๑๒.๑ จะกำหนดค่าปรับเป็นรายวันในอัตราร้อยละ ๐.๑๐ ของราคาค่าจ้าง

๑๓. การรับประกันผลงาน

ผู้รับจ้างจะต้องรับประกันความชำรุดบกพร่องของระบบที่พัฒนาในโครงการนี้ และต้องรีบจัดการซ่อมแซมแก้ไขให้ใช้การได้ดีดังเดิมภายใน ๗ วัน นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง เป็นระยะเวลาไม่น้อยกว่า ๑ ปี หลังจากส่งงานงวดที่ ๔ และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

๑๔. ข้อสงวนสิทธิ์

๑๔.๑ เงินค่าจ้างสำหรับงานจ้างครั้งนี้ สำนักงานจะมีการลงนามในสัญญาหรือข้อตกลงเป็นหนังสือต่อเมื่อพระราชบัญญัติงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๗ มีผลใช้บังคับและได้รับจัดสรรงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๗ จากสำนักงบประมาณแล้ว และกรณีที่หน่วยงานของรัฐไม่ได้รับจัดสรรงบประมาณเพื่อการจัดซื้อจัดจ้างในครั้งดังกล่าว หน่วยงานของรัฐสามารถยกเลิกการจัดซื้อจัดจ้างได้

ทั้งนี้ การลงนามในสัญญาให้ปฏิบัติตามพระราชบัญญัติการจัดซื้อจัดจ้าง ฯ มาตรา ๖๖ วรรคสอง

๑๔.๒ สำนักงานกิจการยุติธรรมสงวนสิทธิ์ที่จะบอกเลิกสัญญาว่าจ้าง ในกรณีที่ผู้ว่าจ้างไม่อาจทำสัญญาจ้างตามที่ได้เจรจาตกลงหรือมีเหตุจำเป็นอื่น ๆ ที่เป็นอุปสรรคซึ่งทำให้ไม่สามารถดำเนินการจ้างได้ ให้ถือว่าเป็นอันเลิกไป ผู้รับจ้างไม่มีสิทธิ์โต้แย้งและเรียกร้องค่าเสียหายใด ๆ ทั้งสิ้น

๑๔.๓ สำนักงานกิจการยุติธรรมขอสงวนสิทธิ์ในการเปลี่ยนแปลงบุคลากรหลักตามที่ระบุไว้ในข้อเสนอทั้งนี้ เพื่อประโยชน์ของราชการเป็นสำคัญ และจะต้องดำเนินการโดยไม่มีเงื่อนไข ยกเว้นได้รับการยินยอมจากผู้ว่าจ้าง

๑๔.๔ ลิขสิทธิ์ในฐานข้อมูลและเอกสารทุกฉบับ ต้องเป็นกรรมสิทธิ์ของสำนักงานกิจการยุติธรรม และขอสงวนสิทธิ์มิให้ผู้รับจ้างนำไปใช้ในกิจกรรมอื่นโดยไม่ได้รับการยินยอมจากสำนักงานกิจการยุติธรรม