ข้อเสนอแนะมาตรฐาน



มาตรฐานการออกแบบและพัฒนาเว็บแอปพลิเคชัน สำหรับใช้อ้างอิงในการจัดทำขอบเขตของงาน และรายละเอียดคุณลักษณะเฉพาะ (ข้อกำหนด)

สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) — BDI
วันที่จัดทำ 14 สิงหาคม 2569

บทนำและวิธีใช้เอกสาร

เอกสารฉบับนี้มีวัตถุประสงค์เพื่อให้ผู้ร่างข้อกำหนดใช้สำหรับการออกแบบพัฒนา ทดสอบ ส่งมอบ และดูแลเว็บแอปพลิเคชันของหน่วยงาน โดยจัดหมวดตามลักษณะผู้ใช้และระดับขนาดของโครงการ เพื่อให้ผู้จัดทำข้อกำหนดข้อกำหนดสามารถเลือกใช้ตามความเหมาะสมที่เกี่ยวข้อง ลดความซ้ำซ้อนและกำหนดหลักฐานตรวจรับได้อย่างชัดเจน

ทั้งนี้ ผู้ร่างข้อกำหนดไม่ควรคัดลอกข้อกำหนดทั้งหมดโดยไม่พิจารณาขอบเขตและลักษณะเฉพาะของโครงการที่จะดำเนินการ ผู้ร่างข้อกำหนดควรเลือกข้อที่เกี่ยวข้อง โดยปรับคำตามบริบทของโครงการให้มีความเหมาะสมและคุ้มค่าในเชิงงบประมาณและทรัพยากรอื่น ๆ และควรพิจารณาเติมค่าปริมาณ เกณฑ์ผ่าน รูปแบบหลักฐาน และผู้อนุมัติด้วย

สถานะ	ส่วนที่ใช้	หลักการนำไปอ้างอิงใน ข้อกำหนด
ข้อบังคับ	หัวข้อ 1 และ 2	ใช้สำหรับอ้างอิงเป็นแนวปฏิบัติหลักของการพัฒนาและทดสอบระบบเว็บแอปพลิเคชันสำหรับหน่วยงานภาครัฐ
ข้อบังคับ	หัวข้อ 3 และ 4	ให้เลือกประเภทข้อกำหนดเพิ่มเติมที่ตรงกับประเภทโครงการ
ข้อบังคับ	หัวข้อ 5	ข้อกำหนดเพิ่มเติมสำหรับระบบขนาดใหญ่มูลค่าสูงหรือมีผลกระทบสูง
ข้อเสนอแนะ	หัวข้อ 6	ใช้เมื่อเหมาะสมกับบริบท งบประมาณ และความเสี่ยง เมื่อเลือกใส่ใน ข้อกำหนด แล้วให้ถือเป็นข้อผูกพันของสัญญา
ข้อเสนอแนะ	[ ]	ตามที่อ้างอิงภาคผนวก 1: รายการเอกสารอ้างอิง

หลักการตีความและการกำหนดในการตรวจรับโครงการ

- เว็บแอปพลิเคชันหมายรวมถึง โปรแกรมคอมพิวเตอร์หรือระบบงานที่สามารถเข้าถึงและใช้งานผ่านเว็บเบราว์เซอร์ โดยผู้ใช้ไม่จำเป็นต้องติดตั้งโปรแกรมหลักลงในเครื่องหรืออุปกรณ์ของตน และให้หมายความรวมถึงระบบที่ออกแบบให้รองรับการใช้งานบนอุปกรณ์เคลื่อนที่ในรูปแบบ Responsive Web Design
- การพัฒนา ข้อกำหนด ของโครงการระบบสารสนเทศ สามารถอ้างอิงมาตรฐานและแนวทางปฏิบัติในเอกสารฉบับนี้ โดยพิจารณาขอบเขต งบประมาณ ความเสี่ยง และเลือกข้อที่เกี่ยวข้องเพื่อปรับคำตามบริบทของผู้ว่าจ้างได้ตามความเหมาะสม
- โครงการขนาดใหญ่มูลค่าสูงในเอกสารนี้หมายถึงโครงการที่มีวงเงินตาม ข้อกำหนด มากกว่า 200 ล้านบาท ทั้งนี้ หน่วยงานอาจนำข้อกำหนดดังกล่าวไปใช้กับโครงการวงเงินต่ำกว่าที่มีผลกระทบสูง เป็นภารกิจสำคัญ หรือประมวลผลข้อมูลอ่อนไหวจำนวนมากได้
- ข้อกำหนดใช้หลักความเป็นกลางทางเทคโนโลยี ผู้เสนอราคาสามารถเสนอวิธีเทียบเท่าได้เมื่อแสดงผลลัพธ์ ความมั่นคงปลอดภัย การตรวจพิสูจน์ได้ และต้นทุนตลอดอายุระบบที่ไม่ด้อยกว่า
- ข้อกำหนด ต้องระบุค่าที่วัดได้และวิธีการวัดเพิ่มเติมตามบริบท เช่น จำนวนผู้ใช้พร้อมกัน, เวลาตอบสนอง, Availability, RTO/RPO, อายุ Log และ SLA ไม่ควรใช้คำว่า “เหมาะสม” โดยไม่มีเกณฑ์หรือผู้อนุมัติ
- หลักฐานประกอบการตรวจรับต้องเชื่อมโยงกับรหัสข้อกำหนดแต่ละข้อได้อย่างชัดเจน เพื่อให้ตรวจสอบย้อนกลับได้ว่าดำเนินการครบถ้วนแล้ว โดยอาจใช้เอกสารการออกแบบ รายงานผลการสแกนด้านความมั่นคงปลอดภัย รายงานทดสอบ บันทึกการอนุมัติการสาธิตการทำงาน ภาพหน้าจอ หรือไฟล์ตั้งค่าที่ตรวจสอบได้ ทั้งนี้ หลักฐานต้องอ้างอิงรุ่นของระบบ สภาพแวดล้อม และช่วงเวลาที่จัดทำให้ตรงกับรุ่นของระบบที่ส่งมอบ

- กฎหมายและมาตรฐานที่อ้างถึงให้หมายถึงฉบับที่มีผลใช้บังคับหรือฉบับล่าสุด ณ วันที่ส่งมอบ เว้นแต่ ข้อกำหนด ระบุเวอร์ชันเฉพาะเพื่อความเข้ากันได้กับระบบเดิม

หลักการกำหนดบทบาทและของผู้เกี่ยวข้องกับโครงการ

ในการนำข้อกำหนดในเอกสารฉบับนี้ไปใช้จัดทำขอบเขตของงานของผู้เกี่ยวข้องกับโครงการ ให้กำหนดบทบาทและความรับผิดชอบของผู้เกี่ยวข้องตามหลักการที่ระบุไว้ในส่วนนี้ เพื่อให้เกิดความชัดเจนในการดำเนินงาน เว้นแต่ข้อกำหนดใดจะกำหนดผู้รับผิดชอบไว้เป็นการเฉพาะ

1. **ผู้รับจ้าง** หมายถึง บุคคลธรรมดา นิติบุคคล หรือกลุ่มนิติบุคคล เช่น กิจการร่วมค้า (Joint Venture) กิจการค้าร่วม (Consortium) ที่เป็นคู่สัญญากับหน่วยงานผู้ว่าจ้าง และมีหน้าที่รับผิดชอบผูกพันตามสัญญาในการออกแบบ พัฒนา จัดหา กำหนดค่า เชื่อมต่อ ทดสอบ ติดตั้ง ส่งมอบ และจัดทำหลักฐานที่เกี่ยวข้อง รวมถึงการดำเนินการให้ระบบมีคุณลักษณะและความสามารถเป็นไปตามข้อกำหนด
2. **ผู้ว่าจ้าง** รับผิดชอบการกำหนดนโยบาย วัตถุประสงค์ ขอบเขต เจ้าของระบบ เจ้าของข้อมูล ระดับความสำคัญของบริการ เกณฑ์การยอมรับ ระดับบริการ สิทธิการเข้าถึง การอนุมัติ การยอมรับความเสี่ยง และการตรวจรับผลการดำเนินงาน เพื่อให้มั่นใจว่าระบบมีคุณลักษณะครบถ้วนตามข้อกำหนดและสามารถใช้งานได้จริง
3. **การดำเนินการร่วมกัน** ใช้กับกิจกรรมที่ต้องอาศัยข้อมูล การตัดสินใจ หรือการมีส่วนร่วมจากทั้งผู้ว่าจ้างและผู้รับจ้าง เช่น กระบวนการรวบรวมและวิเคราะห์ความต้องการ การยืนยันความต้องการ การออกแบบกระบวนงาน การทบทวนสถาปัตยกรรม การย้ายและกระทบยอดข้อมูล การทดสอบการยอมรับของผู้ใช้ การนำระบบขึ้นใช้งานจริง การซ้อมแผนตอบสนองและกู้คืนระบบ และการถ่ายทอดความรู้
4. ข้อความว่า **“ระบบต้อง”** ให้หมายถึงผู้รับจ้างต้องจัดให้ระบบมีคุณลักษณะดังกล่าวและส่งมอบหลักฐานประกอบการตรวจรับ เว้นแต่เป็นความสามารถของระบบหรือบริการกลางที่ผู้ว่าจ้างเป็นผู้จัดเตรียม
5. ข้อความว่า **“ต้องจัดให้มี”** ให้ผู้รับจ้างเป็นผู้ดำเนินการหรือจัดเตรียม เว้นแต่กิจกรรมนั้นเกี่ยวข้องกับการกำหนดนโยบาย การอนุมัติ การให้ข้อมูล หรือการตัดสินใจที่อยู่ในอำนาจของผู้ว่าจ้าง ซึ่งให้ถือเป็นความรับผิดชอบร่วมกัน
6. ในกรณีที่ผู้ว่าจ้างมีระบบหรือบริการกลางรองรับอยู่แล้ว เช่น ระบบบริหารจัดการตัวตนและสิทธิการเข้าถึงของผู้ใช้งาน (Identity Management) ระบบบันทึกเหตุการณ์ ระบบเฝ้าระวังความมั่นคงปลอดภัย ระบบสำรองข้อมูล หรือแพลตฟอร์มเชื่อมโยงข้อมูล ผู้รับจ้างรับผิดชอบการเชื่อมต่อ กำหนดค่า และทดสอบการทำงานร่วมกัน ส่วนผู้ว่าจ้างรับผิดชอบการจัดให้มีบริการกลาง การอนุมัติสิทธิ การกำหนดนโยบายที่เกี่ยวข้อง และทำงานร่วมกันกับผู้รับจ้างในการเชื่อมต่อระบบ
7. ก่อนประกาศขอบเขตของงาน ผู้ว่าจ้างต้องทบทวนข้อกำหนดที่เลือกใช้และระบุความรับผิดชอบที่แตกต่างจากหลักการข้างต้นไว้ใน ข้อกำหนด ให้ชัดเจน รวมถึงระบุผู้จัดทำ ผู้ทบทวน ผู้อนุมัติ และผู้รับรองหลักฐานในกิจกรรมสำคัญ

ทั้งนี้ โครงสร้างการบริหารโครงการของฝ่ายผู้ว่าจ้างต้องสามารถรองรับหน้าที่ที่ระบุในข้อที่ 1 รวมถึงระบุกระบวนการอนุมัติของฝ่ายผู้ว่าจ้าง เพื่อใช้ในการกำกับดูแล ให้ข้อเสนอแนะ อนุมัติผลการดำเนินงาน และตรวจรับงานของโครงการ ในขณะที่โครงสร้างการบริหารโครงการของฝ่ายผู้รับจ้างต้องรองรับหน้าที่ในข้อที่ 2 และระบุกระบวนการควบคุมงานของฝ่ายผู้รับจ้าง เพื่อใช้ในการบริหารวางแผน ดำเนินงาน ประสานงาน ส่งมอบงาน และรับผิดชอบให้ผลการดำเนินงานเป็นไปตามข้อกำหนดและสัญญา

ระบบรหัสข้อกำหนด

รหัส	ความหมาย
STD	มาตรฐาน
GDL	แนวปฏิบัติ (Guideline)
PUB	เว็บแอปพลิเคชันสำหรับภายนอก (Public-facing Application)
INT	เว็บแอปพลิเคชันสำหรับภายใน (Internal Application)
LRG	ระบบขนาดใหญ่มูลค่าสูงหรือผลกระทบสูง
OPT	ข้อเสนอแนะเพิ่มเติม
DEV	การออกแบบและพัฒนา
SEC	ความมั่นคงปลอดภัย
TEST	มาตรการทดสอบความปลอดภัย
PM	การบริหารโครงการ
HR	บุคลากร

สารบัญ

บทนำและวิธีใช้เอกสาร **2**

หลักการตีความและการกำหนดในการตรวจรับโครงการ **2**

หลักการกำหนดบทบาทและของผู้เกี่ยวข้องกับโครงการ **3**

ระบบรหัสข้อกำหนด **4**

1. มาตรฐานการพัฒนาระบบเว็บแอปพลิเคชัน **6**

2. แนวปฏิบัติสำหรับการพัฒนาระบบเว็บแอปพลิเคชัน **8**

2.1 ข้อกำหนดด้านการออกแบบและพัฒนา 8

2.2 ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยระบบ 10

2.3 มาตรการการทดสอบความปลอดภัยระบบ 11

3. แนวปฏิบัติสำหรับเว็บแอปพลิเคชันสำหรับภายนอก (Public-facing Application) ทั่วไป **14**

3.1 ข้อกำหนดด้านการออกแบบและพัฒนา 14

3.2 ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยระบบ 14

4. แนวปฏิบัติสำหรับเว็บแอปพลิเคชันสำหรับภายใน (Internal Application) ทั่วไป **16**

4.1 ข้อกำหนดด้านการออกแบบและพัฒนา 16

4.2 ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยระบบ 16

5. ข้อกำหนดเพิ่มเติมสำหรับระบบขนาดใหญ่ มูลค่าสูง หรือมีผลกระทบสูง **17**

5.1 ข้อกำหนดด้านการออกแบบและพัฒนาเพิ่มเติม 17

5.2 ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยระบบเพิ่มเติม 19

6. ข้อเสนอแนะเพิ่มเติม **20**

6.1 การบริหารโครงการขนาดใหญ่ 20

6.2 บุคลากรที่จำเป็นสำหรับโครงการขนาดใหญ่ 21

6.3 สถาปัตยกรรม การส่งมอบ และประสิทธิภาพ 23

6.4 ประสบการณ์ผู้ใช้และการปรับปรุงบริการ 23

6.5 การยกระดับความมั่นคงปลอดภัย 24

การเตรียมความพร้อมขององค์กรก่อนเริ่มโครงการ **25**

ข้อพิจารณาสำคัญสำหรับการนำไปจัดทำ ข้อกำหนด **25**

ภาคผนวก 1: รายการเอกสารอ้างอิง **26**

ภาคผนวก 2: กฎหมาย ประกาศ มาตรฐาน และแนวปฏิบัติที่เกี่ยวข้อง **27**

ภาคผนวก 3: อภิธานศัพท์ **29**

1. มาตรฐานการพัฒนาระบบเว็บแอปพลิเคชัน

การพัฒนาระบบเว็บแอปพลิเคชันต้องดำเนินการตามมาตรฐานด้านการพัฒนาซอฟต์แวร์และความมั่นคงปลอดภัยควบคู่กันตลอดวงจรชีวิตของระบบ ตั้งแต่การออกแบบ พัฒนา ทดสอบ นำขึ้นใช้งาน ไปจนถึงการบำรุงรักษา เพื่อให้ระบบมีคุณภาพ ปลอดภัย เชื่อถือได้ และสามารถตรวจสอบได้ โดยให้อ้างอิงมาตรฐานดังต่อไปนี้

กฎหมายและมาตรฐานบริการดิจิทัลภาครัฐ

STD-DEV-01 ผู้รับจ้างต้องออกแบบและพัฒนาระบบเว็บแอปพลิเคชันให้สอดคล้องกับกฎหมาย ประกาศ มาตรฐาน และข้อกำหนดที่เกี่ยวข้องของภาครัฐ ซึ่งมีผลใช้บังคับ ณ วันที่ส่งมอบ [ดังรายการตามภาคผนวก 2 ณ สิงหาคม 2569]

STD-DEV-02 ผู้รับจ้างต้องพัฒนาระบบเว็บแอปพลิเคชันโดยแสดงตัวตนของหน่วยงานผู้ว่าจ้างอย่างชัดเจนบนเว็บไซต์หรือระบบบริการ และใช้ชื่อโดเมน/ใบรับรองดิจิทัลที่หน่วยงานผู้ว่าจ้างอนุมัติ โดยจัดให้มีข้อมูลติดต่อ นโยบายความเป็นส่วนตัว เงื่อนไขการใช้งาน และช่องทางแจ้งปัญหาหรือร้องเรียนที่เข้าถึงได้ง่าย เพื่อให้ผู้ใช้สามารถตรวจสอบความน่าเชื่อถือของบริการได้

STD-DEV-03 ผู้รับจ้างต้องพัฒนาระบบเว็บแอปพลิเคชันให้สามารถรองรับผู้ให้บริการ Digital ID ที่น่าเชื่อถือและระดับความน่าเชื่อถือของการยืนยันตัวตนที่เหมาะสมกับความเสี่ยงของธุรกรรม [รายการเอกสารอ้างอิง1, 2] รวมทั้งหลีกเลี่ยงการสร้างบัญชีหรือการเก็บหลักฐานยืนยันตัวตนซ้ำโดยไม่จำเป็น และรองรับการยืนยันตัวตนหลายปัจจัย (Multi-factor Authentication) - ในกรณีที่การให้บริการบนระบบจำเป็นต้องมีการพิสูจน์หรือยืนยันตัวตนและผลการประเมินความเสี่ยงกำหนดว่าต้องทำ

มาตรฐานด้านการเข้าถึงสำหรับทุกคน

STD-DEV-04 ผู้รับจ้างต้องออกแบบระบบให้รองรับการเข้าถึงและใช้งานได้โดยคนทุกกลุ่ม ตาม Web Content Accessibility Guidelines (WCAG) 2.2 [รายการเอกสารอ้างอิง 3] ระดับ AA หรือเวอร์ชันล่าสุดที่ได้รับการรับรอง โดยอย่างน้อยต้องรองรับการใช้งานด้วยแป้นพิมพ์ โปรแกรมอ่านหน้าจอ และตัวบ่งชี้ตำแหน่งโฟกัส ทั้งนี้ ต้องไม่ต่ำกว่ามาตรฐานเว็บไซต์ภาครัฐ เวอร์ชัน 3.0 [รายการเอกสารอ้างอิง 4]

มาตรฐานด้านธรรมาภิบาลข้อมูล และการเชื่อมโยงข้อมูลผ่าน API

STD-DEV-05 สำหรับระบบที่มีการประมวลผลข้อมูลส่วนบุคคล ผู้ว่าจ้างต้องกำหนดให้มีกลไกหรือคณะกรรมการด้านธรรมาภิบาลข้อมูลที่มีอำนาจพิจารณาและอนุมัติการใช้ การเชื่อมโยง และการแลกเปลี่ยนข้อมูลได้ตามบริบทของโครงการ ผู้รับจ้างต้องจัดให้มีผู้เชี่ยวชาญด้านธรรมาภิบาลข้อมูล และที่ปรึกษาด้านกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเข้าร่วมในคณะทำงาน ทั้งนี้ บุคลากรดังกล่าวอาจเป็นบุคลากรส่วนกลางหรือคณะทำงานร่วมที่สนับสนุนหลายโครงการได้ โดยไม่จำเป็นต้องเป็นตำแหน่งเต็มเวลาประจำแต่ละโครงการ

STD-DEV-06 ผู้ว่าจ้างต้องกำหนดธรรมาภิบาลข้อมูลของระบบอย่างชัดเจน โดยระบุเจ้าของข้อมูล บริกรข้อมูล แหล่งที่มา ความหมาย รูปแบบ คุณภาพ ชั้นความลับ ระยะเวลาเก็บรักษา สิทธิการเข้าถึง และเงื่อนไขการแลกเปลี่ยนข้อมูล พร้อมจัดทำบัญชีข้อมูลและเมทาดาทาตามกรอบธรรมาภิบาลข้อมูลภาครัฐ [รายการเอกสารอ้างอิง 5] และมาตรฐานบัญชีข้อมูลภาครัฐ [รายการเอกสารอ้างอิง 6]

STD-DEV-07 ผู้รับจ้างต้องออกแบบและพัฒนาการเชื่อมโยงข้อมูลโดยใช้มาตรฐานเปิด OpenAPI [รายการเอกสารอ้างอิง 7] และรูปแบบข้อมูลที่เครื่องสามารถอ่านและประมวลผลได้ (Machine-readable Format) ทั้งนี้ API ที่พัฒนาใหม่ต้องใช้มาตรฐานการรับ-ส่งข้อมูลแบบ RESTful API หรือรูปแบบเทียบเท่า และใช้ JSON เป็นรูปแบบข้อมูลหลัก โดยอาจรองรับรูปแบบข้อมูลอื่นเพิ่มเติมได้เมื่อจำเป็นต่อการเชื่อมต่อกับระบบเดิมที่มีอยู่

STD-DEV-08 ผู้รับจ้างต้องจัดทำเอกสารสัญญาบริการ API โดยใช้ OpenAPI Specification เวอร์ชัน 3.0 ขึ้นไป หรือมาตรฐานเทียบเท่า พร้อมกำหนดรายละเอียดที่จำเป็น เช่น เวอร์ชันของ API รูปแบบการจัดการข้อผิดพลาด เงื่อนไขการเปลี่ยนแปลงเวอร์ชัน และนโยบายการยกเลิกการใช้งานเวอร์ชันเดิม

STD-DEV-09 ผู้รับจ้างต้องออกแบบและพัฒนา API โดยมีกลไกยืนยันตัวตนและให้สิทธิที่เหมาะสม อ้างอิง OAuth 2.0 [รายการเอกสารอ้างอิง 8] /OIDC [รายการเอกสารอ้างอิง 9] หรือมาตรฐานเทียบเท่า ตรวจสอบผู้ออก ผู้รับ อายุ และลายมือชื่อของโทเคน บังคับใช้ขอบเขตสิทธิ จำกัดอัตราเรียกใช้ ตรวจสอบโครงสร้างข้อมูล และป้องกันการเรียกดูทรัพยากรของผู้อื่น

มาตรฐานด้านความมั่นคงปลอดภัยของแอปพลิเคชัน

STD-SEC-01 ผู้รับจ้างต้องร่วมกับผู้ว่าจ้างในการจัดทำข้อกำหนดความปลอดภัยของแอปพลิเคชันโดยอ้างอิง OWASP Application Security Verification Standard (ASVS) [รายการเอกสารอ้างอิง 10] โดยสำหรับระบบทั่วไป สามารถใช้ ASVS Level 2 และระบบภารกิจสำคัญ ระบบผลกระทบสูง หรือประมวลผลข้อมูลอ่อนไหวมาก ให้ใช้ ASVS Level 3 รวมทั้งออกแบบให้ครอบคลุมช่องโหว่ตาม OWASP Top 10 [รายการเอกสารอ้างอิง 11] ฉบับปัจจุบัน

มาตรฐานด้านการเข้ารหัสและโปรโตคอล

STD-SEC-02 ผู้รับจ้างต้องออกแบบและพัฒนาระบบให้ข้อมูลที่รับ-ส่งระหว่างผู้ใช้ ระบบย่อย และระบบภายนอกได้รับการเข้ารหัสด้วย HTTPS/TLS [รายการเอกสารอ้างอิง 12, 13] เวอร์ชัน 1.2 ขึ้นไป หรือมาตรฐานอื่นตามที่หน่วยงานผู้ว่าจ้างกำหนด ทั้งนี้ สำหรับข้อมูลอ่อนไหว ต้องมีการเข้ารหัสทั้งในระหว่างการรับ-ส่งข้อมูลและขณะจัดเก็บข้อมูล (Encryption at Rest) พร้อมจัดให้มีกลไกการบริหารจัดการกุญแจเข้ารหัส การหมุนเวียนกุญแจ และการตรวจสอบการใช้งานกุญแจอย่างเหมาะสม นอกจากนี้ ผู้รับจ้างต้องร่วมกับผู้ว่าจ้างในการกำหนดวิธีการจัดการไฟล์สำรองข้อมูล (Backup) และไฟล์ส่งออกข้อมูล (Export) ให้มีความมั่นคงปลอดภัยและสอดคล้องกับระดับความอ่อนไหวของข้อมูล

มาตรฐานสถาปัตยกรรม Zero Trust

STD-SEC-03 ผู้รับจ้างต้องร่วมกับผู้ว่าจ้างในการกำหนดแนวทางการประยุกต์ใช้หลักการ Zero Trust และ Security and Privacy by Design โดยอ้างอิงสาระสำคัญของ NIST SP 800-207 [รายการเอกสารอ้างอิง 14] และหลักการที่ไม่ให้ความเชื่อถือแก่ผู้ใช้ระบบ หรือการเชื่อมต่อจากตำแหน่งของเครือข่ายเพียงอย่างเดียว การเข้าถึงทรัพยากรสำคัญของระบบต้องมีการตรวจสอบตัวตน สิทธิการเข้าถึง สถานะของอุปกรณ์ และบริบทที่เกี่ยวข้องอย่างเหมาะสม พร้อมทั้งออกแบบการแบ่งส่วนเครือข่าย ระบบ หรือภาระงาน เพื่อลดความเสี่ยงจากการเคลื่อนย้ายของผู้โจมตีภายในระบบ ทั้งนี้ ผู้ว่าจ้างต้องมีการทบทวนและปรับปรุงแนวทางดังกล่าวเมื่อสภาพแวดล้อมของระบบ รูปแบบการใช้งาน หรือภัยคุกคามด้านความมั่นคงปลอดภัยเปลี่ยนแปลงไป

มาตรฐานด้านการคุ้มครองข้อมูลส่วนบุคคล

STD-SEC-04 ผู้รับจ้างต้องจัดการข้อมูลส่วนบุคคลและข้อมูลอ่อนไหวตามหลักการจำกัดวัตถุประสงค์ การเก็บรวบรวมเท่าที่จำเป็น และการจำกัดระยะเวลาเก็บรักษาข้อมูล โดยต้องจัดให้มีประกาศความเป็นส่วนตัว ควบคุมการเปิดเผยข้อมูล และรองรับการใช้สิทธิของเจ้าของข้อมูลตามกฎหมาย รวมทั้งต้องปฏิบัติตามมาตรฐานการจัดระดับชั้นข้อมูลของหน่วยงานผู้ว่าจ้าง ทั้งนี้ ในกรณีที่มีการประมวลผลข้อมูลอ่อนไหวหรือมีการเชื่อมโยงข้อมูลจากหลายฐานข้อมูล ผู้รับจ้างต้องร่วมกับผู้ว่าจ้างประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลและความเสี่ยงที่เกี่ยวข้อง พร้อมดำเนินมาตรการลดความเสี่ยงให้แล้วเสร็จก่อนเปิดใช้งานระบบ โดยอ้างอิงกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศที่ออกตามกฎหมายดังกล่าว [รายการเอกสารอ้างอิง 15, 16, 17, 18]

มาตรฐานด้านการทดสอบความปลอดภัย

STD-TEST-SEC-01 ผู้รับจ้างต้องร่วมกับผู้ว่าจ้างต้องทดสอบความสอดคล้องตามระดับที่กำหนดใน STD-SEC-01 ถึง STD-SEC-04

2. แนวปฏิบัติสำหรับการพัฒนาระบบเว็บแอปพลิเคชัน

หัวข้อนี้แสดงแนวปฏิบัติในการจัดทำ ข้อกำหนด สำหรับเว็บแอปพลิเคชัน (Web Application) ทั้งในด้านการออกแบบและพัฒนารวมไปถึงการรักษาและทดสอบความมั่นคงปลอดภัย

หลักการตีความและการใช้ระบบหรือแพลตฟอร์มร่วมกัน

ในการดำเนินการตามข้อกำหนดด้านต่าง ๆ ที่ระบุไว้ในเอกสารต่อไปนี้ ผู้ว่าจ้างและผู้รับจ้างอาจพิจารณาใช้ระบบ แพลตฟอร์ม เครื่องมือ หรือบริการกลางของหน่วยงานผู้ว่าจ้างร่วมกันได้ ไม่จำเป็นต้องจัดหาระบบแยกเฉพาะสำหรับแต่ละข้อกำหนดหรือแต่ละโครงการ ทั้งนี้ ระบบหรือแพลตฟอร์มดังกล่าวต้องสามารถรองรับหน้าที่ที่เกี่ยวข้องได้ครบถ้วน เช่น Operational Monitoring, Audit Logging, Observability และ Security Monitoringรวมทั้งต้องสามารถแยกสิทธิการเข้าถึง การเก็บรักษาข้อมูล การค้นหา การแจ้งเตือน และหลักฐานประกอบการตรวจรับให้สอดคล้องกับข้อกำหนดแต่ละประเภทได้อย่างชัดเจน

2.1 ข้อกำหนดด้านการออกแบบและพัฒนา

GDL-DEV-01 ผู้ว่าจ้างและผู้รับจ้างต้องร่วมกันกำหนดโครงสร้างการบริหารงานสำหรับการพัฒนา การส่งมอบ การดำเนินงานและการบำรุงรักษาระบบให้ชัดเจน โดยต้องระบุเจ้าของบริการ เจ้าของระบบ และส่วนงานที่รับผิดชอบการดำเนินงาน พร้อมทั้งกำหนดวัตถุประสงค์ ขอบเขต ผู้ใช้เป้าหมาย กระบวนงานที่ระบบต้องรองรับ ผลลัพธ์ที่ต้องการ และตัวชี้วัดความสำเร็จของบริการไว้ในเอกสารโครงการและขอบเขตของงาน เพื่อให้การพัฒนาและการส่งมอบระบบสอดคล้องกับความต้องการใช้งานจริง และสามารถบริหารจัดการระบบต่อเนื่องได้ภายหลังเปิดใช้งาน

GDL-DEV-02 ผู้ว่าจ้างและผู้รับจ้างต้องร่วมกันจัดทำข้อกำหนดความต้องการของระบบ ที่รวมถึงความต้องการเชิงธุรกิจ (Business Requirement) ข้อกำหนดเชิงฟังก์ชั่นงาน (Functional Requirements) และข้อกำหนดที่ไม่ใช่เชิงฟังก์ชั่นงาน (Non-functional Requirements) เช่น ความพร้อมใช้งาน ประสิทธิภาพ ความสามารถรองรับผู้ใช้ ความมั่นคงปลอดภัย การเข้าถึงสำหรับทุกคน และการบำรุงรักษา โดยกำหนดเกณฑ์ยอมรับที่วัดผลได้สำหรับแต่ละข้อ และแนบรายละเอียดเชิงวิศวกรรมซอฟต์แวร์ประกอบการออกแบบระบบ รวมทั้งข้อสรุปจากคณะกรรมการร่าง ข้อกำหนด เพื่อใช้ในการประเมินความคุ้มค่าด้านงบประมาณ

GDL-DEV-03 ผู้รับจ้างและผู้รับจ้างต้องร่วมกันดำเนินงานตามวงจรการพัฒนาซอฟต์แวร์ (Software Development Life Cycle: SDLC) ที่จัดทำเป็นลายลักษณ์อักษร โดยครอบคลุมขั้นตอนการวางแผน การวิเคราะห์ความต้องการ การออกแบบ การพัฒนา การทดสอบ การติดตั้ง การส่งมอบ และการบำรุงรักษาระบบ ทั้งนี้ ผู้รับจ้างต้องเลือกวิธีการบริหารและพัฒนาโครงการให้เหมาะสมกับลักษณะของงาน เช่น Agile, V-Model, Spiral หรือรูปแบบผสมผสาน และต้องจัดให้มีกลไกที่สามารถตรวจสอบย้อนกลับได้ตั้งแต่ความต้องการของระบบ การออกแบบ โค้ดหรือองค์ประกอบของระบบ กรณีทดสอบ ผลการทดสอบ ไปจนถึงผลการตรวจรับงาน

GDL-DEV-04 ผู้รับจ้างต้องจัดให้มีกระบวนการควบคุมการกำหนดค่าและการเปลี่ยนแปลงของระบบ (Configuration Control) โดยต้องระบุรายการองค์ประกอบของระบบที่อยู่ภายใต้การควบคุม เช่น ซอร์สโค้ด ไฟล์ตั้งค่า สคริปต์ ฐานข้อมูล โครงสร้างระบบ เอกสารออกแบบ และเวอร์ชันของซอฟต์แวร์ที่เกี่ยวข้อง พร้อมกำหนดวิธีการขอเปลี่ยนแปลง การพิจารณาอนุมัติ การบันทึกประวัติการเปลี่ยนแปลง การควบคุมเวอร์ชัน และการตรวจสอบให้มั่นใจว่ารุ่นของระบบที่ติดตั้ง ทดสอบ และส่งมอบสอดคล้องกับหลักฐานประกอบการตรวจรับ ทั้งนี้ ให้ประยุกต์ใช้แนวทาง Configuration Management ตาม CMMI หรือมาตรฐานเทียบเท่า

GDL-DEV-05 ผู้รับจ้างต้องร่วมกับผู้ว่าจ้างในการออกแบบบริการโดยยึดผู้ใช้เป็นศูนย์กลาง (User-centered Design) โดยศึกษาความต้องการและข้อจำกัดของผู้ใช้จริง วิเคราะห์เส้นทางการรับบริการตั้งแต่ต้นจนจบ (User Journey) และทดสอบต้นแบบหรือส่วนสำคัญกับผู้ใช้เป้าหมายก่อนนำขึ้นใช้งานจริง

GDL-DEV-06 ผู้รับจ้างต้องจัดทำและปรับปรุงเอกสารสถาปัตยกรรมให้เป็นปัจจุบัน อย่างน้อยประกอบด้วยเอกสารออกแบบระดับสูง (High-level Design) แผนภาพส่วนประกอบและการติดตั้ง แผนภาพจุดเชื่อมต่อระบบ (Component Diagram) แผนภาพที่ใช้แสดงขั้นตอนการทำงานของระบบหรือกระบวนการทางธุรกิจ (Activity Diagram) รายการเทคโนโลยี และเหตุผลของการตัดสินใจทางสถาปัตยกรรมที่สำคัญ

GDL-DEV-07 ผู้รับจ้างต้องสำรวจความสามารถที่บริการกลางภาครัฐรองรับอยู่แล้ว และประเมินการเชื่อมต่อหรือการใช้ประโยชน์จากแพลตฟอร์มดังกล่าวก่อนการออกแบบระบบ เช่น ระบบแลกเปลี่ยนข้อมูลกลาง (Government Data Exchange: GDX) ระบบ Digital ID ระบบชำระเงิน ระบบพอร์ทัลกลาง หรือระบบแจ้งเตือน โดยบันทึกผลการประเมินและเหตุผล กรณีไม่เลือกใช้ เพื่อหลีกเลี่ยงการลงทุนซ้ำซ้อน โดยให้อ้างอิงกฎหมาย แผน มาตรฐาน และแนวปฏิบัติด้านรัฐบาลดิจิทัลที่เกี่ยวข้อง [รายการเอกสารอ้างอิง 19, 20, 21, 22, 23]

GDL-DEV-08 ผู้รับจ้างต้องจัดเก็บซอร์สโค้ด สคริปต์ฐานข้อมูล ไฟล์กำหนดค่า และเอกสารทางเทคนิคในระบบควบคุมเวอร์ชันที่ผู้ว่าจ้างสามารถเข้าถึงและตรวจสอบได้ การเปลี่ยนแปลงทุกครั้งต้องเชื่อมโยงกับคำขอหรือรายการงานที่ตรวจสอบย้อนกลับได้ และต้องผ่านการทบทวนโค้ดโดยบุคคลอื่นอย่างน้อยหนึ่งคนก่อนผนวกรวมเข้าสู่ชุดโค้ดหลักของระบบ หรือสาขาหลักในระบบควบคุมเวอร์ชัน (Main Branch) ที่ใช้เป็นฐานสำหรับการทดสอบ ติดตั้ง หรือส่งมอบระบบ

GDL-DEV-09 ผู้รับจ้างต้องจัดทำแผนการทดสอบและกรณีทดสอบล่วงหน้า โดยเสนอให้ผู้ว่าจ้างพิจารณาและอนุมัติก่อนดำเนินการทดสอบ ทั้งนี้ ต้องทดสอบอย่างน้อยในระดับ Unit Test, Integration Test, System Test และ User Acceptance Test โดยกรณีทดสอบต้องครอบคลุมเส้นทางการใช้งานปกติ กรณีข้อมูลผิดพลาด กรณีขอบเขต และการจัดการข้อผิดพลาด

GDL-DEV-10 ผู้รับจ้างต้องกำหนดและทดสอบเกณฑ์ด้านประสิทธิภาพและความจุระบบ เช่น เวลาตอบสนอง จำนวนผู้ใช้พร้อมกัน ปริมาณธุรกรรมที่รองรับได้ ขนาดข้อมูล และช่วงเวลาที่มีการใช้งานสูงสุด โดยใช้ข้อมูลประมาณการที่ผู้ว่าจ้างเห็นชอบ และต้องแสดงให้เห็นว่าระบบรองรับภาระงานตามเกณฑ์โดยไม่สูญเสียความถูกต้องของข้อมูล

GDL-DEV-11 ผู้รับจ้างต้องจัดให้มีการทดสอบอัตโนมัติ (Test Automation) สำหรับกรณีที่เหมาะสมในการดำเนินการ พร้อมจัดเก็บผลการทดสอบ หลักฐานการทดสอบ รายการข้อบกพร่อง หลักฐานการแก้ไข และผลการทดสอบซ้ำให้ตรวจสอบได้ โดยผลการทดสอบในขั้นตอนสำคัญ โดยเฉพาะ System Test และ User Acceptance Test ต้องได้รับการพิจารณาและอนุมัติจากผู้ว่าจ้างก่อนส่งมอบหรือเปิดใช้งานระบบ

GDL-DEV-12 ผู้รับจ้างต้องแยกสภาพแวดล้อมสำหรับการพัฒนาและทดสอบ (Development/Test Environment) ออกจากระบบที่ใช้งานจริง (Production Environment) ทั้งในระดับบัญชีผู้ใช้ สิทธิ เครือข่าย ข้อมูล และทรัพยากรตามความเหมาะสม โดยสำหรับโครงการขนาดใหญ่หรือระบบที่มีความสำคัญสูง ต้องจัดให้มีสภาพแวดล้อมก่อนใช้งานจริง (Staging Environment) เพื่อทดสอบความพร้อมก่อนนำขึ้น Production Environment ทั้งนี้ ห้ามใช้ข้อมูลจริงในสภาพแวดล้อมดังกล่าว เว้นแต่ได้รับอนุมัติเป็นลายลักษณ์อักษรและผ่านการทำให้เป็นนิรนามหรือการปกปิดข้อมูลอย่างเพียงพอ

GDL-DEV-13 ผู้รับจ้างต้องจัดให้มีระบบบันทึกเหตุการณ์ (Log System) และการเฝ้าระวังระบบที่เพียงพอต่อการติดตามคุณภาพบริการ การวิเคราะห์ปัญหา การตรวจสอบย้อนหลัง และการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยต้องบันทึกข้อมูลสำคัญ เช่น สถานะบริการ เวลาตอบสนอง อัตราความผิดพลาด การใช้ทรัพยากร เหตุการณ์ของธุรกรรม การเข้าใช้งาน การเปลี่ยนแปลงสิทธิหรือการตั้งค่าสำคัญ และเหตุการณ์ผิดปกติที่เกี่ยวข้องกับภัยคุกคาม ทั้งนี้ ต้องกำหนดการเก็บรักษา การป้องกันการแก้ไข การควบคุมการเข้าถึง และการส่งมอบหรือเปิดเผย Log ให้เป็นไปตามกฎหมายและนโยบายที่เกี่ยวข้อง [รายการเอกสารอ้างอิง 24, 25, 26]

GDL-DEV-14 ก่อนส่งมอบ ผู้รับจ้างต้องจัดทำและส่งมอบเอกสาร ทรัพย์สิน และหลักฐานที่เกี่ยวข้องให้สอดคล้องกับรุ่นของระบบที่ส่งมอบ โดยอย่างน้อยต้องประกอบด้วย ข้อกำหนดทางธุรกิจ (Business Requirement) เอกสารข้อกำหนดความต้องการระบบ (SRS) เอกสารสถาปัตยกรรมระบบ เอกสารออกแบบรายละเอียด เอกสารธรรมาภิบาลข้อมูล แผนรองรับปริมาณการใช้งาน แผนการทดสอบ แผนการติดตั้งและนำขึ้นระบบ (Deployment Plan) คู่มือปฏิบัติการ รายการกำหนดค่าระบบ (Configuration Items) แผนการยุติการใช้งานระบบหรือองค์ประกอบของระบบ (End-of-Life Plan) ซอร์สโค้ดและคำสั่งสร้างระบบ แบบจำลองและพจนานุกรมข้อมูล เอกสาร API คู่มือผู้ใช้และผู้ดูแลระบบ รายการบัญชีผู้ใช้และสิทธิการเข้าถึง ผลการทดสอบ และรายการข้อจำกัดที่ทราบ

GDL-DEV-15 ผู้รับจ้างต้องร่วมกับผู้ว่าจ้าง ในการกำหนดแผนบำรุงรักษาและข้อตกลงระดับการให้บริการ (SLA) ซึ่งระบุเวลาทำการ ช่องทางรับแจ้ง ระดับความรุนแรง ระยะเวลาตอบสนองและแก้ไข การสำรองอะไหล่หรือทรัพยากรที่จำเป็น การปรับปรุงเวอร์ชัน และขั้นตอนยกระดับปัญหา รวมทั้งผู้รับจ้างต้องถ่ายทอดความรู้ให้บุคลากรของผู้ว่าจ้างก่อนสิ้นสุดสัญญา

GDL-DEV-16 ข้อมูลของหน่วยงานผู้ว่าจ้างต้องสามารถส่งออกได้ในรูปแบบมาตรฐาน เปิดเผยโครงสร้างได้ และนำไปใช้ต่อกับระบบอื่นได้ และเพื่อลดความเสี่ยงจากการผูกติดกับผู้รับจ้างหรือผู้ให้บริการรายใดรายหนึ่งเกินสมควร ผู้รับจ้างต้องจัดทำแผนการย้ายระบบหรือการยุติบริการ โดยครอบคลุมการส่งคืนข้อมูล ซอร์สโค้ด เอกสารที่เกี่ยวข้อง การเพิกถอนสิทธิการเข้าถึง และการลบข้อมูลของหน่วยงานผู้ว่าจ้างออกจากระบบของผู้รับจ้างหรือผู้ให้บริการ ทั้งนี้ ในระหว่างที่สัญญาบำรุงรักษายังมีผลใช้บังคับ หากการย้ายระบบการปรับปรุงการส่งออกข้อมูล หรือการเพิ่ม API เพื่อแลกเปลี่ยนข้อมูลเป็นการดำเนินการเพื่อให้ระบบมีคุณลักษณะครบถ้วนตามข้อกำหนดเดิม ผู้รับจ้างต้องรับผิดชอบค่าใช้จ่ายดังกล่าว เว้นแต่เป็นความต้องการใหม่หรือการขยายขอบเขตงานตามสัญญา ให้ดำเนินการตามกระบวนการบริหารการเปลี่ยนแปลงและค่าใช้จ่ายที่ผู้ว่าจ้างอนุมัติเป็นลายลักษณ์อักษร

GDL-DEV-17 ผู้รับจ้างจะต้องระบุข้อกำหนดพื้นฐานของคุณภาพซอฟต์แวร์ที่ส่งมอบ และขอความเห็นชอบจากผู้ว่าจ้างเพื่อใช้ในการวัดและรายงานผล

2.2 ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยระบบ

GDL-SEC-01 ผู้รับจ้างต้องออกแบบระบบโดยควบคุมการเข้าถึงตามหลักให้สิทธิ์น้อยที่สุดและปฏิเสธเป็นค่าเริ่มต้น โดยตรวจสอบสิทธิจากฝั่งเซิร์ฟเวอร์ทุกครั้ง รวมถึงตรวจสอบความเป็นเจ้าของข้อมูลและขอบเขตหน่วยงานหรือผู้ใช้ก่อนอนุญาตให้ดู แก้ไข ดาวน์โหลด หรือดำเนินธุรกรรม

GDL-SEC-02 ผู้รับจ้างต้องออกแบบและพัฒนาระบบโดยห้ามระบุข้อมูลลับดังต่อไปนี้ใน ซอร์สโค้ด สคริปต์ (Script) ไฟล์โปรแกรมที่รันได้ (Executable File) หรือไฟล์อื่นใดที่ระบบอาจอ่านและประมวลผลเป็นคำสั่งได้ โดยข้อมูลลับดังกล่าวประกอบด้วย รหัสผ่าน, API Key, โทเคน, Connection String, กุญแจเข้ารหัส หรือข้อมูลที่เป็นความลับอื่น ทั้งนี้ ต้องใช้ระบบจัดการข้อมูลความลับที่รองรับการกำหนดสิทธิ การหมุนเวียน การยกเลิก และการบันทึกการใช้งาน

GDL-SEC-03 ในกรณีที่ผู้รับจ้างต้องออกแบบและพัฒนาการจัดเก็บรหัสผ่านด้วยฟังก์ชันแฮชที่มี Salt และสามารถตั้งค่าความเข้มแข็งของการคำนวณให้เหมาะสมกับมาตรฐานปัจจุบันได้ เช่น Argon2id, scrypt หรือ PBKDF2 ทั้งนี้ ระบบต้องรองรับรหัสผ่านที่มีความยาวเพียงพอ ไม่บังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านตามรอบเวลาโดยไม่มีเหตุจำเป็น และต้องตรวจสอบรหัสผ่านกับรายการรหัสผ่านที่เคยรั่วไหลหรือคาดเดาได้ง่าย โดยผู้ว่าจ้างต้องกำหนดนโยบายรหัสผ่านและการยืนยันตัวตนของระบบ และขอความเห็นชอบจากผู้ว่าจ้าง

GDL-SEC-04 ผู้รับจ้างต้องตั้งค่าเสริมความมั่นคงปลอดภัย (Hardening) ให้กับระบบปฏิบัติการ เว็บเซิร์ฟเวอร์ ฐานข้อมูล เฟรมเวิร์ก และบริการทั้งหมดที่เกี่ยวข้อง โดยต้องปิดบริการ บัญชี ตัวอย่าง พอร์ต หรือค่าตั้งต้นที่ไม่จำเป็น เปลี่ยนรหัสผ่านเริ่มต้น และจัดทำแผนบริหารแพตช์ที่ระบุระยะเวลา วิธีทดสอบ และขั้นตอนการติดตั้งแพตช์ให้ชัดเจน โดยผู้ว่าจ้างต้องกำหนดหรืออนุมัตินโยบายและระดับความเสี่ยงที่ยอมรับได้สำหรับการ Hardening และการติดตั้งแพตช์

GDL-SEC-05 ผู้ว่าจ้างต้องกำหนดนโยบายการยืนยันตัวตนและการควบคุมการเข้าถึงสำหรับบัญชีผู้ดูแลระบบ บัญชีสิทธิสูง การเข้าถึงจากระยะไกล และการเข้าถึงข้อมูลอ่อนไหว โดยต้องกำหนดให้มีการยืนยันตัวตนหลายปัจจัย (Multi-Facข้อกำหนด Authentication: MFA) ตามระดับความเสี่ยงของการใช้งาน และผู้รับจ้างต้องออกแบบ พัฒนา และตั้งค่าระบบให้เป็นไปตามนโยบายดังกล่าว โดยการเข้าถึงระดับผู้ดูแลระบบ (Administraข้อกำหนด) ต้องผ่านจุดคัดกรองและตรวจสอบสิทธิ์ที่กำหนดไว้ก่อนเข้าสู่ระบบภายใน เช่น Bastion Host, Privileged Access Management (PAM) หรือช่องทางเทียบเท่า ซึ่งต้องสามารถบันทึกกิจกรรม จำกัดสิทธิ จำกัดคำสั่ง หรือกำหนดระยะเวลาการใช้งานได้อย่างเหมาะสม และขอความเห็นชอบจากผู้ว่าจ้าง

GDL-SEC-06 ผู้ว่าจ้างต้องกำหนดประเภทเหตุการณ์ด้านความมั่นคงปลอดภัยที่ต้องบันทึกตามระดับความเสี่ยงของระบบ และผู้รับจ้างต้องออกแบบ ตั้งค่า และจัดเก็บบันทึกเหตุการณ์ให้ครอบคลุมอย่างน้อยการเข้าสู่ระบบทั้งที่สำเร็จและล้มเหลว การเปลี่ยนแปลงสิทธิ การดำเนินการของผู้ดูแลระบบ การเข้าถึงหรือส่งออกข้อมูลสำคัญ การเปลี่ยนแปลงการตั้งค่าระบบ และการเรียกใช้ API ที่มีความเสี่ยง ทั้งนี้ บันทึกเหตุการณ์ต้องระบุเวลาที่สามารถเทียบเคียงกันได้ ป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต และต้องไม่บันทึกรหัสผ่าน โทเคน หรือข้อมูลส่วนบุคคลเกินกว่าที่จำเป็น

GDL-SEC-07 ผู้ว่าจ้างต้องกำหนดเกณฑ์การยอมรับความเสี่ยงและระยะเวลาที่ต้องแก้ไขช่องโหว่ตามระดับความรุนแรง ส่วนผู้รับจ้างต้องจัดให้มีกระบวนการบริหารจัดการช่องโหว่ (Vulnerability Management) ข้อผิดพลาดจากการกำหนดค่าระบบ (Security

Misconfiguration) และประกาศช่องโหว่จากผู้ผลิตหรือแหล่งข้อมูลที่น่าเชื่อถืออย่างเป็นระบบ โดยครอบคลุมการตรวจพบ การประเมินและจัดลำดับความรุนแรง การแก้ไข การทดสอบซ้ำเพื่อยืนยันผล การปิดประเด็น และการจัดเก็บหลักฐานให้ตรวจสอบได้

GDL-SEC-08 ผู้รับจ้างต้องเข้ารหัสข้อมูลสำรอง (Backup Encryption) และควบคุมสิทธิการเข้าถึงข้อมูลสำรองแยกจากระบบงานหลัก

GDL-SEC-09 ผู้รับจ้างควรจัดให้มีสำเนาข้อมูลสำรองที่ไม่สามารถแก้ไขหรือลบได้โดยง่าย (Immutable Backup) หรือมาตรการเทียบเท่า เพื่อป้องกันความเสียหายจากการลบข้อมูล การโจมตีด้วยมัลแวร์เรียกค่าไถ่ หรือการเข้ารหัสข้อมูลโดยผู้โจมตี

GDL-SEC-10 ผู้รับจ้างต้องจัดทำและทดสอบแผนตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัย ครอบคลุมการเตรียมพร้อม การตรวจพบ การจำกัดผลกระทบ การกำจัดสาเหตุ การกู้คืน การสื่อสารกับผู้เกี่ยวข้อง และการทบทวนบทเรียน โดยต้องระบุช่องทางประสานงาน ผู้รับผิดชอบ อำนาจตัดสินใจ และขั้นตอนกรณีต้องหยุดหรือจำกัดบริการเพื่อควบคุมความเสี่ยง

GDL-SEC-11 ผู้รับจ้างต้องเสนอแนวปฏิบัติและการบริหารการทำงานที่เกี่ยวข้องกับสิทธิการเข้าถึงระบบ และขอความเห็นชอบจากผู้ว่าจ้าง โดยผู้รับจ้างและบุคลากรภายนอกต้องได้รับสิทธิแบบมีวันสิ้นสุด ใช้บัญชีเฉพาะบุคคล ห้ามใช้บัญชีร่วม และอยู่ภายใต้ข้อตกลงรักษาความลับ (NDA) ข้อกำหนดแจ้งเหตุ การตรวจสอบกิจกรรม และการคืนหรือลบข้อมูลเมื่อสิ้นสุดงาน

2.3 มาตรการการทดสอบความปลอดภัยระบบ

ข้อกำหนดในหัวข้อนี้ กำหนดแนวทางการทดสอบความมั่นคงปลอดภัยของระบบตลอดวงจรการพัฒนาและส่งมอบ ไม่จำกัดเฉพาะการทดสอบก่อนส่งมอบงานเท่านั้น โดยครอบคลุมการวางแผนทดสอบ การกำหนดขอบเขต การทดสอบซอร์สโค้ด ส่วนประกอบซอฟต์แวร์ ข้อมูลความลับ ค่ากำหนดระบบ โครงสร้างพื้นฐาน แอปพลิเคชัน เครือข่าย การบันทึกเหตุการณ์ การตอบสนองเหตุการณ์ และการทดสอบโดยผู้เชี่ยวชาญตามระดับความเสี่ยง ทั้งนี้ ผลการทดสอบและหลักฐานการแก้ไขต้องเชื่อมโยงกับรุ่นของระบบที่ส่งมอบและใช้เป็นเงื่อนไขประกอบการตรวจรับหรือการอนุมัติก่อนนำระบบขึ้นใช้งานจริง

GDL-TEST-01 ผู้รับจ้างต้องจัดทำแผนทดสอบความปลอดภัยก่อนเริ่มการทดสอบ โดยระบุขอบเขตการทดสอบให้ชัดเจน รวมถึงรายการ URL หรือ API ที่ต้องทดสอบ บัญชีทดสอบ ข้อมูลที่ใช้ในการทดสอบ วิธีทดสอบ เครื่องมือ ผู้รับผิดชอบ กำหนดการ ข้อจำกัด กติกาการทดสอบ ช่องทางแจ้งเหตุฉุกเฉิน และเกณฑ์การผ่านการทดสอบ ทั้งนี้ แผนดังกล่าวต้องได้รับความเห็นชอบจากหน่วยงานผู้ว่าจ้าง โดยเจ้าของระบบและผู้รับผิดชอบด้านความมั่นคงปลอดภัยก่อนดำเนินการทดสอบ

GDL-TEST-02 ผู้ว่าจ้างต้องจัดให้มีหรืออนุมัติผลการประเมินความเสี่ยงและรายการทรัพย์สินของระบบ เพื่อใช้เป็นฐานในการกำหนดขอบเขตการทดสอบความปลอดภัย และผู้รับจ้างต้องกำหนดขอบเขตการทดสอบโดยอ้างอิงผลการประเมินความเสี่ยงและรายการทรัพย์สินดังกล่าว ให้ครอบคลุมช่องทางการเข้าถึง ขอบเขตความเชื่อถือของระบบ (Trust Boundary) บทบาทผู้ใช้งาน การเชื่อมต่อกับระบบภายนอก และตรรกะธุรกิจที่มีผลกระทบสูง ทั้งนี้ การทดสอบต้องไม่จำกัดเฉพาะการสแกนหน้าเว็บ แต่ต้องครอบคลุมองค์ประกอบและเส้นทางการใช้งานที่มีความเสี่ยงสำคัญของระบบ

GDL-TEST-03 ผู้ว่าจ้างต้องกำหนดหรืออนุมัติรอบการตรวจสอบความปลอดภัยของซอร์สโค้ด และเกณฑ์การยอมรับผลการตรวจสอบก่อนนำโค้ดไปใช้งาน และผู้รับจ้างต้องดำเนินการทดสอบความปลอดภัยของซอร์สโค้ดแบบ Static Application Security Testing (SAST) กับซอร์สโค้ดที่มีการเปลี่ยนแปลงก่อนนำไปรวมกับชุดโค้ดหลัก และต้องตรวจสอบโค้ดทั้งระบบตามรอบที่กำหนด โดยต้องปรับแต่งกฎการตรวจสอบให้เหมาะสมกับภาษาและเฟรมเวิร์กที่ใช้ ตรวจสอบและคัดกรองผลบวกลวง พร้อมจัดเก็บหลักฐานรุ่นของโค้ด ผลการตรวจสอบ และผลการแก้ไขให้ตรวจสอบย้อนหลังได้

GDL-TEST-04 ผู้ว่าจ้างต้องกำหนดหรืออนุมัติเกณฑ์การยอมรับความเสี่ยงของส่วนประกอบซอฟต์แวร์ภายนอกและสถานะการสิ้นสุดการสนับสนุน และผู้รับจ้างต้องตรวจสอบส่วนประกอบซอฟต์แวร์ด้วยเครื่องมือ Software Composition Analysis (SCA) และตรวจสอบความถูกต้องของเอกสาร SBOM ทุกครั้งที่มีการสร้างรุ่นซอฟต์แวร์เพื่อส่งมอบ พร้อมติดตามช่องโหว่อย่างต่อเนื่องหลังเปิดใช้งานจริง โดยรายงานต้องครอบคลุมไลบรารีทางตรงและทางอ้อม เวอร์ชันที่ใช้ ประเภทใบอนุญาตสิทธิ์ สถานะ End-of-Life ช่องโหว่ที่พบ และแนวทางแก้ไขหรือควบคุมความเสี่ยง

GDL-TEST-05 ผู้ว่าจ้างต้องกำหนดหรืออนุมัติเกณฑ์การจัดการข้อมูลความลับที่พบในซอร์สโค้ดและผู้รับจ้างต้องใช้เครื่องมือ Secret Scanning เพื่อตรวจหาคีย์ โทเคน รหัสผ่าน และข้อมูลความลับในซอร์สโค้ด ประวัติระบบควบคุมเวอร์ชัน ไฟล์กำหนดค่า และชิ้นงานที่เกี่ยวข้อง หากพบข้อมูลความลับ ต้องเพิกถอนหรือหมุนเวียนข้อมูลดังกล่าวทันที พร้อมแก้ไขแหล่งที่มาของปัญหา ทั้งนี้ การลบข้อความออกจากโค้ดเพียงอย่างเดียวไม่ถือว่าเป็นการแก้ไขที่เพียงพอ

GDL-TEST-06 ผู้ว่าจ้างต้องกำหนดหรืออนุมัติค่ามาตรฐานอ้างอิงด้านความมั่นคงปลอดภัย (Security Baseline) สำหรับโครงสร้างพื้นฐาน ระบบคลาวด์ คอนเทนเนอร์ และไฟล์อิมเมจของระบบที่ใช้ในโครงการ และผู้รับจ้างต้องตรวจสอบค่ากำหนด (Configuration) และอิมเมจของระบบ (System Image) ด้วยเครื่องมือที่เหมาะสม เมื่อมีการใช้โครงสร้างพื้นฐานในรูปแบบโค้ด (Infrastructure as Code: IaC) คอนเทนเนอร์หรือการกำหนดค่าระบบคลาวด์ โดยต้องครอบคลุมสิทธิการเข้าถึง เครือข่าย การเข้ารหัส การเปิดเผยบริการ อิมเมจพื้นฐาน (Base Image) และแพ็กเกจที่ติดตั้ง ทั้งนี้ ต้องแก้ไขรายการที่ไม่สอดคล้องกับ Security Baseline ก่อนนำขึ้นใช้งาน

GDL-TEST-07 ผู้รับจ้างต้องดำเนินการทดสอบความปลอดภัยของแอปพลิเคชันขณะระบบทำงาน (Dynamic Application Security Testing: DAST) บนสภาพแวดล้อม Test หรือ Pre-production ที่มีลักษณะใกล้เคียงกับ Production อย่างน้อยก่อนส่งมอบซอฟต์แวร์แต่ละรุ่นหลัก (Major Build) และหลังการเปลี่ยนแปลงที่มีผลกระทบต่อเส้นทางรับข้อมูล การยืนยันตัวตน การกำหนดสิทธิ หรือการเชื่อมต่อกับระบบภายนอก

GDL-TEST-08 ผู้ว่าจ้างต้องกำหนดเกณฑ์การจัดระดับความรุนแรง และผู้รับจ้างต้องดำเนินการตรวจสอบช่องโหว่ (Vulnerability Scanning) ของแอปพลิเคชันและโครงสร้างพื้นฐานอย่างน้อยปีละ 1 ครั้ง รวมทั้งก่อนเปิดใช้งานครั้งแรก และหลังการเปลี่ยนแปลงที่มีนัยสำคัญ โดยต้องตรวจสอบผลการสแกน คัดกรองผลที่ไม่ถูกต้อง ดำเนินการแก้ไข และทดสอบซ้ำเพื่อยืนยันผล พร้อมจัดเก็บหลักฐานให้ตรวจสอบได้

GDL-TEST-09 สำหรับระบบภารกิจสำคัญหรือระบบที่มีผลกระทบสูง ผู้รับจ้างต้องจัดให้มีการทดสอบเจาะระบบแบบ Manual Penetration Testing โดยบุคคลที่สามที่เป็นอิสระ ก่อนเปิดใช้งานครั้งแรก อย่างน้อยปีละ 1 ครั้ง หรือหลังการเปลี่ยนแปลงสถาปัตยกรรมหรือกลไกความปลอดภัยที่มีนัยสำคัญ ทั้งนี้ ผู้ทดสอบต้องมีประสบการณ์หรือคุณวุฒิที่เกี่ยวข้อง ใช้วิธีการทดสอบที่เป็นมาตรฐาน ไม่มีส่วนรับผิดชอบโดยตรงต่อการพัฒนาส่วนที่ทดสอบ และต้องลงนามข้อตกลงรักษาความลับ (NDA) ก่อนเริ่มงาน โดยการทดสอบต้องครอบคลุมตรรกะธุรกิจและการใช้งานหลายบทบาท เช่น การข้ามขั้นตอน การแก้ไขค่าในคำขอ การใช้รายการซ้ำ การแข่งขันของธุรกรรม การเข้าถึงข้อมูลของผู้อื่น การยกระดับสิทธิ และการหลีกเลี่ยงข้อจำกัดของระบบ ซึ่งเป็นกรณีที่เครื่องมืออัตโนมัติอาจตรวจไม่พบ

GDL-TEST-10 ผู้ว่าจ้างต้องกำหนดหรืออนุมัติขอบเขตเครือข่าย เส้นทางการเข้าถึงที่ได้รับอนุญาต และผู้รับจ้างต้องทดสอบการตั้งค่าและขอบเขตเครือข่ายให้ครอบคลุม Web Application Firewall, Security Group, Private Endpoint, Administrative Path, Transport Layer Security (TLS), Certificate, Domain Name System (DNS) และการเปิดเผยพอร์ต เพื่อยืนยันว่าระบบเปิดให้เข้าถึงเฉพาะเส้นทางที่ได้รับอนุญาต และไม่มีบริการสำหรับผู้ดูแลระบบหรือบริการที่มีความเสี่ยงเปิดต่อสาธารณะโดยไม่จำเป็น

GDL-TEST-11 ผู้รับจ้างต้องทดสอบว่าระบบ Logging, Moniข้อกำหนดing และ Alerting สามารถตรวจจับ บันทึก และแจ้งเตือนกิจกรรมที่เกิดขึ้นระหว่างการทดสอบได้อย่างถูกต้อง โดยอย่างน้อยต้องครอบคลุมการเข้าสู่ระบบล้มเหลว การยกระดับสิทธิ การดึงข้อมูลจำนวนมาก และการเปลี่ยนแปลงค่ากำหนดสำคัญของระบบ พร้อมจัดเก็บหลักฐานผลการทดสอบให้ตรวจสอบได้

GDL-TEST-12 ผู้ว่าจ้างต้องกำหนดหรืออนุมัติแผนตอบสนองเหตุการณ์และแผนกู้คืนระบบ รวมถึงความถี่ในการทดสอบ ผู้มีอำนาจตัดสินใจ ช่องทางสื่อสาร เกณฑ์ความสำเร็จ และแนวทางเชื่อมโยงกับระบบเฝ้าระวัง เช่น SIEM, SOAR หรือระบบเทียบเท่า และในช่วงพัฒนาและก่อนส่งมอบ ผู้รับจ้างต้องทดสอบแผนดังกล่าวก่อนส่งมอบตามขอบเขตของรุ่นระบบที่ส่งมอบ โดยตรวจสอบว่าระบบสามารถส่ง Log หรือ Security Event ที่จำเป็นไปยังระบบเฝ้าระวังได้ถูกต้อง และใช้ประกอบการตรวจพบเหตุการณ์ การยกระดับ การจำกัดผลกระทบ การกู้คืน และการสื่อสารได้จริง ในช่วงรับประกันหรือบำรุงรักษา ในช่วงรับประกันหรือบำรุงรักษา ผู้รับจ้างต้องร่วมกับผู้ว่าจ้างทบทวนและทดสอบแผนตามความถี่ที่กำหนดหรือเมื่อมีการเปลี่ยนแปลงสำคัญ พร้อมกำหนดผู้รับผิดชอบ ระยะเวลาแก้ไขข้อค้นพบ และแนวทางปรับปรุงกฎแจ้งเตือนหรือ Playbook ที่เกี่ยวข้อง

GDL-TEST-13 ผู้รับจ้างต้องจัดให้สภาพแวดล้อมทดสอบแยกจาก Production และใช้ข้อมูลสังเคราะห์หรือข้อมูลที่ทำให้เป็นนิรนามในการทดสอบ หากจำเป็นต้องทดสอบบน Production ต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้ว่าจ้างก่อนดำเนินการ โดยต้องกำหนดช่วงเวลาทดสอบ ผลกระทบสูงสุดที่ยอมรับได้ แผนหยุดทดสอบ และการเฝ้าระวังอย่างใกล้ชิด

GDL-TEST-14 ผู้รับจ้างต้องจัดทำรายงานผลการทดสอบ โดยระบุระดับความรุนแรง หลักฐานประกอบ ขั้นตอนการทำซ้ำ ทรัพย์สินหรือระบบที่ได้รับผลกระทบ สาเหตุ แนวทางแก้ไข และข้อจำกัดของการทดสอบให้ครบถ้วน เพื่อให้ผู้ว่าจ้างสามารถพิจารณาความเสี่ยงและติดตามการแก้ไขได้อย่างชัดเจน

GDL-TEST-15 ผู้รับจ้างต้องแก้ไขช่องโหว่ระดับวิกฤต (Critical) หรือระดับสูง (High) ให้แล้วเสร็จก่อนนำซอฟต์แวร์รุ่นใหม่ (New Software Build) ขึ้นใช้งานจริง หากมีเหตุฉุกเฉินที่ไม่สามารถแก้ไขได้ทัน ต้องได้รับการอนุมัติยอมรับความเสี่ยง (Risk Acceptance) จากผู้มีอำนาจจากหน่วยงานผู้ว่าจ้างเป็นลายลักษณ์อักษร พร้อมกำหนดมาตรการควบคุมความเสี่ยงชั่วคราว และระยะเวลาแก้ไขให้แล้วเสร็จอย่างชัดเจน

GDL-TEST-16 ผู้รับจ้างต้องดำเนินการทดสอบซ้ำหลังการแก้ไข โดยทดสอบประเด็นเดิมและส่วนอื่นของระบบที่อาจได้รับผลกระทบจากการแก้ไข (Regression Security Testing) ทั้งนี้ ห้ามปิดข้อค้นพบจากคำยืนยันของผู้พัฒนาเพียงอย่างเดียว และต้องจัดเก็บหลักฐานผลการทดสอบก่อนแก้ไข หลังแก้ไข และผลการทดสอบซ้ำให้ตรวจสอบได้

GDL-TEST-17 ผู้รับจ้างต้องจัดให้ผลการทดสอบความปลอดภัยและหลักฐานการแก้ไขเป็นส่วนหนึ่งของ Pre-deployment Gate และเอกสารตรวจรับ โดยต้องยืนยันได้ว่ารุ่นของระบบที่นำขึ้นใช้งานตรงกับรุ่นที่ผ่านการทดสอบ ผ่านหมายเลข Build, Commit, Image Digest หรือกลไกยืนยันรุ่นที่เทียบเท่า

GDL-TEST-18 ผู้รับจ้างต้องจัดทำรายงานผลการทดสอบอย่างน้อย 2 ระดับ ได้แก่ รายงานสำหรับผู้บริหาร ซึ่งต้องสรุปขอบเขตการทดสอบ ระดับความเสี่ยง แนวโน้ม ประเด็นคงค้าง และผลกระทบต่อภารกิจ และรายงานเชิงเทคนิค ซึ่งต้องมีรายละเอียดเพียงพอให้ทีมแก้ไขและผู้ทดสอบรายอื่นสามารถทวนสอบได้ ทั้งนี้ ต้องควบคุมชั้นความลับและสิทธิการเข้าถึงรายงานให้เหมาะสมกับความอ่อนไหวของข้อมูล

GDL-TEST-19 ผู้รับจ้างต้องจัดเก็บบันทึกและหลักฐานที่เกี่ยวข้องกับการทดสอบความปลอดภัย เช่น แผนทดสอบ เครื่องมือและเวอร์ชันที่ใช้ ข้อมูลผลการทดสอบต้นฉบับ รายงานผลการทดสอบ การอนุมัติ ข้อยกเว้น หลักฐานการแก้ไข และผลการทดสอบซ้ำ (Retest) ตามระยะเวลาที่ผู้ว่าจ้างกำหนด เพื่อรองรับการตรวจประเมิน การติดตามแนวโน้ม และการสืบสวนเหตุการณ์ในอนาคต

GDL-TEST-20 ผู้รับจ้างต้องดำเนินการทดสอบซ้ำและเฝ้าระวังต่อเนื่องตามแนวทางที่กำหนดโดยผู้ว่าจ้าง รวมถึงการสแกนเมื่อมีช่องโหว่ใหม่ที่เกี่ยวข้อง การทดสอบหลังติดตั้งแพตช์สำคัญ และการทบทวนขอบเขตการทดสอบเมื่อมีการเพิ่มฟังก์ชัน ผู้ใช้งาน ข้อมูล หรือการเชื่อมต่อกับระบบใหม่

3. แนวปฏิบัติสำหรับเว็บแอปพลิเคชันสำหรับภายนอก (Public-facing Application) ทั่วไป

เว็บแอปพลิเคชันสำหรับภายนอก (Public-facing Application) หมายถึง เว็บไซต์ ระบบบริการอิเล็กทรอนิกส์ พอร์ทัล แบบคำขอออนไลน์ เว็บบนอุปกรณ์เคลื่อนที่ หรือ API ที่ประชาชน ภาคธุรกิจ หน่วยงานคู่ความร่วมมือ หรือผู้ใช้นอกเครือข่ายของหน่วยงาน สามารถเข้าถึงผ่านอินเทอร์เน็ตหรือเครือข่ายสาธารณะ ระบบประเภทนี้มีพื้นผิวการโจมตีและผลกระทบต่อความเชื่อมั่นของประชาชนสูง จึงต้องให้ความสำคัญเป็นพิเศษกับความพร้อมใช้งาน การเข้าถึงสำหรับทุกคน การคุ้มครองข้อมูล การยืนยันตัวตน และการป้องกันการโจมตีจากภายนอก การบังคับใช้ข้อกำหนดในหัวข้อ 3 เป็นข้อกำหนดขั้นต่ำสำหรับเว็บแอปพลิเคชันภายนอกทุกระบบ โดยข้อกำหนด ต้องเลือกค่าปริมาณและระดับบริการให้เหมาะกับภารกิจและความเสี่ยงของระบบ

3.1 ข้อกำหนดด้านการออกแบบและพัฒนา

PUB-DEV-01 ผู้รับจ้างต้องออกแบบส่วนติดต่อผู้ใช้โดยคำนึงถึงประสบการณ์ผู้ใช้งาน (User Experience: UX) และความเหมาะสมของส่วนติดต่อผู้ใช้ (User Interface: UI) ให้ใช้งานง่าย สอดคล้องกับกระบวนงานของผู้ใช้ ลดความซับซ้อนที่ไม่จำเป็น

PUB-DEV-02 ผู้รับจ้างต้องออกแบบสถาปัตยกรรมของระบบในลักษณะโมดูล (Modular Architecture) โดยแยกความรับผิดชอบของส่วนประกอบอย่างเหมาะสม ลดการผูกติดระหว่างโมดูล และรองรับการบำรุงรักษาหรือขยายระบบโดยไม่กระทบต่อโมดูลอื่นที่ไม่เกี่ยวข้องโดยตรงเกินสมควร สำหรับระบบที่ต้องรองรับการขยายตัวตามปริมาณการใช้งาน ผู้รับจ้างต้องออกแบบให้แยกสถานะและข้อมูลถาวรออกจากตัวประมวลผลของแอปพลิเคชัน เพื่อให้สามารถขยายบริการได้อย่างเหมาะสม

PUB-DEV-03 ผู้รับจ้างต้องออกแบบส่วนติดต่อผู้ใช้ที่รองรับการแสดงผลแบบตอบสนองต่อขนาดหน้าจอ (Responsive Web Design) ทั้งนี้ ระบบต้องทำงานได้บนเว็บเบราว์เซอร์ที่ใช้งานแพร่หลายโดยทั่วไปและอุปกรณ์ที่ผู้ว่าจ้างกำหนด โดยผู้รับจ้างต้องจัดทำรายการรุ่นที่รองรับและผลการทดสอบความเข้ากันได้ก่อนส่งมอบ

PUB-DEV-04 ผู้รับจ้างต้องออกแบบระบบโดยประยุกต์ใช้หลักการให้ข้อมูลแก่ภาครัฐเพียงครั้งเดียว (Once-only Principle) เท่าที่กฎหมาย สิทธิการเข้าถึงข้อมูล และความพร้อมของแหล่งข้อมูลอนุญาต [20, 21] โดยระบบต้องสามารถตรวจสอบและเรียกใช้ข้อมูลจากแหล่งข้อมูลภาครัฐที่เชื่อถือได้ [21, 23] เพื่อลดการขอเอกสารหรือข้อมูลซ้ำจากประชาชน ทั้งนี้ ต้องแจ้งให้ผู้ใช้ทราบอย่างเหมาะสมเมื่อมีการนำข้อมูลจากหน่วยงานอื่นมาใช้

PUB-DEV-05 ผู้ว่าจ้างต้องกำหนดหรืออนุมัตินโยบายและขั้นตอนการเผยแพร่ข้อมูลสู่สาธารณะ รวมถึงประเภทข้อมูลที่ห้ามเผยแพร่และผู้มีอำนาจอนุมัติการเผยแพร่ ผู้รับจ้างต้องออกแบบระบบที่เผยแพร่เนื้อหาสู่สาธารณะให้มีมาตรการป้องกันการเผยแพร่ข้อมูลส่วนบุคคล ข้อมูลลับ หรือข้อมูลที่ยังไม่ได้รับอนุมัติให้เผยแพร่ เช่น การกำหนดสิทธิผู้ใช้งาน ขั้นตอนตรวจทานและอนุมัติเนื้อหา การแจ้งเตือนก่อนเผยแพร่ และการบันทึกประวัติการเผยแพร่ เพื่อให้สามารถตรวจสอบย้อนหลังได้ [15, 16, 17]

3.2 ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยระบบ

PUB-SEC-01 ผู้รับจ้างต้องจัดให้บัญชีผู้ดูแลระบบ บัญชีที่มีสิทธิสูง และบัญชีที่สามารถเข้าถึงข้อมูลอ่อนไหวใช้การยืนยันตัวตนหลายปัจจัย (Multi-facข้อกำหนด Authentication: MFA) การมอบและเพิกถอนสิทธิต้องผ่านการอนุมัติ มีอายุสิทธิตามความจำเป็น และได้รับการทบทวนเป็นระยะตามระดับความเสี่ยงตามกรอบเวลาที่ผู้ว่าจ้างกำหนด

PUB-SEC-02 ผู้รับจ้างต้องออกแบบและพัฒนาระบบให้จัดการเซสชันอย่างปลอดภัย โดยใช้คุกกี้ที่กำหนดค่า Secure, HttpOnly และ SameSite ตามความเหมาะสม มีการหมดอายุของเซสชันเมื่อไม่มีการใช้งาน เพิกถอนเซสชันเมื่อผู้ใช้ออกจากระบบหรือมีการเปลี่ยนแปลงสิทธิ ป้องกันการโจมตีแบบ Cross-Site Request Forgery (CSRF) และไม่เปิดเผยโทเคนหรือข้อมูลลับผ่าน URL บันทึกเหตุการณ์ หรือพื้นที่จัดเก็บที่สคริปต์ฝั่งผู้ใช้เข้าถึงได้โดยไม่จำเป็น

PUB-SEC-03 ผู้รับจ้างต้องออกแบบและพัฒนาระบบให้ตรวจสอบข้อมูลนำเข้าจากผู้ใช้ ไฟล์ และระบบภายนอก ณ ฝั่งเซิร์ฟเวอร์ โดยตรวจสอบชนิดข้อมูล รูปแบบ ขนาด ช่วงค่า และรายการที่อนุญาต ข้อมูลที่แสดงผลต้องผ่านการเข้ารหัสหรือทำให้ปลอดภัยตามบริบท และการเข้าถึงฐานข้อมูลต้องใช้คำสั่งแบบมีพารามิเตอร์หรือกลไกที่เทียบเท่า เพื่อป้องกันการโจมตี เช่น Injection, Cross-Site Scripting (XSS), Path Traversal, Server-Side Request Forgery (SSRF) และการโจมตีที่เกี่ยวข้อง

PUB-SEC-04 ผู้รับจ้างต้องออกแบบและพัฒนาฟังก์ชันอัปโหลดไฟล์ให้มีการจำกัดชนิดและขนาดไฟล์ ตรวจสอบเนื้อหาไฟล์ตามความเหมาะสม เปลี่ยนชื่อไฟล์หรือจัดเก็บด้วยชื่อที่ระบบกำหนด สแกนมัลแวร์ และควบคุมสิทธิการดาวน์โหลด ทั้งนี้ ห้ามอาศัยเพียงนามสกุลไฟล์หรือค่า Content-Type ที่ได้รับจากผู้ใช้ในการตัดสินว่าไฟล์นั้นปลอดภัยหรือได้รับอนุญาต

PUB-SEC-05 ผู้รับจ้างต้องจัดให้ระบบที่เปิดให้เข้าถึงจากอินเทอร์เน็ตมี Web Application Firewall (WAF) และมาตรการป้องกันหรือบรรเทาการโจมตีแบบ Distributed Denial of Service (DDoS) ที่เหมาะสมกับปริมาณการใช้งานและความสำคัญของบริการ พร้อมกำหนดผู้รับผิดชอบในการปรับแต่งกฎ เฝ้าระวังเหตุการณ์ และทบทวนประสิทธิผลของมาตรการอย่างสม่ำเสมอ

PUB-SEC-06 ผู้รับจ้างต้องตั้งค่าความปลอดภัยของเว็บเซิร์ฟเวอร์และเบราว์เซอร์อย่างเหมาะสม เช่น HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), X-Content-Type-Options, Referrer-Policy และข้อจำกัดการฝังหน้าเว็บ โดยต้องกำหนดค่าให้เหมาะสมกับสถาปัตยกรรมของระบบและทดสอบว่าไม่กระทบต่อการให้บริการ ทั้งนี้ ต้องปิดหรือปรับแต่งหน้าแสดงข้อผิดพลาดและข้อมูลเวอร์ชันไม่ให้เปิดเผยรายละเอียดภายในเกินจำเป็น

4. แนวปฏิบัติสำหรับเว็บแอปพลิเคชันสำหรับภายใน (Internal Application) ทั่วไป

เว็บแอปพลิเคชันสำหรับภายใน (Internal Application) หมายถึง ระบบที่ใช้สนับสนุนการปฏิบัติงานของเจ้าหน้าที่ของหน่วยงานผู้ว่าจ้าง ผู้รับจ้าง หรือหน่วยงานคู่เชื่อมโยงที่ได้รับอนุญาต และไม่ได้มีวัตถุประสงค์ให้ประชาชนทั่วไปเข้าถึง เช่น ระบบสารบรรณ ระบบบุคลากร ระบบการเงิน ระบบวิเคราะห์ข้อมูล ระบบบริหารงานคดี หรือพอร์ทัลเจ้าหน้าที่ แม้ระบบจะอยู่หลังเครือข่ายภายใน ระบบประเภทนี้ต้องไม่ถือว่าปลอดภัยโดยอัตโนมัติจากตำแหน่งเครือข่าย แต่ต้องควบคุมตัวตน สิทธิ อุปกรณ์ ข้อมูล และการตรวจสอบย้อนหลังตามหลัก Zero Trust การบังคับใช้ข้อกำหนดในหัวข้อ 4 เป็นข้อกำหนดขั้นต่ำสำหรับเว็บแอปพลิเคชันภายในทุกระบบ รวมถึงระบบที่เปิดให้เจ้าหน้าที่เข้าถึงจากระยะไกลผ่านช่องทางที่หน่วยงานควบคุม

4.1 ข้อกำหนดด้านการออกแบบและพัฒนา

INT-DEV-01 ผู้รับจ้างต้องวิเคราะห์และปรับปรุงกระบวนงานก่อนพัฒนาระบบ (Process Re-engineering) โดยจัดทำแผนภาพกระบวนงานปัจจุบันและกระบวนงานที่ปรับปรุงแล้ว (Workflow) ให้แสดงลำดับการดำเนินการ กฎทางธุรกิจ ลำดับการอนุมัติ การส่งกลับ การมอบหมายแทน และการยกเลิกอย่างชัดเจน รวมถึงเอกสารหรือข้อมูลที่ต้องจัดเก็บ เพื่อป้องกันไม่ให้ระบบเป็นเพียงการถ่ายโอนขั้นตอนที่ซ้ำซ้อนจากกระดาษไปเป็นดิจิทัล ทั้งนี้ ระบบต้องสามารถบันทึกผู้ดำเนินการ วันเวลา เหตุผล และสถานะก่อนและหลังการดำเนินการ เพื่อใช้เป็นหลักฐานและตรวจสอบย้อนหลังได้

INT-DEV-02 ผู้รับจ้างต้องออกแบบและพัฒนาระบบให้เชื่อมต่อกับระบบบริหารตัวตนขององค์กรหรือระบบ Single Sign-on ที่ผู้ว่าจ้างกำหนด เมื่อมีระบบดังกล่าวใช้งานอยู่ และต้องออกแบบบทบาทผู้ใช้ให้สอดคล้องกับโครงสร้างงาน การมอบหมายหน้าที่ และหลักแบ่งแยกหน้าที่ (Segregation of Duties) ทั้งนี้ ต้องหลีกเลี่ยงการสร้างฐานบัญชีผู้ใช้แยกต่างหากโดยไม่จำเป็น

INT-DEV-03 ผู้รับจ้างต้องออกแบบสถาปัตยกรรมของระบบให้เป็นแบบโมดูล โดยแยกส่วนติดต่อผู้ใช้ ตรรกะทางธุรกิจ การเชื่อมต่อกับระบบอื่น และชั้นข้อมูลอย่างเหมาะสมตามแนวทาง 3-tier Architecture หรือแนวทางที่เทียบเท่า ทั้งนี้ ต้องลดการผูกติดระหว่างส่วนประกอบ เพื่อให้สามารถปรับปรุง ขยาย หรือเปลี่ยนเทคโนโลยีบางส่วนได้โดยไม่จำเป็นต้องแก้ไขระบบทั้งหมด

4.2 ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยระบบ

INT-SEC-01 ผู้รับจ้างต้องออกแบบให้ Application Layer, Database Layer และบริการภายในที่ไม่จำเป็นต้องเปิดต่อสาธารณะอยู่ในเครือข่ายส่วนตัวหรือเขตเครือข่ายที่มีการควบคุม โดยห้ามผูก Public IP ให้กับฐานข้อมูลหรือบริการจัดเก็บข้อมูล ทั้งนี้ ต้องเปิดเส้นทางการเชื่อมต่อเฉพาะต้นทาง ปลายทาง และพอร์ตที่จำเป็นตามหลัก Deny by Default

INT-SEC-02 ผู้รับจ้างต้องออกแบบและตั้งค่าการเข้าถึงจากภายนอกสถานที่หรือภายนอกเครือข่ายของหน่วยงานให้ผ่านช่องทางที่ผู้ว่าจ้างควบคุม เช่น VPN, Zero Trust Network Access, Private Endpoint หรือวงจรสื่อสารส่วนตัว พร้อมใช้การยืนยันตัวตนหลายปัจจัย (MFA) และบันทึกการเชื่อมต่ออย่างครบถ้วน ทั้งนี้ ห้ามเปิดพอร์ตสำหรับบริหารระบบจากอินเทอร์เน็ตโดยตรง

INT-SEC-03 ผู้รับจ้างต้องออกแบบและพัฒนาระบบให้รองรับการบริหารตัวตนและสิทธิจากศูนย์กลาง โดยใช้การควบคุมสิทธิแบบ Role-based Access Control (RBAC) หรือ Attribute-based Access Control (ABAC) ตามความเหมาะสม ให้สิทธิเท่าที่จำเป็นตามหน้าที่ แยกบทบาทที่ขัดกัน และกำหนดกระบวนการอนุมัติ ทบทวน เปลี่ยนแปลง และเพิกถอนสิทธิเมื่อมีการย้ายงาน ลาออก หรือสิ้นสุดสัญญา

INT-SEC-04 ผู้รับจ้างต้องออกแบบหรือกำหนดเงื่อนไขการเข้าถึงระบบสำคัญให้รองรับการบังคับใช้นโยบายของผู้ว่าจ้างกับเครื่องผู้ใช้และเครื่องผู้ดูแลระบบ เช่น การอัปเดตแพตช์ การป้องกันมัลแวร์ การเข้ารหัสดิสก์ การล็อกหน้าจอ และการตรวจสภาพอุปกรณ์ก่อนอนุญาตให้เข้าถึงตามระดับความเสี่ยง

5. ข้อกำหนดเพิ่มเติมสำหรับระบบขนาดใหญ่ มูลค่าสูง หรือมีผลกระทบสูง

หัวข้อ 5 ใช้เป็นข้อกำหนดเพิ่มเติมสำหรับเว็บแอปพลิเคชันขนาดใหญ่ มูลค่าสูง หรือมีผลกระทบสูง ไม่ว่าจะเป็นเว็บแอปพลิเคชันสำหรับภายนอกหรือเว็บแอปพลิเคชันสำหรับภายใน โดยโครงการต้องปฏิบัติตามข้อกำหนดสำหรับระบบทั่วไปตามประเภทของระบบในหัวข้อ 3 หรือหัวข้อ 4 แล้วแต่กรณี และเลือกปฏิบัติตามข้อกำหนดในหัวข้อ 5 เพิ่มเติม โดยพิจารณาให้ใช้กับทรัพยากรที่อยู่ภายใต้การควบคุมของโครงการ และให้สามารถใช้บริการกลางของหน่วยงานหรือกลไกที่มีผลลัพธ์เทียบเท่าได้ โดยไม่จำเป็นต้องจัดซื้อระบบใหม่แยกเฉพาะโครงการ **ทั้งนี้ หน่วยงานอาจนำข้อกำหนดในหัวข้อนี้ไปใช้กับโครงการวงเงินไม่เกิน 200 ล้านบาทที่เป็นระบบภารกิจสำคัญ มีผลกระทบสูง หรือประมวลผลข้อมูลอ่อนไหวจำนวนมากได้**

5.1 ข้อกำหนดด้านการออกแบบและพัฒนาเพิ่มเติม

LRG-DEV-01 ผู้รับจ้างต้องจัดให้กระบวนการ CI/CD ครอบคลุมการควบคุมและบริหารจัดการส่วนประกอบซอฟต์แวร์หลัก การลงลายมือชื่อดิจิทัล การตรวจสอบความถูกต้องของส่วนประกอบซอฟต์แวร์ (Integrity Verification) การอนุมัติตามบทบาทและสิทธิที่กำหนด (Role-based Approval) และการแบ่งแยกหน้าที่ระหว่างการพัฒนาซอฟต์แวร์กับการนำซอฟต์แวร์ขึ้นใช้งาน ทั้งนี้ ต้องสามารถย้อนกลับไปใช้ซอฟต์แวร์รุ่นก่อนหน้าได้ (Rollback) เมื่อเกิดปัญหาหรือไม่ผ่านเกณฑ์ที่กำหนด

LRG-DEV-02 ผู้รับจ้างต้องจัดทำแบบจำลองความจุและการเติบโตของระบบ (Capacity and Growth Model) ให้ครอบคลุมอย่างน้อยตลอดอายุสัญญาหรือตามระยะเวลาที่ผู้ว่าจ้างกำหนด โดยพิจารณาจำนวนผู้ใช้ ปริมาณธุรกรรม พื้นที่จัดเก็บข้อมูล แบนด์วิดท์ งานประมวลผลตามรอบ (Batch Processing) รายงานขนาดใหญ่ การเชื่อมต่อกับระบบอื่น ภาระงานสูงสุดที่คาดการณ์ และส่วนเผื่อสำหรับการเติบโต พร้อมกำหนดจุดที่ต้องขยายระบบ ต้นทุนที่คาดการณ์ และทดสอบระบบภายใต้ภาระงานสูงสุดดังกล่าวก่อนนำขึ้นใช้งานจริง

LRG-DEV-03 ผู้รับจ้างต้องออกแบบองค์ประกอบสำคัญของระบบไม่ให้มีจุดล้มเหลวเพียงจุดเดียว (Single Point of Failure: SPOF) และรองรับความพร้อมใช้งานสูง (High Availability: HA) โดยใช้กลไกบริหารและกระจายภาระงาน (Load Balancing) การทำงานข้ามโซนความพร้อมใช้งานหรือศูนย์ข้อมูล และการปรับขนาดระบบตามภาระงานโดยอัตโนมัติหรือกลไกที่ให้ผลเทียบเท่า ทั้งนี้ ต้องดำเนินการทดสอบการสลับการทำงาน (Failover) เพื่อยืนยันว่าบริการยังคงดำเนินต่อไปได้เมื่อองค์ประกอบสำคัญขัดข้อง

LRG-DEV-04 ผู้รับจ้างต้องร่วมกับผู้ว่าจ้างกำกับและทบทวนสถาปัตยกรรมโซลูชัน (Solution Architecture Governance) ให้สอดคล้องกับสถาปัตยกรรมองค์กร มาตรฐานข้อมูล ระบบบริหารตัวตน เครือข่าย การเชื่อมต่อระบบ และแพลตฟอร์มกลางของหน่วยงาน ก่อนอนุมัติแบบรายละเอียดและเมื่อมีการเปลี่ยนแปลงสำคัญ โดยสถาปัตยกรรมต้องแยกส่วนประกอบ ส่วนประมวลผล ข้อมูล สถานะของระบบ และบริการสนับสนุนออกจากกันอย่างเหมาะสม เพื่อรองรับการขยายระบบ การบำรุงรักษา และการจำกัดผลกระทบจากความล้มเหลว ทั้งนี้ การเลือกใช้ Microservices, Event-driven Architecture หรือ Serverless Architecture ต้องมีเหตุผลรองรับ และต้องคุ้มค่ากับความซับซ้อนและต้นทุนที่เพิ่มขึ้น

LRG-DEV-05 ผู้รับจ้างต้องจัดเตรียมและบริหารโครงสร้างพื้นฐาน รวมถึงค่ากำหนดของระบบ ต้องดำเนินการด้วยโครงสร้างพื้นฐานในรูปแบบโค้ด (Infrastructure as Code: IaC) หรือกลไกอัตโนมัติที่ควบคุมเวอร์ชัน ตรวจสอบย้อนกลับ และทดสอบได้ พร้อมกระบวนการอนุมัติ การตรวจจับความคลาดเคลื่อนระหว่างค่ากำหนดที่ใช้งานจริงกับค่าที่กำหนดไว้ (Configuration Drift Detection) และการย้อนกลับเมื่อเกิดข้อผิดพลาด (Rollback) โดยห้ามปรับแก้สภาพแวดล้อมใช้งานจริงโดยตรงโดยไม่มีบันทึกและการอนุมัติผ่านกระบวนการบริหารการเปลี่ยนแปลง

LRG-DEV-06 ผู้รับจ้างต้องแยกขอบเขตด้านการบริหารจัดการ ความมั่นคงปลอดภัย และผลกระทบจากความขัดข้องระหว่างสภาพแวดล้อมใช้งานจริง (Production) สภาพแวดล้อมที่ไม่ใช่ระบบใช้งานจริง (Non-production) ระบบด้านความมั่นคงปลอดภัย (Security) ระบบบันทึกเหตุการณ์ (Logging) และระบบเครือข่าย (Network) อย่างชัดเจน โดยใช้สถาปัตยกรรมแบบหลายบัญชี (Multi-account Architecture) โครงสร้างพื้นฐานแบบแลนดิ้งโซน (Landing Zone) หรือโครงสร้างเทียบเท่าที่สามารถบังคับใช้นโยบาย ควบคุมสิทธิ และตรวจสอบจากศูนย์กลางได้

LRG-DEV-07 ผู้รับจ้างต้องจัดให้มีสภาพแวดล้อมก่อนใช้งานจริง (Staging/Pre-production Environment) ที่มีองค์ประกอบโครงสร้าง และค่ากำหนดใกล้เคียงกับระบบใช้งานจริงเพียงพอสำหรับการทดสอบการเชื่อมต่อ ประสิทธิภาพ ความมั่นคงปลอดภัย การย้ายข้อมูล การติดตั้งแพตช์ และการซ้อมนำระบบขึ้นใช้งานจริง (Cutover Rehearsal) โดยค่ากำหนดของสภาพแวดล้อมดังกล่าวและระบบใช้งานจริงต้องสร้างจากแหล่งอ้างอิงเดียวกันเท่าที่เหมาะสม และต้องใช้ข้อมูลสังเคราะห์หรือข้อมูลที่ผ่านการปกปิดหรือทำให้เป็นนิรนามแล้ว

LRG-DEV-08 เมื่อระบบมีบริการย่อยหรือส่วนต่อประสานโปรแกรมประยุกต์ (API) จำนวนมาก หรือเปิดให้หลายหน่วยงานและภาคส่วนใช้งาน ผู้รับจ้างต้องจัดให้มีระบบบริหารจัดการ API แบบรวมศูนย์ (Centralized API Management) หรือกลไกที่เทียบเท่า พร้อมจัดทำบัญชีรายการบริการ (Service Catalog) ที่ผู้ว่าจ้างสามารถเข้าถึง ตรวจสอบ และปรับปรุงให้เป็นปัจจุบันได้

LRG-DEV-09 ผู้รับจ้างต้องจัดให้มีระบบสังเกตการณ์แบบรวมศูนย์ (Centralized Observability) ที่สามารถเชื่อมโยงข้อมูลบันทึกเหตุการณ์ (Logs) ตัวชี้วัดการทำงานของระบบ (Metrics) และข้อมูลเส้นทางการประมวลผลของคำขอ (Traces) ข้ามส่วนประกอบและข้ามระบบได้ พร้อมกำหนด Service Level Indicator(SLI) และ Service Level Objective (SLO) สำหรับบริการสำคัญ ระบบดังกล่าวต้องมี Dashboard, Alerting และ Runbook ที่ผู้ว่าจ้างสามารถเข้าถึงได้ เพื่อให้ทีมปฏิบัติการประเมินผลกระทบต่อผู้ใช้งาน วิเคราะห์สาเหตุของปัญหา และกู้คืนบริการได้ตาม Service Level Agreement (SLA)

LRG-DEV-10 ผู้รับจ้างต้องจัดทำสถาปัตยกรรมเพื่อรองรับความต่อเนื่องในการให้บริการและการกู้คืนระบบ (Disaster Recovery System) โดยอ้างอิงผล Business Impact Analysis - BIA และกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ (Recovery Time Objective: RTO) และจุดเป้าหมายในการกู้คืนข้อมูล (Recovery Point Objective: RPO) สำหรับแต่ละบริการและชุดข้อมูล ทั้งนี้ ต้องออกแบบสถานที่สำรอง (Disaster Recovery Site) ให้เหมาะสมกับระดับความจำเป็น ความสำคัญ และผลกระทบของระบบ

LRG-DEV-11 กรณีมีการย้ายข้อมูล รวมข้อมูล หรือทดแทนระบบเดิม ผู้รับจ้างต้องจัดทำแผนย้ายข้อมูลให้ครอบคลุมการทำความสะอาดข้อมูล (Data Cleansing) การแมปและแปลงข้อมูล (Data Mapping and Transformation) การตรวจสอบคุณภาพ การกระทบยอดข้อมูล (Data Reconciliation) การจัดการข้อมูลตกค้าง การเก็บรักษาประวัติที่กฎหมายกำหนด การทดลองย้ายข้อมูล และการตรวจสอบความครบถ้วนของข้อมูลก่อนและหลังการย้าย ทั้งนี้ แผนดังกล่าวต้องกำหนดแผนหยุดระบบ แผนย้อนกลับ เกณฑ์ยอมรับ ผู้รับผิดชอบ และหลักฐานการตรวจสอบให้ชัดเจน โดยผู้ว่าจ้างต้องรับรองผลการย้ายและความครบถ้วนของข้อมูลก่อนนำระบบขึ้นใช้งานจริง

LRG-DEV-12 ผู้ว่าจ้างต้องจัดทำแผนหลีกเลี่ยงการผูกติดกับผู้ขาย (Vendor Lock-in Mitigation Plan) และแผนยุติหรือเปลี่ยนผู้ให้บริการ (Exit Plan) ให้ครอบคลุมรูปแบบการส่งออกข้อมูล มาตรฐานอินเทอร์เฟซ สิทธิในซอร์สโค้ดและชิ้นงาน สคริปต์โครงสร้างพื้นฐาน ใบอนุญาต เอกสาร API เอกสารทางเทคนิค และองค์ความรู้ที่จำเป็นต่อการโอนย้ายไปยังผู้ให้บริการหรือแพลตฟอร์มอื่น ทั้งนี้ ต้องกำหนดแนวทางคงบริการระหว่างการเปลี่ยนผ่าน การถ่ายทอดความรู้ และค่าใช้จ่ายที่เกี่ยวข้องให้ชัดเจน

LRG-DEV-13 ผู้รับจ้างต้องจัดทำแผนวงจรชีวิตเทคโนโลยี (Technology Lifecycle Plan) โดยระบุรุ่นที่ใช้ วันที่สิ้นสุดการสนับสนุน เส้นทางการอัปเกรด ความเข้ากันได้ขององค์ประกอบ และแผนเปลี่ยนทดแทนเทคโนโลยีที่หมดหรือใกล้สิ้นสุดการสนับสนุน กรณีมีระบบเดิม ผู้รับจ้างต้องจัดทำแผนเปลี่ยนผ่านและยุติระบบเดิมให้ครอบคลุมการทำงานคู่ขนาน การเก็บรักษาประวัติ การปิดการเชื่อมต่อ การย้ายผู้ใช้งาน การลดภาระการดูแลรักษา การยุติระบบเดิม ผู้รับผิดชอบ และกำหนดเวลา ทั้งนี้ ห้ามออกแบบให้ระบบพึ่งพาเทคโนโลยีที่ใกล้สิ้นสุดการสนับสนุนโดยไม่มีแผนเปลี่ยนทดแทนที่ได้รับอนุมัติจากผู้ว่าจ้าง

LRG-DEV-14 ผู้รับจ้างต้องจัดทำแผนสำรองและกู้คืนข้อมูล กำหนด Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) ตามความสำคัญของบริการ

5.2 ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยระบบเพิ่มเติม

LRG-SEC-01 ผู้ว่าจ้างต้องจัดให้มีการทบทวนสถาปัตยกรรมความมั่นคงปลอดภัยโดยผู้เชี่ยวชาญที่เป็นอิสระจากทีมพัฒนาหลัก ครอบคลุม Trust Boundary การไหลของข้อมูล รูปแบบการยืนยันตัวตน การแบ่งส่วนเครือข่าย การจัดการกุญแจ การเชื่อมต่อภายนอก และมาตรการกู้คืน ก่อนอนุมัติแบบรายละเอียด

LRG-SEC-02 ผู้รับจ้างต้องใช้ระบบบริหารจัดการบัญชีสิทธิสูง (Privileged Access Management: PAM) หรือกลไกเทียบเท่าสำหรับบัญชีผู้ดูแลระบบและบัญชีบริการสำคัญ โดยรองรับการให้สิทธิแบบชั่วคราวและตามเวลาที่จำเป็น (Just-in-time Access) การอนุมัติ การหมุนเวียนข้อมูลรับรอง (Credential Rotation) การบันทึกกิจกรรมหรือเซสชัน (Session Recording) การยกเลิกสิทธิทันทีเมื่อสิ้นสุดความจำเป็น และช่องทางเข้าถึงฉุกเฉิน (Emergency Access) ที่ต้องได้รับการตรวจสอบภายหลัง

LRG-SEC-03 ผู้รับจ้างต้องจัดให้มีระบบบริหารกุญแจเข้ารหัสและใบรับรองดิจิทัลจากศูนย์กลาง พร้อมจัดทำบัญชีรายการที่ระบุเจ้าของ วัตถุประสงค์ ระบบที่ใช้งาน อายุ การหมุนเวียน การเพิกถอน การสำรอง และประวัติการใช้งาน สำหรับกุญแจที่มีผลกระทบสูงต้องใช้โมดูลรักษาความมั่นคงปลอดภัยของฮาร์ดแวร์ (Hardware Security Module: HSM) หรือบริการที่ให้การคุ้มครองเทียบเท่าตามผลการประเมินความเสี่ยง

LRG-SEC-04 ผู้รับจ้างต้องรวบรวมและวิเคราะห์ข้อมูลบันทึกและการแจ้งเตือนด้านความมั่นคงปลอดภัยเข้าสู่ระบบบริหารจัดการเหตุการณ์และข้อมูลความมั่นคงปลอดภัย (SIEM) ศูนย์เฝ้าระวัง หรือบริการเทียบเท่าที่หน่วยงานผู้ว่าจ้างกำหนด พร้อมจัดทำกรณีใช้งานสำหรับตรวจจับเหตุการณ์ผิดปกติอย่างน้อย ได้แก่ การยึดหรือใช้บัญชีผิดปกติ การยกระดับสิทธิ การส่งออกข้อมูลจำนวนมาก การใช้บัญชีบริการ และการเปลี่ยนค่ากำหนดสำคัญ โดยกำหนดระยะเวลาการตรวจพบ การแจ้งเตือน และการตอบสนองตามระดับความรุนแรงของเหตุการณ์

LRG-SEC-05 ให้ผู้รับจ้างนำผลการทดสอบจาก GDL-TEST-03 ถึง GDL-TEST-07 เข้าสู่ CI/CD Security Gate และการบริหารควบคุมข้อยกเว้น ซึ่งระบุเจ้าของความเสี่ยง เหตุผล มาตรการควบคุมชดเชย (Compensating Controls) ผู้อนุมัติ และวันหมดอายุของข้อยกเว้นอย่างชัดเจน

LRG-SEC-06 ผู้รับจ้างต้องการควบคุมความมั่นคงปลอดภัยของห่วงโซ่อุปทานซอฟต์แวร์ (Software Supply Chain) โดยใช้คลังชิ้นงานที่เชื่อถือได้ (Trusted Artifact Repository) จำกัดแหล่งดาวน์โหลด ตรวจสอบแหล่งที่มา เวอร์ชัน ใบอนุญาต สถานะการสนับสนุน ลายมือชื่อดิจิทัล และความถูกต้องของชิ้นงานก่อนติดตั้ง

LRG-SEC-07 ผู้รับจ้างต้องจัดให้ผู้รับจ้างช่วง ผู้ให้บริการคลาวด์ และผู้ให้บริการภายนอกที่สามารถเข้าถึงข้อมูลหรือระบบสำคัญผ่านการประเมินความเสี่ยง โดยครอบคลุมการประมวลผลข้อมูล การแยกผู้เช่า การบริหารบุคลากร การควบคุมการเข้าถึง การแจ้งเหตุการบริหารช่องโหว่ การตรวจประเมิน การเก็บและลบข้อมูล ความต่อเนื่องของบริการ และการยุติบริการ และผู้รับจ้างต้องกำหนดข้อกำหนดดังกล่าว รวมถึงสิทธิของผู้ว่าจ้างในการตรวจประเมินและขอหลักฐานการปฏิบัติตามไว้ในสัญญา พร้อมจัดทำทะเบียนผู้ให้บริการตลอดห่วงโซ่อุปทานให้เป็นปัจจุบัน

LRG-SEC-08 ผู้รับจ้างต้องจัดทำและซ้อมแผนตอบสนองเหตุการณ์ (Incident Response) และแผนกู้คืนจากเหตุไซเบอร์ (Cyber Recovery) แบบบูรณาการอย่างน้อยปีละหนึ่งครั้ง โดยมีผู้บริหาร เจ้าของระบบ เจ้าของข้อมูล ฝ่ายกฎหมาย ฝ่ายสื่อสาร ผู้ให้บริการ และทีมเทคนิคเข้าร่วม การซ้อมต้องครอบคลุมสถานการณ์สำคัญตามความเสี่ยง เช่น บัญชีสิทธิสูงถูกยึด มัลแวร์เรียกค่าไถ่ ข้อมูลรั่วไหล และระบบเชื่อมต่อสำคัญขัดข้อง พร้อมกำหนดผู้รับผิดชอบ ระยะเวลา และติดตามการแก้ไขข้อค้นพบจากการซ้อมจนแล้วเสร็จ

LRG-SEC-09 ผู้รับจ้างต้องออกแบบระบบสำรองและกู้คืนให้มีสำเนาข้อมูลที่แยกจากโดเมนการบริหารของระบบงานจริง และมีมาตรการป้องกันการแก้ไขหรือลบภายในระยะเวลาที่กำหนด โดยต้องสามารถกู้คืนได้โดยไม่พึ่งพาบัญชี ระบบบริหารตัวตน หรือบริการอื่นที่อาจได้รับผลกระทบจากเหตุเดียวกัน ทั้งนี้ ต้องทดสอบการกู้คืนในสถานการณ์ที่บัญชีผู้ดูแลถูกยึด ระบบหลักถูกเข้ารหัส หรือข้อมูลถูกลบหรือทำลาย พร้อมตรวจสอบความครบถ้วนถูกต้องของข้อมูลและค่ากำหนดภายหลังการกู้คืน

6. ข้อเสนอแนะเพิ่มเติม

ข้อเสนอแนะในหัวข้อนี้เป็นแนวทางที่ช่วยในการวางบุคลากร และการบริหารโครงการอย่างเหมาะสม ยกระดับประสบการณ์ผู้ใช้ ความทนทาน ความมั่นคงปลอดภัย และความสามารถขององค์กร แต่ไม่จำเป็นสำหรับทุกโครงการ หน่วยงานควรเลือกใช้ให้สอดคล้องกับผลการประเมินความเสี่ยง ลักษณะภาระงาน ความพร้อมของบุคลากร และต้นทุนตลอดอายุระบบ แนวทางที่เลือกอาจจะถูกประยุกต์ใช้ได้โดยไม่จำเป็นต้องกำหนดใน ข้อกำหนด ทั้งนี้ เมื่อข้อใดถูกนำไปกำหนดใน ข้อกำหนด แล้ว ข้อนั้นย่อมเป็นข้อผูกพันที่ต้องมีเกณฑ์ตรวจรับเช่นเดียวกับข้อบังคับ

6.1 การบริหารโครงการขนาดใหญ่

OPT-PM-01 ผู้รับจ้างร่วมกับผู้ว่าจ้างจัดทำแผนแม่บทโครงการแบบบูรณาการ (Integrated Master Plan) ซึ่งครอบคลุมขอบเขต โครงสร้างงาน กำหนดการ งบประมาณ ทรัพยากร การจัดซื้อ การวิเคราะห์กระบวนงาน การออกแบบ การพัฒนา การเชื่อมต่อระบบ การย้ายข้อมูล การทดสอบ การฝึกอบรม การนำระบบขึ้นใช้งานจริง และการยุติระบบเดิม โดยหมุดหมาย (Milestones) และงวดชำระเงินต้องผูกกับผลส่งมอบ หลักฐาน และเกณฑ์ตรวจรับที่พิสูจน์ได้ ไม่ผูกกับระยะเวลาเพียงอย่างเดียว

OPT-PM-02 ผู้รับจ้างร่วมกับผู้ว่าจ้างกำหนดบทบาทและความรับผิดชอบด้วยตารางความรับผิดชอบ (RACI Matrix) หรือเครื่องมือเทียบเท่า ให้ครอบคลุมเจ้าของกระบวนงาน หน่วยงานเทคโนโลยีสารสนเทศ เจ้าของข้อมูล ฝ่ายความมั่นคงปลอดภัย ผู้รับจ้าง ผู้รับจ้างช่วง ผู้ให้บริการ และผู้ตรวจรับ พร้อมกำหนดผู้มีอำนาจอนุมัติความต้องการ สถาปัตยกรรม ความมั่นคงปลอดภัย ข้อมูล การทดสอบ การเปลี่ยนแปลง การนำระบบขึ้นใช้งาน และการตอบสนองเหตุการณ์

OPT-PM-03 ผู้รับจ้างมีกระบวนการบริหารความต้องการและตารางตรวจสอบย้อนกลับของความต้องการ (Requirements Traceability Matrix) ซึ่งควบคุมเวอร์ชัน แหล่งที่มา ลำดับความสำคัญ เกณฑ์ยอมรับ และสถานะของแต่ละความต้องการ โดยต้องจัดลำดับความสำคัญร่วมกับเจ้าของบริการหรือเจ้าของกระบวนงาน และกำหนดเกณฑ์ยอมรับสำหรับกฎธุรกิจ กระบวนงาน รายงาน ข้อมูล และการเชื่อมต่อระบบ พร้อมกำหนดวิธีจัดการข้อขัดแย้งและการเปลี่ยนแปลงโดยไม่สูญเสียความสามารถในการตรวจสอบย้อนกลับ

OPT-PM-04 ผู้รับจ้างรวบรวมการเปลี่ยนแปลงขอบเขต กระบวนงาน บุคลากร ข้อมูล ระบบเดิม สถาปัตยกรรม งบประมาณ กำหนดการ คุณภาพ ความมั่นคงปลอดภัย หรือสัญญา เพื่อนำเสนอผ่านคณะกรรมการควบคุมการเปลี่ยนแปลง (Change Control Board) หรือกลไกอนุมัติที่กำหนดไว้ โดยให้มีการวิเคราะห์ผลกระทบต่อประโยชน์ ต้นทุน เวลา ความเสี่ยง การคุ้มครองข้อมูล และข้อผูกพันตามสัญญา พร้อมจัดทำแผนย้อนกลับสำหรับการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบใช้งานจริง

OPT-PM-05 ผู้รับจ้างร่วมกับผู้ว่าจ้างจัดทำและทบทวนบันทึกความเสี่ยง สมมติฐาน ประเด็นปัญหา และการพึ่งพา (Risks, Assumptions, Issues and Dependencies: RAID Log) อย่างสม่ำเสมอ โดยครอบคลุมความเสี่ยงด้านเทคนิค การย้ายและคุณภาพข้อมูล การเชื่อมต่อระบบเดิม การยอมรับของผู้ใช้ การขาดบุคลากร การพึ่งพาผู้ขาย กฎหมาย ความมั่นคงปลอดภัย การเงิน และความต่อเนื่องของงาน พร้อมระบุเจ้าของความเสี่ยง มาตรการตอบสนอง กำหนดเวลา และสถานะการดำเนินการ

OPT-PM-06 ผู้รับจ้างกำหนดจุดตรวจสอบและอนุมัติโครงการ (Stage Gates) อย่างน้อยก่อนอนุมัติแบบรายละเอียด ก่อนเริ่มพัฒนาเต็มรูปแบบ ก่อนย้ายข้อมูล ก่อนการทดสอบการยอมรับของผู้ใช้ (UAT) ก่อนนำระบบขึ้นใช้งานจริง (Cutover) ก่อนยุติระบบเดิม และก่อนปิดโครงการ โดยแต่ละ Gate ต้องระบุรายการหลักฐาน เกณฑ์ผ่าน ผู้มีอำนาจอนุมัติ และเงื่อนไขที่ต้องแก้ไขก่อนผ่าน Gate อย่างชัดเจน

OPT-PM-07 ผู้รับจ้างจัดทำแผนบริหารคุณภาพ แผนทดสอบรวม และเกณฑ์สิ้นสุดการทดสอบ (Exit Criteria) ให้ครอบคลุมฟังก์ชัน กฎธุรกิจ กระบวนงาน สิทธิการเข้าถึง การเชื่อมต่อ ประสิทธิภาพ ความพร้อมใช้งาน ความมั่นคงปลอดภัย การเข้าถึงสำหรับทุกคน การย้ายข้อมูล และ UAT พร้อมกำหนดผู้รับผิดชอบและความเป็นอิสระของผู้ทดสอบ โดยเจ้าของกระบวนงานและเจ้าของข้อมูลต้องรับรองผลการทดสอบในส่วนที่ตนรับผิดชอบ

OPT-PM-08 ผู้รับจ้างจัดให้มีการประกันคุณภาพหรือการตรวจทานอิสระ (Independent Assurance/Independent Verification and Validation: IV&V) ในประเด็นสำคัญตามระดับความเสี่ยง เช่น สถาปัตยกรรม ความมั่นคงปลอดภัย การประมาณการ กำหนดการ คุณภาพซอฟต์แวร์ การย้ายข้อมูล คุณภาพข้อมูล และความพร้อมก่อนใช้งาน โดยผู้ตรวจทานต้องมีความเป็นอิสระจากผู้รับผิดชอบการส่งมอบงานในส่วนที่ตรวจสอบ และข้อค้นพบต้องมีผู้รับผิดชอบ กำหนดเวลา และติดตามจนปิดประเด็น

OPT-PM-09 ผู้ว่าจ้างจัดให้มีกระบวนการกำกับผู้รับจ้าง และห่วงโซ่อุปทาน ซึ่งครอบคลุมการอนุมัติผู้รับจ้างช่วง การวัดผลตาม SLA และตัวชี้วัดผลการดำเนินงาน (Key Performance Indicators: KPI) ข้อกำหนดด้านความมั่นคงปลอดภัย ใบอนุญาต ทรัพย์สินทางปัญญา การควบคุมการเข้าถึง การแจ้งเหตุ การส่งมอบ SBOM และแผนถ่ายทอดความรู้ โดยสัญญาต้องกำหนดสิทธิของหน่วยงานในการตรวจสอบซอร์สโค้ด ชิ้นงาน บุคลากร และหลักฐานการปฏิบัติตามข้อกำหนด รวมถึงสิทธิในการตรวจประเมินผู้รับจ้างช่วงและผู้ให้บริการที่เกี่ยวข้อง

OPT-PM-10 ผู้รับจ้างร่วมกับผู้ว่าจ้างจัดทำแผนการสื่อสารและการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสีย โดยระบุกลุ่มเป้าหมาย เนื้อหาที่ต้องสื่อสาร ผู้รับผิดชอบ ความถี่ ช่องทาง และกระบวนการรับข้อคิดเห็น พร้อมจัดให้มีรายงานสถานะโครงการอย่างสม่ำเสมอ ซึ่งแสดงความก้าวหน้า งบประมาณ กำหนดการ ความเสี่ยง คุณภาพ การเปลี่ยนแปลง ประเด็นที่ต้องตัดสินใจ และการดำเนินการตามมติ

OPT-PM-11 ผู้รับจ้างจัดทำแผนนำระบบขึ้นใช้งานจริง (Cutover Plan) และแผนย้อนกลับ (Rollback Plan) ที่ผ่านการซ้อม โดยระบุลำดับกิจกรรม การหยุดรับรายการ การย้ายและกระทบยอดข้อมูล การเปิดสิทธิ การสื่อสาร การสนับสนุนช่วงเริ่มใช้งาน เกณฑ์การตัดสินใจเดินหน้าหรือหยุด (Go/No-Go Criteria) ผู้มีอำนาจตัดสินใจ และวิธีตรวจสอบความครบถ้วนของธุรกรรมและข้อมูลภายหลังเปิดบริการ

OPT-PM-12 ผู้ว่าจ้างร่วมกับผู้รับจ้างจัดทำแผนบริหารการเปลี่ยนแปลงองค์กร การสื่อสาร การฝึกอบรม และการรับบริการ โดยวิเคราะห์ผลกระทบต่อบทบาท ขั้นตอนการปฏิบัติงาน นโยบาย และทักษะของผู้ใช้ เจ้าหน้าที่สนับสนุน ผู้ดูแลระบบ และผู้บริหาร พร้อมจัดฝึกอบรมตามบทบาท จัดให้มีระบบช่วยเหลือในช่วงเริ่มใช้งาน และวัดความพร้อม การเข้าอบรม การยอมรับ อัตราการใช้งานจริง ข้อผิดพลาดของผู้ใช้ ปัญหาที่พบ และผลของมาตรการปรับปรุง

OPT-PM-13 ก่อนสิ้นสุดโครงการ ผู้รับจ้างควรดำเนินการส่งมอบสู่หน่วยงานปฏิบัติการอย่างเป็นทางการ โดยตรวจสอบความพร้อมด้านบุคลากร กระบวนการ เครื่องมือ เอกสาร บัญชีผู้ใช้ สิทธิ ใบอนุญาต ระบบเฝ้าระวัง การสำรองและกู้คืน การสนับสนุน แผนบำรุงรักษา และ SLA พร้อมจัดทำรายงานปิดโครงการ บทเรียนจากโครงการ การทบทวนภายหลังนำระบบขึ้นใช้งาน (Post-implementation Review) และแผนติดตามผลประโยชน์ตามระยะเวลาที่กำหนด

6.2 บุคลากรที่จำเป็นสำหรับโครงการขนาดใหญ่

OPT-HR-01 ผู้รับจ้างจัดตั้งทีมสหสาขาวิชาชีพที่มีบทบาทครบถ้วนตามขอบเขตและความซับซ้อนของโครงการ โดยอย่างน้อยต้องมีผู้รับผิดชอบระดับบริหาร เจ้าของกระบวนงาน เจ้าของผลิตภัณฑ์หรือระบบ ผู้จัดการโครงการ นักวิเคราะห์ธุรกิจ สถาปนิกระบบ นักพัฒนาซอฟต์แวร์ ผู้ทดสอบ ผู้เชี่ยวชาญ DevSecOps หรือแพลตฟอร์ม ผู้ฝึกอบรม ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย และผู้ว่าจ้างจัดให้มีผู้แทนฝ่ายปฏิบัติการ รวมทั้งบุคลากรด้านการบริหารการเปลี่ยนแปลง และการสนับสนุนบริการตามลักษณะของโครงการ

OPT-HR-02 โครงการต้องมีบทบาทด้านสถาปัตยกรรมที่ครอบคลุมสถาปัตยกรรมโซลูชันหรือแอปพลิเคชัน สถาปัตยกรรมข้อมูล สถาปัตยกรรมการเชื่อมต่อและ API และสถาปัตยกรรมความมั่นคงปลอดภัย โดยเมื่อโครงการมีการรวม ย้าย หรือปรับโครงสร้างข้อมูลจำนวนมาก ควรมีเจ้าของข้อมูล บริกรข้อมูล และบุคลากรด้านการย้ายข้อมูล คุณภาพข้อมูล และการบริหารฐานข้อมูล รวมทั้งต้องมีผู้เชี่ยวชาญด้านระบบเดิมและการเชื่อมต่อ ซึ่งสามารถออกแบบและทดสอบการเชื่อมโยง ตลอดจนกำหนดเจ้าของหรือผู้ประสานงานของระบบปลายทางแต่ละระบบได้ ทั้งนี้บุคลากรหนึ่งคนอาจรับผิดชอบมากกว่าหนึ่งบทบาทได้เมื่อแสดงให้เห็นว่ามีสมรรถนะเพียงพอ มีเวลาปฏิบัติงานเหมาะสม และไม่ก่อให้เกิดความขัดแย้งด้านการแบ่งแยกหน้าที่

OPT-HR-03 ผู้รับจ้างร่วมกับผู้ว่าจ้างควรจัดให้มีบุคลากรด้านการออกแบบบริการ กระบวนงาน และประสบการณ์ผู้ใช้ตามลักษณะของระบบ เช่น การวิจัยผู้ใช้และการออกแบบบริการ (User Research/Service Design) การออกแบบประสบการณ์และส่วนติดต่อผู้ใช้ (UX/UI) และการออกแบบเนื้อหา (Content Design) เพื่อให้ข้อกำหนด การออกแบบ และการทดสอบครอบคลุมผู้ใช้งานจริง ความสามารถในการเข้าถึง และคุณภาพของเนื้อหาหรือกระบวนงานภาครัฐ

OPT-HR-04 ผู้รับจ้างควรมีบุคลากรด้านการประกันคุณภาพที่ครอบคลุมการบริหารการทดสอบ (Test Management) การทดสอบอัตโนมัติ (Test Automation) การทดสอบประสิทธิภาพ (Performance Testing) และการทดสอบความมั่นคงปลอดภัย (Security Testing) โดยผู้รับผิดชอบการยอมรับผลการทดสอบต้องมีความเป็นอิสระจากผู้พัฒนาส่วนที่ทดสอบในระดับที่เหมาะสมกับความเสี่ยงของระบบ

OPT-HR-05 ผู้รับจ้างควรมีบุคลากรด้านการดำเนินงาน ด้านความเชื่อถือได้ (Reliability) และการสนับสนุนบริการตามเทคโนโลยีและระดับบริการที่กำหนด เช่น วิศวกร DevSecOps วิศวกรแพลตฟอร์มหรือคลาวด์ วิศวกรความเชื่อถือได้ของระบบ (Site Reliability Engineer) ผู้บริหารฐานข้อมูล วิศวกรเครือข่าย เจ้าหน้าที่ศูนย์บริการ (Service Desk) ผู้รับผิดชอบการบริหารการเปลี่ยนแปลง และผู้รับผิดชอบการฝึกอบรมและสนับสนุนผู้ใช้

OPT-HR-06 ผู้รับจ้างควรกำหนดคุณสมบัติขั้นต่ำ ความรู้ ทักษะ ประสบการณ์ สมรรถนะ และระยะเวลาปฏิบัติงานของแต่ละบทบาทเป็นลายลักษณ์อักษร โดยระบุจำนวนวันทำงาน สัดส่วนเวลา หรือจำนวนบุคลากรเต็มเวลาเทียบเท่า (Full-time Equivalent: FTE) ตามความเหมาะสม และพิจารณาผลงานหรือประสบการณ์ที่เกี่ยวข้องเป็นหลัก ใบรับรองวิชาชีพอาจใช้เป็นหลักฐานประกอบ แต่ต้องไม่ใช้ทดแทนความสามารถในการปฏิบัติงานจริง

OPT-HR-07 ผู้รับจ้างควรกำหนดให้มีนักพัฒนา วิศวกร DevSecOps วิศวกรแพลตฟอร์ม และผู้ดูแลระบบควรผ่านการฝึกอบรมด้านการเขียนโค้ดที่ปลอดภัย (Secure Coding) หรือการบริหารระบบอย่างปลอดภัย (Secure Administration) ตามบทบาทก่อนเริ่มงานหรือภายในระยะเวลาที่หน่วยงานกำหนด และบุคลากรทุกคนที่เกี่ยวข้องกับโครงการ ควรได้รับการฝึกอบรมด้านความมั่นคงปลอดภัย ความเป็นส่วนตัว และการจัดชั้นข้อมูลตามบทบาท พร้อมจัดเก็บหลักฐานการเข้าร่วมและผลการประเมินตามที่หน่วยงานกำหนด

OPT-HR-08 บุคลากรที่เข้าถึงข้อมูลอ่อนไหวหรือระบบสำคัญของผู้รับจ้างควรผ่านการตรวจสอบประวัติตามกฎหมายและนโยบายของหน่วยงาน ลงนามข้อตกลงรักษาความลับก่อนเริ่มปฏิบัติงาน ใช้บัญชีเฉพาะบุคคล และได้รับสิทธิแบบมีระยะเวลาสิ้นสุดตามความจำเป็น และเมื่อบุคลากรออกจากโครงการ เปลี่ยนหน้าที่ หรือสิ้นสุดสัญญา ต้องเพิกถอนสิทธิ ปิดบัญชี และคืนทรัพย์สินของหน่วยงานโดยทันที ทั้งนี้ ข้อผูกพันด้านการรักษาความลับต้องคงอยู่ภายหลังสิ้นสุดการปฏิบัติงานหรือการจ้าง

OPT-HR-09 ควรแบ่งแยกหน้าที่อย่างน้อยระหว่างผู้พัฒนา ผู้ทดสอบ ผู้อนุมัติการเปลี่ยนแปลง ผู้ปล่อยระบบ และผู้ตรวจสอบบันทึกเหตุการณ์ โดยห้ามบุคคลเดียวควบคุมกระบวนการสำคัญตั้งแต่ต้นจนจบโดยไม่มีการทบทวนหรืออนุมัติจากบุคคลอื่น กรณีข้อจำกัดด้านจำนวนบุคลากรทำให้ไม่สามารถแยกบุคคลได้เต็มรูปแบบ สามารถกำหนดกลไกอื่นเสริม ได้แก่ มาตรการควบคุมทดแทน การอนุมัติเพิ่มเติม และการตรวจสอบย้อนหลังอย่างชัดเจน

OPT-HR-10 ผู้รับจ้างควรจัดทำแผนอัตรากำลังและแผนทดแทนบุคลากรสำหรับบทบาทสำคัญ โดยระบุรายชื่อ บทบาท ช่วงเวลาปฏิบัติงาน และผู้สำรอง การเปลี่ยนบุคลากรหลักต้องได้รับความเห็นชอบจากหน่วยงาน บุคลากรทดแทนต้องมีคุณสมบัติและประสบการณ์ไม่ต่ำกว่าบุคลากรเดิม และต้องมีระยะเวลาส่งมอบงานที่เพียงพอโดยไม่กระทบกำหนดการ คุณภาพ หรือความต่อเนื่องของโครงการ

OPT-HR-11 ผู้รับจ้างควรดำเนินการถ่ายทอดความรู้เชิงปฏิบัติให้แก่บุคลากรของหน่วยงานอย่างต่อเนื่องตลอดโครงการ ไม่จำกัดเฉพาะช่วงก่อนปิดโครงการ โดยครอบคลุมสถาปัตยกรรม และ Operating Model การเฝ้าระวัง การตรวจสอบเหตุการณ์ และการแก้ไขปัญหา โดยก่อนการตรวจรับขั้นสุดท้ายให้ประเมินว่าทีมของหน่วยงานหรือผู้ให้บริการที่หน่วยงานกำหนดสามารถปฏิบัติหน้าที่ตาม Operating Model และขอบเขตความรับผิดชอบที่ตกลงไว้ได้

6.3 สถาปัตยกรรม การส่งมอบ และประสิทธิภาพ

OPT-ARCH-01 ผู้รับจ้างควรพิจารณาจัดทำแพลตฟอร์มสำหรับนักพัฒนาภายใน (Internal Developer Platform: IDP) และเส้นทางมาตรฐานสำหรับการพัฒนา (Golden Path) ที่รวบรวมแม่แบบโครงการ กระบวนการ CI/CD ระบบบันทึกเหตุการณ์ (Logging) ระบบติดตามการทำงาน (Moniข้อกำหนดing) การจัดการข้อมูลลับ (Secrets Management) การสแกนด้านความมั่นคงปลอดภัย (Security Scanning) และเอกสารที่เกี่ยวข้อง เพื่อให้หลายทีมสามารถพัฒนาระบบภายใต้มาตรฐานเดียวกัน และลดภาระในการจัดการโครงสร้างพื้นฐาน

OPT-ARCH-02 องค์กรที่ใช้คลาวด์หลายโครงการควรพิจารณากำหนดสถาปัตยกรรมอ้างอิง นโยบายบัญชีและเครือข่าย มาตรฐานความปลอดภัย การบริหารต้นทุน และการแลกเปลี่ยนแนวปฏิบัติระหว่างทีม

OPT-ARCH-03 สำหรับบริการที่มีผู้ใช้งานกระจายในหลายพื้นที่ ผู้รับจ้างร่วมกับผู้ว่าจ้างควรพิจารณาใช้เครือข่ายนำส่งเนื้อหา (Content Delivery Network: CDN) การจัดเก็บข้อมูลชั่วคราว (Caching) และการปรับแต่งทรัพยากรฝั่งผู้ใช้ เช่น การย่อขนาดไฟล์ (Minification) การปรับแต่งรูปภาพ (Image Optimization) และการโหลดเมื่อจำเป็น (Lazy Loading) เพื่อเพิ่มประสิทธิภาพและลดเวลาตอบสนองของระบบ พร้อมกำหนดวิธีล้างข้อมูลแคช (Cache Invalidation) และมาตรการป้องกันไม่ให้ข้อมูลอ่อนไหวถูกจัดเก็บไว้ในแคช

OPT-ARCH-04 ผู้รับจ้างร่วมกับผู้ว่าจ้างในระบบภารกิจสำคัญอาจพิจารณา Multi-region Deployment, Warm Standby, Pilot Light หรือ Active-Active เพิ่มเติมจากข้อกำหนดพื้นฐาน เมื่อผล Business Impact Analysis แสดงว่าความล้มเหลวระดับภูมิภาคไม่สามารถยอมรับได้และงบประมาณสอดคล้องกับเป้าหมาย RTO/RPO

OPT-ARCH-05 ผู้รับจ้างร่วมกับผู้ว่าจ้างควรพิจารณาใช้ Chaos Engineering หรือการทดสอบ Fault Injection ในสภาพแวดล้อมที่ควบคุม เพื่อยืนยันว่าระบบและทีมปฏิบัติการรับมือกับความล้มเหลวของส่วนประกอบ การหน่วงเวลา และการสูญเสียการเชื่อมต่อได้ตามที่ออกแบบ

6.4 ประสบการณ์ผู้ใช้และการปรับปรุงบริการ

OPT-UX-01 สำหรับบริการสาธารณะ ผู้รับจ้างร่วมกับผู้ว่าจ้างควรพิจารณาพัฒนาเว็บแอปพลิเคชันแบบ Progressive Web Application: PWA เมื่อมีประโยชน์ต่อการติดตั้งบนหน้าจอหลัก การแจ้งเตือน และการใช้งานแบบออฟไลน์ โดยต้องกำหนดประเภทข้อมูลที่อนุญาตให้จัดเก็บบนอุปกรณ์อย่างชัดเจน พร้อมมาตรการป้องกันการเปิดเผยข้อมูลบนอุปกรณ์ที่ใช้งานร่วมกัน

OPT-UX-02 ผู้รับจ้างร่วมกับผู้ว่าจ้างควรจัดให้มีการวิจัยผู้ใช้และทดสอบการใช้งานเป็นรอบอย่างต่อเนื่องหลังเปิดบริการ รวมทั้งวิเคราะห์จุดที่ผู้ใช้ยกเลิกหรือขอความช่วยเหลือ และนำผลเข้าสู่ Backlog การปรับปรุงที่มีเจ้าของและลำดับความสำคัญ

OPT-UX-03 ผู้รับจ้างร่วมกับผู้ว่าจ้างควรใช้ Web Analytics หรือ Product Analytics ที่เคารพความเป็นส่วนตัวเพื่อวัดปริมาณใช้งาน ความสำเร็จของงาน เวลาที่ใช้ และข้อผิดพลาด โดยหลีกเลี่ยงการเก็บข้อมูลส่วนบุคคลเกินจำเป็นและกำหนดอายุข้อมูลอย่างชัดเจน

OPT-UX-04 ผู้ว่าจ้างร่วมกับผู้รับจ้างควรจัดให้มีช่องทางรับความคิดเห็น ร้องเรียน และติดตามสถานะที่เชื่อมโยงกับบริการเพื่อเพิ่มความโปร่งใสและให้หน่วยงานเห็นปัญหาจริงของผู้ใช้ โดยต้องกำหนด SLA และการคุ้มครองข้อมูลของผู้ร้องเรียน

OPT-UX-05 ผู้รับจ้างร่วมกับผู้ว่าจ้างบริการที่มีผู้ใช้หลากหลายควรพิจารณารองรับหลายภาษา เนื้อหาแบบอ่านง่าย และช่องทางช่วยเหลือทางเลือก โดยทดสอบกับกลุ่มผู้ใช้จริงและไม่อาศัยการแปลอัตโนมัติโดยไม่มีการทบทวนในส่วนของเนื้อหาที่มีผลทางกฎหมายหรือสิทธิ

6.5 การยกระดับความมั่นคงปลอดภัย

OPT-SEC-01 ผู้รับจ้างควรพิจารณาใช้ Interactive Application Security Testing (IAST) เพื่อเสริม SAST และ DAST โดยเฉพาะระบบที่พัฒนาและทดสอบบ่อย เพื่อให้ระบุตำแหน่งช่องโหว่ในโค้ดและลดผลบวกลวงได้รวดเร็วขึ้น

OPT-SEC-02 ผู้รับจ้างควรพิจารณา Fuzz Testing สำหรับ API, Parser, File Upload และส่วนที่รับข้อมูลรูปแบบซับซ้อน เพื่อค้นหาข้อผิดพลาด การใช้ทรัพยากรผิดปกติ และช่องโหว่ที่กรณีทดสอบทั่วไปอาจไม่พบ

OPT-SEC-03 ผู้รับจ้างควรจัดทำ Vulnerability Disclosure Policy หรือ Bug Bounty Program สำหรับระบบที่มีความพร้อมด้านการรับและแก้ไขรายงาน โดยกำหนดขอบเขต กติกา ช่องทางปลอดภัย ระยะตอบรับ การคุ้มครองผู้รายงาน และการเปิดเผยข้อมูลร่วมกัน

OPT-SEC-04 ผู้รับจ้างร่วมกับผู้ว่าจ้างควรจัดตั้ง Security Champions ภายในทีมพัฒนาและปฏิบัติการเพื่อให้คำปรึกษาทบทวนการออกแบบ ส่งเสริม Secure Coding และติดตามข้อค้นพบ โดยต้องมีเวลาปฏิบัติงานและการอบรมที่ชัดเจน ไม่ใช่บทบาทเพิ่มเติมโดยไม่มีทรัพยากร

OPT-SEC-05 ผู้รับจ้างควรพิจารณาใช้ Content Security Policy แบบเข้มงวดด้วย Nonce หรือ Hash และลดการอนุญาตสคริปต์แบบกว้าง เมื่อสถาปัตยกรรมและส่วนประกอบรองรับ เพื่อยกระดับการป้องกัน XSS นอกเหนือจากการเข้ารหัสผลลัพธ์

OPT-SEC-06 ระบบภารกิจสำคัญ ผู้ว่าจ้างร่วมกับผู้รับจ้างอาจเพิ่มความถี่ Penetration Testing เป็นทุก 6 เดือน และพิจารณา Red Team, Breach and Attack Simulation หรือ Purple Team Exercise เพื่อประเมินทั้งการป้องกัน การตรวจจับ และการตอบสนองต่อการโจมตีแบบต่อเนื่อง

OPT-SEC-07 ผู้รับจ้างควรจัดทำบัญชีการใช้ การเข้ารหัส และแผนปรับเปลี่ยนอัลกอริทึม รวมถึงประเมินผลกระทบของ Post-quantum Cryptography สำหรับระบบที่ต้องเก็บข้อมูลเป็นเวลานานหรือมีวงจรชีวิตยาว

OPT-SEC-08 ผู้รับจ้างร่วมกับผู้ว่าจ้างพิจารณาให้มีระบบเฝ้าระวังและแจ้งเตือนกิจกรรมผิดปกติที่สามารถเชื่อมโยงเหตุการณ์จากแอปพลิเคชัน โครงสร้างพื้นฐาน WAF และระบบยืนยันตัวตน พร้อมกำหนดผู้รับแจ้ง เกณฑ์ความรุนแรง ขั้นตอนตอบสนอง และระยะเวลาการเก็บบันทึกตามกฎหมายและความเสี่ยงในการพัฒนาระบบเว็บแอปพลิเคชัน

OPT-SEC-09 ผู้รับจ้างควรจัดทำบัญชีรายการส่วนประกอบซอฟต์แวร์ (Software Bill of Materials: SBOM) ให้ครอบคลุมไลบรารี แพ็กเกจ เฟรมเวิร์ก และคอนเทนเนอร์จากภายนอก พร้อมตรวจสอบใบอนุญาต แหล่งที่มา สถานะการสนับสนุน และช่องโหว่อย่างต่อเนื่อง ทั้งนี้ ห้ามใช้ส่วนประกอบที่สิ้นสุดการสนับสนุนหรือมีช่องโหว่ร้ายแรง เว้นแต่มีเหตุจำเป็น ได้รับอนุมัติจากผู้ว่าจ้างเป็นลายลักษณ์อักษร และมีมาตรการลดความเสี่ยงเพิ่มเติมที่เหมาะสม เช่น การจำกัดการใช้งาน การแยกส่วนระบบ การปิดฟังก์ชันที่มีความเสี่ยง การติดตามเฝ้าระวังเพิ่มเติม หรือการกำหนดแผนเปลี่ยนทดแทนภายในระยะเวลาที่กำหนด

OPT-SEC-10 ผู้รับจ้างร่วมกับผู้ว่าจ้างควรจัดทำแบบจำลองภัยคุกคาม (Threat Modeling) สำหรับเส้นทางข้อมูล ธุรกรรม จุดเชื่อมต่อ และองค์ประกอบสำคัญของระบบ โดยใช้วิธีที่เป็นมาตรฐาน เช่น STRIDE หรือวิธีเทียบเท่า และนำผลไปกำหนดมาตรการออกแบบและกรณีทดสอบความปลอดภัย สำหรับเว็บแอปพลิเคชันสำหรับภายนอก (Public-facing Application)

OPT-SEC-11 สถาปัตยกรรม ผู้รับจ้างควรใช้การแบ่งส่วนเครือข่ายระดับย่อย (Micro-segmentation) หรือกลไกเทียบเท่า เพื่อจำกัดการสื่อสารระหว่างภาระงาน (Workloads) ตามหน้าที่และความจำเป็น พร้อมตรวจสอบตัวตนระหว่างบริการ (Service-to-Service Authentication) โดยห้ามเปิดการเชื่อมต่อครอบคลุมทั้งเครือข่าย เว้นแต่มีเหตุผลและได้รับอนุมัติอย่างเป็นทางการ เพื่อพิจารณาการยกระดับด้านการออกแบบและพัฒนาเพิ่มเติมสำหรับระบบขนาดใหญ่ มูลค่าสูงหรือมีผลกระทบสูง

OPT-SEC-12 เมื่อระบบประมวลผลข้อมูลอ่อนไหวหรือมีช่องทางส่งออกข้อมูลที่มีความเสี่ยงสูง ผู้รับจ้างควรจัดให้มีระบบป้องกันการสูญหายหรือรั่วไหลของข้อมูล (Data Loss Prevention: DLP) หรือมาตรการเทียบเท่า ครอบคลุมช่องทางที่เกี่ยวข้อง เช่น การดาวน์โหลดข้อมูลจำนวนมาก อีเมล อุปกรณ์จัดเก็บข้อมูลแบบพกพา และบริการคลาวด์

การเตรียมความพร้อมขององค์กรก่อนเริ่มโครงการ

- ผู้ว่าจ้างแต่งตั้งผู้รับผิดชอบระดับบริหาร เจ้าของกระบวนงาน เจ้าของผลิตภัณฑ์หรือระบบตามลักษณะของโครงการ ที่เป็นผู้รับผิดชอบผลสำเร็จของโครงการและประโยชน์ที่คาดว่าจะได้รับ พร้อมคณะกรรมการกำกับโครงการและสำนักงานบริหารโครงการ (Project Management Office: PMO) หรือกลไกเทียบเท่า สำหรับโครงการขนาดใหญ่ มูลค่าสูง หรือผลกระทบสูง โดยกำหนดอำนาจตัดสินใจ วาระประชุม และเส้นทางยกระดับปัญหา (Escalation Path) เป็นลายลักษณ์อักษร
- ผู้รับจ้างร่วมกับผู้ว่าจ้างจัดทำกฎบัตรโครงการ (Project Charter) และกรณีทางธุรกิจ (Business Case) ที่ได้รับอนุมัติ โดยระบุปัญหา เป้าหมาย ขอบเขต ผลประโยชน์และตัวชี้วัดที่วัดได้ ต้นทุนรวมตลอดอายุระบบ ทางเลือก ความเสี่ยง สมมติฐาน ข้อกำหนดทางกฎหมาย และผลกระทบต่อกระบวนงาน บุคลากร และระบบเดิม พร้อมกำหนดผู้รับผิดชอบต่อการติดตามและทำให้เกิดผลประโยชน์ภายหลังโครงการสิ้นสุด
- ผู้รับจ้างร่วมกับผู้ว่าจ้างจัดทำ Competency Framework และ Individual Development Plan สำหรับบทบาทเทคนิคโครงการ ข้อมูล ความปลอดภัย และปฏิบัติการ พร้อมประเมิน Skill Gap และติดตามผลการพัฒนาอย่างสม่ำเสมอ
- สำหรับตำแหน่งสำคัญ ผู้ว่าจ้างควรส่งเสริมใบรับรองวิชาชีพที่เกี่ยวข้องกับหน้าที่และเทคโนโลยีที่ใช้ ควบคู่กับการประเมินผลงานจริง การทดลองปฏิบัติ และการต่ออายุความรู้
- ผู้ว่าจ้างควรจัดทำ Succession Plan และชุมชนนักปฏิบัติสำหรับบทบาทที่ขาดแคลน เช่น Architect, Security, DevSecOps, Data และ Accessibility เพื่อให้ความรู้ไม่ผูกอยู่กับบุคคลหรือผู้รับจ้างรายเดียว

ข้อพิจารณาสำคัญสำหรับการนำไปจัดทำข้อกำหนด

- เมื่อใช้ผลิตภัณฑ์สำเร็จรูปหรือบริการคลาวด์ ให้ผู้ว่าจ้างปรับถ้อยคำจาก “พัฒนา” เป็น “จัดหา กำหนดค่า เชื่อมต่อ และทดสอบ” แต่ยังคงผลลัพธ์ด้านความปลอดภัย ข้อมูล การตรวจสอบ และการย้ายออก โดย**เนื้อหาที่อาจดำเนินการไม่ได้กับ** SaaS/COTS เช่น
  - ส่งมอบ Source Code
  - จัดทำ SBOM ครบทุกส่วนประกอบ
  - ทำ SAST กับ Source Code ของผลิตภัณฑ์
  - ใช้ IaC กับโครงสร้างพื้นฐานของผู้ให้บริการ
  - ให้หน่วยงาน Build และ Deploy ระบบเอง
  - Session Recording หรือ Micro-segmentation ในระบบที่ผู้ขายควบคุม

  ให้พิจารณาปรับตามความเหมาะสม**หรือตัดออก**
- เมื่อระบบหนึ่งมีทั้งส่วนสาธารณะและส่วนเจ้าหน้าที่ ให้ผู้ว่าจ้างใช้ข้อกำหนด Public-facing กับส่วนที่เปิดต่อภายนอก ใช้ข้อกำหนด Internal กับส่วนหลังบ้าน
- ผู้ว่าจ้างควรกำหนด Requirement Compliance Matrix ในข้อเสนอทางเทคนิค โดยให้ผู้เสนอราคาระบุวิธีปฏิบัติ หลักฐานผลิตภัณฑ์หรือบริการที่เกี่ยวข้อง ข้อยกเว้น และผลกระทบต่อราคาในแต่ละรหัสข้อกำหนด
- ข้อกำหนด ต้องระบุบทบาทของหน่วยงานผู้ว่าจ้าง ผู้รับจ้าง และความรับผิดชอบร่วมกันเฉพาะในกรณีที่แตกต่างจากหลักการกำหนดบทบาทและความรับผิดชอบของเอกสารฉบับนี้
- ข้อกำหนดฉบับนี้เทียบแนวทางกับมาตรฐานภาครัฐไทยและแนวปฏิบัติสากล การนำไปใช้จริงต้องตรวจสอบฉบับที่มีผลใช้บังคับ ณ วันที่จัดทำ ข้อกำหนด และปรับให้สอดคล้องกับกฎหมาย นโยบาย และระดับความเสี่ยงของหน่วยงานเจ้าของโครงการ
- กำหนด สิ่งส่งมอบ ในการตรวจรับแต่ละงวด ให้ชัดเจน และ ยกตัวอย่างของ สิ่งส่งมอบ (Work Products) Project Management Documents, Business requirement, SRS, Teat Plan, Architecture Design, Detail Design, Systems Configuration, test results, codes, deployment plan, security test results, operating and service documents, recovery document etc.

ภาคผนวก 1: รายการเอกสารอ้างอิง

1. มธอ. 11 เล่ม 1-2566 ถึง มธอ. 11 เล่ม 3-2566 ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล
2. มรด. 1-1:2564 และ มรด. 1-2:2564 ว่าด้วยการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ
3. World Wide Web Consortium. Web Content Accessibility Guidelines (WCAG) 2.2 (2023). https://www.w3.org/TR/WCAG22/
4. มสพร. 11-2566 ว่าด้วยมาตรฐานเว็บไซต์ภาครัฐ
5. มรด. 6:2566 มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ (Data Governance Framework Revised: Guideline เวอร์ชัน 2.0)
6. มรด. 3-1:2565 และ มรด. 3-2:2565 มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับแนวทางการจัดทำบัญชีข้อมูลภาครัฐและแนวทางการลงทะเบียนบัญชีข้อมูลภาครัฐ
7. OpenAPI Initiative. OpenAPI Specification, Version 3.2.0 (2025).
8. IETF RFC 6749, The OAuth 2.0 Authorization Framework (2012).
9. OpenID Foundation, OpenID Connect Core 1.0 Incorporating Errata Set 2 (2023).
10. OWASP Foundation. Application Security Verification Standard (ASVS) 5.0 (2025). https://owasp.org/www-project-application-security-verification-standard/
11. OWASP Foundation. OWASP Top 10: 2025 (2025). https://owasp.org/Top10/
12. IETF RFC 9846, The Transport Layer Security Protocol Version 1.3 (2026).
13. IETF RFC 9325 / BCP 195, Recommendations for Secure Use of TLS and DTLS (2022).
14. National Institute of Standards and Technology. Zero Trust Architecture, NIST SP 800-207 (2020). https://csrc.nist.gov/pubs/sp/800/207/final
15. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
16. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
17. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565
18. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565
19. มสพร. 16-2569 มาตรฐานบริการดิจิทัลภาครัฐ เวอร์ชัน 1.0 สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) https://standard.dga.or.th/digital-service-standard/
20. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
21. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง แพลตฟอร์มกลางของงานบริการภาครัฐสำหรับภาคธุรกิจและประชาชน
22. เอกสาร/เงื่อนไขการใช้บริการแพลตฟอร์มดิจิทัลแลกเปลี่ยนข้อมูลของ DGA https://www.dga.or.th/document-sharing/termsandconditions/gdx/
23. บริการ Digital Platform / Services ของ DGA https://www.dga.or.th/our-services/digital-platform-services/
24. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม เรื่องหน้าที่ของผู้ให้บริการในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์
25. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564
26. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

ภาคผนวก 2: กฎหมาย ประกาศ มาตรฐาน และแนวปฏิบัติที่เกี่ยวข้อง

กฎหมาย

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม
- พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 256

ประกาศ

- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565
- ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง แพลตฟอร์มกลางของงานบริการภาครัฐสำหรับภาคธุรกิจและประชาชน
- ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

มาตรฐาน

- มรด. 2-1: 2565: มาตรฐานและหลักเกณฑ์การเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลว่าด้วยเรื่อง กรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (Thailand Government Information eXchange: TGIX)
- มรด. 3-1: 2565: มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ (Government Data Catalog Guideline เวอร์ชัน 1.0)
- มรด. 6: 2566: มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ Data Governance Framework Revised: Guideline เวอร์ชัน 2.0
- มสพร. 8-2565: มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นข้อมูลและการแบ่งปันข้อมูลภาครัฐ (Government Data Classification and Data Sharing Framework)

แนวปฏิบัติ

- NIST SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management (2025)
- OpenAPI Initiative. OpenAPI Specification, Version 3.2.0 (2025)
- IETF RFC 6749, The OAuth 2.0 Authorization Framework (2012)
- IETF RFC 9700 / BCP 240, Best Current Practice for OAuth 2.0 Security (2025)
- IETF RFC 7636, Proof Key for Code Exchange by OAuth Public Clients (2015)
- OpenID Foundation, OpenID Connect Core 1.0 Incorporating Errata Set 2 (2023)
- ISO/IEC 26131:2024, OpenID Connect Core 1.0 Incorporating Errata Set 2.
- IETF RFC 9846, The Transport Layer Security Protocol Version 1.3 (2026).
- IETF RFC 9325 / BCP 195, Recommendations for Secure Use of TLS and DTLS (2022)
- SPDX Specification Version 3.0.1
- ISO/IEC 5962:2021, SPDX Specification V2.2.1
- ECMA-424, CycloneDX Bill of Materials Specification, 2nd Edition (2025)
- World Wide Web Consortium. Web Content Accessibility Guidelines (WCAG) 2.2 (2023). https://www.w3.org/TR/WCAG22/
- OWASP Foundation. Application Security Verification Standard (ASVS) 5.0 (2025) https://owasp.org/www-project-application-security-verification-standard/
- OWASP Foundation. OWASP Top 10: 2025 (2025) https://owasp.org/Top10/
- OWASP Foundation. Web Security Testing Guide (ฉบับปัจจุบัน) https://owasp.org/www-project-web-security-testing-guide/
- Government Digital Service, United Kingdom. Service Standard (ฉบับปัจจุบัน) https://www.gov.uk/service-manual/service-standard
- UK Government. Government Functional Standard GovS 002: Project Delivery (ฉบับปัจจุบัน) https://www.gov.uk/government/publications/project-delivery-functional-standard

- Australian Government Digital Transformation Agency. Digital Service Standard (ฉบับปัจจุบัน)
  https://www.digital.gov.au/policy/digital-experience/digital-service-standard
- Government Technology Agency of Singapore. Digital Service Standards (ฉบับปัจจุบัน)
  https://www.developer.tech.gov.sg/guidelines/standards-and-best-practices/digital-service-standards.html
- National Institute of Standards and Technology. Secure Software Development Framework (SSDF), NIST SP 800-218 (2022)
  https://csrc.nist.gov/pubs/sp/800/218/final

ภาคผนวก 3: อภิธานศัพท์

Zero Trust ไม่ไว้วางใจโดยปริยาย ตรวจสอบและยืนยันสิทธิ์ทุกการเข้าถึง ไม่ว่ามาจากในหรือนอกเครือข่าย

MFA (การยืนยันตัวตนหลายปัจจัย) ยืนยันตัวตนมากกว่าหนึ่งปัจจัย ลดความเสี่ยงถูกสวมรอยแม้รหัสผ่านรั่ว

PAM (การจัดการสิทธิ์ระดับสูง) คุมการเข้าถึงของผู้ดูแลระบบผ่านศูนย์กลาง มีเครื่องกลาง (Bastion) บันทึกเซสชัน และบัญชีฉุกเฉินที่ตรวจสอบได้

HSM ระบบเก็บและบริหารกุญแจเข้ารหัสอย่างปลอดภัย โดย HSM เป็นฮาร์ดแวร์ตามมาตรฐาน FIPS 140-2

TLS 1.2+ โปรโตคอลเข้ารหัสข้อมูลขณะรับส่งบนเครือข่าย บังคับใช้เวอร์ชัน 1.2 ขึ้นไป

WAF ไฟร์วอลล์ระดับแอปพลิเคชัน (Layer 7) กรองการโจมตีเว็บตาม OWASP ก่อนถึงระบบหลังบ้าน

Anti-DDoS ป้องกันการโจมตีแบบถล่มปริมาณทราฟฟิกให้ระบบล่ม โดยสกัดที่ชายขอบเครือข่าย

Audit Log บันทึกการเข้าถึงและแก้ไขที่กันการแก้ย้อนหลัง เก็บอย่างน้อย 90 วัน ตอบได้ว่าใครทำอะไรเมื่อใด

DevSecOps ผนวกความปลอดภัยเข้าในทุกขั้นของการพัฒนาและส่งมอบซอฟต์แวร์แบบอัตโนมัติ

CI/CD ผสานและส่งมอบซอฟต์แวร์อัตโนมัติ ขึ้นระบบผ่านไปป์ไลน์เท่านั้น คนไม่แตะ Production โดยตรง

SAST / DAST ตรวจหาช่องโหว่ในโปรแกรม — SAST วิเคราะห์โค้ดขณะนิ่ง DAST ทดสอบระบบขณะทำงานจริง

SBOM (บัญชีส่วนประกอบซอฟต์แวร์) รายการส่วนประกอบทั้งหมดพร้อมเวอร์ชันและ license ใช้ตรวจช่องโหว่และหยุด build เมื่อพบระดับสูง

IaC (โครงสร้างพื้นฐานในรูปโค้ด) นิยามทรัพยากรโครงสร้างพื้นฐานเป็นโค้ดที่ควบคุมเวอร์ชัน ทำให้สร้างซ้ำและตรวจสอบได้

Landing Zone (Multi-Account) สภาพแวดล้อมคลาวด์พื้นฐานแบบหลายบัญชี แยกบัญชี Production ความปลอดภัย และเก็บ Log พร้อมกรอบควบคุม

BCDR (RTO / RPO) ความต่อเนื่องและกู้คืนระบบ กำหนดเวลาที่ยอมให้ล่ม (RTO) และปริมาณข้อมูลที่ยอมสูญ (RPO)

OpenAPI (OAS) / RESTful API / JSON มาตรฐานเผยแพร่สัญญา API ด้วย OpenAPI 3.0+ โดยใช้ JSON เป็นรูปแบบข้อมูลหลัก

Data Governance (Owner / Steward) ธรรมาภิบาลข้อมูล ทุกชุดข้อมูลมีเจ้าของที่รับผิดชอบ (Owner) และผู้บริบาลดูแลคุณภาพและการเข้าถึง (Steward)

Data Catalog / Metadata ทะเบียนข้อมูลพร้อมคำอธิบาย (metadata) ให้ค้นหาและเข้าใจข้อมูลที่องค์กรมีอยู่

Anonymization (ลบข้อมูลระบุตัวตน) ลบหรือแปลงข้อมูลส่วนบุคคลก่อนนำไปพัฒนา ทดสอบ หรือฝึก AI เพื่อไม่ให้ระบุตัวบุคคลได้

Data Drift ข้อมูลจริงเปลี่ยนไปจากข้อมูลที่ใช้ฝึก ทำให้แบบจำลองแม่นยำลดลง จึงต้องเฝ้าติดตาม

GDX (Government Data Exchange) แพลตฟอร์มกลางสำหรับการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐเพื่อบริการประชาชน

WCAG มาตรฐานออกแบบเว็บให้ทุกคนเข้าถึงได้ บังคับระดับ WCAG 2.1 AA สำหรับแอปพลิเคชันสาธารณะ