



เอกสารข้อกำหนด
(Terms of Reference – TOR)

โครงการศูนย์ข้อมูลการตรวจลงตราของไทย (Visa Data Center - VDC)
เพื่อจัดทำและดูแลระบบตรวจลงตราอิเล็กทรอนิกส์ (e-Visa) ระยะที่ 2

กรมการกงสุล
กระทรวงการต่างประเทศ

123 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง
เขตหลักสี่ กรุงเทพฯ 10210

Handwritten signatures and initials in blue ink, including the name "วิมล" (Vimol) and other illegible marks.

สารบัญ

1. ความเป็นมา
2. วัตถุประสงค์
3. เป้าหมายของโครงการ
4. คุณสมบัติผู้รับจ้าง
 - 4.1 คุณสมบัติทั่วไป
 - 4.2 คุณสมบัติเฉพาะ
5. ขอบเขตของงาน
 - 5.1 คุณสมบัติและจำนวนบุคลากร
 - 5.2 โครงสร้างของระบบแอปพลิเคชัน
 - 5.3 ระบบ e-Visa
 - 5.4 ระบบคลาวด์ e-Visa ระยะที่ 2 (e-Visa Cloud System Phase 2)
 - 5.5 ศูนย์ปฏิบัติการข้อมูลการตรวจลงตรา กรมการกงสุล
 - 5.6 ระบบ Mail Marketing
 - 5.7 ระบบความมั่นคงและความปลอดภัย
 - 5.8 ระบบรักษาความปลอดภัยสำหรับเครื่อง Client
 - 5.9 ระบบสื่อสารเชื่อมโยงข้อมูลกับหน่วยงานอื่น
 - 5.10 ระบบ Web Enquiry
 - 5.11 ระบบ Payment
 - 5.12 การจัดฝึกอบรม
 - 5.13 ระบบสารสนเทศและ Software
 - 5.14 การจัดทำสื่อเพื่อการประชาสัมพันธ์ และสื่อที่ใช้ในการอบรม รวมทั้งข้อมูล และการแปลข้อความต่าง ๆ ในโครงการ
 - 5.15 เงื่อนไขการออกแบบและพัฒนาระบบ การให้บริการและบำรุงรักษา ลิขสิทธิ์ Software
 - 5.16 เงื่อนไขการสิ้นสุดสัญญา
 - 5.17 การจัดทำรายงาน
 - 5.18 การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
 - 5.19 เงื่อนไขการให้บริการในภาพรวมและกรอบระดับการให้บริการ (Service Level Agreement)
6. การทำสัญญา
7. การปฏิบัติตามสัญญา
8. ระยะเวลาดำเนินโครงการ
9. วงเงินงบประมาณ

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

10. เงื่อนไขการส่งมอบงานและการจ่ายเงิน

10.1 การส่งมอบงาน

10.2 การจ่ายเงิน

11. การรับประกัน

12. อัตราค่าปรับ

13. อัตราค่าเสียหาย

14. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

15. เอกสารที่ผู้ยื่นข้อเสนอต้องยื่น

16. ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติม

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

นิยามคำหรือข้อความที่ใช้ในเอกสารนี้

ลำดับ	นิยามคำ/ข้อความ	ความหมาย
1	ผู้ว่าจ้าง	กรมการกงสุล กระทรวงการต่างประเทศ
2	ผู้ยื่นข้อเสนอ	ผู้เข้าร่วมการประกวดราคาทางอิเล็กทรอนิกส์โครงการศูนย์ข้อมูลการตรวจลงตราของไทย (Visa Data Center - VDC) เพื่อจัดทำและดูแลระบบตรวจลงตราอิเล็กทรอนิกส์ (e-Visa) ระยะที่ 2 แต่ยังไม่เป็นผู้รับจ้าง
3	ผู้รับจ้าง	ผู้ชนะการประกวดราคาทางอิเล็กทรอนิกส์ที่มีคุณสมบัติตามที่กำหนด และได้ลงนามในสัญญาโครงการศูนย์ข้อมูลการตรวจลงตราของไทย (Visa Data Center - VDC) เพื่อจัดทำและดูแลระบบตรวจลงตราอิเล็กทรอนิกส์ (e-Visa) ระยะที่ 2
4	VDC	ศูนย์ข้อมูลการตรวจลงตราของไทย (Visa Data Center)
5	ระบบ e-Visa	ระบบตรวจลงตราอิเล็กทรอนิกส์ ระบบ Mobile Application อาจรวมถึงระบบ ABTC และระบบอื่นใดในโครงการ
6	ระบบ e-Visa ระยะที่ 1	ระบบตรวจลงตราอิเล็กทรอนิกส์เดิมที่ใช้งานอยู่ในปัจจุบัน
7	ระบบ e-Visa ระยะที่ 2	โครงการศูนย์ข้อมูลการตรวจลงตราของไทย (Visa Data Center - VDC) เพื่อจัดทำและดูแลระบบตรวจลงตราอิเล็กทรอนิกส์ (e-Visa) ระยะที่ 2
8	ระบบคลาวด์ e-Visa	ระบบคลาวด์ของระบบตรวจลงตราอิเล็กทรอนิกส์ (e-Visa) ระยะที่ 2 ที่ใช้ในโครงการ
9	ศูนย์ปฏิบัติการ ข้อมูลการตรวจ ลงตรา ภายในประเทศ	สถานที่ปฏิบัติงานด้านข้อมูลการตรวจลงตรา ที่กรมการกงสุล กระทรวงการต่างประเทศ
10	ผู้ยื่นคำร้อง	ผู้ยื่นแบบบุคคลทั่วไป (individual) ผู้ยื่นคำร้องแบบกลุ่ม (group) และผู้ยื่นคำร้องแบบ agent
11	Centralized Consular Data Center (CCDC)	ศูนย์บริหารข้อมูลกลางกรมการกงสุล กระทรวงการต่างประเทศ
12	Consular Gateway	ระบบ Gateway กลางเพื่อเชื่อมโยงข้อมูลระหว่างกรมการกงสุล กระทรวงการต่างประเทศ กับหน่วยงานภายในและภายนอก
13	ระบบ Mobile Application	ระบบ Mobile Application “Thai e-Visa” ของ Front Office ระบบ Mobile Application “Thai e-Visa” ของ Back Office และ ระบบ Mobile Application “Visa Checking”

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

1. ความเป็นมา

กรมการกงสุล กระทรวงการต่างประเทศ ได้ดำเนินโครงการศูนย์ข้อมูลการตรวจลงตราของไทย (Visa Data Center - VDC) ซึ่งได้จัดทำและดูแลระบบตรวจลงตราอิเล็กทรอนิกส์ (e-Visa) ระยะที่ 1 ตั้งแต่ปี 2560 เพื่ออำนวยความสะดวกแก่คนต่างชาติที่ประสงค์จะเดินทางเข้าประเทศไทย โดยผู้ยื่นคำร้องขอรับการตรวจลงตราสามารถกรอกและส่งข้อมูลขอรับการตรวจลงตราตามขั้นตอนที่กำหนดในระบบต่อสถานเอกอัครราชทูตหรือสถานกงสุลใหญ่ได้ทุกที่ตลอดเวลาตลอด 24 ชั่วโมง ผ่าน web application: www.thaievisa.go.th โดยไม่ต้องเดินทางไปยื่นเอกสารที่สถานเอกอัครราชทูตหรือสถานกงสุลใหญ่ด้วยตนเอง ในส่วนของเจ้าหน้าที่กงสุลสามารถตรวจสอบข้อมูลของผู้ยื่นคำร้องและเอกสารประกอบ และพิจารณาอนุมัติการตรวจลงตราจากระบบฯ ได้โดยตรง ทำให้การตรวจลงตราเป็นไปด้วยความรวดเร็ว ประหยัดเวลา โปร่งใส และมีประสิทธิภาพ นอกจากนี้ กรมการกงสุล กระทรวงการต่างประเทศ ยังได้พัฒนาระบบการแจ้งผลการอนุมัติการตรวจลงตราด้วยระบบไปรษณีย์อิเล็กทรอนิกส์ไปยังผู้ร้องโดยตรง พร้อมส่งผลการอนุมัติการตรวจลงตราแบบ real-time ไปยังหน่วยงานที่เกี่ยวข้อง อาทิ สำนักงานตรวจคนเข้าเมือง เพื่อใช้ในการคัดกรองคนเข้าเมืองที่สามารถตรวจสอบย้อนกลับข้อมูลการตรวจลงตราได้

โดยที่ระบบดังกล่าวได้รับการพัฒนาและใช้งานเป็นระยะเวลาหลายปีแล้ว กรมการกงสุล กระทรวงการต่างประเทศ จึงประสงค์ที่จะจัดทำโครงการ VDC เพื่อจัดทำ พัฒนา และดูแลระบบตรวจลงตราอิเล็กทรอนิกส์ (e-Visa) ระยะที่ 2 ให้เป็นระบบการตรวจลงตราอิเล็กทรอนิกส์ที่ทันสมัย ครอบคลุมมีประสิทธิภาพสูงขึ้น มีความรวดเร็วของระบบและกระบวนการดำเนินการที่เกี่ยวข้องต่าง ๆ มากขึ้น โดยใช้ระบบเทคโนโลยีสารสนเทศที่ทันสมัย ซึ่งจะตอบโจทยนโยบายการขยายการให้บริการ e-Visa ไปยังสถานเอกอัครราชทูตและสถานกงสุลใหญ่ของไทยทั่วโลกของกระทรวงการต่างประเทศในอนาคต เพื่อรองรับการขอรับการตรวจลงตราที่เพิ่มมากขึ้น และยังเป็นส่วนสำคัญในการขับเคลื่อนเศรษฐกิจของประเทศภายหลังสถานการณ์การแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 (โควิด-2019) รวมทั้งยังเป็นการขยาย e-Service ในการให้บริการประชาชนซึ่งสอดคล้องกับการก้าวไปสู่การเป็น e-Government ของรัฐบาล

2. วัตถุประสงค์

2.1 เพื่อให้มีผู้ดูแลโครงการ VDC ระบบสารสนเทศและอุปกรณ์ที่เกี่ยวข้องในภาพรวม เพื่อสนับสนุนภารกิจของกรมการกงสุล กระทรวงการต่างประเทศ ในการอำนวยความสะดวกแก่ผู้ยื่นคำร้องในการให้บริการตรวจลงตราอิเล็กทรอนิกส์ (e-Visa)

2.2 เพื่อให้มีผู้จัดทำ พัฒนา และดูแลโครงการ VDC ระบบ e-Visa ระยะที่ 2 ระบบสารสนเทศ อุปกรณ์ที่เกี่ยวข้อง ในการอำนวยความสะดวกและสนับสนุนภารกิจแก่สถานเอกอัครราชทูตและสถานกงสุลใหญ่ ในการพิจารณาคำร้องขอรับการตรวจลงตราอิเล็กทรอนิกส์ของคนต่างชาติ

2.3 เพื่อให้มีผู้จัดทำ พัฒนา และดูแลโครงการ VDC ระบบ e-Visa ระยะที่ 2 ระบบสารสนเทศ อุปกรณ์ที่เกี่ยวข้องในการอำนวยความสะดวกและสนับสนุนภารกิจแก่กรมการกงสุล กระทรวงการต่างประเทศ ในการบริหารจัดการระบบการตรวจลงตราอิเล็กทรอนิกส์ (e-Visa) ให้มีประสิทธิภาพ มีความยืดหยุ่น และสามารถปรับเปลี่ยนหรือลดประเภทการตรวจลงตรา เงื่อนไขการตรวจลงตรา หรือเงื่อนไขต่าง ๆ ที่เกี่ยวข้องในอนาคตได้

2.4 เพื่อให้มีผู้จัดทำ พัฒนา และดูแลโครงการ VDC ระบบ e-Visa ระยะที่ 2 ระบบสารสนเทศ อุปกรณ์ที่เกี่ยวข้องในการอำนวยความสะดวก การให้ข้อมูล และการประสานงานกับหน่วยงานความมั่นคงอื่น ๆ ที่ต้อง

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

เชื่อมโยงข้อมูลและบูรณาการการดำเนินการที่เกี่ยวข้องกับกรมการกงสุล กระทรวงการต่างประเทศ เพื่อเพิ่มประสิทธิภาพในการคัดกรองคนเข้าเมือง

2.5 เพื่อให้ผู้จัดทำ พัฒนา และดูแลโครงการ VDC ระบบ e-Visa ระยะที่ 2 ระบบสารสนเทศ อุปกรณ์ที่เกี่ยวข้องของกรมการกงสุล กระทรวงการต่างประเทศ โดยรับผิดชอบช่วงการเปลี่ยนผ่านจากระบบ e-Visa ระยะที่ 1 ไปยังระยะที่ 2 ในการถ่ายโอนและสำรองข้อมูลจากระบบเดิม (ระยะที่ 1) ไปยังระบบใหม่ (ระยะที่ 2) รวมทั้งปรับปรุงระบบอย่างต่อเนื่องในส่วนที่จำเป็นเพื่อให้ระบบดำเนินต่อไปได้อย่างมีประสิทธิภาพ สอดคล้องกับการกิจ หรือตามนโยบายที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

3. เป้าหมายของโครงการ

เพื่อให้ผู้จัดทำ พัฒนา ดูแลโครงการ VDC สำหรับระบบ e-Visa ระยะที่ 2 ระบบสารสนเทศ และอุปกรณ์ที่เกี่ยวข้องของกรมการกงสุล กระทรวงการต่างประเทศ โดยจะต้องจัดทำและพัฒนาระบบให้มีลักษณะแบบ scalable และมีความยืดหยุ่น สามารถปรับเปลี่ยนเงื่อนไขและเพิ่มหรือลดประเภทการตรวจลงตรา และคุณสมบัติผู้ยื่นคำร้องต่าง ๆ ได้ทันทีจากระบบส่วนกลาง สามารถสร้างรายงานเชิงลึกทั้งในเชิงการดำเนินการ และสถิติการตรวจลงตราตามเงื่อนไขต่าง ๆ ที่กำหนดได้ และมีระบบที่เชื่อมโยงข้อมูลรวมทั้งการอนุมัติ หรืออนุญาตกับหน่วยงานภายนอกที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด เพื่อให้การคัดกรอง คนเข้าเมืองมีประสิทธิภาพสูงสุดและสามารถอำนวยความสะดวกแก่ผู้ยื่นคำร้องขอรับการตรวจลงตรา ได้มากขึ้น อันจะเป็นปัจจัยสำคัญในการส่งเสริมให้คนต่างชาติเดินทางเข้าประเทศไทยมากขึ้นตามนโยบาย ของรัฐบาล รวมทั้งต้องพร้อมให้เจ้าหน้าที่กรมการกงสุล กระทรวงการต่างประเทศ มีส่วนร่วมในการพัฒนา และตรวจสอบระบบตลอดโครงการด้วย

4. คุณสมบัติของผู้รับจ้าง

4.1 คุณสมบัติทั่วไป

- 4.1.1 มีความสามารถตามกฎหมาย
- 4.1.2 ไม่เป็นบุคคลล้มละลาย
- 4.1.3 ไม่อยู่ระหว่างเลิกกิจการ
- 4.1.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการ กระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง
- 4.1.5 ไม่เป็นบุคคลซึ่งถูกระงับชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงาน ของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงาน เป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย
- 4.1.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายจัดซื้อจัดจ้างและการบริหาร พัสดุภาครัฐกำหนดในราชกิจจานุเบกษา
- 4.1.7 เป็นนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว
- 4.1.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้รับจ้างรายอื่นที่เข้ายื่นข้อเสนอให้แก่กรมการกงสุล กระทรวง การต่างประเทศ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวาง การแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ในครั้งนี้
- 4.1.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาล ของผู้รับจ้างได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นนั้น

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

4.1.10 ผู้รับจ้างต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement e-GP) ของกรมบัญชีกลาง

4.1.11 ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคล

4.1.12 มูลค่าสุทธิของกิจการ

(1) กรณีผู้รับจ้างเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(2) กรณีผู้รับจ้างเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งยังไม่มีงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียนโดยผู้รับจ้างจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ โดยต้องมีทุนจดทะเบียนไม่ต่ำกว่า 20,000,000 บาท เนื่องจากมูลค่าการจัดซื้อจัดจ้างเกิน 60,000,000 บาท แต่ไม่เกิน 150,000,000 บาท

4.1.13 คู่สัญญาต้องจัดทำและแสดงแผนการทำงานภายใน 30 วัน นับถัดจากวันลงนามในสัญญา

4.2 คุณสมบัติเฉพาะ

ผู้รับจ้างต้องเคยมีผลงานประเภทเดียวกัน (งานพัฒนาระบบสารสนเทศ) กับงานที่จ้างในวงเงินไม่น้อยกว่า 20,000,000 บาท ในสัญญาเดียวและเป็นผลงานที่เสร็จสิ้นแล้วไม่เกิน 5 ปี นับถึงวันยื่นเอกสารเสนอราคาพร้อมรับรองสำเนาถูกต้อง ทั้งนี้ ผู้เสนอราคาจะได้คะแนนเพิ่มขึ้นตามเกณฑ์การให้คะแนน โดยผลงานดังกล่าวจะต้องเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับส่วนราชการ หน่วยงานตามกฎหมายว่าด้วยระเบียบบริหารราชการส่วนท้องถิ่น หน่วยงานอื่นซึ่งมีกฎหมายบัญญัติให้มีฐานะเป็นราชการบริหารส่วนท้องถิ่น รัฐวิสาหกิจ หรือหน่วยงานเอกชนที่เชื่อถือได้

5. ขอบเขตของงาน

5.1 คุณสมบัติและจำนวนบุคลากร

5.1.1 ทีมบริหารโครงการ (จำนวนรวมอย่างน้อย 4 คน)

5.1.1.1 หัวหน้าโครงการ (Project Manager) จำนวนอย่างน้อย 1 คน มีคุณสมบัติ ดังนี้

- (1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาโทด้านเทคโนโลยีสารสนเทศ หรือสาขาคอมพิวเตอร์ หรือสาขาการบริหารจัดการเทคโนโลยี หรือสาขาอื่นใดที่เกี่ยวข้อง
- (2) มีประสบการณ์ไม่น้อยกว่า 10 ปี ในการบริหารโครงการที่เกี่ยวข้องกับการพัฒนาระบบสารสนเทศ โดยการบริหารแต่ละโครงการต้องมีมูลค่าไม่น้อยกว่า 15 ล้านบาท และไม่น้อยกว่า 3 โครงการ โดยเป็นโครงการที่ตรวจรับเสร็จสิ้นแล้ว

5.1.1.2 ผู้ประสานงานโครงการ จำนวนอย่างน้อย 2 คน มีคุณสมบัติ ดังนี้

- (1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี
- (2) มีประสบการณ์ทำงานประสานงานโครงการภาครัฐ รวมกันไม่น้อยกว่า 3 ปี

5.1.1.3 ผู้เชี่ยวชาญด้านภาษาอังกฤษ จำนวนอย่างน้อย 1 คน มีคุณสมบัติ ดังนี้

- (1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี
- (2) สามารถใช้ภาษาอังกฤษในการฟัง พูด อ่าน และเขียนได้เป็นอย่างดี และมีผลการทดสอบภาษาอังกฤษ IELTS ได้คะแนนไม่ต่ำกว่า 6 หรือ TOEFL ได้คะแนนไม่ต่ำกว่า 79 คะแนน (Internet-base) โดยผลการสอบมีอายุไม่เกิน 2 ปี นับถึงวันที่ยื่นข้อเสนอ

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

5.1.2 ทีมพัฒนาระบบ (จำนวนรวมอย่างน้อย 24 คน)

5.1.2.1 นักวิเคราะห์และออกแบบระบบ (System Analyst) จำนวนอย่างน้อย 3 คน
มีคุณสมบัติ ดังนี้

- (1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี สาขาเทคโนโลยีสารสนเทศและการสื่อสาร หรือสาขาวิทยาการคอมพิวเตอร์ หรือสาขาวิศวกรรมคอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้อง
- (2) มีประสบการณ์ในการวิเคราะห์ ออกแบบระบบ การวางระบบ และการเชื่อมโยงระบบ ไม่น้อยกว่า 5 ปี

5.1.2.2 นักออกแบบ UX (User Experience) และ UI (User Interface) จำนวนอย่างน้อย 2 คน มีคุณสมบัติ ดังนี้

- (1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขา คอมพิวเตอร์ หรือสาขาการบริหารจัดการเทคโนโลยี หรือสาขาการออกแบบดิจิทัล หรือสาขาอื่นใดที่เกี่ยวข้อง
- (2) มีประสบการณ์ในออกแบบประสบการณ์การใช้งาน (UX) และส่วนต่อประสาน กับผู้ใช้งาน (UI) ไม่น้อยกว่า 3 ปี

5.1.2.3 นักเขียนโปรแกรม (Programmer) จำนวนอย่างน้อย 13 คน มีคุณสมบัติ ดังนี้

- (1) นักเขียนโปรแกรมอาวุโส (Senior Programmer) จำนวนอย่างน้อย 3 คน
 - (1.1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี สาขาเทคโนโลยีสารสนเทศ และการสื่อสาร หรือสาขาวิทยาการคอมพิวเตอร์ หรือสาขาวิศวกรรมคอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้อง
 - (1.2) มีประสบการณ์ในการพัฒนาระบบสารสนเทศ มากกว่า 5 ปี
- (2) นักเขียนโปรแกรม (Junior Programmer) จำนวนอย่างน้อย 10 คน
 - (2.1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี สาขาเทคโนโลยีสารสนเทศ และการสื่อสาร หรือสาขาวิทยาการคอมพิวเตอร์ หรือสาขาวิศวกรรมคอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้อง
 - (2.2) มีประสบการณ์ในการพัฒนาระบบสารสนเทศมากกว่า 2 ปี

5.1.2.4 นักทดสอบระบบ (Software Tester) จำนวนอย่างน้อย 2 คน มีคุณสมบัติ ดังนี้

- (1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี สาขาเทคโนโลยีสารสนเทศและการสื่อสาร หรือสาขาวิทยาการคอมพิวเตอร์ หรือสาขาวิศวกรรมคอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้อง
- (2) มีประสบการณ์ในการทดสอบระบบอย่างน้อย 2 ปี

5.1.2.5 เจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์ จำนวนอย่างน้อย 1 คน มีคุณสมบัติ ดังนี้

- (1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี สาขาเทคโนโลยีสารสนเทศและการสื่อสาร หรือสาขาวิทยาการคอมพิวเตอร์ หรือสาขาวิศวกรรมคอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้อง
- (2) มีประสบการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ไม่น้อยกว่า 3 ปี
- (3) ได้รับการรับรอง Certification ทางด้าน IT Security อย่างน้อยได้แก่ CCSP หรือ Certification อื่นใดที่อยู่ในระดับ (Tiers) เทียบเท่าหรือสูงกว่าข้างต้น

5.1.2.6 ผู้เชี่ยวชาญระบบคลาวด์ (Cloud Engineer) จำนวนอย่างน้อย 3 คน

- (1) ผู้เชี่ยวชาญระบบคลาวด์อาวุโส (Senior Cloud Engineer) จำนวนอย่างน้อย 1 คน
 - (1.1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี สาขาเทคโนโลยีสารสนเทศ และการสื่อสาร หรือสาขาวิทยาการคอมพิวเตอร์ หรือสาขาวิศวกรรมคอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้อง
 - (1.2) มีประสบการณ์ทำงานที่เกี่ยวข้องไม่น้อยกว่า 5 ปี

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ 380/15 กรรมการ กรรมการ กรรมการ

(1.3) ได้รับ AWS Certified Solutions Architect – Associate หรือ Microsoft Certified: Azure Administrator Associate หรือ Associate Cloud Engineer หรือ Certificate ของผู้ให้บริการ Cloud service อื่นใดที่เกี่ยวข้องและเทียบเท่าหรือสูงกว่าข้างต้น

(1.4) ได้รับ AWS Certified Developer – Associate หรือ Microsoft Certified: Azure Developer Associate หรือ Associate Cloud Engineer หรือ Certificate ของผู้ให้บริการ Cloud service อื่นใดที่เกี่ยวข้องและเทียบเท่าหรือสูงกว่าข้างต้น โดย Certificate ที่ได้รับ จะต้องตรงกับระบบคลาวด์ที่ผู้รับจ้างยื่นข้อเสนอ

(2) ผู้เชี่ยวชาญระบบคลาวด์ (Cloud Engineer) จำนวนอย่างน้อย 2 คน

(2.1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี สาขาเทคโนโลยีสารสนเทศและการสื่อสาร หรือสาขาวิทยาการคอมพิวเตอร์ หรือสาขาวิศวกรรมคอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้อง

(2.2) มีประสบการณ์ทำงานที่เกี่ยวข้องไม่น้อยกว่า 2 ปี

(2.3) ได้รับ AWS Certified Cloud Practitioner หรือ Microsoft Certified: Azure Fundamentals หรือ Google Cloud Digital Leader หรือ Certificate ของผู้ให้บริการ Cloud service อื่นใดที่เกี่ยวข้องและเทียบเท่าหรือสูงกว่าข้างต้น โดย Certificate ที่ได้รับจะต้องตรงกับระบบคลาวด์ที่ผู้รับจ้างยื่นข้อเสนอ เป็นอย่างน้อย 1 คน

(2.4) ได้รับ AWS Certified Solutions Architect – Associate หรือ Microsoft Certified: Azure Administrator Associate หรือ Associate Cloud Engineer หรือ Certificate ของผู้ให้บริการ Cloud service อื่นใดที่เกี่ยวข้องและเทียบเท่าหรือสูงกว่าข้างต้น โดย Certificate ที่ได้รับจะต้องตรงกับระบบคลาวด์ที่ผู้รับจ้างยื่นข้อเสนอ อย่างน้อย 1 คน

5.1.3 ทีมปฏิบัติงาน จำนวนรวมอย่างน้อย 10 คน

5.1.3.1 ผู้เชี่ยวชาญด้านระบบเครือข่าย จำนวนอย่างน้อย 1 คน

(1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี สาขาเทคโนโลยีสารสนเทศและการสื่อสาร หรือสาขาวิทยาการคอมพิวเตอร์ หรือสาขาวิศวกรรมคอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้อง

(2) มีประกาศนียบัตรหรือใบรับรอง CCNP Security หรือเทียบเท่า

(3) มีประสบการณ์ด้านระบบเครือข่ายไม่น้อยกว่า 3 ปี

5.1.3.2 เจ้าหน้าที่สนับสนุนโครงการ (Team Support) จำนวนอย่างน้อย 6 คน โดยมีเจ้าหน้าที่อย่างน้อย 1 คนต่อกะ เพื่อให้มีการปฏิบัติงานต่อเนื่องตลอด 24 ชม. 7 วัน มีคุณสมบัติ ดังนี้

(1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี สาขาเทคโนโลยีสารสนเทศและการสื่อสาร หรือสาขาวิทยาการคอมพิวเตอร์ หรือสาขาวิศวกรรมคอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้อง

(2) มีประสบการณ์ในการทำงานด้านการสนับสนุนด้านเทคโนโลยีสารสนเทศไม่น้อยกว่า 2 ปี

5.1.3.3 เจ้าหน้าที่กฎหมาย จำนวนอย่างน้อย 1 คน มีคุณสมบัติ ดังนี้

(1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี ในสาขาที่เกี่ยวข้องกับกฎหมาย

(2) มีประสบการณ์ในการทำงานด้านกฎหมายไม่น้อยกว่า 2 ปี

(3) ปฏิบัติงาน ณ กองตรวจลงตราและเอกสารเดินทางคนต่างด้าว กรมการกงสุล กระทรวงการต่างประเทศ หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

5.1.3.4 เจ้าหน้าที่ด้านเทคนิค จำนวนอย่างน้อย 2 คน

(1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี สาขาเทคโนโลยีสารสนเทศและการสื่อสาร หรือสาขาวิทยาการคอมพิวเตอร์ หรือสาขาวิศวกรรมคอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้อง

(2) มีประสบการณ์ในการทำงานด้านการสนับสนุนด้านเทคโนโลยีสารสนเทศ ไม่น้อยกว่า 2 ปี

(3) ปฏิบัติงาน ณ กองตรวจลงตราและเอกสารเดินทางคนต่างด้าว กรมการกงสุล กระทรวงการต่างประเทศ หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

ลำดับ	หน้าที่รับผิดชอบ	จำนวน อย่างน้อย (คน)	ประสบการณ์ ขั้นต่ำ (ปี)	สถานที่ปฏิบัติงาน
ทีมบริหาร				
1	หัวหน้าโครงการ (Project Manager)	1	10	กรมการกงสุล / สถานที่ของผู้รับจ้าง
2	ผู้ประสานงานโครงการ	2	3	กรมการกงสุล / สถานที่ของผู้รับจ้าง
3	ผู้เชี่ยวชาญด้านภาษาอังกฤษ	1	-	กรมการกงสุล / สถานที่ของผู้รับจ้าง
ทีมพัฒนาระบบ				
4	นักวิเคราะห์และออกแบบระบบ (System Analyst)	3	5	กรมการกงสุล / สถานที่ของผู้รับจ้าง
5	นักออกแบบ UX (User Experience) และ UI (User Interface)	2	3	กรมการกงสุล / สถานที่ของผู้รับจ้าง
6	นักเขียนโปรแกรมอาวุโส (Senior Programmer)	3	5	กรมการกงสุล / สถานที่ของผู้รับจ้าง
7	นักเขียนโปรแกรม (Junior Programmer)	10	2	กรมการกงสุล / สถานที่ของผู้รับจ้าง
8	นักทดสอบระบบ (Software Tester)	2	2	กรมการกงสุล / สถานที่ของผู้รับจ้าง
9	เจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์	1	3	กรมการกงสุล / สถานที่ของผู้รับจ้าง
10	ผู้เชี่ยวชาญระบบคลาวด์อาวุโส (Senior Cloud Engineer)	1	5	กรมการกงสุล / สถานที่ของผู้รับจ้าง
11	ผู้เชี่ยวชาญระบบคลาวด์ (Cloud Engineer)	2	2	กรมการกงสุล / สถานที่ของผู้รับจ้าง

ประธานกรรมการ กรรมการ กรรมการ

กรรมการ กรรมการ กรรมการ กรรมการ

ทีมปฏิบัติงาน				
12	ผู้เชี่ยวชาญด้านระบบเครือข่าย	1	3	กรมการกงสุล / สถานที่ของผู้รับจ้าง
13	เจ้าหน้าที่สนับสนุนโครงการ (Team Support)	6	2	กรมการกงสุล / สถานที่ของผู้รับจ้าง
14	เจ้าหน้าที่กฎหมาย	1	2	กรมการกงสุล
15	เจ้าหน้าที่ด้านเทคนิค	2	2	กรมการกงสุล

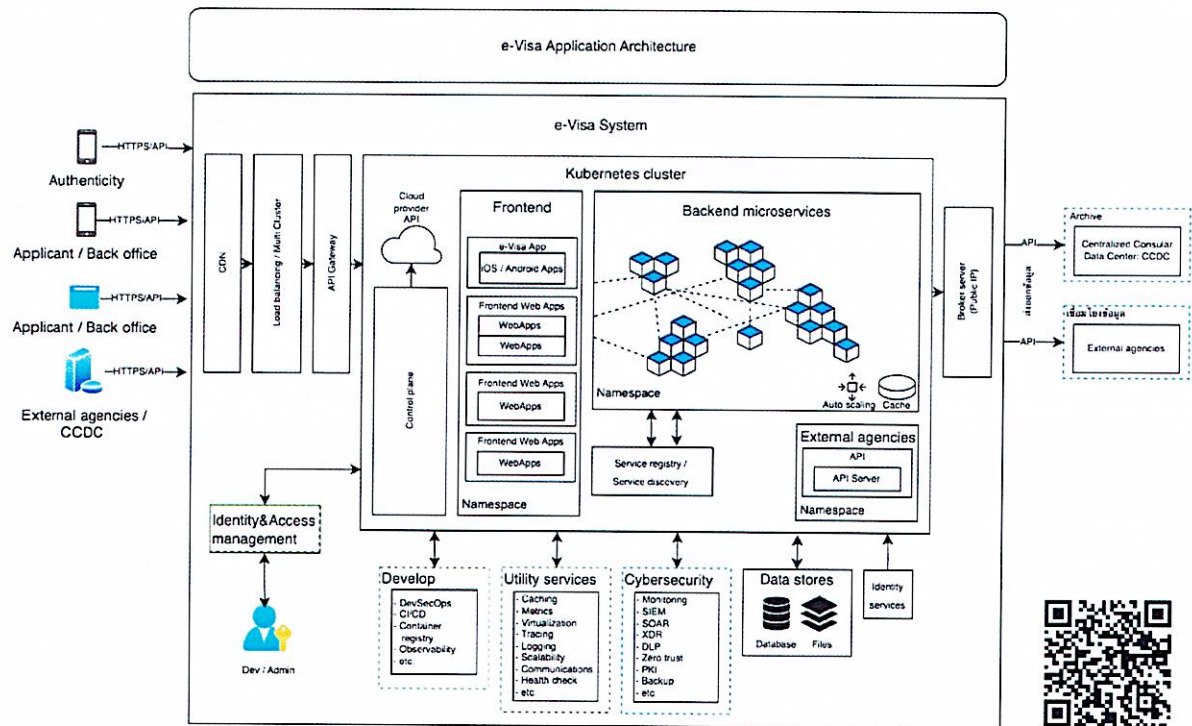
5.1.3.5 ใบประกาศนียบัตรหรือใบรับรองของบุคลากรที่ยื่นข้อเสนอทั้งหมดต้องมีอายุจนถึงวันที่ยื่นข้อเสนอ และต้องต่ออายุให้ครอบคลุมตลอดระยะเวลาตามสัญญา

5.1.3.6 กรณีมีการเปลี่ยนแปลงบุคลากรในโครงการ ผู้รับจ้างต้องจัดหาบุคลากรที่มีใบประกาศนียบัตรหรือใบรับรองเทียบเท่าบุคลากรเดิมมาทดแทน และต้องได้รับความเห็นชอบจากกรมการกงสุล กระทรวงการต่างประเทศ

5.2 โครงสร้างของระบบแอปพลิเคชัน

ออกแบบและพัฒนาระบบ e-Visa โดยการใช้ประโยชน์จากรูปแบบการให้บริการของคลาวด์ (Cloud Service Model) แบบ Cloud Native Application มีการติดตั้ง Infrastructure และตั้งค่าทั้งหมดอยู่ในรูปของ Script โดยการทำ Infrastructure as Code ใช้เทคโนโลยีคอนเทนเนอร์ (Container) พัฒนาระบบโปรแกรมที่แบ่งแยกแอปพลิเคชันเป็นส่วนย่อย (Microservices) มีระบบจัดการคลัสเตอร์แบบอัตโนมัติที่ใช้ในการทำงานด้วย Kubernetes Cluster ใช้กระบวนการพัฒนาและการดูแลรักษาระบบทั้งหมดด้วย DevSecOps และกระบวนการทำงานอัตโนมัติ ทดสอบ และการนำทางเป็นไปอย่างรวดเร็วด้วย CI/CD Pipeline และมีกระบวนการควบคุมเวอร์ชัน (Version Control) ที่ใช้ในการจัดเก็บ บริหาร และส่งมอบโค้ดของโปรเจกต์ซอฟต์แวร์ (Source code) ผ่านระบบจัดเก็บข้อมูลดิจิทัลแบบรวมศูนย์ (Git Repository Management) ที่กรมการกงสุล กระทรวงการต่างประเทศ เตรียมไว้ให้ และออกแบบระบบเพื่อรองรับเทคโนโลยี Zero Trust Network Access (ZTNA) โดยมีการตรวจสอบสิทธิ์และอนุญาตการเข้าถึงระบบในทุกระดับอย่างเข้มงวด ระบบจะตรวจสอบผู้ใช้งานและอุปกรณ์ทุกครั้งก่อนที่จะให้สิทธิ์การเข้าถึงข้อมูลหรือทรัพยากร โดยมีรายละเอียดการออกแบบระบบดังรูปภาพ Application architecture diagram ดังปรากฏตามด้านล่าง

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ



รูปภาพ Application architecture diagram

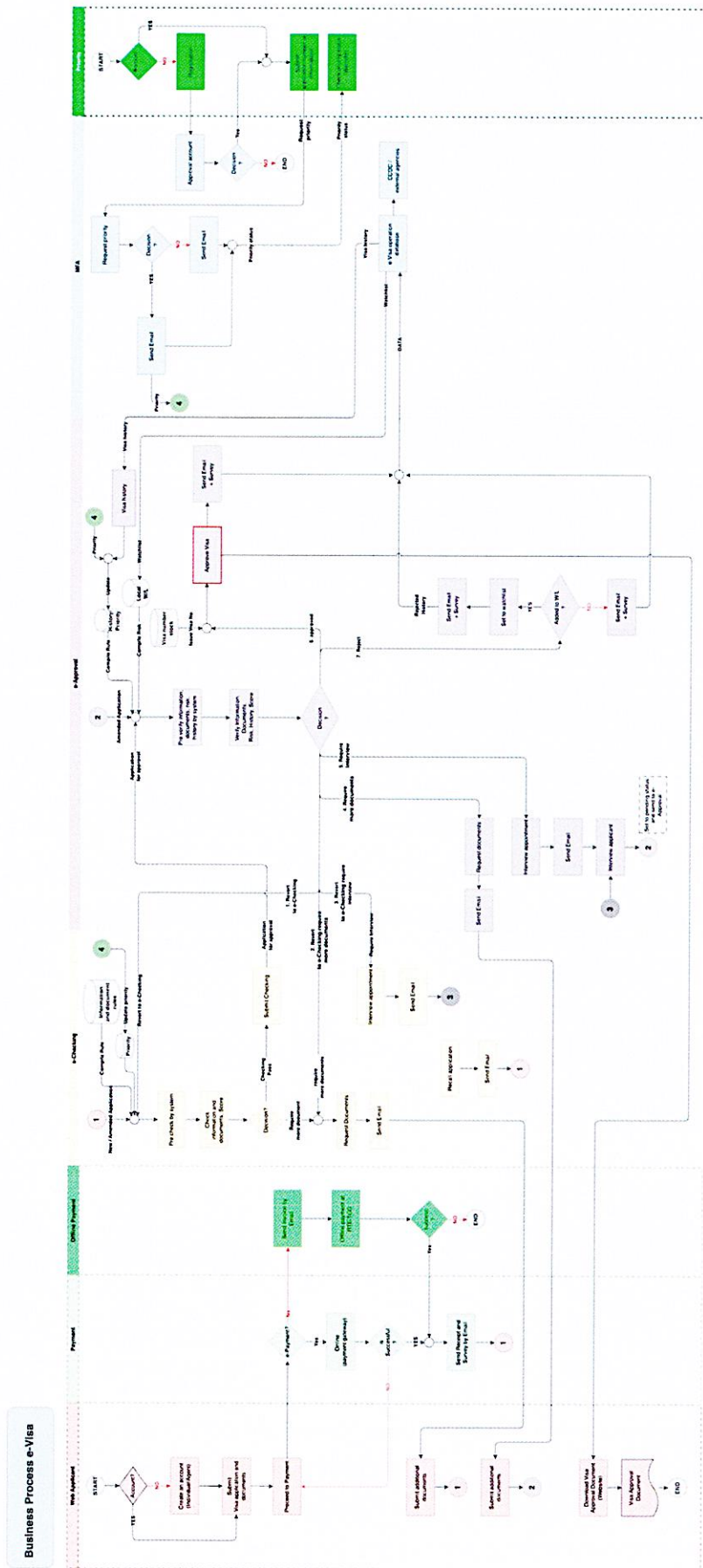
<https://1drv.ms/i/s!Ap8pk0aBGx6Cq8ROWmpM6TX17NRptw?e=twDXRF>

ทั้งนี้ หากผู้รับจ้างสามารถเสนอหรือปรับเปลี่ยนโครงสร้างระบบแอปพลิเคชันได้ตามความเหมาะสม หากผู้รับจ้างแสดงให้เห็นว่าที่เสนอมานี้ดีกว่า และกรมการกงสุล กระทรวงการต่างประเทศไม่เสียเปรียบกับข้อเสนอดังกล่าว

5.3 ระบบ e-Visa

ผู้รับจ้างจะต้องออกแบบ พัฒนา และดูแลระบบให้สอดคล้องกับ Business Process ของกระทรวงการต่างประเทศ ดังปรากฏในแผนภาพ Business Process e-Visa ด้านล่างนี้ และจะต้องมีคุณสมบัติอย่างน้อย ดังต่อไปนี้

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ



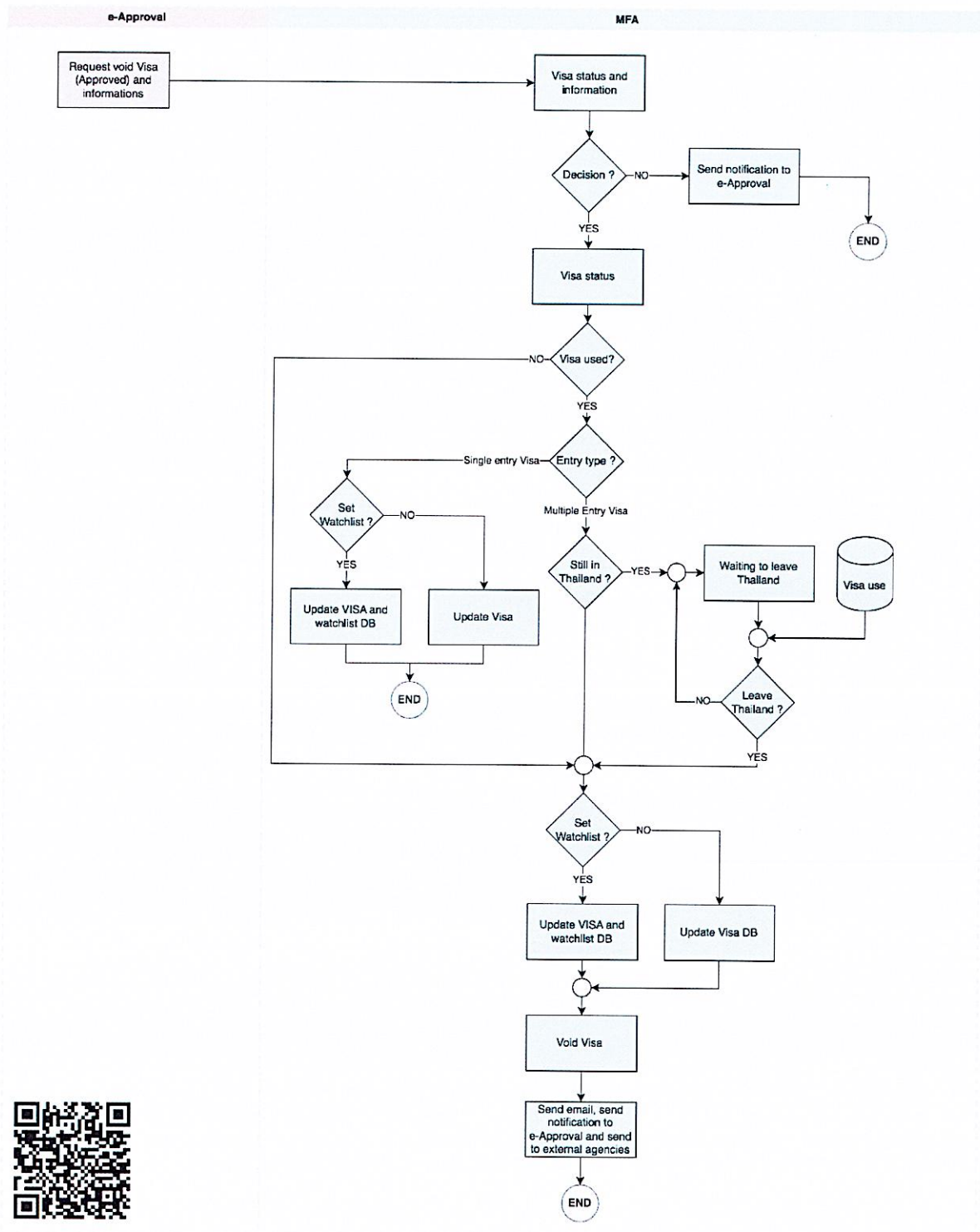
แผนภาพ Business Process e-Visa

<https://1drv.ms/f/s!Ap8pk0aBGx6Cq9cONX97wwMI623A6Q?e=LOUJaC>

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ 3.9 0.7/5 กรรมการ กรรมการ กรรมการ

Business Process e-Visa (Extended)

Request void Visa



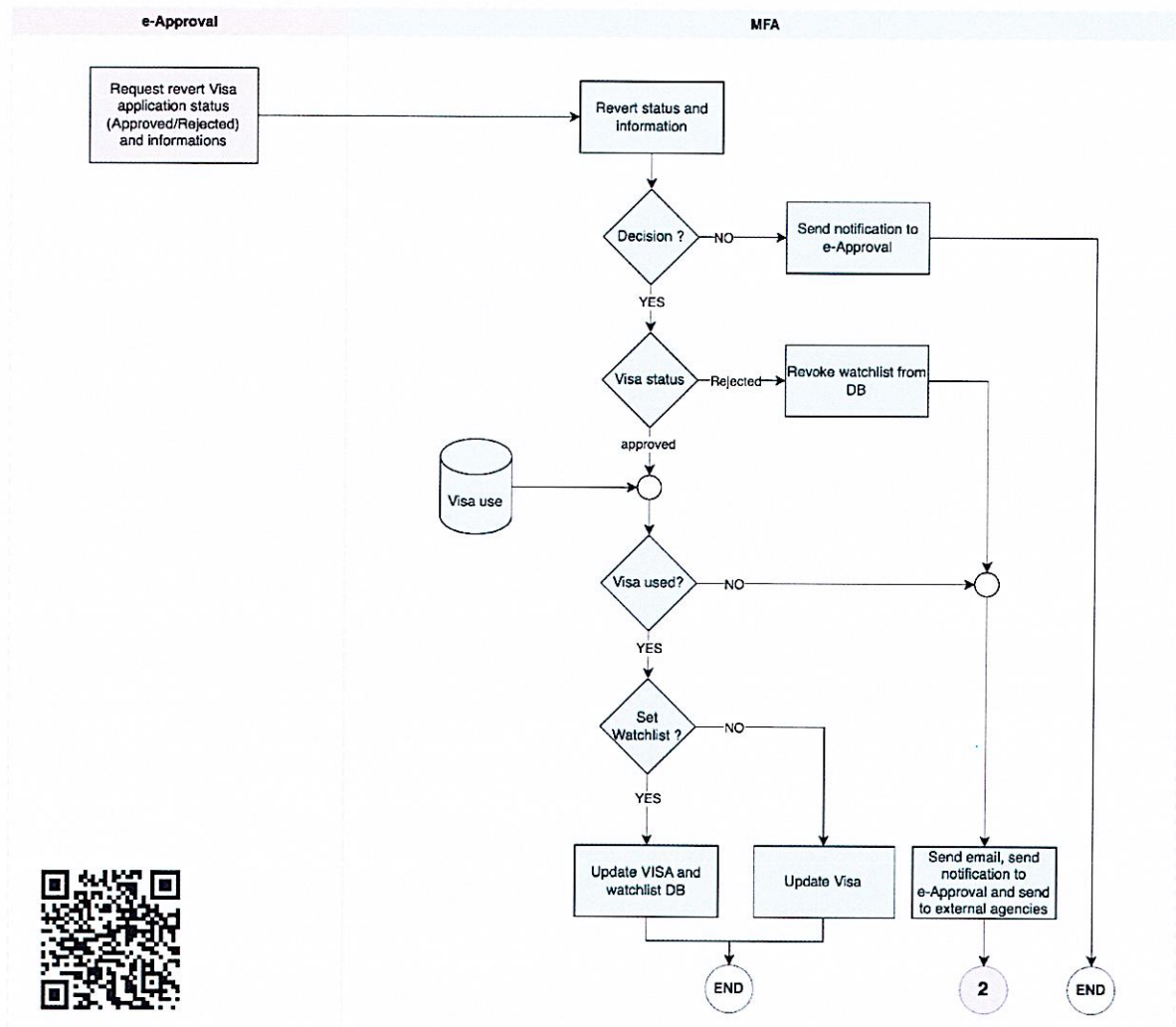
แผนภาพ Business Process e-Visa (extended) Request Void Visa

https://1drv.ms/i/s!Ap8pk0aBGx6Cq9L_A7nC1L9iu07i9O?e=yswdtg

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

Business Process e-Visa (Extended)

Request revert Visa



แผนภาพ Business Process e-Visa (Extended) Request Revert Visa

https://1drv.ms/i/s!Ap8pk0aBGx6Cq9oAtLyf74v6MWM_wg?e=mWtftvT

5.3.1 คุณสมบัติพื้นฐาน

5.3.1.1 สามารถแสดงผลในหลากหลายอุปกรณ์ (responsive) อาทิ เครื่องคอมพิวเตอร์ ตั้งโต๊ะ (PC) โน้ตบุ๊ค แท็บเล็ต (Tablet) โทรศัพท์มือถือ โดยไม่แยก URL address และไม่สูญเสียวัตถุประสงค์ของเนื้อหา หรือมีผลกระทบต่อการใช้งานในทุกขั้นตอน

5.3.1.2 มีการตรวจสอบความถูกต้องครบถ้วนของข้อมูล รวมถึงเงื่อนไขที่จำเป็นก่อนบันทึกข้อมูล (submit)

5.3.1.3 มีระบบป้องกันโปรแกรมอัตโนมัติ (bot) หรือสแปมเพื่อไม่ให้เข้ามาใช้งาน อาทิ ระบบตรวจสอบตัวตน (CAPTCHA) หรืออื่น ๆ ในลักษณะเดียวกัน

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

5.3.1.4 มีเมนูให้ผู้ใช้งานสามารถกด resend อีเมลได้ด้วยตนเอง ในขั้นตอนที่
กรรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.1.5 เว็บไซต์ต้องมีความเร็วการตอบสนอง (respond) ไม่มากกว่า 3 วินาที
หรือตามที่กรรมการกงสุล กระทรวงการต่างประเทศเห็นชอบ

5.3.1.6 รองรับและแสดงผลได้หลายภาษา ตามที่กรรมการกงสุล กระทรวงการต่างประเทศ
กำหนด มีระบบที่แสดงผล 16 ภาษา ได้แก่ 1. อังกฤษ 2. ฝรั่งเศส 3. สเปน 4. รัสเซีย 5. อาหรับ 6. จีน
(Traditional) 7. จีน (Simplified) 8. เยอรมัน 9. เกาหลี 10. ญี่ปุ่น 11. พม่า 12. กัมพูชา 13. ลาว
14. เวียดนาม 15. บาสาซามาลีเซีย และ 16. โปรตุเกส พร้อมทั้งปรับแก้หรือเพิ่มเติมข้อมูลหรือเนื้อหาใน
ระบบ e-Visa ตลอดระยะเวลาตามสัญญา โดยในภาษาอื่นนอกจากอังกฤษ สามารถแสดงผลให้มีภาษาอังกฤษ
กำกับควบคู่ด้วย ทั้งนี้ หากกรรมการกงสุล กระทรวงการต่างประเทศ ต้องการเพิ่มภาษาอื่นนอกจากภาษา
ที่กำหนด สามารถเพิ่มได้โดยให้กรรมการกงสุล กระทรวงการต่างประเทศเป็นผู้แปลภาษา

5.3.1.7 รองรับการทำงานที่มีจำนวนผู้ร้องขอรับการตรวจลงตราได้ไม่ต่ำกว่า
20,000,000 ราย และรองรับการใช้งานพร้อมกันสูงสุด (Concurrent sessions) ไม่น้อยกว่า 1,000 sessions
ตลอดระยะเวลาตามสัญญา

5.3.1.8 มีระบบสำรวจความเห็นจากผู้ร้อง (survey) โดยเก็บสถิติเพื่อประมวลผล
ความพึงพอใจ ให้คะแนนแยกตามประเภทการให้บริการ มีช่องความคิดเห็น ให้สถานเอกอัครราชทูต
หรือสถานกงสุลใหญ่ เข้าถึงได้ และกรรมการกงสุล กระทรวงการต่างประเทศ สามารถดูข้อมูลได้ทั้งหมด
โดยสามารถแก้ไขหรือเพิ่มข้อความได้ โดยสามารถส่งอีเมล สำรวจความเห็นไปยังอีเมล ของผู้ยื่นคำขอได้
ตามที่กรรมการกงสุล กระทรวงการต่างประเทศ กำหนด

5.3.1.9 สามารถจัดการ เปิด - ปิด ระบบการขอ e-Visa ได้โดยไม่กระทบกับการทำงาน
ของอีกระบบหนึ่ง โดยกำหนดเงื่อนไขตามที่กรรมการกงสุล กระทรวงการต่างประเทศ กำหนด

5.3.1.10 สามารถแสดงประวัติการดำเนินการในทุกขั้นตอนของแต่ละคำร้องได้
โดยต้องแสดงวันที่ดำเนินการ สิ่งที่ทำเนิการ เหตุเหตุ (หากมี) IP Address และ Location ที่ดำเนินการ
หรือตามที่กรรมการกงสุล กระทรวงการต่างประเทศ กำหนด

5.3.1.11 สามารถขึ้นข้อความประกาศ หรือแจ้งเตือนได้ตามที่กรรมการกงสุล กระทรวง
การต่างประเทศ กำหนด

5.3.2 ระบบ Front Office สำหรับรับคำร้อง มีคุณสมบัติพื้นฐาน และประกอบด้วยโมดูล
ดังนี้

5.3.2.1 คุณสมบัติพื้นฐานของระบบ

(1) พัฒนาระบบในรูปแบบ Web Application เพื่อรองรับคำร้อง e-Visa
(2) มีการตรวจสอบสิทธิ์การเข้าใช้งาน ตามที่กรรมการกงสุล กระทรวงการ
ต่างประเทศ กำหนด

(3) สามารถดำเนินการตาม Business Flow และ UX/UI ที่กรรมการกงสุล
กระทรวงการต่างประเทศ เห็นชอบ

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

5.3.2.2 โมดูลแสดงรายละเอียดข้อมูลในการยื่นคำร้อง (Information) มีรายละเอียด ดังนี้

- (1) มีหน้าจอแสดงภาพรวมหรือขั้นตอนการยื่นขอ e-Visa โดยสังเขป
ง่ายต่อการทำความเข้าใจของผู้ใช้งาน
- (2) มีหน้าจอแสดงข้อมูลรายละเอียดของประเภทของ e-Visa ตามที่กรมการกงสุล
กระทรวงการต่างประเทศ เห็นชอบ
- (3) มีหน้าจอสืบค้นคุณสมบัติหรือประเภทของ Visa ที่กำหนดได้จากสัญชาติ
ถิ่นพำนัก ประเภทหนังสือเดินทาง วัตถุประสงค์ของการเดินทาง หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ
กำหนด
- (4) สามารถเข้าถึงและแสดงผลข้อมูลข้างต้นได้ โดยไม่ต้องเข้าสู่ระบบ

5.3.2.3 โมดูลผู้ใช้งาน (User) มีรายละเอียด ดังนี้

- (1) มีการลงทะเบียนบัญชีผู้ใช้งาน โดยจัดเก็บข้อมูลตามแบบฟอร์มที่
กรมการกงสุล กระทรวงการต่างประเทศ กำหนด
- (2) มีการยืนยันบัญชีผู้ใช้งานผ่านอีเมล Authentication ก่อนการเข้าสู่ระบบในครั้งแรก
- (3) มีระบบ Two-Factor Authentication (2FA) โดยใช้อีเมล และ Google
authentication โดยให้ผู้ใช้งานสามารถเลือกใช้งานได้ สำหรับการเข้าใช้งานระบบทุกครั้ง
- (4) ผู้ใช้งานสามารถลงทะเบียนได้ 2 รูปแบบ ได้แก่ แบบบุคคลทั่วไป
(Individual) และแบบผู้แทนยื่นคำร้อง (Agent)
- (5) บัญชีผู้แทนยื่นคำร้อง (Agent) สามารถสร้าง แก้ไข ระบุ บัญชีย่อย
(Sub-agent) ได้ไม่เกินจำนวนบัญชีย่อยที่ผู้ว่าจ้างกำหนด
- (6) มีหน้าจอให้ผู้ใช้งานสามารถ Reset Password ของตัวเองได้ในกรณีที่ลืม
Password

5.3.2.4 โมดูลการยื่นคำร้อง มีรายละเอียด ดังนี้

- (1) โมดูลมีคุณสมบัติพื้นฐานดังนี้
 - (1.1) มีหน้าจอในการยื่นขอ e-Visa ตรงตามเงื่อนไขที่กรมการกงสุล
กระทรวงการต่างประเทศ กำหนด
 - (1.2) สามารถอ่านข้อมูลจากภาพ data page ของหนังสือเดินทางที่ผู้ยื่น
คำร้องอัปโหลดเข้ามาเพื่อกรอกข้อมูลในแบบฟอร์มแบบอัตโนมัติ (auto fill) โดยจะต้องมีความถูกต้อง
อย่างน้อยร้อยละ 90 ของจำนวนคำร้อง
 - (1.3) ในการเก็บไฟล์ภาพและไฟล์เอกสารแนบ ระบบจะต้องเก็บให้อยู่ใน
รูปแบบเดียวกัน อาทิ เก็บไฟล์ภาพเป็น JPEG ทั้งหมด ไฟล์เอกสารแนบเป็น PDF ทั้งหมด หรือเป็นไปตาม
ที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด
 - (1.4) สามารถตรวจสอบคุณภาพและความคมชัดของไฟล์ภาพถ่ายและไฟล์
เอกสารแนบอื่น ๆ ก่อนนำเข้าระบบ โดยตรวจสอบจากค่าต่าง ๆ อาทิ ค่าความละเอียด (resolution)
ขนาดไฟล์ (size) สัดส่วนของภาพใบหน้าปรากฏ รวมถึงเป็นไปตามกฎอื่น ๆ ตามที่กรมการกงสุล
กระทรวงการต่างประเทศ กำหนด

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

(1.5) สามารถตรวจสอบความถูกต้องสมบูรณ์ของภาพถ่ายที่ผู้ใช้งาน upload ว่าเป็นบุคคลเดียวกับภาพถ่ายใน Data page รวมถึงความถูกต้องสมบูรณ์ของเอกสารทั้งหมดอย่างอัตโนมัติ โดยใช้เทคโนโลยี อาทิ AI เพื่อประกอบการพิจารณาคำร้อง ซึ่งได้รับความเห็นชอบจากกรมการกงสุล กระทรวงการต่างประเทศ

(1.6) สามารถตั้งเงื่อนไขในการกรอกข้อมูลได้ตรงตามเงื่อนไขที่ กรมการกงสุล กระทรวงการต่างประเทศ กำหนด อาทิ ชนิดอักษร (Text) ชนิดตัวเลข (Decimal) ความยาวของอักษร (Length) ความจำเป็นในการกรอก (Required Field)

(1.7) สามารถบันทึกแบบฟอร์มฉบับร่าง (save draft) ซึ่งสามารถแก้ไขเพิ่มเติมได้ในภายหลัง

(1.8) มีการตรวจสอบการยื่นคำร้องซ้ำซ้อน ตามเงื่อนไขที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(1.9) สามารถรองรับการยื่นคำร้องแบบกลุ่ม (Group) ได้ ในกรณีที่ผู้ยื่นคำร้อง

เดินทางร่วมกันมากกว่า 1 คน และมีกำหนดการเดินทาง ที่พัก หรือ เงื่อนไขอื่น ๆ ตรงตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด โดยจะต้องสามารถส่งไปพิจารณาอนุมัติผลในคราวเดียวกันได้

(1.10) ผู้ร้องสามารถแก้ไขข้อมูลการยื่นคำร้องในส่วนที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนดได้

(2) ประเภทการยื่นคำร้องมี 2 ประเภทดังนี้ เป็นอย่างน้อย หรือเป็นไปตามที่ กรมการกงสุล กระทรวงการต่างประเทศ เห็นชอบ

(2.1) แบบบุคคลทั่วไป (Individual) คือ ผู้ที่ยื่นคำร้องด้วยตนเอง

(2.2) แบบผู้แทนยื่นคำร้อง (Agent) มีรายละเอียด ดังนี้

(2.2.1) คุณสมบัติขั้นพื้นฐานของ Agent

- สามารถบันทึกคำร้องได้หลายคำร้อง รวมถึงตรวจสอบและแก้ไข คำร้องได้

- สามารถตั้งค่าให้ Agent ยื่นคำร้องได้ในบางเงื่อนไข อาทิ บางประเภทคำร้อง หรือเงื่อนไขอื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

- มีระบบลงทะเบียนบัญชี Agent โดยสามารถกรอกข้อมูล ส่วนบุคคล อีเมล แบนเอกสารที่เกี่ยวข้อง และกรอกข้อมูลอื่น ๆ ได้ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด และ Agent จะต้องยืนยันตัวตนด้วยอีเมลก่อนเริ่มใช้งาน

- สามารถจำกัดจำนวนการบันทึกคำร้องต่อวัน ของ Agent ได้

- สามารถตั้งค่า Blacklist/Watchlist ของ Agent ได้จากอีเมล หรือตามเงื่อนไขที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

- สามารถระงับบัญชี Agent ได้ในกรณีที่ไม่มีกรการใช้งาน เป็นระยะเวลาที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

- กรมการกงสุล กระทรวงการต่างประเทศ สามารถอนุมัติบัญชี และระงับบัญชี Agent ได้เป็นรายบุคคล

(2.2.2) ประเภทของผู้แทนยื่นคำร้อง (Agent) มีอย่างน้อย 2 ประเภท ดังนี้

- บัญชีผู้แทนหลัก (Main-agent) สามารถสร้าง แก้ไข และระงับบัญชีผู้แทนย่อยซึ่งอยู่ภายใต้บัญชีหลักของตนเองได้ตามจำนวนสูงสุดตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

- บัญชีผู้แทนย่อย (Sub-agent) ไม่สามารถสร้างบัญชีผู้แทนย่อย ภายใต้บัญชีตนเองได้

5.3.2.5 โมดูลชำระค่าธรรมเนียม มีรายละเอียด ดังนี้

- (1) รองรับการชำระค่าธรรมเนียมทั้งในรูปแบบ online และ offline
- (2) สามารถชำระค่าธรรมเนียมการยื่น ในรูปแบบ online payment โดยการเชื่อมต่อข้อมูล API กับ payment gateway ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด
- (3) สามารถชำระค่าธรรมเนียมการยื่น ในรูปแบบ offline payment โดยผู้รับจ้างต้องพัฒนาระบบให้สามารถรองรับการชำระเงินแบบ offline และเชื่อมต่อข้อมูล API กับระบบ e-Visa รวมถึง payment gateway อื่น ๆ ตามเงื่อนไขที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด
- (4) มีระบบพิมพ์เอกสารแสดงรายละเอียดการยื่นของ e-Visa เพื่อเป็นเอกสารประกอบการชำระค่าธรรมเนียมแบบ offline มีระบบในการ generate unique code / barcode / QR code พร้อมอุปกรณ์ที่เชื่อมโยงกับคอมพิวเตอร์ของสถานเอกอัครราชทูต หรือสถานกงสุลใหญ่ ในการรับชำระค่าธรรมเนียม
- (5) สามารถออกใบเสร็จให้กับผู้ร้องได้ผ่านช่องทางอิเล็กทรอนิกส์ หรือช่องทางอื่น ๆ ที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

5.3.2.6 โมดูลตรวจสอบผลคำร้อง มีรายละเอียด ดังนี้

- (1) มีส่วนแสดงสถานะการยื่น e-Visa โดยจำแนกตามสถานะ Incomplete, Ready to Submit, Submitted, Finished ของการยื่น e-Visa เป็นรายการ หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด
- (2) สามารถส่งอีเมลเพื่อแจ้งสถานะการตรวจสอบผล e-Visa ได้ อาทิ อนุมัติ ปฏิเสธ ขอเอกสารเพิ่ม เรียกสัมภาษณ์ หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด
- (3) สามารถดาวน์โหลดผลการอนุมัติ e-Visa ได้
- (4) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.2.7 โมดูลแก้ไขข้อมูลการยื่นคำร้อง

- (1) สามารถให้ผู้ใช้งานแก้ไขข้อมูล (รวมถึงไม่อนุญาต) การยื่น e-Visa รวมถึงเปลี่ยนแปลงเอกสารประกอบคำยื่นขอ e-Visa ตามเงื่อนไขที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด
- (2) มีระบบเก็บ log การแก้ไขข้อมูลและมีการแสดงผลคำร้องที่มีการแก้ไข ให้แตกต่างจากคำร้องปกติ โดยแสดงสถานะ วันเวลาที่มีการแก้ไข และรายละเอียดตามที่กรมการกงสุล หรือหน่วยงานอื่น ๆ กระทรวงการต่างประเทศ กำหนด
- (3) สามารถโยกย้ายคำร้องระหว่างสถานเอกอัครราชทูต สถานกงสุลใหญ่ได้

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

(4) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.3 ระบบ Back Office สำหรับการบริการจัดการคำร้อง มีคุณสมบัติพื้นฐาน และประกอบด้วย โมดูลต่าง ๆ ดังนี้

5.3.3.1 คุณสมบัติพื้นฐานของระบบ

- (1) พัฒนาระบบในรูปแบบ Web Application เพื่อรองรับคำร้อง e-Visa
- (2) มีการตรวจสอบสิทธิ์การเข้าใช้งาน โดยใช้ข้อมูล Username และ Password ประกอบกับการใช้ TOTP (Time-based One-Time Password) ในการเข้าสู่ระบบ โดย TOTP ต้องเป็นไปตาม RFC 6238 และสามารถใช้งานได้กับ Google Authenticator และ Microsoft Authenticator เป็นอย่างน้อย
- (3) สามารถดำเนินการตาม Business Flow และ UX/UI ที่กรมการกงสุล กระทรวงการต่างประเทศ เห็นชอบ
- (4) สามารถ download เอกสารเพื่อดำเนินการพิจารณาแบบ offline ได้ โดยสามารถเก็บ log การ download เอกสารของผู้ร้องด้วย และสามารถตรวจสอบย้อนกลับไปยังบัญชี ผู้ใช้งานที่ download เอกสารนั้นได้โดยมีการซ่อนข้อความไว้ในเอกสารหรือใช้เทคนิคอื่นที่เทียบเท่า หรือดีกว่า
- (5) สามารถอ่านข้อมูลจากภาพ data page ของหนังสือเดินทางที่ผู้ยื่น คำร้องอัปโหลดเข้ามาเพื่อเปรียบเทียบกับข้อมูลยื่นคำร้อง พร้อมทั้งมีการแจ้งเตือนความถูกต้องของข้อมูล โดยจะต้องมีความถูกต้องอย่างน้อยร้อยละ 90 ของจำนวนคำร้อง
- (6) สามารถตรวจสอบคุณภาพและความคมชัดของไฟล์ภาพถ่ายและไฟล์เอกสาร แนบอื่น ๆ พร้อมทั้งมีการแจ้งเตือนความถูกต้องของข้อมูลโดยจะต้องมีความถูกต้องอย่างน้อยร้อยละ 90 ของ จำนวนคำร้อง โดยตรวจสอบจากค่าต่าง ๆ อาทิ ค่าความละเอียด (resolution) ขนาดไฟล์ (size) สัดส่วน ของภาพใบหน้าปรากฏ รวมถึงเป็นไปตามกฎอื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด
- (7) สามารถตรวจสอบความถูกต้องสมบูรณ์ของภาพถ่ายที่ผู้ใช้งาน upload ว่าเป็นบุคคลเดียวกับภาพถ่ายใน Data page รวมถึงความถูกต้องสมบูรณ์ของเอกสารทั้งหมดอย่างอัตโนมัติ โดยใช้เทคโนโลยี อาทิ AI เพื่อประกอบการพิจารณาคำร้อง พร้อมทั้งมีการแจ้งเตือนความถูกต้องของข้อมูล โดยจะต้องมีความถูกต้องอย่างน้อยร้อยละ 90 ของจำนวนคำร้อง ซึ่งได้รับความเห็นชอบจากกรมการกงสุล กระทรวงการต่างประเทศ
- (8) มีระบบ Widget สามารถปรับแต่งหน้าจอ ฟังก์ชัน คุณลักษณะตามความต้องการของผู้ใช้งานได้
- (9) มีระบบ authentication ที่รองรับระบบการเข้าถึงเครือข่ายแบบ Zero Trust Network Access (ZTNA) ตามข้อ 5.8 สำหรับการเข้าใช้งานระบบทุกครั้ง

5.3.3.2 โมดูล e-Checking

- (1) มีหน้าให้เจ้าหน้าที่สามารถตรวจสอบข้อมูลคำร้องที่ยื่นเข้ามาได้

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

(2) มีหน้าแสดงรายการคำร้องรอตรวจสอบพร้อมแสดงสถานะคำร้อง สามารถตรวจสอบข้อมูลและเอกสารที่ผู้ยื่นคำร้องบันทึกเข้ามาได้

(3) มีการแสดงผลการเปรียบเทียบกับเงื่อนไขที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด และสามารถแสดงรายละเอียดผลการเปรียบเทียบ เพื่อใช้ประกอบการพิจารณาได้

(4) สามารถแสดงประวัติการขอ e-Visa ในแต่ละรายการ รวมถึงประวัติการเดินทางเข้า-ออก (ถ้ามี) เพื่อใช้ประกอบการพิจารณาได้

(5) สามารถให้เจ้าหน้าที่ขอเอกสารเพิ่มเติมจากผู้ร้องได้ พร้อมแจ้งเตือนให้ผู้ร้องทราบผ่านทางอีเมล โดยเจ้าหน้าที่สามารถระบุประเภทเอกสารที่ต้องการเพิ่มเติมได้ และปรับสถานะคำร้องเป็น “Requesting Document” หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด ในขณะที่เอกสารที่ไม่ได้ต้องการเพิ่มเติมจะไม่สามารถเข้ามาแก้ไขได้

(6) เมื่อผู้ร้องส่งเอกสารที่เจ้าหน้าที่มีการขอเพิ่มเติมเข้ามา คำร้องจะถูกปรับสถานะไปรอพิจารณาอีกครั้ง “Wait for Checking” หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(7) สามารถแสดงรายการคำร้องที่ต้องการความเร่งด่วน (Priority) พร้อมแสดงสถานะกำกับได้ และเจ้าหน้าที่กระทรวงการต่างประเทศ สามารถระบุคำร้องให้เป็น Priority ได้ด้วยตนเอง

(8) เจ้าหน้าที่สามารถตั้งค่าความเร่งด่วนของคำร้องให้เป็น ปกติ ด่วน ด่วนมาก ด่วนที่สุด หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนดได้

(9) เจ้าหน้าที่สามารถบันทึกสถานะคำร้องที่พิจารณา โดยสามารถระบุหมายเหตุเพิ่มเติมในการพิจารณาได้ แบ่งเป็น

(9.1) Document Completed อนุมัติเบื้องต้นแบบทั่วไป

(9.2) Document Completed with Risk อนุมัติเบื้องต้น

แบบมีความเสี่ยง

(9.3) Requesting Document ขอเอกสารเพิ่มเติม

(9.4) หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(10) สามารถถอยสถานะการพิจารณาคำร้อง เช่น Approve Reject หรือสถานะอื่น ๆ ได้ตามเงื่อนไขที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(11) มีหน้าแสดงรายการคำร้องที่ตรวจสอบแล้ว พร้อมแสดงสถานะคำร้อง สามารถตรวจสอบข้อมูลและเอกสารที่ผู้ยื่นคำร้องบันทึกเข้ามา รวมถึงข้อมูลอื่น ๆ ที่ใช้ประกอบการพิจารณาได้

(12) ในแต่ละหน้าที่แสดงรายการคำร้อง สามารถค้นหาทุกข้อมูลของผู้ยื่นคำร้องบันทึกเข้ามา สามารถสืบค้นแบบขั้นสูง (Advance Search) สามารถใช้หลายตัวกรองพร้อมกันในการค้นหาแต่ละครั้ง และสามารถกำหนดช่วงเวลาที่ค้นหาได้ รวมถึงมีระบบ Autocomplete เพื่อช่วยในการค้นหา หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(13) มีปุ่ม Filter ข้อมูลแบบ Shortcut ให้สามารถเลือกชุดข้อมูล

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

ที่จะแสดงได้โดยง่ายในคลิกเดียว อาทิ Individual Agent หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด โดยสามารถปรับตั้งค่าได้เป็นรายผู้ใช้งาน (User) ได้

(14) มีระบบ Custom Column ให้เจ้าหน้าที่สามารถเลือก Column ข้อมูลที่ต้องการแสดงได้ด้วยตนเอง โดยสามารถปรับตั้งค่าได้เป็นรายผู้ใช้งาน (User)

(15) มีระบบ Multiple Sort สามารถจัดเรียงข้อมูลได้ทุกข้อมูลตามที่ยื่นคำร้องบันทึกเข้ามา โดยผู้ใช้งานสามารถจัดการเรียงข้อมูลได้ด้วยตนเอง และจัดเรียงข้อมูลได้พร้อมกันหลายข้อมูล อาทิ เรียงวันที่ และ ประเภท Visa พร้อมกัน หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(16) สามารถแสดงยอดจำนวนรายการของคำร้องที่สถานะต่าง ๆ ได้ โดยสามารถคลิกเข้าไปดูรายละเอียดได้ (Drill down)

(17) สามารถแสดงเอกสารที่ละรายการ หรือสามารถแสดงเอกสาร ทั้งหมดได้

(18) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.3.3 โมดูล Approval

(1) มีหน้าแสดงรายการคำร้องที่ผ่านกระบวนการพิจารณาคำร้องจากโมดูล Checking Visa Application ตามข้อ 5.3.3.2 ที่รอการ Approve e-Visa พร้อมแสดงสถานะคำร้อง และสามารถตรวจสอบข้อมูลและเอกสารที่ยื่นคำร้องบันทึกเข้ามาได้

(2) สามารถแสดงผลและดำเนินการได้ตาม function ในข้อ 5.3.2.2

(3) เจ้าหน้าที่ Approval สามารถมอบหมายให้เจ้าหน้าที่ในสถานเอกอัครราชทูต และสถานกงสุลใหญ่ดำเนินการนัดหมายผู้ร้องเพื่อขอสัมภาษณ์ประกอบการพิจารณาได้ตามข้อ 5.3.3.8 โมดูลนัดสัมภาษณ์ โดยสถานะคำร้องจะถูกปรับไปเป็น Interview

(4) สามารถแสดงผลการสัมภาษณ์ และรายละเอียดการสัมภาษณ์ ตามข้อ 5.3.3.8 โมดูลนัดสัมภาษณ์ ในแต่ละคำร้องได้

(5) เจ้าหน้าที่สามารถบันทึกสถานะการออก e-Visa ได้ โดยสามารถระบุหมายเหตุ (Remark) เพิ่มเติมในการพิจารณาได้ แบ่งเป็น

(5.1) Reverse ส่งกลับไปให้ Checking Visa Application เพื่อตรวจสอบอีกครั้ง

(5.2) Approve อนุมัติ Visa

(5.3) Reject ปฏิเสธการขอ Visa โดยไม่ติด Watchlist และต้องระบุเหตุผลการปฏิเสธได้

(5.4) Reject ปฏิเสธการขอ Visa โดยให้ติด Watchlist และต้องระบุเหตุผลการปฏิเสธได้

(5.5) Interview ขอสัมภาษณ์เพิ่มเติม

(5.6) Requesting Document ขอเอกสารเพิ่มเติม

(5.7) หรือสถานะอื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(6) มีหน้าแสดงรายการคำร้องที่ผ่านกระบวนการอนุมัติ Visa แสดงสถานะคำร้อง สามารถตรวจสอบข้อมูลและเอกสารที่ยื่นคำร้องบันทึกเข้ามา รวมถึงข้อมูลอื่น ๆ ที่ใช้ประกอบการพิจารณาได้

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

(7) สามารถถอยสถานะการพิจารณาคำร้อง เช่น Approve Reject หรือสถานะอื่น ๆ และสามารถเชื่อมโยงข้อมูลไปยังหน่วยงานที่เกี่ยวข้องได้ตามเงื่อนไขที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(8) โมดูล Approval ต้องทำงานได้ทุกโมดูลของ e-Checking

(9) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.3.4 โมดูลการยกเลิก (Void)

(1) ระบบสามารถยกเลิก e-Visa ที่ออกไปแล้วได้ โดยให้สามารถกำหนดให้ผู้ร้องติด watchlist หรือสถานะอื่น ๆ และต้องระบุเหตุผลการยกเลิกได้

(2) ระบบสามารถเชื่อมโยงข้อมูลการยกเลิก e-Visa ไปยังหน่วยงานที่เกี่ยวข้องได้

5.3.3.5 โมดูล Dashboard

(1) สามารถแสดงข้อมูล การดำเนินงาน สถิติต่างๆ ในรูปแบบของ dashboard รวมทั้งรายการ Priority list ได้ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(2) สามารถแสดงข้อมูลในรูปแบบ กราฟ และแผนที่ รวมถึงมี Filter ให้ค้นหาได้ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(3) สามารถปรับแต่ง Dashboard ให้แตกต่างกันเป็นรายบุคคลได้

(4) มีระบบรับ-ส่งข้อความ เผยแพร่ประกาศสำคัญ ข้อมูลต่างๆ ระหว่างเจ้าหน้าที่ในสำนักงาน และเจ้าหน้าที่จากส่วนกลาง หรือเจ้าหน้าที่จากสถานเอกอัครราชทูตและสถานกงสุลใหญ่อื่น ๆ โดยมีการเข้ารหัสเพื่อรักษาความปลอดภัยและป้องกันข้อมูลรั่วไหล

(5) สามารถสร้าง Dashboard อื่น ๆ ได้ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

5.3.3.6 โมดูล Report และการค้นหาข้อมูล (Query)

(1) สามารถ export รายงานเป็นไฟล์ Excel CSV และ PDF ได้เป็นอย่างดี

(2) รายงานคำร้องที่อยู่ในสถานะต่าง ๆ อาทิ รออนุมัติ อนุมัติแล้ว ไม่อนุมัติ โดยแสดงเป็น รายวัน รายเดือน หรือช่วงเวลาตามที่กำหนดได้

(3) รายงานการจัดเก็บค่าธรรมเนียมการตรวจลงตรา โดยสามารถกำหนด cutoff time ได้ และสามารถค้นหาเป็นรายวัน รายเดือน หรือช่วงเวลาตามที่กำหนดได้

(4) รายงานสถิติจำนวนการตรวจลงตรา โดยแยกเป็นรายประเภท และสามารถค้นหาเป็นรายวัน รายเดือน หรือช่วงเวลาตามที่กำหนดได้

(5) รายงานการออกไปเสร็จ ให้มีรูปแบบตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(6) สามารถออกรายงานอื่น ๆ ได้ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(7) สามารถกำหนดสิทธิ์การเข้าถึงรายงานได้ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(8) สามารถปรับแต่ง report ได้เองจาก report ด้านล่าง อาทิ

- Excel, CSV, PDF

- Daily Report

ประธานกรรมการ กรรมการ กรรมการ กรรมการ

กรรมการ กรรมการ กรรมการ กรรมการ

- Daily Visa Report
- Summary Visa Report
- Summary Issued Report
- Visa Issued Report

(9) มีหน้าแสดงรายการคำร้องขอรับการตรวจลงตรา โดยแสดงข้อมูลตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(10) สามารถค้นหาทุกข้อมูลที่ยื่นคำร้องบันทึกเข้ามา หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด โดยสามารถสืบค้นแบบขั้นสูง (Advance Search) สามารถใช้หลายตัวกรองพร้อมกันในการค้นหาแต่ละครั้ง และกำหนดช่วงเวลาที่สามารถได้ รวมถึงมีระบบ Autocomplete เพื่อช่วยในการค้นหา

(11) มีระบบ Custom Column ให้ผู้ใช้งานสามารถเลือก Column ข้อมูลที่ต้องการดูได้ด้วยตนเอง

(12) มีระบบ Multiple Data Sort สามารถจัดเรียงข้อมูลได้ทุกข้อมูลตามที่ผู้ยื่นคำร้องบันทึกเข้ามา หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด โดยผู้ใช้งานสามารถจัดเรียงข้อมูลได้เอง และจัดเรียงข้อมูลได้พร้อมกันหลายข้อมูล อาทิ เรียงวันที่ และ ประเภท Visa พร้อมกัน

(13) สามารถแสดงยอดจำนวนรายการออก e-Visa ได้

(14) สามารถพิมพ์รายงานการออก e-Visa ในรูปแบบ Excel, CSV และ PDF ได้

(15) มี Filter ข้อมูลแบบ Shortcut ให้สามารถเลือกชุดข้อมูลที่จะแสดงได้โดยง่าย อาทิ Individua Agent หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(16) มีรายงานที่แสดงในระบบที่เป็นแบบข้อมูล dynamic หรือสามารถ drill-down ดูข้อมูลที่เกี่ยวข้องที่ปรากฏได้ทั้งระบบ

(17) สามารถควบคุมการมองเห็นข้อมูลของแต่ละ User ได้ เช่น ผู้ใช้งานของสำนักงานในต่างประเทศให้เห็นเฉพาะข้อมูลในสำนักงานตนเอง ผู้ใช้งานของส่วนกลางให้เห็นข้อมูลทั้งหมด หรือเป็นไปตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(18) มี dashboard ที่สามารถปรับแต่ง (custom) ได้เองแยกตามแต่ละผู้ใช้งาน

(19) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.3.7 โมดูลตรวจสอบข้อมูลผู้ยื่นคำร้อง โดยหน่วยงานภายนอก

(1) สามารถส่งได้ทั้งแบบอัตโนมัติหากเข้าเงื่อนไข และแบบ manual และสามารถกำหนดข้อมูล และเอกสารแนบที่ต้องการส่งตรวจได้

(2) สามารถแบ่ง Tier หน่วยงานที่จะ login เข้ามาตรวจสอบ โดยสามารถทำได้พร้อมกันในหลายหน่วย (Parallel Checking and Approval)

(3) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.3.8 โมดูลนัดสัมภาษณ์ (Appointment)

(1) สามารถจัดการการสัมภาษณ์แบบ online/offline ดูตารางนัดหมาย และบริหารจัดการนัดหมายเวลาสัมภาษณ์ได้

(2) สามารถเรียกดูข้อมูลไฟล์วิดีโอ/ไฟล์เสียงย้อนหลังได้

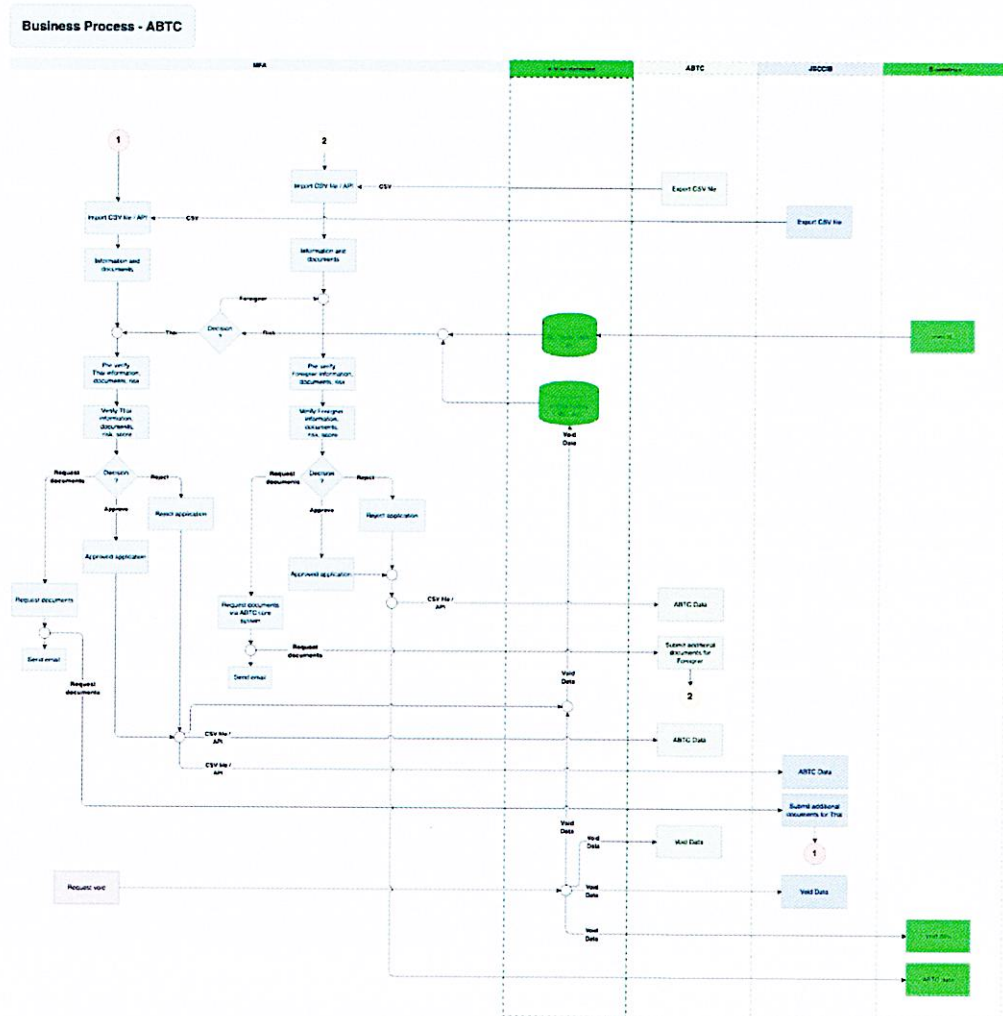
ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

(3) สามารถตั้งค่าคุณสมบัติของไฟล์ที่บันทึก โดยกำหนดค่าความละเอียด (resolution) และรูปแบบการเข้ารหัสไฟล์ (codec) ระยะเวลาการจับเก็บไฟล์ และคุณสมบัติอื่น ๆ ได้ตามที่กรรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(4) ผู้ร้อง และเจ้าหน้าที่สามารถเลื่อนวันนัดหมายได้ด้วยตนเอง

(5) อื่น ๆ ตามที่กรรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.3.9 โมดูล APEC Business Travel Card (ABTC)



แผนภาพ Business Process ABTC

<https://1drv.ms/i/s!Ap8pk0aBGx6Cq8RO0fXCDUOlqjlqqg?e=0jTje5>

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

คุณสมบัติพื้นฐาน

1) พัฒนาระบบเพื่อทำหน้าที่เป็นศูนย์ประมวลคำร้องเกี่ยวกับบัตร ABTC ของทั้งผู้สมัครบัตรชาวต่างชาติและผู้สมัครชาวไทย ซึ่งเชื่อมโยงข้อมูลกับระบบ e-Visa

1.1) กรณีผู้สมัครบัตรจากต่างชาติ

ระบบต้องสามารถเชื่อมโยงกับระบบ ABTC Core System ของออสเตรเลีย (<https://www.abtc-aps.org>) เพื่อรับคำร้องจากระบบ ABTC Core System และนำมาพิจารณาคำร้องโดยมีการตรวจสอบเพื่อประเมินความเสี่ยงกับฐานข้อมูลที่เกี่ยวข้อง อาทิ Blacklist/Watchlist และแจ้งผลการพิจารณากลับไปยัง ABTC Core System ทั้งนี้ ระบบจะเก็บข้อมูลตาม field ที่ได้รับจาก ABTC Core System เพื่อใช้ในการประมวลผลและตรวจสอบสิทธิในการเข้าประเทศไทย ร่วมกับการขอรับการตรวจลงตราผ่านระบบ e-Visa

1.2) กรณีผู้สมัครบัตรคนไทย

ระบบต้องสามารถเชื่อมโยงกับเว็บไซต์ของคณะกรรมการคณะกรรมการร่วมภาคเอกชน 3 สถาบัน (กกร.) (<https://abtc-jsccib.org>) เพื่อรับคำร้องจากเว็บไซต์ดังกล่าวและนำมาพิจารณาคำร้องและแจ้งผลกลับไปยังเว็บไซต์ของ กกร. ข้างต้น

2) สามารถแสดงประวัติการดำเนินการในทุกขั้นตอนของแต่ละคำร้องได้ โดยต้องแสดงวันที่ดำเนินการ สิ่งที่ทำเนิการ เหตุ (หากมี) IP Address และ Location ที่ดำเนินการ หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

3) ระบบ backoffice สำหรับประมวลคำร้อง มีคุณสมบัติพื้นฐาน ดังนี้

3.1) คุณสมบัติพื้นฐานของระบบ backoffice

- (1) พัฒนาระบบในรูปแบบ Web Application เพื่อบริหารจัดการคำร้อง
- (2) มีการตรวจสอบสิทธิการใช้งาน โดยใช้ข้อมูล Username และ Password ประกอบกับการใช้ TOTP (Time-based One-Time Password) เป็นอย่างน้อย
- (3) สามารถดำเนินการตาม Business Flow ABTC และ UX/UI ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

(4) สามารถ download เอกสารเพื่อดำเนินการพิจารณาแบบ offline ได้ โดยสามารถเก็บ log การ download เอกสารของผู้ร้อง และสามารถตรวจสอบย้อนกลับไปยังบัญชีผู้ใช้งานที่ download เอกสารนั้นได้ โดยมีการซ่อนข้อความไว้ในเอกสารหรือใช้เทคนิคอื่นที่เทียบเท่าหรือดีกว่า

3.2) โมดูล e-Checking และ e-Approval

- (1) สามารถตรวจสอบข้อมูลคำร้องของผู้ร้องที่ยื่นเข้ามาได้
- (2) มีหน้าแสดงรายการคำร้องรอตรวจสอบพร้อมแสดงสถานะคำร้อง สามารถตรวจสอบข้อมูลและเอกสารที่ผู้ยื่นคำร้องบันทึกเข้ามาได้
- (3) มีการแสดงผลการเปรียบเทียบกับเงื่อนไขที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด และสามารถแสดงรายละเอียดผลการเปรียบเทียบ เพื่อใช้ประกอบการพิจารณาได้
- (4) สามารถแสดงประวัติการขอ ABTC ในแต่ละรายการ เพื่อใช้ประกอบการพิจารณาได้

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

(5) สามารถให้เจ้าหน้าที่ตั้ง remark ที่คำร้องเพื่อขอเอกสารเพิ่มเติมได้โดยกรณีของผู้สมัครต่างชาติ จะขอเอกสารเพิ่มเติมผ่าน ABTC Core System และในกรณีของผู้สมัครไทย จะขอเอกสารเพิ่มเติมผ่านเว็บไซต์ของ กกร.

(6) เมื่อผู้ร้องส่งเอกสารที่เจ้าหน้าที่มีการขอเพิ่มเติมเข้ามา คำร้องจะถูกปรับสถานะไปรอพิจารณาอีกครั้ง “Wait for Checking” หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(7) สามารถแสดงรายการคำร้องที่ต้องการความเร่งด่วน (Priority) พร้อมแสดงสถานะกำกับได้ และเจ้าหน้าที่กระทรวงการต่างประเทศสามารถระบุคำร้องให้เป็น Priority ได้ด้วยตนเอง

(8) สามารถบันทึกสถานะคำร้องที่พิจารณา โดยสามารถระบุหมายเหตุเพิ่มเติมในการพิจารณาได้ แบ่งเป็น

(8.1) Document Completed อนุมัติเบื้องต้นแบบทั่วไป

(8.2) Document Completed with Risk อนุมัติเบื้องต้นแบบมีความเสี่ยง

(8.3) Requesting Document ขอเอกสารเพิ่มเติม

(8.4) หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(9) สามารถถอยสถานะการพิจารณาคำร้อง หรือสถานะอื่น ๆ ได้ตามเงื่อนไขที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

(10) มีหน้าแสดงรายการคำร้องที่ตรวจสอบแล้ว พร้อมแสดงสถานะคำร้องสามารถตรวจสอบข้อมูลและเอกสารที่ผู้ยื่นคำร้องบันทึกเข้ามา รวมถึงข้อมูลอื่น ๆ ที่ใช้ประกอบการพิจารณาได้

(11) สามารถค้นหาทุกข้อมูลของผู้ยื่นคำร้องบันทึกเข้ามา และสามารถสืบค้นแบบขั้นสูง (Advance Search) สามารถใช้หลายตัวกรองพร้อมกันในการค้นหาแต่ละครั้ง และสามารถกำหนดช่วงเวลาที่สามารถได้ รวมถึงมีระบบ Autocomplete เพื่อช่วยในการค้นหา หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(12) มีปุ่ม Filter ข้อมูลแบบ Shortcut ให้สามารถเลือกชุดข้อมูลที่จะแสดงได้โดยง่ายในคลิกเดียว อาทิ Individual Agent หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด โดยสามารถปรับตั้งค่าได้เป็นรายผู้ใช้งาน (User)

(13) มีระบบ Custom Column ให้เจ้าหน้าที่สามารถเลือก Column ข้อมูลที่ต้องการแสดงได้ด้วยตนเอง โดยสามารถปรับตั้งค่าได้เป็นรายผู้ใช้งาน (User)

(14) มีระบบ Multiple Sort สามารถจัดเรียงข้อมูลได้ทุกข้อมูลตามที่ยื่นคำร้องบันทึกเข้ามา โดยผู้ใช้งานสามารถจัดการเรียงข้อมูลได้ด้วยตนเอง และจัดเรียงข้อมูลได้พร้อมกันหลายข้อมูลตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(15) สามารถแสดงยอดจำนวนรายการของคำร้องที่สถานะต่าง ๆ ได้ โดยสามารถคลิกเข้าไปดูรายละเอียดได้ (Drill down)

(16) สามารถแสดงเอกสารที่ละรายการ หรือสามารถแสดงเอกสารทั้งหมดได้

(17) เจ้าหน้าที่สามารถบันทึกสถานะการออก ABTC ได้ โดยสามารถระบุหมายเหตุ (Remark) เพิ่มเติมในการพิจารณาได้ แบ่งเป็น

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

- 1) Approve อนุมัติ
- 2) Reject ปฏิเสธการขอ
- 3) Pending กรณีขอเอกสารเพิ่มเติม
- 4) หรือสถานะอื่น ๆ ตามที่กรมการกงสุล กระทรวงการ

ต่างประเทศ กำหนด

(18) มีหน้าแสดงรายการคำร้องที่ผ่านกระบวนการอนุมัติ แสดงสถานะคำร้องสามารถตรวจสอบข้อมูลและเอกสารที่ผู้ยื่นคำร้องบันทึกเข้ามา รวมถึงข้อมูลอื่น ๆ ที่ใช้ประกอบการพิจารณาได้

3.3) โมดูลการยกเลิก (Void)

(1) ระบบสามารถยกเลิก Pre-clearance ที่ออกไปแล้วได้ โดยให้สามารถกำหนดให้ผู้ร้องติด watchlist หรือสถานะอื่น ๆ และต้องระบุเหตุผลการยกเลิกได้

(2) ระบบสามารถเชื่อมโยงข้อมูลการยกเลิก Pre-clearance ไปยังหน่วยงานที่เกี่ยวข้องได้

3.4) โมดูล Risk Management

ฟังก์ชันการจัดการ Blacklist/Watchlist ประกอบด้วย

- สามารถเชื่อม web service กับสำนักงานตรวจคนเข้าเมืองเพื่อรับข้อมูล Blacklist/Watchlist ได้ทั้งแบบอัตโนมัติและแบบ manual

- สามารถค้นหาผู้ติด Blacklist/Watchlist ได้โดยค้นจากชื่อ นามสกุล หมายเลขหนังสือเดินทาง หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนดได้

- สามารถตรวจสอบ log การดึงข้อมูลโดยสำนักงานตรวจคนเข้าเมืองได้

- สามารถ monitor สถานะการเชื่อมโยงข้อมูลกับระบบงานภายนอกอื่นได้

- สามารถเก็บประวัติการสืบค้นข้อมูล Blacklist/Watchlist ของเจ้าหน้าที่ได้ และสามารถดูรายงานประวัติการสืบค้นข้อมูลได้

- สามารถเปรียบเทียบรูปภาพใบหน้าของผู้ร้องกับฐานข้อมูล

Blacklist/Watchlist ของระบบ e-Visa พร้อมทั้งแจ้งเตือนว่าผู้ร้องติด Blacklist/Watchlist ได้

- สามารถเพิ่มข้อมูลภาพใบหน้าของผู้ติด Blacklist/Watchlist ลงในฐานข้อมูล Blacklist/Watchlist ของระบบ e-Visa ได้

- อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

3.5) โมดูล Dashboard

(1) สามารถแสดงข้อมูล การดำเนินงาน สถิติต่างๆ ในรูปแบบของ Dashboard รวมทั้งรายการ Priority list ได้ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

(2) สามารถแสดงข้อมูลในรูปแบบ กราฟ และแผนที่ รวมถึงมี Filter ให้ค้นหาได้ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(3) สามารถปรับแต่ง Dashboard ให้แตกต่างกันเป็นรายบุคคลได้

(4) สามารถสร้าง Dashboard อื่น ๆ ได้ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(5) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

3.6) โมดูล Report และการค้นหาข้อมูล (Query)

- (1) สามารถ export รายงานเป็นไฟล์ Excel CSV และ PDF ได้เป็นอย่างน้อย
- (2) รายงานคำร้องที่อยู่ในสถานะต่าง ๆ อาทิ รออนุมัติ อนุมัติแล้ว ไม่อนุมัติ โดยแสดงเป็น รายวัน รายเดือน หรือช่วงเวลาตามที่กำหนดได้
- (3) รายงานสถิติ โดยแยกเป็นรายประเภท และสามารถค้นหาเป็นรายวัน รายเดือนหรือช่วงเวลาตามที่กำหนดได้
- (4) สามารถออกรายงานอื่น ๆ ได้ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด
- (5) สามารถกำหนดสิทธิ์การเข้าถึงรายงานได้ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด
- (6) สามารถปรับแต่ง report ได้เองจาก report ด้านล่าง อาทิ
 - Excel, CSV, PDF
 - Daily Report
 - Daily Pre-clearance Report
 - Summary Pre-clearance Report
- (7) มีหน้าแสดงรายการ ABTC โดยแสดงข้อมูลตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด
- (8) สามารถค้นหาทุกข้อมูลที่ยื่นคำร้องบันทึกเข้ามา หรือตามที่ กรมการกงสุล กระทรวงการต่างประเทศ กำหนด โดยสามารถสืบค้นแบบขั้นสูง (Advance Search) สามารถใช้หลายตัวกรอง พร้อมกันในการค้นหาแต่ละครั้ง และกำหนดช่วงเวลาที่จะค้นหาได้ รวมถึงมีระบบ Autocomplete เพื่อช่วยในการค้นหา
- (9) มีระบบ Custom Column ให้ผู้ใช้งานสามารถเลือก Column ข้อมูล ที่ต้องการดูได้ด้วยตนเอง
- (10) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

3.7) โมดูลการส่งข้อมูลการพิจารณา

- (1) สามารถส่งผลการพิจารณาไปยัง ABTC Core System และ เว็บไซต์ของ กกร.
- (2) แจ้งผลการอนุมัติและปฏิเสธไปยังหน่วยงานปฏิบัติ อาทิ สตม.

5.3.3.10 โมดูล Visa Checking / Web Enquiry

- (1) มีระบบบริหารจัดการ ผู้ใช้งาน และสิทธิ์การเข้าถึงข้อมูลการตรวจลงตรา อิเล็กทรอนิกส์
- (2) มีระบบการตรวจสอบเอกสารแจ้งการตรวจลงตราของศูนย์ข้อมูลการตรวจลงตรา (Visa Data Center) และเอกสารอื่น ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด
- (3) ระบบสามารถอ่าน QR code ซึ่งปรากฏอยู่บนเอกสารแจ้งการตรวจลงตราของ ศูนย์ข้อมูลการตรวจลงตรา (Visa Data Center)
- (4) มีระบบบันทึกกิจกรรมการใช้งาน (Log) ของผู้ใช้งานระบบทั้งหมด โดยสามารถ ค้นหา ตรวจสอบ และออกรายงานได้

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

(5) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.3.11 โมดูล Administrative Management การกำหนดสิทธิ/การกำหนดการใช้งานของสถานเอกอัครราชทูตหรือสถานกงสุลใหญ่ เจ้าหน้าที่ส่วนกลางสามารถกำหนดสิทธิ เพิ่ม/ลด/ยกเลิกสิทธิของผู้ใช้งาน ในระบบทั้งหมด และตรวจสอบประวัติการเข้าใช้งานของผู้ใช้ได้ หรือเป็นไปตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

5.3.3.12 โมดูล Operation Date Management กำหนดวันหยุด/วันหยุดพิเศษ โดยต้องสามารถให้สถานเอกอัครราชทูต สถานกงสุลใหญ่ หรือกระทรวงการต่างประเทศ สามารถกำหนดวันหยุด/วันหยุดพิเศษ ได้ด้วยตนเอง

5.3.3.13 โมดูล Supporting Document Mapping

- (1) สามารถกำหนดเงื่อนไขในการเรียกเอกสารจากผู้ยื่นคำร้องในแต่ละประเภทได้
- (2) สามารถกำหนดเงื่อนไขตาม ประเภท Visa สัญชาติ สถานะภาพ หรือกำหนดเงื่อนไขอื่น ๆ ตามที่กระทรวงการต่างประเทศกำหนด เพื่อขอข้อมูลเพิ่มเติมอื่น ๆ จากผู้ยื่นคำร้องได้
- (3) สามารถกำหนดค่าธรรมเนียมในการยื่นคำร้องโดยสามารถกำหนดให้มีความแตกต่างกันในรายประเทศ หรือทั้งหมดพร้อมกันได้ และสามารถกำหนดเป็น 0 หรือ ฟรีค่าธรรมเนียมได้
- (4) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.3.14 โมดูล Risk Management

- (1) ฟังก์ชันการจัดการ Watchlist
 - (1.1) สามารถกำหนดข้อมูลรายชื่อผู้ติด Watchlist และระยะเวลาติด Watchlist ได้
 - (1.2) สามารถแชร์ข้อมูลระหว่าง สถานเอกอัครราชทูตหรือสถานกงสุลใหญ่ และ/หรือส่วนกลาง รวมทั้งหน่วยงานภายนอกได้
 - (1.3) สามารถจัดทำรายงานได้ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด
 - (1.4) เก็บประวัติการเพิ่ม/แก้ไข/ลบ ข้อมูล Watchlist ของเจ้าหน้าที่
- (2) ฟังก์ชันการจัดการ Blacklist/Watchlist ประกอบด้วย
 - (2.1) สามารถเชื่อม web service กับสำนักงานตรวจคนเข้าเมือง เพื่อรับข้อมูล Blacklist/Watchlist ได้ทั้งแบบอัตโนมัติและแบบ manual
 - (2.2) สามารถค้นหาผู้ติด Blacklist/Watchlist ได้โดยค้นจากชื่อ นามสกุล หมายเลขหนังสือเดินทาง หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนดได้
 - (2.3) สามารถตรวจสอบ log การดึงข้อมูลโดยสำนักงานตรวจคนเข้าเมืองได้
 - (2.4) สามารถ monitor สถานะการเชื่อมโยงข้อมูลกับระบบงานภายนอกอื่นได้
 - (2.5) สามารถเก็บประวัติการสืบค้นข้อมูล Blacklist/Watchlist ของเจ้าหน้าที่ได้ และสามารถดูรายงานประวัติการสืบค้นข้อมูลได้
- (3) ฟังก์ชันการกำหนดระดับความเสี่ยง

เจ้าหน้าที่ส่วนกลางสามารถปรับตั้งค่าระดับความเสี่ยง โดยกำหนดเงื่อนไขและ Business Flow เป็นการเฉพาะเพิ่มเติมได้ในแต่ละระดับความเสี่ยง โดยแบ่งระดับความเสี่ยงเป็น 3 ระดับ หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด โดยสามารถตั้งค่าเกณฑ์/เงื่อนไขของระดับความเสี่ยงโดยพิจารณาจากเงื่อนไขต่าง ๆ เช่น ประเทศ สัญชาติ ประเภทวีซ่า หรือตามกรมการกงสุล

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

กระทรวงการต่างประเทศ กำหนด หรือใช้เทคโนโลยีอื่นประกอบในการพิจารณาความเสี่ยง โดยสามารถ
แบ่งระดับความเสี่ยง ดังนี้

- เสี่ยงต่ำ (สีเขียว)
- เสี่ยงกลาง (สีเหลือง)
- เสี่ยงสูง (สีแดง)
- ความเสี่ยงอื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด
ทั้งนี้จะต้องออกแบบให้สามารถปรับตั้งค่าเงื่อนไข และ Business Flow

ของแต่ละระดับได้โดยง่าย และเป็นไปตามที่ผู้ว่าจ้างกำหนด

(4) สามารถกำหนดเงื่อนไขคำร้องที่จะต้องจัดส่งให้หน่วยงานความมั่นคง หรือ
หน่วยงานอื่น ๆ ที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด เพื่อทำการตรวจสอบให้โดยอัตโนมัติ

(5) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.3.15 โมดูลการจัดการผู้ยื่นคำร้อง

- สามารถกำหนดให้ผู้ยื่นคำร้องเป็น Watchlist หรือยกเลิก Watchlist ได้
- สามารถดูประวัติการยื่นคำร้องของผู้ร้องได้
- สามารถตรวจสอบเส้นทางการยื่นคำร้องของผู้ร้องได้

5.3.3.16 โมดูลการจัดการทั่วไป

- (1) สามารถเพิ่ม/ลดประเภท Visa เงื่อนไขเกี่ยวกับผู้ที่มีสิทธิ์ยื่น ประเภท
ของเอกสาร
- (2) สามารถกำหนดประเภทวีซ่า (enable/disable) และสามารถกำหนดเงื่อนไข
ของผู้ที่มีสิทธิ์ยื่น ประเภทของเอกสาร รวมถึงค่าธรรมเนียม

(3) สามารถแก้ไขข้อมูลการออก e-Visa และส่งข้อมูลที่แก้ไข โดยข้อมูลที่แก้ไข
สามารถส่งไปยังผู้ร้องได้อีกครั้งรวมทั้งหน่วยงานที่เกี่ยวข้องที่มีการเชื่อมโยงได้

(4) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.3.17 โมดูลการจัดการหมายเลข Visa

- (1) โมดูลนี้ใช้สำหรับให้เจ้าหน้าที่ของกรมการกงสุล กระทรวงการต่าง
ประเทศ ใช้สำหรับการบริหารจัดการหมายเลข Visa
- (2) Sticker Stock แสดงข้อมูลของจำนวน Visa Sticker ทั้งหมดที่มีใน Stock
- (3) Global Sticker Stock แสดงข้อมูลจำนวน Visa Sticker Stock ของ
สถานเอกอัครราชทูต และสถานกงสุลใหญ่ ที่เปิดใช้งานระบบ e-Visa
- (4) มีระบบแจ้งเตือนทั้งในส่วน of สถานเอกอัครราชทูต และสถานกงสุลใหญ่ และ
ส่วนกลาง ว่า Sticker Stock ที่ได้รับจัดสรร ใกล้จะหมดลง ตามเงื่อนไขที่กรมการกงสุล กระทรวง
การต่างประเทศ กำหนด
- (5) มีระบบที่สามารถจัดสรร Sticker Stock ล่วงหน้าได้ โดยส่วนกลาง โดยต้องม
ีการกดยืนยันการรับหมายเลขจากสถานเอกอัครราชทูต และสถานกงสุลใหญ่ และมีการบันทึก (log) การรับ
Sticker Stock ดังกล่าว พร้อมระบุเจ้าหน้าที่ที่เกี่ยวข้อง เวลา และหมายเหตุ (หากมี)

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

(6) มีระบบจัดทำรายงาน Sticker Inventory/Stock ที่เป็นทั้งสามารถดูในระบบ แบบ dynamic/real-time และเป็นรูปแบบรายงาน ที่สามารถเลือกการแสดงผลรายงานได้ตามที่เจ้าหน้าที่กำหนด (dynamic) หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(7) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.3.18 โมดูล Priority

- (1) มีระบบจัดการ priority สำหรับบุคคลผู้ต้องการได้รับอนุมัติเร่งด่วน
- (2) หน่วยงานอื่น ๆ สามารถยื่นข้อมูลของผู้ที่ต้องการ priority เข้ามาได้
- (3) เจ้าหน้าที่ backoffice สามารถจัดการอนุมัติสิทธิ์ หรือเพิกถอนสิทธิ์ Priority ได้
- (4) มีระบบลงทะเบียนสำหรับหน่วยงานภายนอกที่ต้องการขอสิทธิ์ Priority
- (5) มีช่องทางออนไลน์ให้หน่วยงานอื่น ๆ สามารถตรวจสอบการอนุมัติสิทธิ์

Priority ได้

(6) มีหน้ารายการแสดงผลผู้ร้องที่ได้รับอนุมัติ e-Visa จากการสั่งการ (PRIORITY input/list) โดยให้กรมการกงสุล กระทรวงการต่างประเทศ หรือสถานเอกอัครราชทูตและสถานกงสุลใหญ่สามารถเพิ่ม ลบ แก้ไข รายการได้ โดยใส่ชื่อนามสกุลและเลขหนังสือเดินทาง หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด โดยเมื่อมีผู้ร้องยื่นคำร้องในระบบที่ตรงกับเงื่อนไข จะต้องมีการแสดงผลเป็นแถบสีพิเศษว่า ผู้ร้องดังกล่าวเป็นกลุ่ม PRIORITY เพื่อให้สถานเอกอัครราชทูต และสถานกงสุลใหญ่ทราบและรีบพิจารณาการออก Visa ทั้งนี้ สามารถเข้าสู่รายการคำร้องของกลุ่ม PRIORITY ได้จากระบบ dashboard ของเจ้าหน้าที่ ซึ่งได้รับข้อมูลจากส่วนกลาง หรือมีการนำเข้าสู่ระบบจากเจ้าหน้าที่ในสถานเอกอัครราชทูต และสถานกงสุลใหญ่

(7) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.3.19 Web service

(1) คุณสมบัติพื้นฐานของ Web service มีดังนี้

- สามารถเชื่อมต่อ web service หน่วยงานที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด เพื่อรับส่งข้อมูลได้ทั้งแบบอัตโนมัติและแบบ manual
- สามารถกระทบบยอด (Reconcile) และเปรียบเทียบความถูกต้องตรงกัน ของข้อมูลระหว่างต้นทางและปลายทางได้ หากต้นทาง/ปลายทางมีบริการรองรับ
- สามารถควบคุมเปิด/ปิดการใช้งาน Web service ได้
- มีการจัดเก็บ log การใช้งาน

(2) บริการ Web service ได้แก่

- Blacklist/Watchlist web service มีการรับข้อมูล Blacklist/Watchlist จาก สตม.
- Approval web service
 - 1) เมื่อเจ้าหน้าที่สถานเอกอัครราชทูตและสถานกงสุลใหญ่อนุมัติ (Approve) คำร้อง จะมีการส่งข้อมูลการตรวจลงตราไปให้ สตม. โดยอัตโนมัติแบบ real-time
 - 2) สามารถดู log การจัดส่งข้อมูลได้ แบบรายวัน รายเดือน หรือตามช่วงเวลาที่กำหนดได้

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

(3) Web service อื่น ๆ

สามารถส่งข้อมูลให้หน่วยงานภายในกระทรวง/หน่วยงานภาครัฐ หรือหน่วยงานอื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนดให้ดำเนินการได้

5.3.3.20 โมดูลคำร้องขอของสถานเอกอัครราชทูต สถานกงสุลใหญ่ และ กระทรวงการต่างประเทศ

- (1) มีระบบคำขอลอยสถานะการออกวีซ่าได้
- (2) มีระบบคำขอยกเลิกหมายเลขวีซ่าได้ (Void Visa Sticker)
- (3) มีระบบแก้ไขรายละเอียดของ remark ได้
- (4) มีระบบแก้ไขรายละเอียดการออกวีซ่าได้
- (5) มีระบบให้ผู้ดูแลระบบสามารถอนุมัติ/ไม่อนุมัติคำขอได้
- (6) หรือระบบอื่น ๆ ตามกรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.4 ระบบการลงทะเบียนขอความอนุเคราะห์อำนวยความสะดวกสำหรับหน่วยงานภายนอก

5.3.4.1 มีระบบ online ที่ให้หน่วยงานสมัครบัญชีผู้ใช้และมีการลงทะเบียนข้อมูล เจ้าหน้าที่ของหน่วยงานที่สมัคร

5.3.4.2 ระบบสามารถให้กรมการกงสุล กระทรวงการต่างประเทศ อนุมัติการลงทะเบียน ให้หน่วยงานภายนอกและเจ้าหน้าที่ของหน่วยงานภายนอก

5.3.4.3 เมื่อได้รับการอนุมัติ ระบบจะส่งอีเมล พร้อม Username/Password ให้เจ้าหน้าที่ผู้สมัคร โดยการใช้งานในครั้งแรกต้องให้ผู้ใช้งานเปลี่ยน Password

5.3.4.4 ระบบดังกล่าว สามารถผลิต report เป็น word/PDF/Excel ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

5.3.4.5 ระบบดังกล่าว ดำเนินการแบบ standalone และสามารถเชื่อมโยงฐานข้อมูล เข้ากับระบบ e-Visa ในการส่งต่อคำร้องไปเป็น PRIORITY List ในระบบ e-Visa

5.3.4.6 มีมาตรฐานความปลอดภัย และการบริหารระบบสารสนเทศเช่นเดียวกับระบบ e-Visa ทั้งหมด

5.3.4.7 อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.3.5 ระบบ Mobile Application

ผู้รับจ้างต้องพัฒนา Mobile Application ดังนี้

5.3.5.1 ระบบ Mobile Application “Thai e-Visa” ของ Front Office

- (1) มีโมดูลการใช้งานทั้งหมดครบถ้วนตามข้อ 5.3.1 และ 5.3.2
- (2) สามารถติดตั้งใช้งานได้ทั้งในระบบ Android IOS และ Tablet และต้องสามารถรองรับการทำงานทั้งโทรศัพท์มือถือ และแท็บเล็ตได้อย่างมีประสิทธิภาพ

(3) ผู้รับจ้างต้องใช้ account สำหรับการพัฒนา Mobile Application “Thai e-Visa” ตาม account ที่กรมการกงสุลกำหนด

(4) ระบบที่พัฒนาต้องติดตั้งระบบบน cloud ให้สามารถรองรับการใช้งานตามจำนวน ผู้ใช้งานได้อย่างมีประสิทธิภาพ

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ 3.8 07/5 กรรมการ Jantana กรรมการ An กรรมการ

(5) มีระบบ Two-Factor Authentication (2FA) ที่รองรับรองรับมาตรฐานของสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (ETDA) AAL ระดับ 2 จากเอกสาร ชมธอ. 20-2566

(6) ผู้รับจ้างต้องรับผิดชอบค่าใช้จ่ายและค่าบำรุงรักษา รวมทั้งค่าใช้จ่ายทั้งหมดในการติดตั้งใช้งาน Mobile Application “Thai e-Visa” ทั้งในระบบ Android IOS และ Tablet ตลอดระยะเวลาที่รับประกันตามสัญญา

(7) รองรับและแสดงผลได้หลายภาษาตามข้อ 5.3.1.6

(8) พัฒนาระบบให้รองรับการอัปเดตของ android และ iOS

(9) มีระบบรักษาความปลอดภัยของข้อมูล อาทิ ระบบป้องกันการ Capture หน้าจอระบบใส่ลายนิ้วมือ

(10) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

(11) ในกรณีที่มีการพัฒนาฟังก์ชันการใช้งานอื่น ๆ เพิ่มเติม ผู้รับจ้างต้องแจ้งให้กรมการกงสุลรับทราบและอนุมัติก่อนการดำเนินงาน

5.3.5.2 ระบบ Mobile Application “Thai e-Visa” ของ Back Office

(1) มีโมดูลการใช้งานทั้งหมดครบถ้วนตามข้อ 5.3.1 และ 5.3.3

(2) สามารถติดตั้งใช้งานได้ทั้งในระบบ Android IOS และ Tablet และต้องสามารถรองรับการทำงานทั้งโทรศัพท์มือถือ และแท็บเล็ตได้อย่างมีประสิทธิภาพ

(3) ผู้รับจ้างต้องใช้ account สำหรับการพัฒนา Mobile Application “Thai e-Visa” ตาม account ที่กรมการกงสุลกำหนด

(4) ระบบที่พัฒนาต้องติดตั้งระบบบน cloud ให้สามารถรองรับการใช้งานตามจำนวนผู้ใช้งานได้อย่างมีประสิทธิภาพ

(5) มีระบบ Two-Factor Authentication (2FA) ที่รองรับการเข้าใช้งานระบบทุกครั้งผ่านระบบการเข้าถึงเครือข่ายแบบ Zero Trust Network Access (ZTNA) ตามข้อ 5.8.1

(6) ผู้รับจ้างต้องรับผิดชอบค่าใช้จ่ายและค่าบำรุงรักษา รวมทั้งค่าใช้จ่ายทั้งหมดในการติดตั้งใช้งาน Mobile Application “Thai e-Visa” ทั้งในระบบ Android IOS และ Tablet ตลอดระยะเวลาที่รับประกันตามสัญญา

(7) รองรับและแสดงผลได้หลายภาษาตามข้อ 5.3.1.6

(8) พัฒนาระบบให้รองรับการอัปเดตของ android และ iOS

(9) มีระบบรักษาความปลอดภัยของข้อมูล อาทิ ระบบป้องกันการ Capture หน้าจอระบบใส่ลายนิ้วมือ

(10) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

(11) ในกรณีที่มีการพัฒนาฟังก์ชันการใช้งานอื่น ๆ เพิ่มเติม ผู้รับจ้างต้องแจ้งให้กรมการกงสุลรับทราบและอนุมัติก่อนการดำเนินงาน

5.3.5.3 ระบบ Mobile Application “Visa Checking”

(1) มีโมดูลการใช้งานทั้งหมดครบถ้วนตามข้อ 5.3.3.10

(2) สามารถติดตั้งใช้งานได้ทั้งในระบบ Android IOS และ Tablet และต้องสามารถรองรับการทำงานทั้งโทรศัพท์มือถือ และแท็บเล็ตได้อย่างมีประสิทธิภาพ

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

(3) ผู้รับจ้างต้องใช้ account สำหรับการพัฒนา Mobile Application “Thai e-Visa” ตาม account ที่กรมการกงสุลกำหนด

(4) ระบบที่พัฒนาต้องติดตั้งระบบบน cloud ให้สามารถรองรับการใช้งานตามจำนวนผู้ใช้งานได้อย่างมีประสิทธิภาพ

(5) มีระบบ authentication ที่รองรับการเข้าใช้งานระบบทุกครั้งผ่านระบบการเข้าถึงเครือข่ายแบบ Zero Trust Network Access (ZTNA) ตามข้อ 5.8.1

(6) ผู้รับจ้างต้องรับผิดชอบค่าใช้จ่ายและค่าบำรุงรักษา รวมทั้งค่าใช้จ่ายทั้งหมดในการติดตั้งใช้งาน Mobile Application “Thai e-Visa” ทั้งในระบบ Android IOS และ Tablet ตลอดระยะเวลาที่รับประกันตามสัญญา

(7) รองรับและแสดงผลได้หลายภาษาตามข้อ 5.3.1.6

(8) พัฒนาระบบให้รองรับการอัปเดตของ android และ iOS

(9) มีระบบรักษาความปลอดภัยของข้อมูล อาทิ ระบบป้องกันการ Capture หน้าจอ ระบบใส่ลายนิ้วมือ

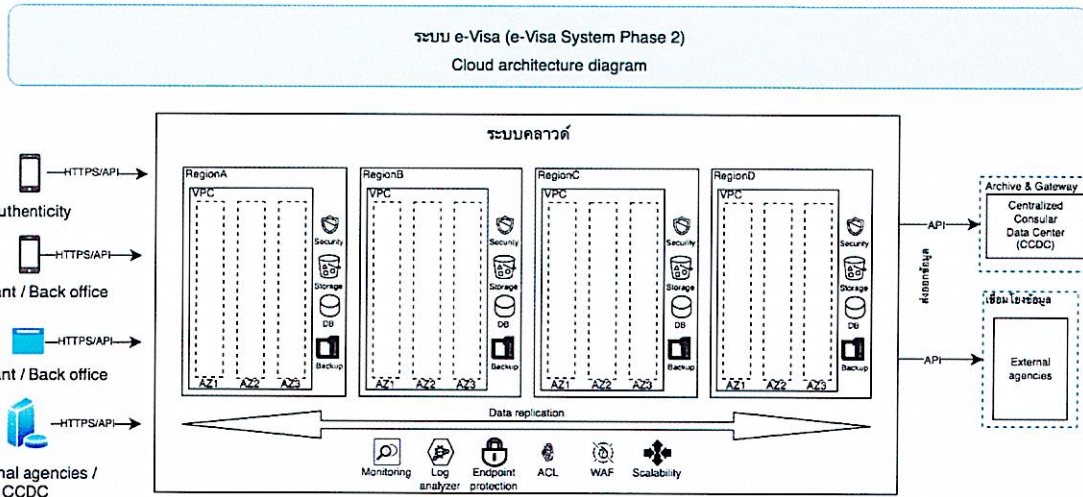
(10) อื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

(11) ในกรณีที่มีการพัฒนาฟังก์ชันการใช้งานอื่น ๆ เพิ่มเติม ผู้รับจ้างต้องแจ้งให้กรมการกงสุลรับทราบและอนุมัติก่อนการดำเนินงาน

5.4 ระบบคลาวด์ e-Visa ระยะที่ 2 (e-Visa Cloud System Phase 2)

ผู้รับจ้างต้องมีการออกแบบ จัดทำ จัดหา บริหารจัดการและดูแลระบบคลาวด์โดยสามารถรองรับคำร้องผู้ขอรับการตรวจลงตราได้ไม่ต่ำกว่า 20,000,000 รายการ ตลอดระยะเวลาตามสัญญา จนครบสัญญา ทั้งนี้ ระบบคลาวด์จะต้องมี 4 Regions อยู่ทั่วโลก ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด โดยออกแบบให้สามารถดำเนินการโดยไม่มีความเสี่ยงของการขัดข้องและต้องเปิดให้บริการ และมีประสิทธิภาพสูงสุด ทั้งเรื่องความเร็วของการเข้าถึงระบบของผู้ร้อง เจ้าหน้าที่ผู้ใช้งาน และการเชื่อมโยงข้อมูลกับหน่วยงานที่เกี่ยวข้องแบบ real-time โดยมีรายละเอียดคุณสมบัติ ดังนี้

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ



รูปสถาปัตยกรรมการตรวจลงตรา และมาตรฐานของระบบคลาวด์ e-Visa ระยะที่ 2

<https://1drv.ms/i/s!Ap8pk0aBGx6Cq8RPqFWSAol2H1FEXg?e=sJnDku>



5.4.1 ผู้รับจ้างจะต้องเสนอระบบคลาวด์มีมาตรฐาน ดังนี้

5.4.1.1 ระบบคลาวด์ที่เสนอต้องผ่านมาตรฐาน ISO9001, ISO27001, ISO27017, ISO27018, SOC1, SOC2, SOC3, PCI DSS, ISO20000-1 เป็นอย่างน้อย

5.4.1.2 ระบบคลาวด์ที่เสนอต้องผ่านมาตรฐานความมั่นคงปลอดภัยของ CSA STAR จาก Cloud Security Alliance (CSA) ดังนี้ CSA STAR Self-Assessment, CSA STAR Certification, CSA STAR Attestation

5.4.1.3 ระบบคลาวด์ที่เสนอต้องมี Region Data Center แบบ full service ที่เปิดให้บริการไม่น้อยกว่า 20 แห่ง และไม่น้อยกว่า 20 ประเทศทั่วโลก

5.4.1.4 ระบบคลาวด์ที่เสนอต้องสามารถสร้างบริการในหลาย Region Data Center โดยต้องมีที่ตั้งไม่น้อยกว่า 20 ประเทศ กระจายในแต่ละภูมิภาคทั่วโลก เช่น Asia Pacific, Europe, Middle East, Africa, North และ South America

5.4.1.5 ระบบคลาวด์ที่เสนอต้องมีระดับความพร้อมใช้งาน (Uptime) ร้อยละ 99.99

5.4.2 ออกแบบ จัดทำ จัดหา บริหารจัดการและดูแลสถาปัตยกรรมระบบคลาวด์ e-Visa ระยะที่ 2

5.4.2.1 ออกแบบ จัดทำ จัดหา บริหารจัดการและดูแลระบบคลาวด์ e-Visa ระยะที่ 2 ให้เกิดประสิทธิภาพสูงสุด เป็นระบบที่มีสภาพพร้อมใช้งานสูงหรือที่เรียกว่า High Availability (HA) โดยที่มีจำนวน Region ที่ทำงานพร้อมกันอย่างน้อย 4 Region ในรูปแบบ Active / Active เพื่อกระจายการให้บริการให้ครอบคลุมทั่วโลก ซึ่งทุก ๆ ภูมิภาคจะให้บริการพร้อม ๆ กันทั้งหมด หากเกิดเหตุให้ Region หนึ่งหยุดทำงาน หรือเครือข่ายใน Region นั้นเสียหาย ระบบ Region ที่เหลือก็จะรับภาระงานทดแทน ทำให้ไม่สูญเสียการบริการ (Fault Tolerance) โดยเน้นการออกแบบที่หลีกเลี่ยงการเกิดปัญหาจากจุดเดียว (Single-Point of Failure) และรองรับการทำ Site Replication ข้อมูลให้เท่ากันกับ Region ทั้งหมด และต้องออกแบบให้ระบบมีกระบวนการสำรองระหว่าง Region ด้วย โดยออกแบบให้มีความมั่นคงปลอดภัย

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

ในการรับ - ส่งข้อมูลระหว่าง Region รวมทั้งพร้อมรองรับการขยายการให้บริการระบบงานในสถานเอกอัครราชทูต และสถานกงสุลใหญ่ทั่วโลกในอนาคต

5.4.2.2 ออกแบบ จัดทำ จัดหา บริหารจัดการและดูแลให้ระบบคลาวด์ e-Visa ระยะที่ 2 ของแต่ละ Region มีระบบที่มีสภาพพร้อมใช้งานสูง หรือที่เรียกว่า High Availability (HA) โดยที่มีจำนวน Availability Zone ที่ทำงานพร้อมกันอย่างน้อย 3 zone ในรูปแบบ Active / Active ซึ่งทุก ๆ zone จะให้บริการพร้อม ๆ กันทั้งหมด หากเกิดเหตุให้ zone ใด zone หนึ่งหยุดทำงาน ระบบคลาวด์ของ Region นั้น จะยังคงรับภาระงานทดแทน ทำให้ไม่สูญเสียการบริการ (Fault Tolerance) โดยเน้นการออกแบบที่หลีกเลี่ยงการเกิดปัญหาจากจุดเดียว (Single-Point of Failure) และรองรับการทำ Site Replication ข้อมูลให้เท่ากันกับทั้ง 3 zone และต้องออกแบบให้ระบบมีกระบวนการสำรองระหว่าง site ด้วย โดยออกแบบให้มีความมั่นคงปลอดภัยในการรับ - ส่งข้อมูลระหว่าง zone โดยที่มี 4 Region 12 zone เป็นอย่างน้อย

5.4.2.3 ออกแบบ จัดทำ จัดหา บริหารจัดการและดูแลระบบคลาวด์ e-Visa ระยะที่ 2 ส่งข้อมูลคำร้องขอรับการตรวจลงตราและข้อมูลเอกสารแนบ ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนดมายังศูนย์บริหารข้อมูลกลางกรมการกงสุล (CCDC) เพื่อสำเนาข้อมูลการตรวจลงตราไว้ที่ประเทศไทย

5.4.2.4 ออกแบบ จัดทำ จัดหา บริหารจัดการและดูแล ระบบคลาวด์ e-Visa รองรับกับการเชื่อมโยงข้อมูลกับหน่วยงานภายนอก เพื่อบูรณาการข้อมูลกับหน่วยงานที่เกี่ยวข้อง โดยจะต้องมีระบบกลางในการรับ-ส่งข้อมูล (Broker) โดยมีการเชื่อมต่อในรูปแบบ API (Application Programming Interface) หรือเชื่อมต่อแบบอื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด ทั้งนี้ จะต้องออกแบบให้สามารถเชื่อมต่อกับหน่วยงานภายนอกได้ทั้งแบบเชื่อมต่อโดยตรงหรือผ่าน consular gateway และสามารถปรับเปลี่ยนรูปแบบการเชื่อมต่อได้ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด โดยไม่ต้องแก้ไขโปรแกรม โดยเป็นการเชื่อมโยงข้อมูลกับหน่วยงานต่าง ๆ ดังนี้

- สำนักงานตรวจคนเข้าเมือง (สตม.)
- สำนักข่าวกรองแห่งชาติ (สขช.)
- หน่วยงานที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

ทั้งนี้ รูปแบบการเชื่อมโยงข้อมูลจะเป็นไปตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.4.2.5 ออกแบบ จัดทำ จัดหา บริหารจัดการและดูแลระบบคลาวด์ e-Visa รองรับการใช้งานระบบ e-Visa สำหรับประชาชนในรูปแบบเว็บแอปพลิเคชันโดยจะต้องมีการเข้ารหัสข้อมูล (Encryption) เพื่อเพิ่มความปลอดภัย ในการสื่อสารหรือส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต รองรับการใช้งานผ่านมาตรฐาน TLS 1.2 (Transport Layer Security) หรือใหม่กว่า และรองรับการใช้งานระบบการเข้าถึงเครือข่ายแบบ Zero Trust Network Access (ZTNA) กับผู้ใช้งานระบบ e-Visa ในส่วนของเจ้าหน้าที่ กระทรวงการต่างประเทศ ทั้งที่อยู่ในประเทศไทย และอยู่ในสำนักงานในต่างประเทศได้เป็นอย่างดี ไม่ติดขัด หรือสะดุด ทั้งนี้ ระบบ e-Visa ต้องสามารถรองรับการใช้งานพร้อมกันสูงสุด (Concurrent sessions) ไม่น้อยกว่า 1,000 คน มี Throughput ที่เพียงพอ ในการรองรับกับการใช้งานพร้อมกันได้

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

5.4.2.6 รายละเอียดทรัพยากรขั้นต่ำของระบบคลาวด์มีมาตรฐานและมืองค์ประกอบของระบบ ดังต่อไปนี้

(1) ระบบ Cloud Server มีรายละเอียดอย่างน้อย ดังนี้

- มีพื้นที่ประมวลผล (instance) บนคลาวด์ สำหรับวัตถุประสงค์ทั่วไป หรือการประมวลผลที่ปรับให้เหมาะสมกับหน่วยความจำ
- มีโปรเซสเซอร์ให้เลือกใช้ อาทิ Intel, AMD, NVIDIA สามารถทำ Compute Optimizer เพื่อบริหารทรัพยากรที่เหมาะสมที่สุดสำหรับปริมาณงาน ต้นทุนและปรับปรุงประสิทธิภาพ

(2) ระบบ Cloud Object Storage มีรายละเอียดอย่างน้อย ดังนี้

- เป็น Object Storage ที่มีความสามารถในการปรับขนาด ความพร้อมใช้งานของข้อมูล ความปลอดภัยและประสิทธิภาพ รองรับการจัดเก็บและปกป้องข้อมูลจำนวนเท่าใดก็ได้สำหรับการใช้งาน เช่น Data Lake แอปพลิเคชันบนคลาวด์ บนอุปกรณ์เคลื่อนที่ สามารถจัดระเบียบข้อมูล และกำหนดค่าการควบคุมการเข้าถึงที่ปรับแต่งอย่างละเอียด
- ระบบ Object Storage สามารถจัดสรรพื้นที่จัดเก็บข้อมูลแบบ Object Storage แบบมีคุณสมบัติในการป้องกันข้อมูลแบบ Write Once, Read Many (WORM) ได้
- ระบบ Object Storage ต้องสามารถกำหนดค่าและบังคับใช้การควบคุมการเข้าถึงข้อมูล, ปกป้องข้อมูลจากผู้ที่ไม่ได้รับอนุญาต
- ระบบ Object Storage ต้องรองรับคุณสมบัติที่ช่วยรักษาการควบคุมเวอร์ชันข้อมูล ป้องกันการลบโดยไม่ตั้งใจ
- ระบบ Object Storage ต้องสามารถมองเห็นการใช้งานพื้นที่จัดเก็บของ Object

- ระบบ Object Storage มีความทนทาน (Durability) ไม่น้อยกว่า 99.999999999% และความพร้อมใช้งาน 99.99% ต่อปี

(3) ระบบสร้างและจัดการเซิร์ฟเวอร์เสมือน (Virtual Private Server)

มีรายละเอียดอย่างน้อย ดังนี้

- สามารถสร้างเครื่อง Cloud Server ที่พร้อมใช้งานจาก Blueprint บน Console หรือ API ที่ใช้งานได้อย่างง่าย
- มี Blueprint ให้เลือกสร้าง Cloud Server ดังต่อไปนี้เป็นอย่างน้อย Windows Server Only, Windows Server +, SQL Server Express, Linux Only, Linux + WordPress, Linux + Node.js, Linux + Nginx
- สามารถ Remote เครื่อง Cloud Server ผ่าน Public IP ได้
- มีความสามารถในการสำรองข้อมูลของเครื่อง Cloud Server ได้ผ่านหน้า Console

(4) ระบบฐานข้อมูลเชิงสัมพันธ์ Relational Database Service มีรายละเอียด

อย่างน้อย ดังนี้

- Relational Database Service RDS เป็นฐานข้อมูลเชิงสัมพันธ์ที่มี

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

การจัดการซึ่งมีเครื่องมือฐานข้อมูลให้เลือก เช่น MySQL-Compatible Edition, PostgreSQL-Compatible Edition, MySQL, MariaDB, PostgreSQL, Oracle หรือ Microsoft SQL Server

- สามารถจัดเตรียม การแพตช์ การสำรองข้อมูล การกู้คืน การตรวจจับความล้มเหลว และการซ่อมแซม built-in automated failover from your primary database to a synchronously replicated secondary database. Using Read Replicas

- สามารถปรับขนาด (Scale out) การปรับใช้ฐานข้อมูลเดียวสำหรับ workload ฐานข้อมูลที่มีปริมาณมาก

- สามารถกู้คืนฐานข้อมูล Database โดยวิธี point in time recovery ได้

(5) บริการแคชในหน่วยความจำ มีรายละเอียดอย่างน้อย ดังนี้

- เป็นระบบ Cache สามารถตั้งค่า จัดการ และปรับขนาดสภาพแวดล้อมในหน่วยความจำใน Cloud ปรับขนาดได้

- สามารถจัดการสภาพแวดล้อมให้สามารถทำงานร่วมกับ Redis และ Memcached ได้

(6) ระบบ Application Load Balancer มีรายละเอียดอย่างน้อย ดังนี้

- เป็น Load balance ทำงานที่ Layer 7 สามารถกำหนดเส้นทางการรับส่งข้อมูลไปยังเป้าหมาย ตามเนื้อหาของคำขอ Application Load Balancer

- สามารถปรับสมดุลโหลด (Elastic Load Balancing) ของทราฟฟิก HTTP และ HTTPS ให้การกำหนดเส้นทางการกำหนดเป้าหมายรวมถึงไมโครเซอร์วิสและแอปพลิเคชันที่ใช้คอนเทนเนอร์ Application Load Balancer

- สามารถตรวจสอบการใช้การเข้ารหัสและโปรโตคอล SSL/TLS ล่าสุดตลอดเวลา

- สามารถกระจายทราฟฟิก HTTP/HTTPS ไปยังเป้าหมาย อาทิ อินสแตนซ์ไมโครเซอร์วิส และคอนเทนเนอร์ตามคำขอ

(7) ระบบการยืนยันตัวตน มีรายละเอียดอย่างน้อย ดังนี้

- มีระบบจัดการการยืนยันตัวตนและการให้สิทธิ์ผู้ใช้สำหรับเว็บและแอปบนอุปกรณ์เคลื่อนที่ ด้วยกลุ่มผู้ใช้ (users)

- สามารถเพิ่มฟังก์ชันการลงชื่อสมัครใช้และการลงชื่อเข้าใช้ในแอปของได้ด้วย Identity Pools (Federated Identities)

- สามารถรับข้อมูลรับรองชั่วคราวที่อนุญาตให้ผู้ใช้เข้าถึงทรัพยากรที่เฉพาะเจาะจงไม่ว่าผู้ใช้อยู่ไม่ระบุตัวตนหรือลงชื่อเข้าใช้

(8) ระบบเครือข่ายจัดเก็บและส่งเนื้อหาเว็บ (Content Delivery Network: CDN) มีรายละเอียดอย่างน้อย ดังนี้

- รองรับเครือข่ายการจัดส่งเนื้อหา (CDN) ที่สร้างขึ้นเพื่อประสิทธิภาพสูง ความปลอดภัย และความเสถียรของนักพัฒนา

- รองรับผู้ใช้ในประเทศ ระดับมิลลิวินาทีด้วยการบีบอัดข้อมูลในตัว และมีความสามารถในการประมวลผลแบบ Edge

- มีการเข้ารหัสระดับฟิลด์

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

(9) คุณลักษณะของบริการระบบ Network Firewall มีรายละเอียดอย่างน้อย ดังนี้

- เป็น stateful firewall ที่สามารถบริหารจัดการได้
- มีบริการตรวจจับและป้องกันการบุกรุกสำหรับระบบคลาวด์ส่วนตัวเสมือน (VPC)

(10) ระบบบริการ DNS มีรายละเอียดอย่างน้อย ดังนี้

- มีความพร้อมใช้งานสูง ปรับขนาดได้ และปลอดภัย เหมาะสำหรับการใช้งาน

กับแอปพลิเคชันทุกประเภท

- โครงสร้างพื้นฐานที่กระจายอยู่ทั่วโลก
- รองรับการ Multi-AZ
- มีความพร้อมใช้งาน (availability) 99.9%
- รองรับ DNSSEC

(11) ระบบติดตามกิจกรรมและเหตุการณ์ต่าง ๆ มีรายละเอียดอย่างน้อย ดังนี้

- การตรวจสอบและวิเคราะห์ (Audit and Analysis) สามารถตรวจสอบการกระทำต่าง ๆ ที่เกิดขึ้นในบัญชี อาทิ การสร้าง การแก้ไข และการลบทรัพยากร พร้อมช่วยในการวิเคราะห์และตรวจจับกิจกรรมที่ไม่พึงประสงค์หรือผิดปกติได้เป็นอย่างน้อย

- การแจ้งเตือน (Alerting) ตั้งค่าการแจ้งเตือนเมื่อมีกิจกรรมที่น่าสงสัยเกิดขึ้นตามบันทึก และการแจ้งเตือนสามารถส่งไปยังช่องทางต่าง ๆ อาทิ อีเมล SMS หรือระบบการจัดการเหตุการณ์อื่น ๆ ได้เป็นอย่างน้อย

- การปฏิบัติตามข้อกำหนด (Compliance) บันทึกการทำงานที่ถูกจัดเก็บสามารถใช้เป็นหลักฐานในการตรวจสอบการปฏิบัติงานและการตรวจสอบภายในได้เป็นอย่างน้อย

- การรายงานและการวิเคราะห์ (Reporting and Analytics) รองรับการสร้างรายงานตามความต้องการ และใช้เครื่องมือวิเคราะห์เพื่อสืบค้นและประมวลผลข้อมูลบันทึกได้อย่างมีประสิทธิภาพได้เป็นอย่างน้อย

(12) บริการตรวจจับภัยคุกคามอัจฉริยะมีรายละเอียดอย่างน้อย ดังนี้

- สามารถทำงานได้ในลักษณะ Cloud Detection and Response (CDR)

- การวิเคราะห์พฤติกรรม (Behavioral Analysis) สามารถเรียนรู้การทำงานของอุปกรณ์ต่าง ๆ ในระบบ Cloud เพื่อวิเคราะห์และตรวจจับพฤติกรรมที่ผิดปกติ อาทิ การเรียนรู้ของเครื่อง (Machine Learning) รวมทั้ง สามารถตรวจสอบการเข้าถึงที่น่าสงสัยและกิจกรรมที่มีความเสี่ยงสูงได้เป็นอย่างน้อย

- การตรวจจับภัยคุกคาม (Threat Detection) ตรวจจับภัยคุกคามที่รู้จักและที่ไม่รู้จัก อาทิ มัลแวร์ การโจมตีแบบ brute force และการบุกรุก พร้อมมีการแจ้งเตือนแบบเรียลไทม์เมื่อพบกิจกรรมที่ต้องสงสัยได้เป็นอย่างน้อย

- การผสมรวมข้อมูล (Data Integration) ผสมรวมข้อมูลจากแหล่งต่าง ๆ อาทิ การบันทึกการทำงานของคลาวด์ บันทึก DNS และข้อมูล flow ของเครือข่าย พร้อมสามารถรวมข้อมูลจากบริการด้านความปลอดภัยอื่น ๆ เพื่อการวิเคราะห์แบบครบวงจรได้เป็นอย่างน้อย

(13) บริการตรวจสอบช่องโหว่และการประเมินความปลอดภัย มีรายละเอียดอย่างน้อย ดังนี้

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

- การตรวจสอบช่องโหว่ (Vulnerability Assessment) สามารถสแกนหาช่องโหว่ในระบบและแอปพลิเคชันต่าง ๆ อย่างต่อเนื่อง พร้อมรายงานและให้คำแนะนำสำหรับการแก้ไขช่องโหว่ที่พบได้เป็นอย่างน้อย

- การตรวจสอบการปฏิบัติตามข้อกำหนด (Compliance Checks) สามารถตรวจสอบความสอดคล้องกับมาตรฐานและกฎระเบียบต่าง ๆ อาทิ CIS Benchmarks, HIPAA, และ PCI-DSS พร้อมรายงานสถานะความปลอดภัยและการปฏิบัติตามข้อกำหนดได้เป็นอย่างน้อย

- การบูรณาการกับบริการอื่น (Service Integration) สามารถผสานรวมกับระบบการจัดการการรักษาความปลอดภัยอื่น ๆ เพื่อเสริมกระบวนการป้องกัน พร้อมแจ้งเตือนและรายงานไปยังระบบการจัดการเหตุการณ์และการเฝ้าระวังได้เป็นอย่างน้อย

(14) บริการสนับสนุนการจัดการความปลอดภัยมีรายละเอียดอย่างน้อย ดังนี้

- การรวมข้อมูลด้านความปลอดภัย (Security Data Aggregation) สามารถรวมข้อมูลจากบริการด้านความปลอดภัยต่าง ๆ ในระบบคลาวด์ และสร้างภาพรวมของสถานะความปลอดภัยไว้ที่เดียวได้เป็นอย่างน้อย รวมถึงสามารถประเมินความเสี่ยงและจัดลำดับความสำคัญของเหตุการณ์ที่ตรวจพบ

- การตรวจสอบและการแจ้งเตือน (Monitoring and Alerting) สามารถตรวจสอบสถานะความปลอดภัยแบบ real-time พร้อมแจ้งเตือนเมื่อพบกิจกรรมที่ผิดปกติหรือมีความเสี่ยงได้เป็นอย่างน้อย

- การวิเคราะห์และรายงาน (Analytics and Reporting) มีเครื่องมือที่สามารถวิเคราะห์เพื่อประเมินและตรวจจับปัญหาด้านความปลอดภัย พร้อมสร้างรายงานที่มีรายละเอียดเกี่ยวกับสถานะความปลอดภัยและการปฏิบัติตามข้อกำหนดได้เป็นอย่างน้อย

- การตอบสนอง (Threat Response) ระบบจะต้องสามารถดำเนินการตอบสนองต่อภัยคุกคามโดยอัตโนมัติตามขั้นตอนที่กำหนดไว้ล่วงหน้า (playbook) อาทิ การแยกอุปกรณ์ที่ถูกโจมตีออกจากเครือข่าย การจำกัดการเข้าถึง หรือการหยุดการทำงานของกระบวนการที่เป็นอันตราย ซึ่งเป็นการลดความเสียหายและจำกัดการแพร่กระจายของภัยคุกคามในระบบคลาวด์

(15) บริการจัดการข้อมูลที่ละเอียดอ่อน มีรายละเอียดอย่างน้อย ดังนี้

- การค้นพบข้อมูลที่ละเอียดอ่อน (Sensitive Data Discovery) มีการค้นพบและจำแนกข้อมูลที่ละเอียดอ่อน อาทิ ข้อมูลส่วนบุคคล (PII) และข้อมูลทางการเงินและสามารถวิเคราะห์และจัดหมวดหมู่ข้อมูลตามระดับความเสี่ยงได้เป็นอย่างน้อย

- การปกป้องข้อมูล (Data Protection) สามารถแนะนำแนวทางและเครื่องมือในการปกป้องข้อมูลที่ละเอียดอ่อนรวมถึงการเข้ารหัสและการควบคุมการเข้าถึงได้เป็นอย่างน้อย

- การปฏิบัติตามข้อกำหนด (Compliance Support) สามารถปฏิบัติตามข้อกำหนดด้านการปกป้องข้อมูล อาทิ GDPR รวมถึงสร้างรายงานเกี่ยวกับสถานะและความปลอดภัยของข้อมูลที่ละเอียดอ่อนได้เป็นอย่างน้อย

(16) บริการการจัดการคีย์เข้ารหัส มีรายละเอียดอย่างน้อย ดังนี้

- การสร้างและการจัดการคีย์ (Key Creation and Management) สามารถสร้างคีย์เข้ารหัสสำหรับการปกป้องข้อมูล จัดการวงจรชีวิตของคีย์ ตั้งแต่การสร้าง การหมุนเวียน การปิดใช้งาน และการลบคีย์ได้เป็นอย่างน้อย

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

- การเข้ารหัสและถอดรหัส (Encryption and Decryption) รองรับการเข้ารหัสและถอดรหัสข้อมูลที่มีความปลอดภัยสูง และการใช้คีย์เข้ารหัสในการปกป้องข้อมูลทั้งในขณะพักและขณะส่งข้อมูลได้เป็นอย่างดี

- การควบคุมการเข้าถึง (Access Control) สามารถกำหนดนโยบายการเข้าถึงคีย์ เพื่อควบคุมว่าผู้ใช้หรือบริการใดมีสิทธิ์ในการใช้คีย์ และสนับสนุนการตรวจสอบและบันทึกการใช้งานคีย์เพื่อการติดตามและการตรวจสอบความปลอดภัยได้เป็นอย่างดี

- การรวมระบบ (Integration) ผสานรวมกับบริการอื่น ๆ ในระบบ Cloud เพื่อใช้คีย์เข้ารหัสในการปกป้องข้อมูล พร้อมสนับสนุนการเข้ารหัสข้อมูลในบริการต่างๆ อาทิ การจัดเก็บข้อมูล การประมวลผล และการส่งข้อมูลได้เป็นอย่างดี

- การปฏิบัติตามข้อกำหนด (Compliance) ปฏิบัติตามมาตรฐานและข้อกำหนดด้านความปลอดภัย อาทิ GDPR พร้อมสร้างรายงานและบันทึกการใช้งานคีย์เพื่อการตรวจสอบและการปฏิบัติตามข้อกำหนดได้เป็นอย่างดี

(17) บริการการตรวจสอบระบบและตอบสนองเหตุการณ์ มีรายละเอียดอย่างน้อย ดังนี้

- การตรวจสอบและบันทึก (Monitoring and Logging) สามารถเก็บรวบรวมและตรวจสอบข้อมูล metrics จากทรัพยากรต่าง ๆ ในระบบ อาทิ CPU, memory และการใช้งาน storage พร้อมสามารถบันทึกเหตุการณ์และการทำงานของระบบเพื่อการวิเคราะห์และแก้ไขปัญหาได้เป็นอย่างดี

- การแจ้งเตือน (Alerting) สามารถตั้งค่าการแจ้งเตือนตามเงื่อนไขที่กำหนด อาทิ การใช้ทรัพยากรเกินขีดจำกัดหรือข้อผิดพลาดในแอปพลิเคชัน พร้อมสามารถส่งการแจ้งเตือนไปยังช่องทางต่าง ๆ อาทิ อีเมล SMS, หรือระบบการจัดการเหตุการณ์อื่น ๆ ได้เป็นอย่างดี

- การสร้าง dashboard (Dashboard Creation) สามารถสร้าง dashboard ที่ปรับแต่งได้ เพื่อแสดงข้อมูล matrix และ logs รวมทั้งรวมข้อมูลจากหลายแหล่งเพื่อสร้างภาพรวมของประสิทธิภาพและสถานะของระบบได้เป็นอย่างดี

- การเก็บข้อมูลและการวิเคราะห์ (Data Storage and Analytics) เก็บรักษาข้อมูล matrix และ logs ในระยะยาวเพื่อการวิเคราะห์และการตรวจสอบย้อนหลัง พร้อมมีเครื่องมือวิเคราะห์ในการสืบค้นและประมวลผลข้อมูลเพื่อค้นหาสาเหตุของปัญหาและการปรับปรุงประสิทธิภาพได้เป็นอย่างดี

- การจัดการเหตุการณ์ (Event Management) สร้างและจัดการเหตุการณ์อัตโนมัติเมื่อพบการทำงานที่ผิดปกติหรือการแจ้งเตือนที่กำหนด พร้อมผสานรวมกับเครื่องมือจัดการเหตุการณ์อื่น ๆ เพื่อการตอบสนองต่อเหตุการณ์อย่างรวดเร็วและมีประสิทธิภาพได้เป็นอย่างดี

- การปรับขนาดอัตโนมัติ (Auto Scaling) ปรับขนาดทรัพยากรโดยอัตโนมัติตามการใช้งานและเงื่อนไขที่กำหนด ช่วยให้ระบบสามารถตอบสนองต่อความต้องการที่เปลี่ยนแปลงได้อย่างรวดเร็วและมีประสิทธิภาพได้เป็นอย่างดี

- การตรวจสอบประสิทธิภาพของแอปพลิเคชัน (Application Performance Monitoring) ตรวจสอบประสิทธิภาพของแอปพลิเคชันเพื่อระบุปัญหาคอขวดและการทำงานที่ไม่เป็นไปตามคาดหวัง พร้อมวิเคราะห์และปรับปรุงประสิทธิภาพของแอปพลิเคชันตามข้อมูลที่ได้รับได้เป็นอย่างดี

- รองรับการส่งข้อมูล Log Files ทั้งในส่วนของ logs จากระบบปฏิบัติการ (System logs) logs จากแอปพลิเคชันต่าง ๆ (Application logs) logs จากระบบรักษาความปลอดภัย (Security logs) logs จากอุปกรณ์เครือข่าย (Network logs) และ logs จากระบบอื่นใดที่กรมการกงสุล

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

กระทรวงการต่างประเทศกำหนด มายังระบบเผื่อระวัง ตรวจสอบและวิเคราะห์ภัยคุกคามทางไซเบอร์ ที่กรมการกงสุลเตรียมไว้ให้

ทั้งนี้ ผู้รับจ้าง จะต้องจัดทำแผน มาตรการจัดการ หากเกิดเหตุผู้ให้บริการ cloud ที่ผู้รับจ้างเลือกมาถูกจำกัดการเข้าใช้งานในบางประเทศ หรือทั้งหมด เพื่อให้ระบบ e-Visa สามารถกลับมาใช้งานได้เป็นปกติตาม SLA

5.5 ศูนย์ปฏิบัติการข้อมูลการตรวจลงตรา กรมการกงสุล

5.5.1 ปรับปรุงเป็นห้องปฏิบัติการข้อมูลการตรวจลงตรา กรมการกงสุล ให้สามารถรองรับการทำงานสำหรับเจ้าหน้าที่ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.5.2 อุปกรณ์ภายในศูนย์ปฏิบัติการข้อมูลการตรวจลงตรา กรมการกงสุล

ผู้รับจ้างต้องจัดซื้ออุปกรณ์ภายในศูนย์ปฏิบัติการข้อมูลการตรวจลงตรา และดูแลบำรุงรักษาให้พร้อมใช้งานตลอดระยะเวลาของสัญญา ดังนี้

(1) เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานประมวลผล จำนวน 15 เครื่อง คุณลักษณะพื้นฐาน ดังนี้

- มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 8 แกนหลัก (8 Core) และ 14 แกนเสมือน (14 Thread) และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง (Turbo Boost หรือ Max Boost) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 4 GHz จำนวน 1 หน่วย

- หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันขนาดไม่น้อยกว่า 18 MB

- มีหน่วยความจำหลัก (RAM) ชนิด DDR5 ขนาดไม่น้อยกว่า 32 GB หรือดีกว่า

- มีหน่วยจัดเก็บข้อมูล ชนิด Solid State แบบ M.2 ขนาดความจุไม่น้อยกว่า 1 TB หรือดีกว่า

- มีจอภาพที่รองรับความละเอียดไม่น้อยกว่า 1,920 x 1,200 pixel และมีขนาดไม่น้อยกว่า 14 นิ้ว ความสว่างอย่างน้อย 400 nits

- มีกล้องความละเอียดไม่น้อยกว่า 1080p

- มีช่องเชื่อมต่อ (Interface) แบบ USB 3.2 gen 1 หรือดีกว่า ไม่น้อยกว่า 2 ช่อง

- มีช่องเชื่อมต่อแบบ HDMI หรือ VGA จำนวนไม่น้อยกว่า 1 ช่อง

- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า แบบติดตั้งภายใน (Internal) หรือภายนอก (External) จำนวนไม่น้อยกว่า 1 ช่อง

- สามารถใช้งานได้ไม่น้อยกว่า Wi-Fi (IEEE 802.11 ax) และ Bluetooth

- ติดตั้งระบบปฏิบัติการ Window 11 pro หรือดีกว่าที่มีลิขสิทธิ์ถูกต้องตามกฎหมายและเป็นสิทธิ์การใช้งานแบบซื้อขาด

- ติดตั้งชุดโปรแกรมจัดการสำนักงาน Microsoft office 2021 หรือดีกว่าที่มีลิขสิทธิ์ถูกต้องตามกฎหมายและเป็นสิทธิ์การใช้งานแบบซื้อขาด

- รับประกันเป็นเวลา 3 ปี ในกรณีที่เกิดปัญหาทางด้าน Hardware โดยเข้ามาทำการแก้ไข หรือซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) ทั้งค่าแรงและอะไหล่ ภายในวันทำการถัดไป (Next Business Day Response)

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

(2) เครื่องคอมพิวเตอร์ (Desktop) สำหรับงานประมวลผล จำนวน 15 เครื่อง
คุณลักษณะพื้นฐาน ดังนี้

- มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 8 แกนหลัก (8 Core) และ 16 แกนเสมือน (16 Thread) และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง (Turbo Boost หรือ Max Boost) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 4.4 GHz จำนวน 1 หน่วย

- หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันขนาดไม่น้อยกว่า 20 MB

- มีหน่วยความจำหลัก (RAM) ชนิด DDR5 หรือดีกว่า มีขนาดไม่น้อยกว่า 32 GB

- มีหน่วยจัดเก็บข้อมูล ชนิด Solid State แบบ M.2 ขนาดความจุไม่น้อยกว่า 1 TB หรือดีกว่า

- มี Bluetooth เพื่อรองรับการเชื่อมต่อจากอุปกรณ์ภายนอก

- มีระบบเสียงและลำโพงติดตั้งมาพร้อมบนแผงวงจรหลัก (Built-in on board)

- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 1 ช่อง

- มีแป้นพิมพ์อักษรภาษาไทย ภาษาอังกฤษ ตัวเลข และเครื่องหมายต่าง ๆ ติดอยู่บนแป้นพิมพ์อย่างถาวร แบบ USB หรือดีกว่า

- มี Optical Mouse มีพอร์ตเชื่อมต่อแบบ USB หรือดีกว่า พร้อมแผ่นรอง (Mouse Pad)

- มีวงจรควบคุมอุปกรณ์ป้อนเข้า - ส่งออก (I/O & Communication ports) ดังนี้

- (1) มีช่องต่อจอภาพชนิด HDMI Port หรือดีกว่า จำนวนไม่น้อยกว่า 1 Port

- (2) มีช่องเชื่อมต่อ (Interface) แบบ USB 2.0 และ USB 3.0 หรือดีกว่า รวมกันไม่น้อยกว่า 4 ช่อง โดยด้านหน้าของตัวเครื่อง ต้องมี USB 3.0 ไม่น้อยกว่า 1 ช่อง และด้านหลังของตัวเครื่องต้องมี USB 3.0 ไม่น้อยกว่า 1 ช่อง

- มีจอแสดงผลขนาดไม่น้อยกว่า 23 นิ้ว มีความละเอียดหน้าจอไม่น้อยกว่า 2,560 x 1440 อัตราการรีเฟรชหน้าจอไม่น้อยกว่า 60 Hz จำนวน 1 หน่วย

- อุปกรณ์มาตรฐานทุกชิ้น ได้แก่ ตัวเครื่องคอมพิวเตอร์ เมาส์ แป้นพิมพ์ และจอภาพต้องเป็นผลิตภัณฑ์ภายใต้เครื่องหมายการค้าเดียวกันทั้งหมด

- มี BIOS ที่มีลิขสิทธิ์และมีเครื่องหมายการค้าเดียวกับเครื่องคอมพิวเตอร์

- เป็นผลิตภัณฑ์ที่เสนอต้องได้รับการรับรองมาตรฐาน FCC หรือ มาตรฐานผลิตภัณฑ์อุตสาหกรรม (มอก.) พร้อมเอกสารมาแสดง

- เป็นผลิตภัณฑ์ที่ได้รับมาตรฐาน UL หรือ CSA หรือ ETL หรือ EPEAT โดยมีเอกสารรับรองตรงตามรุ่นที่เสนอ

- ผลิตภัณฑ์ที่เสนอต้องได้รับการรับรองมาตรฐาน FCC, UL และ EPEAT โดยมีเอกสารรับรองตรงตามรุ่นที่เสนอ

- ติดตั้งระบบปฏิบัติการ Window 11 pro หรือดีกว่าที่มีลิขสิทธิ์ถูกต้องตามกฎหมายและเป็นสิทธิ์การใช้งานแบบซื้อขาด

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

- ติดตั้งชุดโปรแกรมจัดการสำนักงาน Microsoft office 2021 หรือดีกว่าที่มีลิขสิทธิ์
ถูกต้องตามกฎหมายและเป็นสิทธิ์การใช้งานแบบซื้อขาด

- ได้รับการรับรองมาตรฐาน ISO 9001 และมาตรฐานด้านสิ่งแวดล้อม
ISO 14001 พร้อมเอกสารรับรองหรือยืนยันหรืออ้างอิงจากเจ้าของมาตรฐาน

- รับประกันเป็นเวลา 3 ปี ในกรณีที่เกิดปัญหาทางด้าน Hardware
โดยเข้ามาทำการแก้ไข หรือซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) ทั้งค่าแรงและอะไหล่ ภายใน
วันทำการถัดไป (Next Business Day Response)

- ผู้รับจ้างต้องมีหนังสือสนับสนุนทางด้านเทคนิคและบริการหลังการขาย
จากบริษัทผู้ผลิตหรือบริษัทสาขาผู้ผลิตในประเทศไทยเพื่อสามารถให้บริการได้อย่างมีประสิทธิภาพตลอด
ระยะเวลาประกัน

5.5.3 โครงข่ายสื่อสารพร้อมอุปกรณ์เชื่อมต่อโครงข่ายสาธารณะ (Internet) ซึ่งมีความเร็ว
ในการใช้งานอินเทอร์เน็ตภายในประเทศ (Domestic Internet) ไม่น้อยกว่า 100 Mbps และระหว่างประเทศ
(International Internet) ไม่น้อยกว่า 100 Mbps

5.6 ระบบ Mail Marketing

5.6.1 การจัดหาและดำเนินการ รวมทั้งการเตรียมความพร้อมจัดการระบบ Mail Marketing ของระบบ

(1) ผู้รับจ้างจะต้องจัดหาระบบการให้บริการจดหมายอิเล็กทรอนิกส์ โดยใช้บริการ
จดหมายอิเล็กทรอนิกส์ภายใต้โดเมน @thaiveisa.go.th หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ
กำหนด ตลอดระยะเวลาสัญญา โดยจัดหาให้กับระบบ e-Visa ระยะที่ 1 ในปัจจุบัน และระบบ e-Visa
ระยะที่ 2

(2) ผู้รับจ้างจะต้องจัดหาระบบการให้บริการจดหมายอิเล็กทรอนิกส์ให้สามารถใช้งาน
ร่วมกับระบบ e-Visa ของกรมการกงสุล กระทรวงการต่างประเทศ ได้อย่างมีประสิทธิภาพ มีความปลอดภัย
และมี high availability ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(3) หากระบบ SMTP Gateway ที่ให้เข้าใช้บริการ มีการเปลี่ยนแปลง ผู้รับจ้างจะต้องแจ้ง
รายละเอียดให้กรมการกงสุล ทราบล่วงหน้า 2 สัปดาห์เป็นอย่างน้อย

(4) ผู้รับจ้างจะต้องมีระบบอัตโนมัติการส่งอีเมลแบบเรียลไทม์

(5) ผู้รับจ้างจะต้องมีระบบ portal สำหรับบริหารจัดการ marketing อีเมล

- สามารถส่ง report แจ้งจำนวนและสถานการณ์ส่งจดหมายอิเล็กทรอนิกส์ แบบรายวัน
และรายเดือนได้ สามารถรองรับเงื่อนไขในการการค้นหาที่หลากหลายได้ (advance search)

- สามารถ export ข้อมูล log การส่งจดหมายอิเล็กทรอนิกส์เพื่อนำมาตรวจสอบข้อมูลได้

- สามารถตรวจสอบ log การส่งจดหมายอิเล็กทรอนิกส์ ย้อนหลังได้อย่างน้อย 365 วัน

5.6.2 คุณลักษณะเฉพาะทางเทคนิค

(1) ผู้รับจ้างจะต้องเสนอระบบจดหมายอิเล็กทรอนิกส์ที่ให้เข้าใช้บริการในรูปแบบ Cloud
Base โดยมีความพร้อมใช้งาน (availability) ไม่น้อยกว่าร้อยละ 99.90

(2) สามารถส่งต่อจดหมายอิเล็กทรอนิกส์จากระบบ e-Visa ไปยังผู้รับที่ระบุไว้ได้
โดยมีมาตรการเพื่อไม่ให้ถูกจัดว่าเป็น Spam mail / Junk mail

(3) ระบบต้องรองรับการส่งจดหมายอิเล็กทรอนิกส์ได้ไม่ต่ำกว่า 100,000 ฉบับต่อวัน
และไม่ต่ำกว่า 7,000 ฉบับต่อชั่วโมง

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

(4) สนับสนุนข้อมูลการตั้งค่า Sender Policy Framework (SPF) เพื่อเพิ่มความปลอดภัยและความน่าเชื่อถือของจดหมายอิเล็กทรอนิกส์ที่ส่งออก

(5) ระบบ Mail Marketing และระบบ e-Visa ต้องสามารถทำงานร่วมกัน และมีโมดูลในการตรวจสอบว่าอีเมล ส่งไปสำเร็จหรือไม่ และหากยังส่งไม่สำเร็จ ให้มีระบบการ resend อัตโนมัติ และมีการจัดทำรายงานในระบบที่สามารถสืบค้นได้ มีกรณีใดที่ไม่สามารถส่ง โดยรายงานสามารถตรวจสอบได้จากทั้งสถานเอกอัครราชทูต สถานกงสุลใหญ่ และกรมการกงสุล กระทรวงการต่างประเทศ

(6) รองรับการทำงานผ่านบราวเซอร์ Microsoft Edge, Chrome เวอร์ชันล่าสุด, Safari Mac เวอร์ชันล่าสุด และ Firefox desktop เวอร์ชันล่าสุด ได้เป็นอย่างดี

(7) รองรับการนำเข้าข้อมูล Subscriber ในรูปแบบ Excel โดยรองรับไฟล์นามสกุล xls หรือxlsx หรือ CSV

(8) รองรับการสร้างอีเมล Campaign ในรูปแบบ HTML, A/B Testing

(9) รองรับการสร้าง flow ของอีเมล กรณีผู้ร้อง click link ในอีเมล ให้ระบบ auto ส่งอีเมล ตอบกลับไปยังผู้ร้องรายนั้นทันทีแบบอัตโนมัติ (โดย อีเมล ที่ส่งต้องมีการสร้างรอไว้แล้ว)

(10) สามารถใส่ Link ในเนื้อหาอีเมลได้

(11) สามารถตั้งเวลาการส่งอีเมลล่วงหน้าได้ รวมทั้งสามารถกำหนด Sender Email และ Sender Name ได้

(12) สามารถมี Report การส่งอีเมลที่สามารถ export เป็น Excel ได้แบบ realtime

(13) มีการเก็บ Log การใช้งานของระบบการส่งอีเมลและสามารถสืบค้นข้อมูลย้อนหลังได้ 3 ปี เป็นอย่างน้อย

(14) มีระบบแจ้งเตือนการส่งอีเมลที่จัดส่งออกไปได้ว่าส่งไม่สำเร็จ และสามารถแสดงรายละเอียดของการจัดส่งอีเมลได้

(15) สามารถส่งอีเมลซ้ำในกรณีที่จัดส่งอีเมลไม่สำเร็จได้

5.7 ระบบความมั่นคงและความปลอดภัย

5.7.1 ภาพรวมด้านการรักษาความมั่นคงปลอดภัยของระบบ e-Visa ต้องมีอย่างน้อย ดังนี้

5.7.1.1 ผู้ให้บริการจะต้องวางแผนตรวจสอบช่องโหว่ (Vulnerability Scan: VA) อย่างน้อยปีละ 2 ครั้ง (ไม่รวมการทดสอบซ้ำ หรือ Revisit) และทดสอบการบุกรุกระบบ (Penetration Test: Pentest) อย่างน้อยปีละ 1 ครั้ง จากหน่วยงานภายนอก (3rd party) ที่น่าเชื่อถือ และได้รับความเห็นชอบจากกรมการกงสุล กระทรวงการต่างประเทศ (ไม่รวมการทดสอบซ้ำ หรือ Revisit) และต้องทำการทดสอบกับทุกส่วนในระบบงาน อาทิ ระบบเครือข่าย ระบบเซิร์ฟเวอร์ ระบบสารสนเทศ ยกเว้นระบบคลาวด์ ในกรณีพบช่องโหว่ของระบบในโครงการ ผู้ให้บริการจะต้องรีบแจ้งกรมการกงสุล กระทรวงการต่างประเทศ และดำเนินการแก้ไขปรับปรุงเพื่อปิดช่องโหว่ดังกล่าวโดยทันที พร้อมจัดทำรายงานสรุปรายงานให้กรมการกงสุล กระทรวงการต่างประเทศ ทราบ ตลอดระยะเวลาการให้บริการในสัญญา โดยการทดสอบครั้งแรกจะเป็นการดำเนินการหลังจากที่พัฒนาระบบเสร็จสิ้น รวมถึงกรณีที่มีการเชื่อมโยงระบบกับภายนอกเพิ่มเติม ผู้รับจ้างต้องมีการทดสอบระบบการรักษาความมั่นคงปลอดภัย โดยการทดสอบเจาะระบบ (Penetration Test) จากบริษัทมืออาชีพที่ได้รับรองมาตรฐาน ซึ่งผู้รับจ้างเป็นผู้ออกค่าใช้จ่ายทั้งหมด

5.7.1.2 ต้องออกแบบทุกระบบสารสนเทศทั้งหมดในโครงการให้สามารถทำงานได้ต่อเนื่องตลอดเวลา โดยจะต้องมีระบบบันทึกเวลาเกิดเหตุการณ์ที่ระบบหยุดการทำงาน และสรุปเป็นรายงาน คำนวณ

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

ระยะเวลา โดยแสดงผลออกมาในรูปแบบ Dashboard รวมทั้งสามารถส่งออกข้อมูลเป็นในรูปแบบ CSV หรือ Excel ได้ ดังนี้

- (1) ความพร้อมใช้งานของแต่ละระบบงาน รวมถึงระบบสนับสนุนการใช้งาน
- (2) การตอบสนองและการแก้ปัญหาทางเทคนิค
- (3) Recovery Point Objective (RPO) และ Recovery Time Objective (RTO)

(4) การปรับปรุงเงื่อนไขการตรวจลงตราและการเพิ่มหรือลดประเภทการตรวจลงตราในระบบ e-Visa และระบบ Mobile Application ตามนโยบายที่กรมการกงสุลกำหนด

(5) การเพิ่ม หรือพัฒนาโมดูลการใช้งานของระบบ e-Visa และระบบ Mobile Application (refer ไปยัง man-day)

(6) การตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

5.7.1.3 จัดตั้งศูนย์เฝ้าระวังภัยคุกคามทางด้านไซเบอร์และความปลอดภัยของระบบ

เทคโนโลยีสารสนเทศ (CSOC) ที่กรมการกงสุล กระทรวงการต่างประเทศ โดยจะต้องดำเนินการวางแผน ออกแบบ ปรับปรุงห้อง ติดตั้งระบบที่ใช้ในการเฝ้าระวังภัยคุกคามประกอบด้วย

(1) Video wall ชนิด LED module display ไร้ขอบ ความละเอียดสูง มีระยะการรับชมขั้นต่ำ (Pixel Pitch) น้อยกว่าหรือเทียบเท่า 1.25p ขนาดหน้าจอแสดงผลไม่น้อยกว่า 2000 mm x 4500 mm สามารถควบคุมความสว่างหน้าจอได้ และมีระบบควบคุมการแสดงผลผ่านเครือข่าย (Networked Display Control) เพื่อให้สามารถจัดการและควบคุมการแสดงผลได้จากศูนย์กลาง อาทิ การเปลี่ยนแปลงเลย์เอาต์ การสลับแหล่งสัญญาณ

(2) ชุดควบคุมการแสดงผล โดยสามารถรับสัญญาณเข้าได้ไม่น้อยกว่า 8 แหล่ง พร้อมกัน รองรับการทำงานสะท้อนหน้าจอ (Screen Mirroring) และ Airplay จากอุปกรณ์ไร้สายได้ พร้อมสามารถแสดงผลจากหลายแหล่งได้พร้อมกัน ในรูปแบบ Picture in Picture (PIP) และ Picture by Picture (PBP) เป็นอย่างน้อย

(3) ระบบการประชุมทางไกล (Conference) ประกอบด้วยชุดกล้องประชุม รองรับความละเอียด 4K ที่สามารถหมุนได้รอบทิศทางที่มีฟังก์ชัน Auto Tracking สำหรับการติดตามผู้พูดอัตโนมัติ พร้อมด้วยชุดไมค์ประชุมไร้สายที่สามารถเปิด-ปิด เสียงพูดได้ ให้รองรับการเชื่อมต่อแบบ DECT หรือ Wi-Fi เพื่อความเสถียร จำนวนไม่น้อยกว่า 5 ชุด

(4) ชุดคอมพิวเตอร์สำหรับรองรับการเชื่อมต่อระบบประชุมทางไกล อาทิ Webex, Zoom, Microsoft Team, Google meet ได้เป็นอย่างน้อย โดยอุปกรณ์สำหรับการประชุมสามารถใช้งานร่วมกันได้อย่างมีประสิทธิภาพ

(5) นาฬิกาแสดงโซนเวลาโลกแบบดิจิทัล แสดงเวลาท้องถิ่นพร้อมระบุชื่อแต่ละประเทศที่สำคัญ ประเทศละ 1 เรือน จำนวนไม่น้อยกว่า 8 ประเทศ พร้อม sync เวลา กับสถาบันมาตรวิทยาแห่งชาติ

(6) ติดตั้ง Access Point (AP) มาตรฐาน Wi-Fi 6 หรือสูงกว่า จำนวนไม่น้อยกว่า 2 จุด เพื่อรองรับการใช้งาน สามารถทำงานแบบ Mesh Network เพื่อให้ครอบคลุมพื้นที่

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

ได้อย่างต่อเนื่อง รวมถึงอุปกรณ์เครือข่ายและสายสัญญาณที่จำเป็น โดยต่อเชื่อมกับระบบ Network ที่กรรมการกงสุล กระทรวงการต่างประเทศกำหนด

ภายในห้อง CSOC จะต้องรองรับการเปิดใช้งานระบบที่เกี่ยวข้องกับการดูแลระบบ e-Visa อาทิ การป้องกันการโจมตี การเผชิญเหตุ ระบบเฝ้าระวัง ตรวจสอบและวิเคราะห์ภัยคุกคามทางไซเบอร์ ระบบ Monitoring ได้เป็นอย่างดี และสามารถใช้เป็นสถานที่เพื่อดำเนินการเผชิญเหตุภัยคุกคามทางไซเบอร์ของกรรมการกงสุล รวมถึงการพัฒนาบุคลากรของกรรมการกงสุล ในการใช้งานระบบ เพื่อให้พร้อมรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที

5.7.1.4 จัดทำทะเบียนทรัพย์สินสารสนเทศ พร้อมทั้งจัดทำแผนบริหารและประเมินความเสี่ยงของระบบ e-Visa ทุกส่วนงานตั้งแต่ระบบคลาวด์ ระบบสารสนเทศ อุปกรณ์สำหรับผู้ใช้งานปลายทาง (Endpoint Devices) หรือระบบอื่นใดที่เกี่ยวข้องในโครงการ e-Visa โดยดำเนินการประเมินความเสี่ยงของทรัพย์สินสารสนเทศเป็นประจำไม่น้อยกว่าปีละ 1 ครั้ง ตามหลักการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้เป็นไปตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงแนวปฏิบัติที่เกี่ยวข้องของกรรมการกงสุล กระทรวงการต่างประเทศ โดยคำนึงถึงมาตรการควบคุมความเสี่ยง การป้องกันภัยคุกคามทางไซเบอร์ และการรักษาความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล เพื่อให้มั่นใจว่าการให้บริการเป็นไปอย่างปลอดภัยและสอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง

5.7.1.5 จัดทำแผนการตอบสนองภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) และคู่มือที่ระบุและรวบรวมขั้นตอนการดำเนินงานและแผนการปฏิบัติที่เกี่ยวข้องกับด้านความปลอดภัยของระบบและเทคโนโลยีสารสนเทศ (Cyber Security Playbook) เพื่อเตรียมความพร้อมและรับมือและเผชิญเหตุกับเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ที่อาจเกิดขึ้นได้ โดยเน้นเรื่องกระบวนการการควบคุมความเสียหายด้วยวิธีการที่เหมาะสมที่จะป้องกันไม่ให้ความเสียหายกระจายออกไปในวงกว้าง (Containment) การเก็บหลักฐาน และวิเคราะห์เพื่อกำจัดต้นตอของภัยคุกคามให้ออกจากระบบทั้งหมด (Eradication) และการกู้คืนระบบให้กลับมาทำงานปกติ (Recovery) รวมทั้งจัดให้มีการทดสอบแผนตามหัวข้อต่าง ๆ อย่างน้อยปีละ 1 ครั้ง โดยผู้ยื่นข้อเสนอ จะต้องจัดทำแผนการทดสอบของทั้งปี เพื่อให้กรรมการกงสุล กระทรวงการต่างประเทศ พิจารณาก่อน ซึ่งมีหัวข้อขั้นต่ำ ดังนี้

(1) Incident Response Playbook จัดทำขั้นตอนการตอบสนองที่รวดเร็วและมีประสิทธิภาพเมื่อเกิดเหตุการณ์ละเมิดความปลอดภัย โดยมีขั้นตอนขั้นต่ำ อาทิ เตรียมความพร้อม (Prepare) ตรวจสอบ (Detect) วิเคราะห์ (Analyze) จำกัดความรุนแรงหรือการกระทำ (Contain) กำจัด (Eradicate) กู้คืน (Recovery) การดำเนินการหลังจากเหตุการณ์ (Post Incident)

(2) Malware Outbreak Playbook จัดทำขั้นตอนการจัดการกับการแพร่กระจายของมัลแวร์ โดยมีขั้นตอนขั้นต่ำ อาทิ การตรวจสอบและพิจารณาความเสี่ยง การแยกแยะและกำจัดมัลแวร์ การป้องกันการแพร่กระจายต่อไป

(3) Insider Threat Response Playbook จัดทำขั้นตอนการตอบสนองต่อภัยคุกคามจากภายใน โดยมีขั้นตอนขั้นต่ำ อาทิ การตรวจสอบและพิจารณาภัยคุกคาม การสืบสวนและการจัดการกับผู้ที่เป็นภัย

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

(4) Vulnerability Management Playbook จัดทำขั้นตอนการจัดการกับช่องโหว่ในระบบ โดยมีขั้นตอนขั้นต่ำ อาทิ การตรวจสอบและการประเมินความเสี่ยง การจัดการกับช่องโหว่ การพัฒนาแผนการป้องกัน

(5) Data Breach Notification Playbook จัดทำขั้นตอนการจัดการและการแจ้งเตือนเมื่อมีการรั่วไหลข้อมูล โดยมีขั้นตอนขั้นต่ำ อาทิ การตรวจสอบและยืนยันการรั่วไหลข้อมูล การแจ้งเตือนทีมที่เกี่ยวข้อง การปฏิบัติตามกฎหมายที่เกี่ยวข้อง พร้อมแจ้งเตือนให้กรมการกงสุล กระทรวงการต่างประเทศ ทราบ พร้อมจัดทำรายงานกรณีที่เกิดเหตุการณ์ความไม่ปกติต่าง ๆ

5.7.1.6 ต้องมีการสำรองข้อมูล (Backup) ดังนี้

(1) ผู้ยื่นข้อเสนอ จะต้องออกแบบการสำรองข้อมูลสอดคล้องกับหลักการ 3-2-1 โดยจัดเก็บข้อมูลสำรอง 3 ชุดในสื่อที่แตกต่างกันอย่างน้อย 2 ประเภท และเก็บสำเนาข้อมูล 1 ชุดในพื้นที่นอกสถานที่ (Offsite) เพื่อให้รองรับกับกรอบระดับการให้บริการ (SLA) ในข้อ 5.19.2

(2) มีการป้องกันและตรวจสอบ Ransomware ทั้งก่อนและหลังการสำรองข้อมูล

(3) มีเทคโนโลยี Data deduplication เพื่อช่วยลดพื้นที่การจัดเก็บข้อมูล

(4) สามารถทดสอบได้ว่าไฟล์ Backup เป็นไฟล์ที่สมบูรณ์ สามารถ recovery ข้อมูลกลับมาได้จริงและทดสอบ recovery ข้อมูลได้โดยไม่กระทบกับระบบงานปัจจุบันหรือไฟล์ Backup ต้นฉบับแต่อย่างใด อย่างน้อยปีละ 1 ครั้ง พร้อมทั้งเสนอแผนการทดสอบให้กรมการกงสุล กระทรวงการต่างประเทศเห็นชอบก่อน

5.7.1.7 มีระบบป้องกันข้อมูลรั่วไหลของข้อมูล (Data Loss Prevention: DLP)

จะต้องอยู่ใน Leader Quadrant หัวข้อ Enterprise Data Loss Prevention ประจำปีล่าสุด เพื่อลดความเสี่ยงกรณีที่มีการถูกโจรกรรมข้อมูล หรือการส่งออกข้อมูลทั้งโดยตั้งใจหรือไม่ตั้งใจจากบุคคลภายนอก และภายใน โดยระบบจะต้องป้องกันพร้อมแจ้งเตือนผู้ดูแลระบบให้ทราบ และจะต้องมีระบบที่ให้ผู้ดูแลข้อมูลสามารถอนุญาตการนำข้อมูลออกจากระบบ พร้อมทั้งมีระบบรายงานเหตุการณ์ต่าง ๆ เกี่ยวกับข้อมูล ให้ผู้รับผิดชอบทราบความเคลื่อนไหว

5.7.1.8 มีระบบป้องกันการบุกรุกเครือข่าย (Firewall) หรือระบบป้องกันการบุกรุก

เครือข่ายเสมือน (Virtual Firewall) โดยจะต้องมีป้องกันระบบ e-Visa ทุก ๆ จุดที่มีการเชื่อมต่อกับเครือข่ายภายนอก รวมทั้งการออกแบบระบบที่มีการแบ่งโซนหน้าที่ความรับผิดชอบภายใน หรือเซิร์ฟเวอร์ หรือระหว่าง Instance เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต โดยจะต้องรองรับและป้องกันการโจมตีผ่านช่องโหว่ต่าง ๆ จาก IPS signature, Protocol anomaly detection และมีระบบ Rate-based DDoS protection ป้องกัน TCP Syn flood, Port scan, ICMP sweep ได้เป็นอย่างดี

5.7.1.9 มีระบบรักษาความปลอดภัยเว็บแอปพลิเคชันและ API (Web Application and API Protection: WAAP) เพื่อตรวจจับและตรวจสอบการใช้งานที่สามารถป้องกันการดำเนินงาน API ของเว็บแอปพลิเคชันและการโจมตีแบบ DDoS บอทไม่พึงประสงค์ และช่องโหว่ต่าง ๆ ประกอบด้วยคุณสมบัติต่าง ๆ ดังนี้

(1) สามารถตรวจจ็บบรูปแบบการโจมตีใหม่ของผู้ไม่ประสงค์ดีได้อย่างทันท่วงที มีการอัปเดตฐานข้อมูลอยู่เสมอ สามารถปรับแต่งการแจ้งเตือนให้เหมาะสม และระบบจะต้องมีคำแนะนำในการช่วยปรับจูนได้

(2) สามารถสแกนค้นหา API ทำให้มองเห็นถึงการเคลื่อนไหวของ API ทั้งระบบ e-Visa และแอปเดออยู่เสมอ นอกจากนี้จะต้องแยกแยะรูปแบบของทราฟฟิกที่เกิดขึ้นในการทำงาน หรือ

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ 3007 กรรมการ พันทิพย์ กรรมการ กรรมการ

ทราบฟิสิกส์ที่มีค่าผิดปกติทั้งจากการโจมตี หรือการทำงานของระบบผิดปกติ โดยจะต้องสามารถรับรู้และเตือนถึงการโจมตีได้ รวมไปถึงสามารถแยกแยะพฤติกรรม หรือมีช่องทางให้สามารถกำหนดคุณสมบัติของบอทที่ดี และบอทที่เป็นอันตรายได้ สามารถเรียกดูกราฟฟิคของบอทเพื่อประโยชน์ในด้านการวิเคราะห์ข้อมูลต่อไป

(3) สามารถป้องกันการโจมตีในรูปแบบ DDoS Protection ซึ่งการป้องกัน นอกจากต้องสามารถสกัดกั้นรูปแบบการโจมตี แหล่งที่มาของการโจมตีได้ตามเงื่อนไขที่กำหนด รวมถึงรองรับวิธีการทำงานแบบ DevSecOps อาทิ Terraform CLI หรือ API

(4) สามารถจัดทำรายงานภาพรวมของระบบ แสดงสาเหตุและแนวโน้มของปัญหา แสดงผลการวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยได้ระดับเรียลไทม์ พร้อมกับการแจ้งเตือนเมื่อถึงเงื่อนไขที่กำหนด และมี Connector และ API ที่สามารถส่งข้อมูลต่อไปวิเคราะห์ในระบบเฝ้าระวัง ตรวจสอบและวิเคราะห์ภัยคุกคามทางไซเบอร์ในโครงการต่อไป

5.7.1.10 ระบบป้องกันการโจมตีเว็บไซต์ (Web Application Firewall - WAF)

- (1) บริการที่นำเสนอต้องมีสิทธิ์การใช้งานทุก domain ที่มีการใช้งานในโครงการ
- (2) บริการที่เสนอต้องสามารถรองรับการใช้ Bandwidth Consumption ให้เพียงพอต่อการทำงานของระบบ
- (3) บริการที่นำเสนอต้องได้รับการประเมินจาก Gartner Magic Quadrant สำหรับ Cloud Web Application and API Protection ปี 2022 ให้อยู่ในกลุ่ม LEADERS
- (4) สามารถป้องกันการโจมตีผ่านทาง Website ตาม OWASP TOP 10 อาทิ SQL injection, Broken Authentication, Cross-site Scripting
- (5) สามารถตั้งค่า Web Application Firewall (WAF) และสามารถแก้ไขเพิ่ม Custom WAF rules ได้ไม่น้อยกว่า 1,000 rules
- (6) สามารถป้องกันการโจมตีจากในระดับเครือข่าย (DDoS attack) ที่ระดับ Network layer 3, 4 และ 7
- (7) ต้องให้บริการป้องกันการโจมตีในระดับเครือข่าย (DDoS attack) แบบไม่จำกัดจำนวนครั้ง และขนาดของการโจมตี โดยไม่มีค่าใช้จ่ายเพิ่มเติม
- (8) สามารถตั้งค่า IP Firewall โดยสามารถกำหนดเงื่อนไขด้วย IP address, IP address range, Autonomous System Number (ASN) or country ได้
- (9) สามารถตั้งค่า Rate Limit Rules ซึ่งสามารถกำหนดการป้องกันการเข้าถึง Website ได้ในระดับ Unique Visitor
- (10) สามารถตั้งค่า Page Rules ได้ไม่น้อยกว่า 100 rules
- (11) มี Data Center หรือ Point of Presence (PoP) อย่างน้อย 250 จุดทั่วโลก และ POP อย่างน้อย 7 จุดในไทย ซึ่งแต่ละ POP ต้องมีความสามารถ DDoS mitigation, WAF และ CDN ในประเทศไทย
- (12) ผู้ให้บริการต้องให้บริการ authoritative DNS services สำหรับโดเมนสาธารณะ
- (13) มีระบบ Content Caching โดยสามารถทำ Static Content Caching และสามารถกำหนด Cache ในระดับ File Type ได้

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

(14) สามารถทำการ Purge Cache ทั้งหมดได้ในทันที หรือทำการ Custom Purge เฉพาะ URL, Host name และ Tag ได้

(15) มีระบบที่ช่วยเพิ่มประสิทธิภาพและลด Latency ให้กับ Dynamic Content โดยสามารถดูเปอร์เซ็นต์ของประสิทธิภาพที่เพิ่มขึ้น และ Response time ได้ผ่านทาง Dashboard

(16) สามารถทำการตรวจสอบการออกใบรับรอง SSL (certificate transparency monitoring) โดยสามารถแจ้งเตือนเมื่อมีผู้ทำการออกใบรับรองภายใต้ชื่อโดเมนเดียวกันกับของหน่วยงาน

(17) สามารถลดขนาด บีบอัด และทำการลบ Metadata ของไฟล์ โดยสามารถเลือกได้ทั้งแบบ Lossless และ Lossy รวมถึงรองรับ WebP

(18) มีระบบ Always Online ที่สามารถทำการแสดง static content ในกรณีที่ Server ต้นทางไม่สามารถใช้งานได้

(19) ต้องมีเครือข่ายที่มีความสามารถในการป้องกันการโจมตีจากในระดับเครือข่าย (DDoS) ให้เพียงพอต่อการทำงานของระบบ

(20) สามารถแสดงรายงาน (Analytic) บน Dashboard แบบ Real-time หรือ Near Real-time โดย Dashboard ที่แสดงต้องประกอบด้วยข้อมูล Total Requests, Cached Request, Bandwidth Saved, Threat Sources, Top Threat Origin และ Top Traffic Origin ได้เป็นอย่างดี

(21) บริการที่เสนอรองรับการส่ง Raw Log ผ่านทาง Log Push ไปยัง Amazon S3, Azure Blob Storage, Google Cloud Storage, or Sumo Logic ได้เป็นอย่างดี และ Log Pull REST API

(22) สามารถเรียกดู Firewall Event Log และ Audit Log ได้ผ่านทาง Portal ที่ใช้งาน

(23) บริการที่เสนอต้องรองรับการกำหนดสิทธิการใช้งาน และรองรับการทำ Two-Factor Authentication ได้

(24) รองรับการจัดตั้งทั้งแบบการย้าย Name Server และ CNAME ได้

5.7.1.11 กรณีเกิดภัยคุกคามทางไซเบอร์หรือกรณีใด ๆ ที่ก่อให้เกิดความเสียหายต่อระบบ และข้อมูลของโครงการรวมถึงภาพลักษณ์ของกรมการกงสุล กระทรวงการต่างประเทศ ผู้รับจ้างจะต้องเป็นผู้รับผิดชอบความเสียหายที่เกิดขึ้นในทุกกรณี

5.7.2 ระบบ e-Visa ที่พัฒนาขึ้นจะต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ดังนี้

5.7.2.1 จัดให้มีและต่ออายุโดเมนสำหรับระบบ e-Visa backoffice และระบบ Web Enquiry โดยชื่อโดเมนจะเป็นไปตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด พร้อมทั้งจัดหาและต่ออายุใบรับรองความปลอดภัยดิจิทัลแบบ Multi-Domain Extended Validation SSL (EV SSL) สำหรับใช้ในการเข้ารหัสข้อมูลบนเว็บไซต์และบริการออนไลน์ของโครงการ e-Visa รองรับมาตรฐาน TLS1.2 ขึ้นไป รองรับหลายชื่อโดเมน (Multi-Domain) ภายใต้ใบรับรองเดียวกัน และต้องเป็นใบรับรองที่ออกโดยหน่วยงานออกใบรับรอง (Certificate Authority: CA) ที่ได้รับการยอมรับจาก CA/Browser Forum สนับสนุนการตรวจสอบตัวตนขององค์กร (Organization Identity Validation) ตามมาตรฐาน SSL EV รวมถึงรองรับการใช้งานผ่านเบราว์เซอร์ Microsoft Edge, Chrome เวอร์ชันล่าสุด, Safari Mac เวอร์ชันล่าสุด และ Firefox desktop เวอร์ชันล่าสุด ได้เป็นอย่างดี ทั้งนี้ ผู้รับจ้างจะต้องดำเนินการต่ออายุโดเมนและใบรับรองดิจิทัลตลอดอายุของสัญญา

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

5.7.2.2 มีการเข้ารหัสข้อมูลส่วนบุคคล ข้อมูลละเอียดอ่อน หรือข้อมูลตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด ทั้งในระหว่างการส่ง (Data In-Transit) และขณะจัดเก็บ (Data At-Rest) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต โดยการเข้ารหัสข้อมูลในระหว่างการส่งจะใช้โปรโตคอลที่ปลอดภัยเพื่อสร้างช่องทางการสื่อสารระหว่างผู้ใช้งานและระบบ ป้องกันการดักจับข้อมูลหรือการโจมตีประเภท Man-in-the-Middle ในส่วนของการเข้ารหัสข้อมูลขณะจัดเก็บ ข้อมูลจะถูกเก็บในรูปแบบที่ไม่สามารถอ่านได้โดยตรงหากไม่มีคีย์ถอดรหัส โดยจะต้องมีการจัดการคีย์การเข้ารหัสด้วยวิธีการที่ปลอดภัย อาทิ การใช้ระบบ Key Management System (KMS) เพื่อบริหารจัดการคีย์การเข้ารหัสและลดความเสี่ยงจากการสูญหายหรือถูกขโมย นอกจากนี้ ระบบยังสนับสนุนการตรวจสอบและบันทึกการเข้าถึง (Access Logs) เพื่อให้สามารถติดตามและตรวจสอบกิจกรรมที่เกี่ยวข้องกับข้อมูลสำคัญได้อย่างมีประสิทธิภาพ

5.7.2.3 ออกแบบและพัฒนาระบบความมั่นคงปลอดภัยของระบบงานสารสนเทศเพื่อให้สามารถป้องกันการโจมตีจากผู้ไม่ประสงค์ดีตามรายการช่องโหว่ 10 อันดับ สำหรับระบบสารสนเทศบนเว็บ ปีล่าสุด ที่เรียกว่า OWASP Top 10 Vulnerabilities (Open Web Application Security Project) รวมไปถึง OWASP ทั้งหมดที่สอดคล้องกับเทคโนโลยีในการพัฒนาระบบ อาทิ OWASP Kubernetes Top 10, OWASP Mobile Top 10, OWASP API Security Top 10

5.8 ระบบรักษาความปลอดภัยสำหรับเครื่อง Client

5.8.1 ระบบการเข้าถึงเครือข่ายแบบ Zero Trust Network Access (ZTNA)

ผู้รับจ้างต้องจัดหาระบบเครือข่ายความปลอดภัยสำหรับช่องทางการรับ-ส่งข้อมูลที่ กรมการกงสุล กระทรวงการต่างประเทศ กำหนด เพื่อความปลอดภัยและปิดกั้นการเข้าถึงทรัพยากรสารสนเทศจากภายนอกเครือข่าย มีการเข้ารหัสเพื่อเก็บข้อมูลที่เป็นความลับนี้ให้เป็นส่วนตัวหากใช้งานเครือข่ายสาธารณะหรือมีการดักจับข้อมูลผ่านเครือข่าย และเพื่อปกป้องระบบ e-Visa ที่มีการเชื่อมต่อเครือข่ายจากการเข้าถึงโดยไม่ได้รับอนุญาต โดยมีคุณสมบัติที่ใช้งาน ดังนี้

5.8.1.1 ผู้รับจ้างจะต้องเสนอแพลตฟอร์มที่รองรับการทำงานเป็น next-generation Zero Trust Network Access (ZTNA) ซึ่งไม่ใช้การทำงานในรูปแบบของ VPN services

5.8.1.2 แพลตฟอร์มที่นำเสนอจะต้องได้รับการจัดลำดับให้อยู่ในกลุ่ม Leader ในการทำ Secure Access Service Edge (SASE) หรือ Secure Service Edge (SSE) จาก Gartner Magic Quadrant ปี 2023 หรือฉบับล่าสุด

5.8.1.3 แพลตฟอร์มที่นำเสนอจะต้องสามารถอนุญาตเข้าถึง application อย่างปลอดภัย โดยไม่ต้องจำเป็นต้องเชื่อมต่อผู้ใช้เข้ากับระบบเครือข่ายหรือกำหนดรายการ IP Address ภายในให้กับผู้ใช้งาน เพื่อหลีกเลี่ยงความซับซ้อนเพิ่มเติมในการทำ network segmentation ด้วย internal firewall

5.8.1.4 แพลตฟอร์มที่นำเสนอจะต้องเชื่อมต่อผู้ใช้งานเข้ากับ application โดยตรง แทนที่การใช้งานเทคโนโลยี VPN

5.8.1.5 แพลตฟอร์มที่นำเสนอจะต้องซ่อน IP Address จริง ของ application จาก internet ด้วยการเชื่อมต่อในลักษณะ inside-out connection หรือมีแค่ outbound traffic เท่านั้น

5.8.1.6 แพลตฟอร์มที่นำเสนอต้องบังคับใช้การเข้าถึงในรูปแบบ least-privileged access เท่านั้น ด้วยการตรวจสอบ identity และ context ก่อนการเข้าใช้งาน

5.8.1.7 แพลตฟอร์มที่นำเสนอจะต้องตรวจสอบการเข้าถึง application โดยมีหลักการ

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

แบบหนึ่งต่อหนึ่ง โดยอนุญาตให้เฉพาะผู้ใช้ authorized user เข้าถึง application ที่อนุญาตเท่านั้น

5.8.1.8 แพลตฟอร์มที่นำเสนอจะต้องรองรับการทำงานร่วมกับ Identity Provider (IdP) ได้อย่างน้อย 10 IdPs เพื่อการทำ single sign-on (SSO) ให้กับผู้ใช้งานได้

5.8.1.9 รองรับการทำ Single Sign on (SSO) โดย User สามารถ Authentication รองรับ Protocol SAML ได้เป็นอย่างน้อย

5.8.1.10 Agent ที่จำเป็นต้องติดตั้งในการทำงานร่วมกับแพลตฟอร์ม ZTNA จะต้องรองรับการติดตั้งบนระบบปฏิบัติการดังนี้เป็นอย่างน้อย

- (1) ตั้งแต่ Windows 10 ขึ้นไป
- (2) ตั้งแต่ macOSX 10.15 ขึ้นไป
- (3) ตั้งแต่ iOS 14 ขึ้นไป
- (4) ตั้งแต่ Android 13 ขึ้นไป

5.8.1.11 แพลตฟอร์มที่นำเสนอจะต้องเป็นไปตาม Service-initiated ZTNA model ที่แนะนำโดย Gartner หรือ Software-Defined Perimeter (SDP) Architecture ที่เผยแพร่โดย Cloud Security Alliance (CSA) แทนที่การทำ virtual private network (VPN) หรือการใช้ฟังก์ชัน SSL VPN / VPN บน firewall หรือการสร้าง network access policy

5.8.1.12 แพลตฟอร์มที่นำเสนอจะต้องรองรับ TCP และ UDP based applications และไม่จำกัดแค่เพียง web based (http/https) applications เท่านั้น

5.8.1.13 สามารถตรวจสอบ latency ในหน่วย milliseconds (ms) ในการเชื่อมต่อไปยัง internal application ได้

5.8.1.14 แพลตฟอร์มที่นำเสนอจะต้องเลือกตั้งค่าให้รองรับการใช้งานของ users ได้ทั้งใน on premise และ work from anywhere ได้

5.8.1.15 แพลตฟอร์มที่นำเสนอไม่จำเป็นต้องกำหนด dedicated IP address ใด ๆ ให้กับผู้ใช้งาน เพื่อเป็นการหลีกเลี่ยงการเปิดเผย attack surface ให้กับภัยคุกคามจากอินเทอร์เน็ต อาทิ การโจมตีแบบ DDoS ได้

5.8.1.16 ผู้ใช้งานต้องสามารถเข้าถึง Private Application ได้ตลอดเวลา โดยไม่จำเป็นต้องเลือก Gateway ในการเชื่อมต่อแต่ละครั้ง

5.8.1.17 ผู้ใช้งานต้องสามารถเข้าถึง Private Application ได้โดยตรง เมื่อผ่านการตรวจสอบโดยไม่จำเป็นต้องกำหนด Local IP address หรือ VPN Pool ให้กับ User เพื่อทำ Access Control ในการเข้าถึง Private Application

5.8.1.18 แพลตฟอร์มที่นำเสนอจะต้องรองรับการระบุ application ได้อย่างยืดหยุ่นตามรูปแบบดังนี้เป็นอย่างน้อย

- (1) Fully qualified domain name (FQDN) หรือ domain name อาทิ xyz.abc.com
- (2) Local domain name เช่น directory.abc.local
- (3) IP address เช่น 192.0.2.0
- (4) IP Subnet เช่น 10.0.0.0/24
- (5) Wildcard domain เช่น *.abc.co.th

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

(6) Wildcard only เช่น *.*

5.8.1.19 สามารถทำ device posture เพื่อเช็คคุณสมบัติของอุปกรณ์ในการเข้าถึง application ภายใน ได้ เช่น OS version, Firewall status, Antivirus status, Location และ running process ได้

5.8.1.20 แพลตฟอร์มที่นำเสนอสามารถกำหนดสิทธิการใช้งานให้กับผู้ดูแลระบบได้หลายระดับ

5.8.1.21 สามารถกำหนด password เริ่มต้นให้กับผู้ใช้งานได้

5.8.1.22 ระบบจะต้องรองรับการใช้งานได้เป็นอย่างดีในทุกประเทศที่มีสถานเอกอัครราชทูต สถานกงสุลใหญ่ สำนักงานการค้า และกระทรวงการต่างประเทศ ตลอดระยะเวลาตามสัญญา

5.8.1.23 มีมาตรฐานการให้บริการ (SLA) ที่รองรับช่วงเวลาในการบริการ (Uptime) ที่ร้อยละ 99.999

5.8.1.24 แพลตฟอร์มที่นำเสนอจะต้องมี license ที่มีฟังก์ชันการใช้งานรองรับจำนวนผู้ใช้งานอย่างน้อย 1000 users ที่ถูกต้องตามกฎหมาย

5.8.2 ระบบตรวจจับและตอบสนองต่อเหตุการณ์การบุกรุก (Endpoint Detection and Response: EDR)

ผู้รับจ้างต้องจัดหาระบบตรวจจับและตอบสนองต่อเหตุการณ์การบุกรุกให้กับคอมพิวเตอร์สำหรับใช้งานระบบ e-Visa (endpoint) โดยมีคุณสมบัติที่ใช้งาน ดังนี้

5.8.2.1 ระบบเป็นผลิตภัณฑ์ต้องถูกจัดอันดับให้อยู่ในกลุ่ม Leader จากการจัดอันดับของ Gartner Magic Quadrant for Endpoint Protection Platforms สำหรับปี 2023 หรือใหม่กว่า

5.8.2.2 ระบบที่เสนอต้องสามารถเปิดการทำงานในรูปแบบ Endpoint Detection and Response (EDR) เพื่อเก็บข้อมูลการใช้งาน (Activity) ของเครื่อง Endpoint ต่าง ๆ และนำมาวิเคราะห์หาภัยคุกคามแบบ real-time ได้

5.8.2.3 ระบบต้องสามารถนำข้อมูลการแจ้งเตือนภัยคุกคาม (Alerts) มาแปลงให้อยู่ในรูปแบบ MITRE ATT&CK framework เพื่อต่อการทำความเข้าใจ

5.8.2.4 ระบบที่เสนอต้องสามารถเก็บข้อมูลภายในระบบปฏิบัติการ (kernel-mode) ได้มากกว่า 400 Raw events เพื่อนำมาย้อนรอยภัยคุกคามที่เกิดขึ้น (Incident) ได้

5.8.2.5 เป็นระบบที่สามารถสร้าง Indicator of Attack (IoA) เองได้ เพื่อตรวจจับพฤติกรรมที่ผิดปกติ (Malicious behaviors) หรือต้องการตรวจจับพฤติกรรมการทำงานที่องค์กรต้องเฝ้าระวัง ได้อย่างน้อยดังนี้ Process Creation, File Creation, Network Connection (IPv4, IPv6) และ Domain Name

5.8.2.6 เป็นระบบที่ต้องสามารถค้นหาข้อมูลการใช้งาน Source IP address, Domain และ Event ที่เกี่ยวข้องกับข้อมูลการใช้งาน (Activity) ได้

5.8.2.7 เป็นระบบที่สามารถค้นหาข้อมูลการใช้งานภายในที่เกี่ยวข้องกับเครื่องแม่ข่าย Windows, Linux และ Mac (Host Search) ได้

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

5.8.2.8 เป็นระบบที่สามารถค้นหาข้อมูลการใช้งาน Hash (Hash Search) กับเครื่อง Windows และ Mac ได้อย่างน้อยดังต่อไปนี้

- 1) Detect History
- 2) Unresolved Detects
- 3) Process Executions

5.8.2.9 เป็นระบบที่สามารถค้นหาข้อมูลการใช้งาน Username (User Search) กับเครื่อง Windows และ Mac ได้เป็นอย่างน้อย

- 1) User Logon Activities
- 2) Detect History
- 3) Unresolved Detects
- 4) Process Executions

5.8.2.10 แพลตฟอร์มที่นำเสนอจะต้องมี EDR license ที่มีฟังก์ชันการใช้งานครบถ้วน รองรับจำนวนผู้ใช้งานอย่างน้อย 1000 endpoints ที่ถูกต้องตามกฎหมาย

5.8.2.11 ในกรณีที่แพลตฟอร์มที่นำเสนอไม่สามารถใช้งานได้ในบางประเทศ ผู้รับจ้างต้องจัดหาแพลตฟอร์มอื่นที่มีคุณสมบัติเทียบเท่าหรือดีกว่านำมาใช้งานทดแทน ให้สามารถใช้งานได้มีประสิทธิภาพ

5.8.2.12 กรณีที่เกิดการโจมตีที่ EDR ไม่สามารถตรวจจับและป้องกันได้ ผู้รับจ้างจะต้องดำเนินการให้มีการค้นหาภัยคุกคามเชิงรุก (Threat Hunting) โดยใช้ผู้เชี่ยวชาญด้านความปลอดภัย (Human Analysis) โดยบริการดังกล่าวต้องครอบคลุมทุกเครื่องคอมพิวเตอร์ที่ติดตั้ง EDR เพื่อแก้ไขการโจมตีดังกล่าวโดยทันที

5.9 ระบบสื่อสารเชื่อมโยงข้อมูลกับหน่วยงานอื่น

5.9.1 ระบบเชื่อมโยงข้อมูลกับหน่วยงานภายนอก

ผู้รับจ้างต้องจัดเตรียมการเชื่อมโยงและแลกเปลี่ยนข้อมูลการตรวจลงตราระหว่างระบบคลาวด์ e-Visa กับหน่วยงานภายนอกโดยตรง สำหรับใช้ในการตรวจสอบประวัติบุคคลต้องห้าม และจัดเก็บข้อมูลการตรวจลงตรา พร้อมทั้งจัดทำ API สำหรับการเชื่อมโยงข้อมูล โดยผู้รับจ้างต้องเป็นผู้จัดทำ API สำหรับการแลกเปลี่ยนข้อมูล ตลอดระยะเวลาตามสัญญา หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด โดยมีรายละเอียดของข้อมูล ดังนี้

การติดต่อประสานงานกับหน่วยงานภายนอก (Interfaces with Others System)

ระบบภายนอก	รายละเอียดการติดต่อประสานงาน
สำนักงานตรวจคนเข้าเมือง	พัฒนาโปรแกรม เพื่อรองรับการรับ-ส่งข้อมูลได้แบบ Real-Time
สำนักงานข่าวกรองแห่งชาติ	พัฒนาโปรแกรม เพื่อรองรับการรับ-ส่งข้อมูลได้แบบ Real-Time
หน่วยงานอื่น ๆ	รองรับการพัฒนาโปรแกรม เพื่อรองรับการรับ-ส่งข้อมูลได้แบบ Real-Time กับหน่วยงานอื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

5.9.2 ผู้รับจ้างต้องจัดเตรียมการเชื่อมโยงและแลกเปลี่ยนข้อมูลการตรวจลงตราระหว่างระบบคลาวด์ e-Visa กับระบบบริการเชื่อมโยงข้อมูลกรมการกงสุล (Consular gateway) ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด โดยผู้รับจ้างจะต้องออกแบบ และเตรียมช่องทางการเชื่อมโยงข้อมูล e-Visa มาเก็บไว้ที่ศูนย์บริหารข้อมูลกลางกรมการกงสุล (CCDC) ผ่าน API ในรูปแบบ real-time ดังนี้

ระบบงาน	รายละเอียดข้อมูล
ศูนย์บริหารข้อมูลกลางกรมการกงสุล (CCDC)	1. รองรับการส่งข้อมูลอนุมัติการตรวจลงตรา และข้อมูลการอนุมัติการเดินทางเข้าประเทศไทย 2. รองรับการส่งข้อมูลการยื่นขอรับการตรวจลงตรา และข้อมูลการยื่นขออนุมัติการเดินทางเข้าประเทศไทย 3. รองรับการแลกเปลี่ยนข้อมูลอื่น ๆ ตามที่กรมการกงสุล กระทรวงการต่างประเทศ ร้องขอ

5.9.3 ผู้รับจ้างต้องจัดเตรียมการเชื่อมโยงและแลกเปลี่ยนข้อมูลการตรวจลงตราระหว่างระบบคลาวด์ e-Visa กับหน่วยงานภายนอกอื่น พร้อมทั้งจัดทำ API สำหรับการเชื่อมโยงข้อมูล โดยผู้รับจ้างต้องเป็นผู้จัดทำ API สำหรับการแลกเปลี่ยนข้อมูล ตลอดระยะเวลาตามสัญญา หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

5.9.4 ผู้รับจ้างต้องออกแบบระบบให้สามารถเชื่อมต่อกับหน่วยงานภายนอกได้ทั้งแบบเชื่อมต่อโดยตรงหรือผ่าน consular gateway และสามารถปรับเปลี่ยนรูปแบบการเชื่อมต่อได้ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด โดยไม่ต้องแก้ไขโปรแกรม

5.10 ระบบ Web Enquiry

ผู้รับจ้างต้องบำรุงรักษา และพัฒนา/ปรับปรุงระบบ Web Enquiry และบริหารงานที่เกี่ยวข้อง ให้สามารถเชื่อมโยงกับ ระบบ e-Visa ให้ใช้งานได้เป็นปกติ และรับผิดชอบค่าใช้จ่ายใด ๆ ที่เกี่ยวข้องทั้งหมด ตลอดระยะเวลาตามสัญญา และระยะเวลาประกัน ดังนี้

- (1) มีระบบสมัครสมาชิกสำหรับเข้าใช้งานระบบ Web Enquiry (<https://thaievisa.go.th/enquiry/>) ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด
- (2) ระบบสามารถค้นหาข้อมูลด้วยหมายเลขหนังสือเดินทาง หรือ ชื่อ สกุล หรือ Scan QR Code
- (3) ระบบสามารถแสดงข้อมูลการตรวจลงตรา พร้อมรายละเอียดของผู้ร้องได้ ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด
- (4) มีระบบบริหารจัดการ ผู้ใช้งาน และสิทธิ์การเข้าถึงข้อมูลการตรวจลงตราตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด
- (5) ระบบสามารถอ่าน QR code ซึ่งปรากฏอยู่บนเอกสารแจ้งการตรวจลงตราของศูนย์ข้อมูลการตรวจลงตรา (Visa Data Center)
- (6) มีระบบบันทึกกิจกรรมการใช้งาน (Log) ของผู้ใช้งานระบบทั้งหมด โดยสามารถค้นหา ตรวจสอบ และออกรายงานได้

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

5.11 ระบบ payment

ผู้รับจ้างต้องจัดทำ ดำเนินการ รับผิดชอบค่าใช้จ่าย และบริหารโครงการ ให้ระบบ e-Visa มีระบบการชำระเงิน ดังนี้

5.11.1 ระบบ payment แบบ online

ผู้รับจ้างต้องมีระบบการชำระเงินแบบ e-Payment โดยต้องเชื่อมโยงระบบ การชำระเงินของระบบ e-Visa กับทางสถาบันการเงินที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด ในช่องทางการจ่ายเงินที่หลากหลาย อาทิ Wechat pay /Alipay /Visa /Master/ Union Pay/ การโอนระหว่างบัญชีระหว่างธนาคารหรือสถาบันการเงิน รวมทั้งปรับปรุงระบบที่เกี่ยวข้องกับระบบ การชำระเงินแบบ e-Payment แบบ offline หรือการเพิ่มระบบหรือช่องทาง payment แบบอื่นเพื่อ การชำระค่าธรรมเนียม โดยต้องสามารถตรวจสอบยอดการชำระค่าธรรมเนียม และออกรายงานการชำระ ค่าธรรมเนียมตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนดได้ รวมถึงจะต้องปฏิบัติตามมาตรฐาน Payment Card Industry Data Security Standard (PCI DSS) เพื่อรักษาความมั่นคงปลอดภัยของข้อมูล บัตรเครดิตหรือบัตรเดบิตที่ใช้ในการชำระเงิน

5.11.2 ระบบ payment แบบ offline

ผู้รับจ้างต้องพัฒนาระบบการชำระเงินแบบ offline โดยต้องสามารถตรวจสอบ ยอดการชำระค่าธรรมเนียม และออกรายงานการชำระค่าธรรมเนียม พร้อมทั้งเชื่อมต่อข้อมูล API กับระบบ e-Visa รวมถึง payment gateway อื่น ๆ ตามเงื่อนไขที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนดได้

5.11.3 การเพิ่มระบบหรือช่องทาง payment แบบอื่นเพื่อการชำระค่าธรรมเนียม ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนดได้

5.12 การจัดฝึกอบรม

ผู้รับจ้างต้องจัดการฝึกอบรมสอนการใช้งานระบบ e-Visa หรือระบบที่พัฒนาในสัญญา ดังนี้
(1) จัดการฝึกอบรมแก่ผู้ดูแลระบบ จำนวนไม่น้อยกว่า 6 ครั้ง โดยมีรายละเอียด ดังนี้

ลำดับ	หัวข้อการฝึกอบรม	ระยะเวลา	จำนวนผู้อบรม
1	ระบบ e-Visa ในส่วนของผู้ดูแลระบบ	8 ชม.	ไม่น้อยกว่า 10 คน
2	การออกแบบระบบ Business flow, Network, Operation, Database and Design, การ Maintenance ระบบ e-Visa	8 ชม.	ไม่น้อยกว่า 10 คน
3	ระบบสารสนเทศทั้งหมดของโครงการ	24 ชม.	ไม่น้อยกว่า 10 คน
4	ระบบคลาวด์	8 ชม.	ไม่น้อยกว่า 10 คน
5	ด้านแผนการปฏิบัติที่เกี่ยวข้องกับด้านความปลอดภัย ของระบบและเทคโนโลยีสารสนเทศ	8 ชม.	ไม่น้อยกว่า 10 คน
6	การใช้งาน Mobile Application “Thai e-Visa” และ “Visa Checking”	8 ชม.	ไม่น้อยกว่า 10 คน

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

(2) จัดการฝึกอบรมแก่เจ้าหน้าที่กงสุลในต่างประเทศ แบบออนไลน์จำนวนไม่น้อยกว่า 8 ครั้ง ครั้งละไม่น้อยกว่า 2 ชั่วโมง โดยมีรายละเอียด ดังนี้

ลำดับ	หัวข้อการฝึกอบรม	ระยะเวลา	จำนวนผู้อบรม
1	การใช้งานระบบ e-Visa และการใช้งาน Mobile Application “Thai e-Visa” และ “Visa Checking”	16 ชม.	ครั้งละไม่น้อยกว่า 60 คน

(3) จัดการฝึกอบรมแก่เจ้าหน้าที่หน่วยงานภายนอกตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด ไม่น้อยกว่า 4 ครั้ง จำนวนผู้อบรมต่อครั้งไม่น้อยกว่า 20 คน และครั้งละไม่น้อยกว่า 3 ชั่วโมง

(4) จัดฝึกอบรมเทคนิคด้านการออกแบบและการบริหารจัดการระบบคลาวด์ หรือ ด้านความมั่นคงปลอดภัย หรือด้านการพัฒนาระบบ จำนวนไม่น้อยกว่า 3 หลักสูตร และผู้เข้าอบรมต่อหลักสูตรจำนวนไม่น้อยกว่า 3 คน ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(5) จัดฝึกอบรมด้านการออกแบบและพัฒนาระบบ จำนวนไม่น้อยกว่า 4 หลักสูตร หลักสูตรละไม่น้อยกว่า 4 คน

(6) จัดเตรียมเอกสารประกอบการอบรมทั้งรูปแบบเอกสารและ PDF ไฟล์ อาหารว่าง และอาหารกลางวัน รวมทั้ง จัดทำคลิปวิดีโอ คลิปประชาสัมพันธ์ในภาษาต่างประเทศ การบรรยายโดยละเอียด ในแต่ละหัวข้อ ให้สามารถใช้ได้กับผู้รับการอบรมในอนาคต โดยคลิปวิดีโอบรรจุอยู่ในระบบที่สามารถเปิดดูได้จากระบบ e-Visa

(7) ค่าเช่าสถานที่ ค่าอาหารว่าง ค่าอาหารกลางวัน ค่าเอกสาร หรือค่าใช้จ่ายอื่นใดที่เกี่ยวข้องกับการจัดฝึกอบรม ผู้รับจ้างต้องเป็นผู้รับผิดชอบทั้งหมด

ทั้งนี้ หัวข้อการอบรมในแต่ละรายการอาจมีการปรับเปลี่ยนได้ตามความเหมาะสม ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

5.13 ระบบสารสนเทศและ Software

ผู้รับจ้างต้องจัดหา บริหารจัดการ ดูแลระบบสารสนเทศและ Software ที่เกี่ยวข้อง โดยผู้รับจ้างเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมดตลอดระยะเวลาของสัญญา มีคุณสมบัติอย่างน้อย ดังนี้

5.13.1 ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operations Center: CSOC)

(1) จัดให้มีศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operations Center: CSOC) โดยจะต้องมีระบบเฝ้าระวัง ตรวจสอบและวิเคราะห์ภัยคุกคามทางไซเบอร์ ที่สามารถรองรับปริมาณข้อมูลของระบบ e-Visa ได้อย่างเพียงพอ ระบบต้องสามารถรวบรวม วิเคราะห์ และ ตรวจสอบภัยคุกคามจากอุปกรณ์ทั้งหมดที่เชื่อมต่อในระบบ e-Visa ระยะที่ 2 รวมถึงอุปกรณ์สำหรับผู้ใช้งาน ปลายทาง (Endpoint Devices) และต้องสามารถแจ้งเตือนภัยคุกคามแก่กรมการกงสุล กระทรวงการต่างประเทศ การผ่านช่องทางที่กำหนด อาทิ อีเมล และแอปพลิเคชันไลน์ (Line) โดยระบบ ต้องรองรับการเฝ้าระวังและวิเคราะห์ข้อมูลแบบเรียลไทม์ตลอด 24 ชั่วโมง 7 วัน และมีความสามารถในการ วิเคราะห์ความผิดปกติทางด้านเครือข่ายและระบบสารสนเทศด้วย

(2) ดำเนินการวิเคราะห์ภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมเสนอ แนวทางแก้ไขหรือยับยั้งเหตุการณ์ให้กรมการกงสุล กระทรวงการต่างประเทศทราบ

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

โดยการแจ้งเตือนภัยคุกคามจะเป็นไปตามระดับความรุนแรงของเหตุการณ์ กรณีที่เหตุการณ์มีระดับรุนแรงสูง (High) ขึ้นไป จะต้องแจ้งให้กรมการกงสุล กระทรวงการต่างประเทศ ทราบทันทีผ่านทางโทรศัพท์เคลื่อนที่ แอปพลิเคชันไลน์ (Line) หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด และจัดทำรายงาน เหตุการณ์ (Incident Report) ส่วนกรณีเหตุการณ์ที่มีระดับปานกลางถึงต่ำ (Medium - Low) จะต้องแจ้งให้ ทราบทางอีเมล หรือแอปพลิเคชันไลน์ (Line) การแจ้งเตือนต้องเป็นแบบอัตโนมัติและ โดยเนื้อหาในรายงาน ต้องครอบคลุมรายละเอียดที่สำคัญ อาทิ ประเภทของภัยคุกคาม ช่วงเวลาที่เกิดเหตุ ดันทาง (Attacker) และ ปลายทาง (Target) รวมถึงแนวทางหรือการแก้ไขปัญหาเชิงเทคนิค รวมถึงแนวทางป้องกันเพื่อไม่ให้เกิด เหตุการณ์ซ้ำ

(3) ดำเนินการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensic) เพื่อหาสาเหตุของการ โจมตีไซเบอร์ได้ หรือเมื่อได้รับการร้องขอจากกรมการกงสุล กระทรวงการต่างประเทศ โดยการตรวจสอบ แต่ละครั้งต้องดำเนินการให้แล้วเสร็จภายในระยะเวลาไม่เกิน Service Level Agreement โดยผู้ให้บริการ ต้องแจ้งระยะเวลาที่ใช้ในการตรวจสอบให้ผู้ให้บริการทราบล่วงหน้า ทั้งนี้ กระบวนการพิสูจน์หลักฐานต้อง เป็นไปตามมาตรฐานที่ยอมรับในระดับสากลและสามารถนำข้อมูลไปใช้ประกอบการวิเคราะห์เชิงลึกได้

(4) ดำเนินการจัดทำรายงานเฝ้าระวังภัยคุกคามทางไซเบอร์ (Incident Report) รายเดือนและรายงานฉุกเฉินเมื่อพบภัยคุกคามระดับ High หรือ Critical โดยต้องส่งให้กรมการกงสุล กระทรวงการต่างประเทศภายในวันที่ 10 ของเดือนถัดไป รายงานต้องครอบคลุมรายละเอียดที่สำคัญ อาทิ ประเภทของภัยคุกคาม วันและเวลาที่เกิดเหตุ ดันทาง (Attacker) และปลายทาง (Target) รวมถึงแนวทาง แก้ไขเชิงเทคนิคและแนวทางป้องกันเพื่อไม่ให้เกิดเหตุการณ์ซ้ำ รวมถึงจัดทำรายงานประจำเดือนเกี่ยวกับ สถานะภัยคุกคามและข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security News) และส่งให้ กรมการกงสุล กระทรวงการต่างประเทศภายในวันที่ 15 ของเดือนถัดไปผ่านช่องทางที่กำหนด อาทิ อีเมล หรือ Shared File Cloud Service หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(5) ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (CSOC) ต้องมีห้องเฉพาะ (Dedicated Room) สำหรับการปฏิบัติงาน โดยต้องได้รับการรับรองตามมาตรฐานสากล ได้แก่ ISO27001, ISO22301 และ ISO20000-1 นอกจากนี้ ต้องมีมาตรการควบคุมการเข้าถึงที่ปลอดภัย อาทิ ระบบ Access Control หรือระบบกล้องวงจรปิด (CCTV) ที่สามารถบันทึกภาพย้อนหลังได้ไม่น้อยกว่า 90 วัน ทั้งนี้ เพื่อให้ มั่นใจว่าศูนย์ปฏิบัติการมีมาตรฐานความปลอดภัยที่สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์

(6) จัดเตรียมบุคลากรที่มีความสามารถและประสบการณ์ที่เหมาะสมสำหรับการ ปฏิบัติงานภายในศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (CSOC) โดยเจ้าหน้าที่ที่ได้รับมอบหมาย ต้องสามารถปฏิบัติหน้าที่ได้อย่างครอบคลุมทุกด้านของการรักษาความมั่นคงปลอดภัยระบบ e-Visa รวมถึง การเฝ้าระวัง ตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์ ตลอดจนการให้คำแนะนำการ บริหารจัดการระบบรักษาความมั่นคงปลอดภัยเชิงเทคนิค การบริหารความเสี่ยง และการจัดทำรายงานด้านความ มั่นคงปลอดภัยไซเบอร์ตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด โดยบุคลากรที่ปฏิบัติงานต้องมี ความรู้ความสามารถเพียงพอสำหรับการปฏิบัติงานที่ได้รับมอบหมาย และต้องได้รับการฝึกอบรมหรือพัฒนา ทักษะอย่างต่อเนื่องเพื่อให้สามารถรับมือกับภัยคุกคามที่เปลี่ยนแปลงตลอดเวลา ซึ่งบุคลากรที่ปฏิบัติงาน จะต้องเป็นบุคคลเฉพาะที่ได้รับมอบหมายให้ทำงานให้กับกรมการกงสุล กระทรวงการต่างประเทศเท่านั้น และ ต้องไม่มีการแบ่งหน้าที่หรือใช้งานร่วมกับโครงการอื่นของผู้ยื่นข้อเสนอ ทั้งนี้ ผู้รับจ้างต้องรับผิดชอบในการ จัดสรรกำลังคนให้เหมาะสมกับปริมาณงานและระดับความเสี่ยงของระบบที่อยู่ภายใต้การดูแล เพื่อให้มั่นใจว่า

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ

การดำเนินงานของ CSOC เป็นไปอย่างมีประสิทธิภาพและสอดคล้องกับมาตรฐานที่เกี่ยวข้อง

(7) การกำหนดระดับความรุนแรง (Severity Classification) ระดับความรุนแรง (Severity) และดำเนินการตาม Service Level Agreement (SLA) ดังนี้

ระดับความรุนแรง (Severity)	เวลาในการวิเคราะห์และแจ้งเตือน (Detection & Investigation)	เวลาในการตอบสนองยับยั้งภัยคุกคาม (Response and Contain)
Critical	15 นาที	1 ชั่วโมง
High	30 นาที	4 ชั่วโมง
Medium	2 ชั่วโมง	24 ชั่วโมง

โดยเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์จะถูกจำแนกออกเป็น 4 ระดับ ได้แก่
ระดับ Critical – เหตุการณ์ที่ส่งผลกระทบร้ายแรงต่อระบบที่สำคัญ อาทิ ระบบหลักของ e-Visa ล่ม (System Outage) การโจมตีทางไซเบอร์ที่ส่งผลให้ข้อมูลรั่วไหล (Data Breach) การโจมตีแบบ Ransomware ที่ทำให้ระบบไม่สามารถใช้งานได้ (Ransomware Attack) หรือมีพฤติกรรมของผู้บุกรุกที่กำลังดำเนินการโจมตี (Active Threat)

ระดับ High – เหตุการณ์ที่มีผลกระทบสูงต่อความมั่นคงปลอดภัย หรือระบบใช้งานได้ไม่สมบูรณ์ อาทิ การตรวจพบการใช้บัญชีผู้ใช้ที่ไม่ได้รับอนุญาต (Unauthorized Access) การโจมตี DDoS ที่ส่งผลให้ระบบทำงานผิดปกติ การตรวจพบมัลแวร์ที่สามารถแพร่กระจายในระบบเครือข่าย การตรวจพบช่องโหว่ที่ร้ายแรง (Critical Vulnerability) ในระบบที่ยังไม่มีการแพตช์

ระดับ Medium – เหตุการณ์ที่มีความเสี่ยงต่ำหรือเป็นพฤติกรรมที่อาจนำไปสู่ภัยคุกคาม ความพยายามโจมตีที่ยังไม่สำเร็จ อาทิ Brute Force Attack การตรวจพบอีเมลฟิชชิ่งที่มีแนวโน้มเป็นอันตราย การใช้รหัสผ่านที่อ่อนแอ การเข้าถึงเว็บไซต์ที่อาจเป็นอันตราย หรือการแจ้งเตือนจากระบบที่ต้องมีการตรวจสอบเพิ่มเติม

(8) ผู้ยื่นข้อเสนองานจะต้องจัดทำเอกสารในรูปแบบรายงาน ประกอบด้วย

- รายงานเมื่อมีการบุกรุก และโจมตีทางไซเบอร์ประกอบด้วยข้อมูลขั้นต่ำ ดังนี้

1) สรุปสถานะและปัญหาที่พบของระบบเผื่อระวังฯ รวมถึงเครื่อง Server ต่างๆ ที่อยู่ในระบบทั้งหมด

2) สรุปการเผื่อระวังระบบ e-Visa

3) ระบุประเภทของภัยคุกคาม

4) วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

5) ระบุต้นทาง (Attacker) และปลายทาง (Target)

6) ระบุระดับความรุนแรง (Severity)

- รายงานประจำเดือนประกอบด้วยข้อมูลขั้นต่ำ ดังนี้

1) รายงานการลงเวลาเข้า-ออกงานของผู้ปฏิบัติงานประจำศูนย์ปฏิบัติการ CSOC ในแต่ละช่วงเวลาของการปฏิบัติงาน

2) รายงานสรุปผลภาพรวมในการปฏิบัติงานของเหตุการณ์ หรือ

ผู้ปฏิบัติงานที่เกิดขึ้น

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

3) รายงานของผู้บริหาร (Executive Summary) อาทิ สถิติเหตุการณ์ของการเฝ้าระวังภัยคุกคามของระบบ e-Visa

4) รายงานเชิงวิเคราะห์เกี่ยวกับภาพรวมภัยคุกคามด้านความมั่นคงปลอดภัยทางสารสนเทศ

- รายงานอื่น ๆ ตามที่ กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

(9) ดำเนินงานภายใต้ข้อตกลงระดับการให้บริการ (SLA: Service Level Agreement) ที่กำหนดไว้ โดยต้องให้การสนับสนุนกรมการกงสุล กระทรวงการต่างประเทศ ในการแก้ไขปัญหาด้านความมั่นคงปลอดภัยของอุปกรณ์ที่เกี่ยวข้อง เพื่อป้องกันไม่ให้เกิดเหตุการณ์เดิมซ้ำได้อีก นอกจากนี้ต้องสามารถดำเนินการตั้งค่าและปรับแต่งระบบเฝ้าระวังภัยคุกคามไซเบอร์ให้เหมาะสมกับสภาพแวดล้อมของระบบ e-Visa และต้องสามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพภายใต้ระยะเวลาของสัญญาที่กำหนด

5.13.2 ระบบบริหารจัดการงานตรวจลงตรา

5.13.2.1 Asset Management Software

ผู้รับจ้างต้องจัดหา เซิร์ฟเวอร์ หรือจัดซื้อ licenses รวมทั้งบริหารจัดการ ดูแลระบบบริหารจัดการทรัพย์สิน (Asset Management) ที่ tailored made สำหรับของทั้งโครงการ e-Visa เพื่อควบคุมทรัพย์สินและอุปกรณ์ต่าง ๆ ของโครงการได้อย่างมีประสิทธิภาพ อาทิ อุปกรณ์บนระบบคลาวด์ ระบบเซิร์ฟเวอร์ ระบบเครือข่าย คอมพิวเตอร์ ระบบ Monitoring Software Licenses

5.13.2.2 ต้องมีระบบตรวจสอบความถูกต้องครบถ้วนสมบูรณ์ของข้อมูล (Data Integrity) ตลอดกระบวนการ (Data life cycle) หากข้อมูลมีการเปลี่ยนแปลง สามารถตรวจสอบย้อนกลับเพื่อหาสาเหตุได้

5.13.2.3 มีระบบบริหารจัดการข้อกำหนดและนโยบายการใช้งาน (Terms and Policy) มีคุณลักษณะของระบบอย่างน้อย ดังนี้

(1) สร้างข้อกำหนดและนโยบายการใช้งาน ได้มากกว่า 1 แบบ แต่เลือกใช้งาน (Active) ได้เพียงแค่รายการเดียว

(2) สามารถควบคุมเวอร์ชัน (Version Control) ของข้อกำหนดและนโยบายการใช้งานได้

(3) เก็บข้อมูลประวัติการแก้ไข ข้อกำหนดและนโยบายการใช้งานได้

(4) เก็บข้อมูลการให้ความยินยอมของผู้ใช้งาน ตามข้อกำหนดของกรมการกงสุล กระทรวงการต่างประเทศ

(5) มีช่องทางการแก้ไข เปลี่ยนแปลง หรือ ลบ การให้ความยินยอมของผู้ใช้งานได้

(6) มีการเก็บประวัติ การยินยอม การแก้ไขเปลี่ยนแปลง หรือการลบ การให้ความยินยอมของผู้ใช้งาน

(7) รองรับการแสดงผลได้หลายภาษา ตามที่กรมการกงสุลกำหนด มีระบบที่แสดงผล 16 ภาษา ได้แก่ 1. อังกฤษ 2. ฝรั่งเศส 3. สเปน 4. รัสเซีย 5. อาหรับ 6. จีน (Traditional) 7. จีน (Simplified) 8. เยอรมัน 9. เกาหลี 10. ญี่ปุ่น 11. พม่า 12. กัมพูชา 13. ลาว 14. เวียดนาม 15. ภาษามาเลเซีย และ 16. โปรตุเกส

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

5.13.2.4 ระบบจัดการความยินยอมคุกกี้ของเจ้าของข้อมูล (Cookie Consent Management) จะต้องมีความสมบูรณ์อย่างน้อย ดังนี้

(1) สามารถตรวจสอบคุกกี้ (Cookies) และเทคโนโลยีที่เว็บไซต์ใช้ในการจัดเก็บข้อมูลส่วนบุคคลได้

(2) สามารถสร้างคุกกี้แบนเนอร์แบบปรับแต่งได้ (Customized Cookie Banner)

(3) รองรับการแสดงผลคุกกี้แบนเนอร์ได้หลายภาษา ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด มีระบบที่แสดงผล 16 ภาษา ได้แก่ 1. อังกฤษ 2. ฝรั่งเศส 3. สเปน 4. รัสเซีย 5. อาหรับ 6. จีน (Traditional) 7. จีน (Simplified) 8. เยอรมัน 9. เกาหลี 10. ญี่ปุ่น 11. พม่า 12. กัมพูชา 13. ลาว 14. เวียดนาม 15. บาสาซามาลาเซีย และ 16. โปรตุเกส

(4) ผู้ใช้งานเว็บไซต์สามารถใช้สิทธิในการให้ความยินยอมการเก็บ และใช้ข้อมูลในเว็บไซต์ต่าง ๆ ของระบบ e-Visa ได้ โดยมีแบนเนอร์ให้เลือกในการใช้งานครั้งแรก

(5) สามารถจดจำความยินยอมที่ผู้ใช้งานเลือก เพื่อให้ไม่แจ้งเตือนซ้ำในการใช้งานครั้งต่อไป

(6) สามารถปรับแต่งการจัดการความยินยอมโดยใช้กล่องข้อความ (Overlay) บนหน้าเว็บไซต์ได้

(7) รองรับการขอความยินยอมเพื่อใช้ข้อมูลที่อยู่ปัจจุบัน (Geo-Location)

(8) รองรับการเก็บข้อมูลการให้ความยินยอมไว้ได้ไม่เกิน ๒ ปี หรือสามารถกำหนดระยะเวลาการเก็บเองได้ รวมถึงการขอทบทวนการให้ความยินยอม (Re-Consent) และการขอถอนความยินยอมได้

(9) สามารถจัดทำรายงานสรุป และหน้าจอแสดงผลภาพรวม (Dashboard) ได้

- รายงานมาตรฐานในการติดตามและวิเคราะห์ความยินยอม
- สามารถแปลงรายงานเป็นไฟล์ประเภทต่างๆ ได้แก่ PDF File, Excel/CSV File หรือรูปแบบตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด โดยสามารถกำหนดช่วงหรือระยะเวลาการออกรายงานทุกประเภทในภาพรวมได้เป็นรายวัน รายเดือน หรือตามช่วงเวลาที่กำหนด
- สามารถจัดเก็บรายงาน (Archiving of Report) เพื่อใช้อ้างอิงในอนาคต

5.13.3 Business Intelligence

5.13.3.1 รองรับการใช้งานผ่านอุปกรณ์เคลื่อนที่ผ่าน App Store, Google Play, Windows Store ได้เป็นอย่างดี

5.13.3.2 รองรับการใช้งานผ่านเบราว์เซอร์ Microsoft Edge, Chrome เวอร์ชันล่าสุด, Safari Mac เวอร์ชันล่าสุด และ Firefox desktop เวอร์ชันล่าสุด ได้เป็นอย่างดี

5.13.3.3 รายชื่อผู้ใช้งานสามารถใช้รายชื่อเดียวกับ Identity service ที่ผู้รับจ้างเสนอได้

5.13.3.4 ชุดประมวลผลและหน่วยประมวลผลเป็นแบบใช้งานร่วมกัน

5.13.3.5 สามารถแบ่งปันรายงานไปยังผู้ที่ต้องการดูรายงานได้

5.13.3.6 รองรับขนาดของชุดข้อมูลได้ไม่น้อยกว่า 1 GB

5.13.3.7 มี Storage ไม่น้อยกว่า 10 GB ต่อผู้ใช้งาน

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

5.13.3.8 สามารถตรวจสอบการสร้างรายงาน การเผยแพร่เนื้อหาด้วยการวัดจำนวน
ผู้ใช้งานได้

5.13.3.9 ข้อมูลจะต้องมีการเข้ารหัส

5.13.3.10 สามารถสร้างข้อมูลรายงานและแสดงผลแบบ dashboard

5.13.3.11 รองรับการใช้งาน Big Data และ ETL

5.13.3.12 สามารถเชื่อมต่อข้อมูลภายนอกจากบริการบน Cloud และ Server แบบ
On-Premises ได้

5.13.3.13 สามารถตั้งค่าการแจ้งเตือนตามเงื่อนไขที่กำหนดได้

5.13.3.14 สามารถเชื่อมโยงกับฐานข้อมูลของระบบ e-Visa

5.13.4 ชุดโปรแกรมระบบปฏิบัติการ (Operation System)

ชุดโปรแกรมระบบปฏิบัติการ Windows เวอร์ชันล่าสุดสำหรับเครื่องคอมพิวเตอร์
และเครื่องคอมพิวเตอร์โน้ตบุ๊กที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย และจำนวน license เพียงพอกับจำนวนเครื่อง
คอมพิวเตอร์ที่ผู้รับจ้างเสนอในโครงการ

5.13.5 Microsoft Office (Productivity Software)

ชุดโปรแกรมจัดการสำนักงานสำหรับเครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์
โน้ตบุ๊กที่มีลิขสิทธิ์ถูกต้องตามกฎหมายและจำนวน license เพียงพอกับจำนวนเครื่องคอมพิวเตอร์ที่ผู้รับจ้าง
เสนอในโครงการ โดยมีคุณลักษณะพื้นฐานขั้นต่ำ ดังนี้

- มีโปรแกรมสำหรับประมวลคำหรือระบบจัดเตรียมเอกสาร
- มีโปรแกรมสำหรับประเภทตารางการคำนวณ
- มีโปรแกรมสำหรับประเภทการนำเสนอข้อมูล

5.13.6 ระบบสารสนเทศ และ Software อื่น ๆ ตามที่ได้ระบุหรือเกี่ยวข้องกับขอบเขตงานที่
ได้ระบุไว้ใน ข้อ 5

ผู้รับจ้างต้องจัดหาเช่า หรือจัดซื้อ licenses รวมทั้งบริหารจัดการ ดูแล ระบบ
บริหารสารสนเทศที่ได้ระบุไว้ในข้อ 5 ที่ต้องใช้ในการดำเนินโครงการ อาทิ software สำหรับอ่าน MRZ ระบบ
อ่าน OCR ระบบการอ่านภาพและเปรียบเทียบระบบ algorithm หรือระบบสารสนเทศอื่น ๆ ในการ
คัดกรองข้อมูล หรือประมวลผลต่าง ๆ ในโครงการ

5.14 การจัดทำสื่อ เพื่อการประชาสัมพันธ์ และสื่อที่ใช้ในการอบรม รวมทั้งข้อมูลและการแปล
ข้อความต่าง ๆ ในโครงการ

การจัดทำสื่อนั้น ข้อความ ภาพและเสียงต้องมีความสอดคล้อง และไม่ละเมิดลิขสิทธิ์ใด ๆ ทั้งสิ้น
หากมีการเรียกร้องหรือฟ้องร้องผู้รับจ้างต้องเป็นผู้รับผิดชอบทั้งหมด สำหรับ VDO Clip ต้องความละเอียด
ไม่น้อยกว่า Full-HD 1080P และมี subtitle ทั้งภาษาไทยและภาษาต่างประเทศที่ใช้ในระบบ e-Visa
(1. อังกฤษ 2. ฝรั่งเศส 3. สเปน 4. รัสเซีย 5. อาหรับ 6. จีน (Traditional) 7. จีน (Simplified) 8. เยอรมัน
9. เกาหลี 10. ญี่ปุ่น 11. พม่า 12. กัมพูชา 13. ลาว 14. เวียดนาม 15. บาสาซามาลเซีย 16. โปรตุเกส)

ในส่วนข้อความเอกสารของสื่อที่เป็นภาษาต่างประเทศ ผู้รับจ้างต้องจัดจ้างการแปล
จากผู้รับจ้างแปลภาษาที่มีความน่าเชื่อถือ และส่งมอบให้กรมการกงสุล กระทรวงการต่างประเทศ ตรวจสอบ
ทั้งนี้ ค่าใช้จ่ายทั้งหมดเป็นผู้รับจ้างเป็นผู้รับผิดชอบ

5.14.1 ผู้รับจ้างต้องจัดทำสื่อ Infographic ดังนี้

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

5.14.1.1 Infographic สำหรับเชิญชวนใช้งานระบบ e-Visa และระบบ Mobile Application จำนวน 12 ชิ้นงาน (งวดงานที่ 2-5 งวดละ 3 ชิ้นงาน) (16 ภาษา)

5.14.1.2 Infographic สำหรับสอนการใช้งานระบบ e-Visa และระบบ Mobile Application สำหรับผู้ร้อง จำนวน 12 ชิ้นงาน (งวดงานที่ 2-5 งวดละ 3 ชิ้นงาน) (16 ภาษา)

5.14.1.3 Infographic สำหรับสอนการใช้งานระบบ e-Visa และระบบ Mobile Application และงานการตรวจลงตราสำหรับเจ้าหน้าที่ จำนวน 24 ชิ้นงาน (งวดงานที่ 2-5 งวดละ 6 ชิ้นงาน) (16 ภาษา)

5.14.1.4 Infographic สำหรับการตรวจลงตราแต่ละประเภทสำหรับผู้ร้อง 72 ชิ้นงาน (งวดงานที่ 2-5 งวดละ 18 ชิ้นงาน)

5.14.1.5 Infographic สำหรับการพิจารณาตรวจลงตราแต่ละประเภทสำหรับเจ้าหน้าที่ 72 ชิ้นงาน (งวดงานที่ 2-5 งวดละ 18 ชิ้นงาน)

5.14.2 ผู้รับจ้างต้องจัดทำสื่อ Brochure และเอกสารคู่มือ ดังนี้

5.14.2.1 Brochure อธิบายระบบ e-Visa และระบบ Mobile Application จำนวน 2 ชิ้นงาน (แบบสั้น กับแบบละเอียด) (งวดงานที่ 2) (16 ภาษา)

5.14.2.2 ข้อความที่ใช้และปรากฏในระบบ e-Visa 16 ภาษา (งวดงานที่ 1)

5.14.2.3 เอกสารคู่มือการใช้งานระบบ e-Visa และระบบ Mobile Application สำหรับผู้ร้อง 2 ชิ้นงาน (แบบสั้น กับแบบละเอียด) (งวดงานที่ 2) (16 ภาษา)

5.14.2.4 เอกสารคู่มือการขอรับการตรวจตราแต่ละประเภท สำหรับผู้ร้อง 2 ชิ้นงาน (แบบสั้นกับแบบละเอียด) (งวดงานที่ 2) (16 ภาษา)

5.14.2.5 เอกสารคู่มือการใช้งานระบบ e-Visa และระบบ Mobile Application สำหรับเจ้าหน้าที่กระทรวงการต่างประเทศ 2 ชิ้นงาน (แบบสั้นกับแบบละเอียด) (งวดงานที่ 2) (16 ภาษา)

5.14.2.6 เอกสารคู่มือการใช้งานระบบ e-Visa และระบบ Mobile Application สำหรับเจ้าหน้าที่หน่วยงานภายนอก 2 ชิ้นงาน (แบบสั้นกับแบบละเอียด) (งวดงานที่ 2) (ภาษาไทยและภาษาอังกฤษ)

5.14.2.7 เอกสารคู่มือการตรวจลงตราแต่ละประเภทสำหรับเจ้าหน้าที่ 2 ชิ้น (แบบสั้นกับแบบละเอียด) (งวดงานที่ 3) (16 ภาษา)

5.14.3 ผู้รับจ้างต้องจัดทำสื่อ VDO Clip ดังนี้

5.14.3.1 VDO Clip เชิญชวนการใช้ระบบ e-Visa และระบบ Mobile Application แบบยาว 4 นาที 2 ชิ้นงาน (งวดงานที่ 2 และงวดงานที่ 3 งวดงานละ 1 ชิ้นงาน)

5.14.3.2 VDO Clip เชิญชวนการใช้ระบบ e-Visa และระบบ Mobile Application แบบสั้น ไม่เกิน 1 นาที 24 ชิ้นงาน (งวดงานที่ 3- 6 งวดละ 6 ชิ้นงาน)

5.14.3.3 VDO Clip อบรมการใช้งานระบบ e-Visa และระบบ Mobile Application สำหรับผู้ร้อง 2 ชิ้นงาน (แบบสั้น กับแบบละเอียด) (งวดงานที่ 2)

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

5.14.3.4 VDO Clip อบรมการขอรับการตรวจตราแต่ละประเภท สำหรับผู้ร้อง 2 ชั้นงาน (แบบสั้นกับแบบละเอียด) (งวดงานที่ 2 แบบสั้น และงวดงานที่ 3 แบบละเอียด)

5.14.3.5 VDO Clip อบรมการใช้งานระบบ e-Visa และระบบ Mobile Application สำหรับเจ้าหน้าที่กระทรวงการต่างประเทศ 2 ชั้นงาน (แบบสั้นกับแบบละเอียด) (งวดงานที่ 2 แบบสั้น และงวดงานที่ 3 แบบละเอียด)

5.14.3.6 VDO Clip อบรมการใช้งานระบบ e-Visa และระบบ Mobile Application สำหรับเจ้าหน้าที่หน่วยงานภายนอก 2 ชั้นงาน (แบบสั้นกับแบบละเอียด) (งวดงานที่ 2 แบบสั้น และงวดงานที่ 3 แบบละเอียด)

5.14.3.7 VDO Clip อบรมการตรวจลงตราแต่ละประเภทสำหรับเจ้าหน้าที่ 2 ชั้นงาน (แบบสั้นกับแบบละเอียด) (งวดงานที่ 3 แบบสั้น และงวดงานที่ 4 แบบละเอียด)

5.14.4 ผู้รับจ้างต้องจัดทำข้อความที่เกี่ยวกับระบบเพิ่มเติม ทั้งในการปรับระบบ การปรับเปลี่ยนเกี่ยวกับมาตรการการตรวจลงตรา หรือข้อความแจ้งเตือนต่าง ๆ ของระบบ โดยมีการแปล 16 ภาษา ตลอดระหว่างโครงการ โดยในการปรับเปลี่ยน หรือแจ้งเตือน ต้องดำเนินการภายใน 72 ชั่วโมงล่วงหน้า โดยผู้รับจ้างเป็นผู้ดำเนินการและรับผิดชอบค่าใช้จ่ายทั้งหมด

5.14.5 สื่อประชาสัมพันธ์ทั้งหมด ทางผู้รับจ้างจะต้องดำเนินการปรับปรุงให้เป็นปัจจุบัน ตลอดระยะเวลาสัญญา

5.15 เงื่อนไขการออกแบบและพัฒนาระบบ การให้บริการและบำรุงรักษา ลิขสิทธิ์ Software

5.15.1 การออกแบบและพัฒนาระบบ

ภายใน 2 เดือน นับจากวันที่ลงนามในสัญญา ผู้รับจ้างต้องดำเนินการศึกษา วิเคราะห์ และออกแบบระบบให้สอดคล้องกับความต้องการของ Business Flow ของระบบ e-Visa และระบบ Mobile Application และการตรวจลงตราโดยรวม เพื่อให้กรมการกงสุล กระทรวงการต่างประเทศ สอบทานความถูกต้องครบถ้วน และลงนามอนุมัติจากผู้ที่เกี่ยวข้องก่อนเริ่มกระบวนการพัฒนาระบบ โดยมีรายละเอียด ดังนี้

5.15.1.1 ส่งมอบและนำเสนอผลการวิเคราะห์ออกแบบระบบสารสนเทศ ในรูปแบบของเอกสารสถาปัตยกรรมองค์กร (Enterprise Architecture) ที่แสดงรายละเอียดของ

- (1) Business Architecture อาทิ ผังกระบวนการทางธุรกิจ (Business Workflows) ข้อกำหนดทางธุรกิจ (Business Rules) เป็นต้น
- (2) Application Architecture อาทิ Use Case Diagram พร้อมคำอธิบาย
- (3) Data Architecture อาทิ โครงสร้างฐานข้อมูล (Database Schema) แผนภาพกระแสข้อมูล (Data Flow Diagram) แผนภาพ E-R (E-R Diagram) และ พจนานุกรม (Data Dictionary)
- (4) Technology Architecture อาทิ แผนภาพแสดงสถาปัตยกรรมของระบบ พร้อมคำอธิบายโดยอ้างอิงกับ TOGAF 9.2 หรือที่ใหม่กว่า ในรูปแบบ PDF และ Electronic Files ที่แก้ไขเปลี่ยนแปลงได้ด้วย Software ประเภท Office Application

5.15.1.2 ส่งมอบและนำเสนอผลงานต้นแบบ (Prototype) โดยผู้รับจ้างต้อง ออกแบบประสบการณ์การใช้งาน (User Experience) และหน้าจอการใช้งาน (User Interface) ของผู้ใช้งาน ทั้งผู้รับบริการ เจ้าหน้าที่ของกระทรวงฯ และเจ้าหน้าที่หน่วยงานภายนอกให้สามารถใช้งานได้ง่าย

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

และสอดคล้องกับข้อกำหนดและกระบวนการในการตรวจสอบอย่างครบถ้วน พร้อมทั้งจัดทำผลงานต้นแบบ (Prototype) โดยใช้เครื่องมือออกแบบ อาทิ Figma AdobeXD และจัดทำเป็นเอกสารประกอบในรูปแบบ PDF และ Electronic Files ที่แก้ไขเปลี่ยนแปลงได้ด้วย Software ประเภท Office Application

5.15.2 การพัฒนาระบบ

5.15.2.1 ผู้รับจ้างต้องแบ่งสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (Development) การทดสอบ (Testing) และระบบที่ให้บริการจริง (Production) เพื่อควบคุมการทดสอบ และลดผลกระทบที่อาจเกิดขึ้นจากการนำระบบขึ้นใช้งานจริง

5.15.2.2 ผู้รับจ้างต้องมีกระบวนการในการควบคุมเวอร์ชันของคำสั่งในการเขียน โปรแกรมผ่านระบบจัดเก็บข้อมูลดิจิทัลแบบรวมศูนย์ (Git Repository Management) ที่กรมการกงสุล กระทรวงการต่างประเทศ เตรียมไว้ให้ โดยจัดเก็บตั้งแต่เริ่มต้นจนเสร็จสิ้นโครงการ พร้อมทั้งต้องระบุเวอร์ชันของซอร์ฟแวร์ให้สามารถเห็นได้อย่างชัดเจน

5.15.2.3 ผู้รับจ้างต้องมีการแบ่งหน้าที่ของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบ อย่างเหมาะสม โดยไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานตั้งแต่ต้นจนจบกระบวนการ อาทิ แยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง

5.15.2.4 ผู้รับจ้างต้องดำเนินการทดสอบระบบที่พัฒนาหรือมีการเปลี่ยนแปลง โดยทดสอบ Unit Test และ User Acceptance Test (UAT) เป็นอย่างน้อย และมีสภาพแวดล้อมเหมือนกับ งานจริง (Production Environment) เพื่อให้ระบบที่พัฒนาหรือเปลี่ยนแปลงสามารถทำงานได้อย่างถูกต้อง ตามข้อกำหนดของกรมการกงสุล กระทรวงการต่างประเทศ พร้อมทั้งจัดรายงาน กระบวนการและเอกสาร ขออนุมัติจากผู้ที่เกี่ยวข้องก่อนนำระบบขึ้นใช้งานจริง

5.15.2.5 ผู้รับจ้างต้องจัดทำแนวทางการควบคุมการรักษาความมั่นคงปลอดภัย และความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ อาทิ การทำ Data Masking เพื่อป้องกันความเสี่ยง ในการรั่วไหลของข้อมูล

5.15.2.6 ภายหลังผู้รับจ้างได้รับการยืนยันจากกรมการกงสุล กระทรวง การต่างประเทศ ให้ dlp ข้อมูล (Data Migration) ผู้รับจ้างจะต้องดำเนินการถ่ายโอนข้อมูลมายังระบบ e-Visa ระยะที่ 2 ให้แล้วเสร็จภายใน 20 วัน นับจากการปิดระบบ e-Visa ระยะที่ 1 โดยจะต้องทำ ความสะอาดข้อมูล (Data Cleansing) ตรวจสอบความถูกต้องครบถ้วนสมบูรณ์ (Data Integrity) ความเป็นปัจจุบันของข้อมูล (Up-to-date) และพร้อมใช้งาน (Availability) และจัด mapping ข้อมูล ให้ถูกต้อง พร้อมจัดทำรายงานที่เกี่ยวข้องในการถ่ายโอนข้อมูลส่งให้กรมการกงสุล กระทรวงการต่างประเทศ อาทิ แผนการถ่ายโอนข้อมูล รายงานสรุปผลการถ่ายโอนข้อมูล ตามรูปแบบและวันเวลาที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

5.15.2.7 ผู้รับจ้างต้องมีกระบวนการสำหรับการพัฒนาซอฟต์แวร์ แบบ DevSecOps และ CI/CD Pipeline เพื่อรองรับการ Deployment ผ่านระบบจัดเก็บข้อมูลดิจิทัล แบบรวมศูนย์ (Git Repository Management) ที่กรมการกงสุล กระทรวงการต่างประเทศ เตรียมไว้ให้ หากมีเครื่องมืออื่นใด จะต้องได้รับการอนุมัติจากกรมการกงสุล กระทรวงการต่างประเทศ

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

5.15.3 การให้บริการและบำรุงรักษาระบบ

5.15.3.1 การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

(1) ผู้รับจ้างต้องมีการจัดทำทะเบียนรายการทรัพย์สินทั้งซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) พร้อมทั้งมีการปรับปรุงรายการทะเบียนทรัพย์สินอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และดำเนินการบำรุงรักษาให้มีความพร้อมใช้งานอย่างสม่ำเสมอ รวมถึงวางแผนการบริหารจัดการทรัพย์สิน หากมีค่าใช้จ่ายผู้รับจ้างจะเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด

(2) ผู้รับจ้างต้องจัดทำกระบวนการและเอกสารที่เกี่ยวข้องในการควบคุมสิทธิ์การเข้าถึง (Access Control) ของระบบทั้งส่วนของผู้ดูแลระบบ (Admin) และผู้ใช้งาน (User) โดยให้ครอบคลุมกระบวนการ

- การขอสิทธิ์ (Request)
- การอนุมัติสิทธิ์ (Approve) โดยกรรมการกงสุล กระทรวงการ

ต่างประเทศ

- การยกเลิกสิทธิ์ (Terminate)

พร้อมจัดให้มีการทบทวนสิทธิ์ผู้ใช้งาน (Review) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเจ้าหน้าที่ลาออก หรือย้ายตำแหน่งการปฏิบัติหน้าที่

(3) ผู้รับจ้างต้องดำเนินการจัดการบริหารการเปลี่ยนแปลงระบบฯ (Change Management) ดังนี้

- จัดทำแนวปฏิบัติของกระบวนการบริหารความเปลี่ยนแปลง และจัดทำเอกสารที่เกี่ยวข้อง พร้อมทั้งกำหนดหลักเกณฑ์ในการแบ่งประเภทการเปลี่ยนแปลงระบบตามหมวดหมู่ของปัญหา ความรุนแรง และความเร่งด่วน
- จัดทำระบบหรือทะเบียนในการจัดเก็บคำขอเปลี่ยนแปลงระบบฯ
- จัดทำรายงานประจำเดือนและรายงานให้กรรมการกงสุล

กระทรวงการต่างประเทศ ทราบ

(4) ผู้รับจ้างต้องจัดทำกระบวนการและแนวปฏิบัติในการจัดการเหตุผิดปกติ (Incident management) จัดทำแผนการรับมือเหตุผิดปกติ และจัดทำรายงานผลเหตุการณ์ผิดปกติรายงานต่อกรรมการกงสุล กระทรวงการต่างประเทศ เมื่อเหตุการณ์สิ้นสุดลง

(5) ผู้รับจ้างต้องจัดทำเอกสาร Minimum Baseline Standard เพื่อใช้เป็นมาตรฐานในการตั้งค่าระบบ อาทิ ระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์สื่อสารต่าง ๆ และจัดทำชุดคำสั่งสำหรับตั้งค่าระบบอัตโนมัติ (Batch File)

(6) ผู้รับจ้างต้องมีการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging) ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์สื่อสารที่มีความสำคัญ โดยต้องมีรายละเอียดที่ครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่ระบุตัวผู้กระทำผิด และจัดเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย 12 เดือน พร้อมทั้งจัดทำรายงานการวิเคราะห์บันทึกเหตุการณ์รายเดือนและรายงานให้กรรมการกงสุล กระทรวงการต่างประเทศ รับทราบ

(7) ผู้รับจ้างต้องติดตามและดูแลความเพียงพอของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่ครอบคลุม ระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสารและระบบสาธารณูปโภคที่เกี่ยวข้อง พร้อมทั้งวางแผนดำเนินการและกำหนดตัวชี้วัดการใช้ทรัพยากรด้านเทคโนโลยี

ประธานกรรมการ กรรมการ กรรมการ

กรรมการ กรรมการ กรรมการ กรรมการ

สารสนเทศ (Threshold) และจัดทำรายงานประจำเดือนของการติดตามและดูแลรักษาระบบฯ พร้อมทั้งจัดทำ Dashboard สำหรับติดตามสถานะตลอด 24 ชั่วโมง 7 วัน และมีระบบแจ้งเตือนเมื่อการทำงานของระบบ ถึงค่า Threshold ที่กำหนด

(8) ผู้รับจ้างต้องจัดทำแนวปฏิบัติในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม และจัดหาเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติที่ส่งผลกระทบต่อความปลอดภัยของระบบที่มีความสำคัญ พร้อมทั้งจัดทำรายงานประจำเดือนของการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม พร้อมทั้งจัดทำ Dashboard สำหรับติดตามสถานะตลอด 24 ชั่วโมง 7 วัน และมีระบบแจ้งเตือนเมื่อการบุกรุกที่มีความรุนแรงสูง

(9) ผู้รับจ้างต้องจัดทำแนวปฏิบัติในการสำรองข้อมูลให้มีความพร้อมใช้ และมีความปลอดภัย และจัดให้มีระบบหรือทะเบียนในการควบคุมการจัดเก็บข้อมูล โดยระบุ

- ชื่อไฟล์
- วันที่
- ขนาดไฟล์
- ชื่อผู้ดำเนินการสำรองข้อมูล
- ช่วงเวลาที่จัดเก็บ

พร้อมทั้งจัดให้มีการทดสอบการ rollback ข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ 4 ครั้ง พร้อมทั้งจัดทำรายงานการสำรองข้อมูลรายเดือน และรายงานผลการทดสอบการ Roll Back ข้อมูลให้กรรมการกงสุล กระทรวงการต่างประเทศ ทราบ

(10) ผู้รับจ้างต้องจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่อง (BCP: Business Continuity Planning) และแผนการกู้คืนระบบ (DRP: Disaster Recovery Plan) พร้อมทั้งจัดให้มีการทดสอบแผนข้างต้น อย่างน้อยปีละ 1 ครั้ง

(11) ผู้รับจ้างจัดหาเจ้าหน้าที่สอน bot หรือเทคโนโลยี ที่กรรมการกงสุล กระทรวงการต่างประเทศ จะนำมาใช้เพื่อตอบข้อมูลผู้ร้องและผู้ที่เกี่ยวข้อง เพื่อปรับปรุง Chatbot ของ กรรมการกงสุลมีประสิทธิภาพที่ดีขึ้น (Training Chatbot)

(12) ผู้รับจ้างต้องจัดทีม Support เพื่อสนับสนุนการตอบคำถาม ที่เกี่ยวข้องกับการใช้งานระบบตลอด 24 ชม. ทุกช่องทางการสื่อสาร ทั้งในและต่างประเทศ call center กรรมการกงสุล กระทรวงการต่างประเทศ และหน่วยงานภายนอก

5.15.4 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

5.15.4.1 ผู้รับจ้างต้องมีการบริหารความเสี่ยงที่เกิดขึ้นภายในโครงการ อย่างน้อยปีละ 1 ครั้ง พร้อมทั้งจัดทำรายงานการประเมินความเสี่ยง โดยมีเนื้อหาครอบคลุมอย่างน้อย

- (1) การระบุความเสี่ยง (Risk Identification)
- (2) การวิเคราะห์ความเสี่ยง (Risk Analysis)
- (3) การประเมินความเสี่ยง (Risk Evaluation)
- (4) การจัดการความเสี่ยง (Risk Treatment)
- (5) การติดตามและทบทวนความเสี่ยง (Risk Monitoring

and Review)

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

ทั้งนี้ ผู้รับจ้างต้องเป็นผู้ดำเนินการจัดการกับความเสี่ยงที่เกิดขึ้น และหากมีค่าใช้จ่ายที่เกิดขึ้นผู้รับจ้างต้องเป็นผู้รับผิดชอบ

5.15.4.2 การตรวจสอบด้านเทคโนโลยีสารสนเทศ

(1) ผู้รับจ้างต้องจัดทำให้มีการทดสอบระบบจากหน่วยงานภายนอก โดยผู้รับจ้างเป็นผู้ออกค่าใช้จ่ายทั้งหมด และนำเสนอรายงานผลการทดสอบและการแก้ไขแก่กรรมการกงสุล ดังนี้

- การทดสอบเจาะระบบ (Penetration Test) อย่างน้อยปีละ 1 ครั้ง
- การทดสอบ VA จากหน่วยงานภายนอก อย่างน้อยปีละ 2 ครั้ง
- การทดสอบความสามารถของระบบเมื่อถูกใช้งานเกินขีดจำกัด (Stress Test)

- การทดสอบการใช้งานของระบบในสภาวะการใช้งานปกติ (Load Test)

(2) ผู้รับจ้างจะต้องรักษาข้อมูลของกระทรวงการต่างประเทศ เป็นความลับตลอดไป และบุคลากรของผู้รับจ้างทุกคน รวมถึงผู้ที่ผู้รับจ้าง จ้างให้ทำงานเป็นการชั่วคราว (Outsourced Personnel) ที่มีสิทธิเข้าระบบและได้เห็นหรือรับทราบข้อมูลที่เป็นความลับต้องมีการลงนามยินยอมในสัญญาไม่เปิดเผยความลับที่เรียกว่า Non-Disclosure Agreement (NDA) และสัญญาประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ก่อนเข้าทำงานในระบบได้ หากกรรมการกงสุล กระทรวงการต่างประเทศ ตรวจสอบแล้วพบว่าผู้รับจ้างมีการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตและก่อให้เกิดความเสียหาย ผู้รับจ้างต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นทั้งหมด

5.15.5 ลิขสิทธิ์ Software

ผู้รับจ้างต้องเป็นผู้รับภาระการบำรุงรักษาและค่าลิขสิทธิ์ Software ที่ใช้ในโครงการทั้งหมด โดยต้องดำเนินการจัดหา Software ให้กรรมการกงสุล กระทรวงการต่างประเทศ หรือบุคคลอื่นใดที่กรรมการกงสุล กระทรวงการต่างประเทศ มอบหมาย เป็นผู้ได้รับอนุญาตใช้สิทธิในลิขสิทธิ์ และสิทธิการใช้งาน รวมถึงการต่ออายุสิทธิการใช้งาน Software (Licenses/Software Subscriptions) โดยตรงจากเจ้าของลิขสิทธิ์ Software ทั้งปวง โดยผู้รับจ้างเป็นผู้รับภาระการบำรุงรักษาและค่าลิขสิทธิ์ Software ที่ใช้ในโครงการฯ ทั้งหมด ตลอดระยะเวลาโครงการฯ ตั้งแต่เริ่มจนจบโครงการฯ

5.16 เงื่อนไขการสิ้นสุดสัญญา

5.16.1 เมื่อสิ้นสุดโครงการผู้รับจ้างต้องจัดทำรายงานสรุปผลการปิดโครงการ โดยสรุปผลการปฏิบัติงานที่ได้ดำเนินการระหว่างสัญญาโดยมีเนื้อหาอย่างน้อย ดังนี้

- (1) สถิติผลการปฏิบัติงานทั้งหมด
- (2) ประโยชน์ที่ได้รับ
- (3) สรุปปัญหาและอุปสรรคของการบริหารจัดการโครงการ
- (4) รายการฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ที่ส่งมอบให้กรรมการกงสุล กระทรวงการต่างประเทศ
- (5) แผนปฏิบัติการการรื้อถอนอุปกรณ์หรือถอนการติดตั้งซอฟต์แวร์ (Software) โดยละเอียด

(6) ข้อเสนอแนะการปรับปรุง และการพัฒนาโครงการ

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

5.16.2 เมื่อสิ้นสุดสัญญาผู้รับจ้างจะต้องเปิดให้สามารถใช้งานคลาวด์ ตามข้อ 5.4 ทั้งหมดต่อไปอีกเป็นระยะเวลา 3 เดือน นับจากวันสิ้นสุดสัญญา

5.16.3 หากกรมการกงสุล กระทรวงการต่างประเทศ เห็นว่ามีความจำเป็นต้องมีการดำเนินการในการรื้อถอนอุปกรณ์ หรือยกเลิกบริการ ผู้รับจ้างต้องรื้อถอนอุปกรณ์หรือยกเลิกบริการ ทั้งซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) โดยผู้รับจ้างต้องรับผิดชอบค่าใช้จ่ายที่เกี่ยวข้องทั้งหมด ตามรายการ วัน เวลา สถานที่ ที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด

5.16.4 ผู้รับจ้างต้องจัดทำคู่มือการใช้งานระบบฯ สำหรับผู้ดูแลระบบ (Admin) และผู้ใช้งาน (User) โดยจัดทำในรูปแบบเอกสารให้ครอบคลุมทุกโมดูลของระบบที่พัฒนาขึ้น หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด

5.16.5 ผู้รับจ้างต้องส่งมอบ Source Code ที่พัฒนาขึ้นให้เป็นกรรมสิทธิ์ของกรมการกงสุล กระทรวงการต่างประเทศทั้งหมด และห้ามไม่ให้ผู้รับจ้างนำผลงานที่ทำให้กรมการกงสุล กระทรวงการต่างประเทศ หรือส่วนใดส่วนหนึ่งหรือทั้งหมด ไปเผยแพร่ให้ผู้อื่นทราบ หรือนำไปใช้ โดยไม่ได้รับความยินยอมที่เป็นลายลักษณ์อักษรจากกรมการกงสุล กระทรวงการต่างประเทศ

5.16.6 ผู้รับจ้างต้องส่งมอบชื่อผู้ใช้งานและรหัสผ่าน ของระบบงานที่เกี่ยวข้องที่มีสิทธิ์ของผู้ดูแลระบบระดับสูงสุดของระบบที่พัฒนาขึ้น อาทิ ระบบฐานข้อมูล ระบบบริหารจัดการ Cloud และระบบอื่นใดที่เกี่ยวข้องแก่กรมการกงสุล กระทรวงการต่างประเทศ ทั้งหมด

5.16.7 ผู้รับจ้างต้องดำเนินการส่งมอบเอกสารและรายงานตามที่กรมการกงสุล กระทรวงการต่างประเทศ ระบุในข้อ 5.16.1 และจัดทำเป็นเอกสารประกอบในรูปแบบเอกสารรูปเล่ม PDF และ Electronic Files ที่แก้ไขเปลี่ยนแปลงได้ด้วย Software ประเภท Office Application (Word/Excel)

5.16.8 ผู้รับจ้างต้องรับประกันการใช้งานระบบ e-Visa และระบบ Mobile Application ทั้งหมด ตามขอบเขตข้อ 5.3 ให้สามารถทำงานได้เป็นปกติ หลังจากสิ้นสุดสัญญาต่อไปอีก 1 ปี โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น โดยผู้รับจ้างต้องนำเสนอและส่งมอบ Source code ที่ปรับปรุงเป็นปัจจุบันล่าสุด ก่อนสิ้นสุดระยะเวลาการรับประกันให้กรมการกงสุล กระทรวงการต่างประเทศ

5.16.9 ผู้รับจ้างต้องบำรุงรักษา ดูแล และแก้ไขตามขอบเขตข้อ 5 ทั้งหมด ยกเว้นข้อ 5.1.3.3 และ 5.1.3.5 ให้สามารถทำงานได้เป็นปกติ หลังจากสิ้นสุดสัญญาต่อไปอีก 3 เดือน โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น

5.17 การจัดทำรายงาน

ผู้รับจ้างต้องจัดทำรายงานสรุปรายวัน รายเดือน รายงาน Incident และรายงานสรุปหลังสิ้นสุดสัญญา โดยจัดทำในรูปเล่มรายงานและในรูปแบบเอกสารอิเล็กทรอนิกส์ (PDF/Word/Excel) ส่งมอบให้กรมการกงสุล กระทรวงการต่างประเทศ ดังนี้

5.17.1 รายงานสรุปประจำวัน ตั้งแต่ช่วงระยะเวลา 0:00 น. ถึงเวลา 23:59 น. ตามเวลาในประเทศไทยของวันทำการราชการใน Format ที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด สำหรับวันที่ราชการหยุดทำการให้นับเวลา 0:00 น. ของวันทำการก่อนวันหยุดราชการจนกระทั่ง 23:59 น. ของวันหยุดราชการวันสุดท้ายเป็นกรอบระยะเวลาของรายงานประจำวัน จำนวน 1 ชุด โดยส่งรายงานก่อน 16:00 น. ของวันปฏิบัติงานวันถัดไป

(1) รายงานสรุปผลการปฏิบัติงานประจำวันของระบบ e-Visa ทั้งหมด รวมสถิติคำร้อง และการตรวจลงตรา แยกสถานะการพิจารณา แยกประเภทการตรวจลงตรา และแยกสำนักงาน และสถิติภาพรวม

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

(2) รายงานสรุปการดำเนินการบริหารจัดการ บำรุงรักษา ดูแล ปรับปรุง ปฏิบัติงาน ที่เกี่ยวข้องกับระบบ e-Visa และระบบคลาวด์ทั้งหมด

(3) รายงานสรุปปัญหา Incident ที่เกิดกับระบบ e-Visa ระบบ Mobile Application และระบบคลาวด์ แบ่งตามประเภท และระดับความรุนแรง (หากมี)

5.17.2 รายงานสรุปประจำเดือน นับจากวันปฏิบัติงานตามวันทำการราชการวันแรกของเดือน ถึงวันปฏิบัติงานตามวันทำการราชการวันสุดท้ายของเดือน โดยใช้เกณฑ์เวลาตามข้อ 5.17 จำนวน 2 ชุด โดยส่งรายงานภายใน 10 วันของเดือนถัดไป ดังนี้

(1) รายงานสรุปผลการปฏิบัติงานประจำเดือนของระบบ e-Visa ทั้งหมด รวมถึงสถิติ คำร้องและการตรวจลงตรา แยกสถานะการพิจารณา แยกประเภทการตรวจลงตรา และแยกสำนักงาน และสถิติภาพรวม

(2) รายงานสรุปการดำเนินการบริหารจัดการ บำรุงรักษา ดูแล ปรับปรุง ปฏิบัติงาน ที่เกี่ยวข้องกับระบบ e-Visa ระบบ Mobile Application และระบบคลาวด์

(3) รายงานการใช้งาน CPU, RAM, DISK และ Bandwidth ในแต่ละ VM หรือข้อมูล สถิติอื่น ๆ ที่เกี่ยวข้องในทรัพยากรคลาวด์

(4) รายงานสรุปปัญหา Incident ที่เกิดกับระบบ e-Visa ระบบ Mobile Application และระบบคลาวด์ แบ่งตามประเภท และระดับความรุนแรง (หากมี)

5.17.3 รายงานสรุปเป็นรายครั้งกรณีเกิด Incident ที่มีระดับความรุนแรง High และ Critical ตามข้อ 5.13.1 กับระบบ e-Visa ระบบ Mobile Application และระบบคลาวด์ ตามที่ กรมการกงสุล กระทรวงการต่างประเทศร้องขอ จำนวน 1 ชุด โดยส่งรายงานภายใน 3 วันนับจากวันที่เกิด Incident หรือตามที่กรมการกงสุล กระทรวงการต่างประเทศ ร้องขอ

5.17.4 รายงานสรุปการดำเนินโครงการทั้งหมดหลังสิ้นสุดสัญญา จำนวน 2 ชุด โดยจัดส่ง รายงานภายใน 15 วัน นับจากวันสิ้นสุดสัญญา ดังนี้

(1) สถิติผลการปฏิบัติงานทั้งหมด

(2) ประโยชน์ที่ได้รับ

(3) สรุปปัญหาและอุปสรรคของการบริหารจัดการโครงการ

(4) รายการฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ที่ส่งมอบให้กรมการกงสุล กระทรวงการต่างประเทศ

(5) แผนปฏิบัติการการรื้อถอนอุปกรณ์หรือถอนการติดตั้งซอฟต์แวร์ (Software) โดยละเอียด

(6) ข้อเสนอแนะการปรับปรุง หรือพัฒนาโครงการ

5.18 การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

การใด ๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศ ผู้รับจ้างต้องจัดการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศกรมการกงสุล กระทรวงการต่างประเทศ ดังนี้

5.18.1 ประกาศกรมการกงสุล เรื่อง นโยบายในการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2563

5.18.2 ประกาศกรมการกงสุล เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2563

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

5.18.3 ประกาศกรมการกงสุล เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ พ.ศ. 2563

ทั้งนี้ รวมถึงกรณีที่มีการออก แก้ไข กฎหมายหรือประกาศใด ๆ ข้างต้น และการปฏิบัติเพื่อให้เป็นไปตามกฎหมายอื่น ๆ ที่เกี่ยวข้องที่มีผลใช้บังคับในช่วงการดำเนินโครงการภายใต้ข้อกำหนดของสัญญา

5.19 เงื่อนไขการให้บริการในภาพรวมและกรอบระดับการให้บริการ (Service Level Agreement)

ผู้รับจ้างต้องดำเนินการให้บริการ ดังนี้

5.19.1 เงื่อนไขการให้บริการในภาพรวม

- (1) ฝึกอบรมและถ่ายทอดเทคโนโลยีให้กับเจ้าหน้าที่กรมการกงสุล กระทรวงการต่างประเทศ
- (2) กรณีที่เกิดเหตุหรือความจำเป็นที่กรมการกงสุล กระทรวงการต่างประเทศ ต้องใช้บริการเพิ่มเติมของผู้รับจ้าง นอกเหนือจากที่กำหนดไว้ในขอบเขตงาน รวมทั้งในส่วนจำนวนภาระงาน ที่ผู้รับจ้างจะต้องปรับปรุง/พัฒนาระบบ ให้ผู้รับจ้างระบุเกี่ยวกับนโยบาย หลักเกณฑ์ วิธีการ ราคา และเงื่อนไขในการให้บริการเพิ่มเติมอื่น ๆ ให้ชัดเจน
- (3) วัสดุและอุปกรณ์อื่น ๆ ประกอบการดำเนินการในการสำรองข้อมูล e-Visa ผู้รับจ้างจะเป็นผู้จัดหาตามความเห็นชอบของ กรมการกงสุล กระทรวงการต่างประเทศ โดยจัดเตรียมไว้ในจำนวนที่เพียงพอและเหมาะสมตลอดระยะเวลาดำเนินการ
- (4) ข้อมูลเอกสาร Software สิทธิการใช้งาน และกระบวนการ องค์ความรู้ ทั้งหมดที่ใช้ในโครงการศูนย์ข้อมูลการตรวจลงตราของไทย (Visa Data Center - VDC) เพื่อจัดทำและดูแลระบบตรวจลงตราอิเล็กทรอนิกส์ (e-Visa) ระยะที่ 2 ถือเป็นเอกสิทธิ์ของกรมการกงสุล กระทรวงการต่างประเทศ ผู้รับจ้างไม่สามารถนำไปใช้เพื่อประโยชน์ส่วนตัวหรือธุรกิจอื่นใด ๆ ได้
- (5) ผู้รับจ้างจะต้องบำรุงรักษาให้พร้อมใช้ และเปลี่ยนอุปกรณ์เมื่อหมดอายุการใช้งาน และเครื่องมือที่มีความเสื่อมตามระยะเวลาการใช้งาน เพื่อให้อุปกรณ์และเครื่องมือทำงานได้อย่างถูกต้องและครบถ้วนตามข้อกำหนดตลอดระยะเวลาของสัญญา
- (6) ผู้รับจ้างจะต้องจัดทำและเสนอแผนสำรองกรณีฉุกเฉิน (Emergency response) และแผนการดำเนินการอย่างต่อเนื่อง (Business Continuity Plan) โดยให้มีการทดสอบซีกซ้อมแผนสำรองกรณีฉุกเฉินและแผนการดำเนินการอย่างต่อเนื่องอย่างน้อยปีละ 1 ครั้ง ในระหว่างสัญญาการให้บริการ
- (7) ผู้รับจ้างจะต้องยื่นกรอบระดับการให้บริการ (Service Level Agreement: SLA) ที่จะให้บริการกับกรมการกงสุล กระทรวงการต่างประเทศ และผู้รับจ้างต้องจัดทำรายงานประจำเดือนและในรอบครบสัญญาตามกรอบ SLA เพื่อเป็นส่วนหนึ่งในการประเมินผลการให้บริการของผู้รับจ้าง

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

5.19.2 กรอบระดับการให้บริการ (SLA) ที่ผู้รับจ้างจะต้องให้บริการโดย อยู่ในเกณฑ์บริการตามเงื่อนไขที่กำหนดหรือดีกว่า ดังนี้

ลำดับ	กระบวนงาน	หน่วย	หน่วย	หมายเหตุ
ด้านระบบสารสนเทศ ระบบ Mobile Application และระบบฐานข้อมูล				
1	ระยะเวลาในการตอบสนองต่อผู้ใช้งาน (Response Time) ไม่เกิน	3	วินาที	ต้องใช้งานบน environment ที่ใช้งานจริงตามข้อ 5 ยกเว้น ในส่วนของระบบการออกรายงาน
2	Recovery Point Objective (RPO) ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย	1	นาที่	
3	Recovery Time Objective (RTO) ระยะเวลาสูงสุดที่ใช้คืนสภาพระบบให้สามารถใช้งานได้เป็นปกติ	10	นาที่	
4	การปรับปรุงเงื่อนไขการตรวจลงตราและการเพิ่มหรือลดประเภทการตรวจลงตราในระบบ e-Visa และระบบ Mobile Application ตามนโยบายที่กรมการกงสุลกำหนด	72	ชม.	
5	การเพิ่ม หรือพัฒนาโมดูลการใช้งานของระบบ e-Visa และระบบ Mobile Application (refer ไปยัง man-day)	14	วัน	หากเป็นโมดูลที่ต้องใช้เวลาในการพัฒนาเกินกว่า 14 วัน ผู้รับจ้างสามารถขอย้ายระยะเวลาเพิ่มได้ และต้องได้รับความเห็นชอบจากกรมการกงสุล กระทรวงการต่างประเทศ
การถ่ายโอนระบบและข้อมูล (Migration)				
6	การถ่ายโอนข้อมูล (Data Migration) มายังระบบตรวจลงตราอิเล็กทรอนิกส์ (e-Visa) ระยะที่ 2	20	วัน	
ระบบความมั่นคงและความปลอดภัย				
7	เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์มีความรุนแรงระดับ Critical	15	นาที่	หากผู้รับจ้างทราบข้อมูลจากระบบหรือช่องทางอื่น ผู้รับจ้างจะต้องแจ้งให้กรมการกงสุล กระทรวงการต่างประเทศทราบ

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

		1	ชม.	ตอบสนอง และยับยั้งภัยคุกคาม (Response and Contain) และจัดทำรายงานผลการตรวจสอบเบื้องต้น
		24	ชม.	เก็บหลักฐานและวิเคราะห์เพื่อกำจัดการต้นตอของภัยคุกคามให้ออกจากระบบทั้งหมด (Eradication) พร้อมกู้คืนระบบให้กลับมาทำงานปกติ (Recovery) พร้อมจัดทำรายงานเชิงลึก
8	เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์มีความรุนแรงระดับ High	30	นาที	หากผู้รับแจ้งทราบข้อมูลจากระบบหรือช่องทางอื่น ผู้รับแจ้งจะต้องแจ้งให้กรมการกงสุล กระทรวงการต่างประเทศทราบ
		4	ชม.	ตอบสนอง และยับยั้งภัยคุกคาม (Response and Contain) และจัดทำรายงานผลการตรวจสอบเบื้องต้น
		48	ชม.	เก็บหลักฐานและวิเคราะห์เพื่อกำจัดการต้นตอของภัยคุกคามให้ออกจากระบบทั้งหมด (Eradication) พร้อมกู้คืนระบบให้กลับมาทำงานปกติ (Recovery) พร้อมจัดทำรายงานเชิงลึก
9	เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์มีความรุนแรงระดับ Medium	2	ชม.	หากผู้รับแจ้งทราบข้อมูลจากระบบหรือช่องทางอื่น ผู้รับแจ้งจะต้องแจ้งให้กรมการกงสุล กระทรวงการต่างประเทศทราบ
		24	ชม.	ตอบสนอง และยับยั้งภัยคุกคาม (Response and Contain) และจัดทำรายงานผลการตรวจสอบเบื้องต้น

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ

		72	ชม.	เก็บหลักฐานและวิเคราะห์ เพื่อกำจัดต้นตอของภัย คุกคามให้ออกจากระบบ ทั้งหมด (Eradication) พร้อมกู้คืนระบบให้กลับมา ทำงานปกติ (Recovery) พร้อมจัดทำรายงานเชิงลึก
อื่น ๆ				
10	การให้ข้อมูลเพื่อสนับสนุนการใช้งาน ให้กับเจ้าหน้าที่ผ่านช่องทาง Voice และ Non-voice (Service Support)	5	นาที	ต้อง response ภายใน 5 นาที ตลอด 24 ชั่วโมง 7 วัน
11	การแก้ไขปัญหาเชิงเทคนิค การตรวจสอบ ข้อมูลระบบให้กับเจ้าหน้าที่ และ ประสานงานในเชิงเทคนิคกับหน่วยงาน ต่าง ๆ ที่เกี่ยวข้อง	4	ชม.	- แก้ไขปัญหาทางเทคนิค โดยเจ้าหน้าที่ปฏิบัติการศูนย์ ข้อมูลการตรวจลงตรา ตลอด 24 ชั่วโมง 7 วัน - ผู้รับแจ้งสามารถขอขยาย ระยะเวลาเพิ่มได้ เมื่อมีเหตุ สุดวิสัยและต้องได้รับความ เห็นชอบจากกรมการกงสุล กระทรวงการต่างประเทศ

ทั้งนี้ ผู้รับแจ้งจะต้องแสดงระยะเวลาตามข้อกำหนด SLA หรือแสดงเอกสารหลักฐานยืนยัน
ให้คณะกรรมการตรวจรับพัสดุทราบในการตรวจรับงานด้วย

6. การทำสัญญา

ผู้ที่ได้รับการคัดเลือกจะต้องทำสัญญาที่กำหนดกับกระทรวงการต่างประเทศภายใน 7 วันทำการ
(เจ็ดวันทำการ) นับถัดจากวันที่ได้รับแจ้งและจะต้องวางหลักประกันสัญญาเป็นจำนวนร้อยละ 10 (ร้อยละสิบ)
ของมูลค่าทั้งหมดของสัญญาให้กระทรวงการต่างประเทศ ยึดถือไว้ในขณะทำสัญญาโดยใช้หลักประกัน
อย่างหนึ่งอย่างใด ดังต่อไปนี้

6.1 เชื้อที่ธนาคารสั่งจ่ายให้แก่กระทรวงการต่างประเทศโดยเป็นเช็คลงวันที่ที่ทำสัญญา
หรือก่อนหน้านั้น ไม่เกิน 3 วันทำการ (สามวันทำการ) ของทางราชการ

6.2 หนังสือค้ำประกันของธนาคารภายในประเทศตามแบบที่คณะกรรมการนโยบายกำหนด

6.3 พันธบัตรรัฐบาลไทย

หลักประกันนี้จะคืนให้โดยไม่มีดอกเบี้ยภายใน 15 วัน (สิบห้าวัน) นับถัดจากวันที่คู่สัญญา
พ้นจากข้อผูกพันตามสัญญาแล้ว

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

7. การปฏิบัติตามสัญญา

7.1 ผู้รับจ้างจะต้องดำเนินการส่งแผนการปฏิบัติงานเสนอให้กับคณะกรรมการตรวจรับพัสดุ พิจารณาภายใน 30 วัน เพื่อให้คณะกรรมการตรวจรับพัสดุฯ พิจารณาเห็นชอบแผนการดำเนินงาน ก่อนการปฏิบัติงาน

7.2 ถ้าผู้รับจ้างไม่ลงมือปฏิบัติงานภายในกำหนดเวลา หรือไม่สามารถปฏิบัติงานได้ตามเงื่อนไขที่กำหนดในสัญญา ไม่ว่าทั้งหมดหรือบางส่วน หรือผู้รับจ้างไม่ปฏิบัติตามสัญญา หรือทำผิดสัญญาข้อใดข้อหนึ่ง หรือถูกศาลมีคำสั่งให้พิทักษ์ทรัพย์เด็ดขาด หรือมีคำสั่งให้ล้มละลาย หรือเพิกเฉยไม่ปฏิบัติตามคำสั่งของกระทรวงการต่างประเทศหรือผู้ควบคุมงานซึ่งได้รับมอบอำนาจจากกรมการกงสุล กระทรวงการต่างประเทศ และกรมการกงสุล กระทรวงการต่างประเทศ มีสิทธิที่จะบอกเลิกสัญญา

7.3 การที่กรมการกงสุล กระทรวงการต่างประเทศ ไม่ใช้สิทธิเลิกสัญญาดังกล่าวข้างต้น ไม่เป็นเหตุให้ผู้รับจ้างพ้นจากความรับผิดชอบตามสัญญา

7.4 ในกรณีที่กรมการกงสุล กระทรวงการต่างประเทศ ใช้สิทธิบอกเลิกสัญญา ผู้รับจ้างไม่มีสิทธิเรียกร้องค่าเสียหายและค่าใช้จ่ายใด ๆ จากกรมการกงสุล กระทรวงการต่างประเทศ นอกจากนี้ กรมการกงสุล กระทรวงการต่างประเทศ มีสิทธิดังนี้ด้วย คือ

- (1) รับผิดชอบต่อประกันสัญญา
- (2) เรียกค่าใช้จ่ายที่เพิ่มเติมในการจ้างบุคคลอื่นเข้าดำเนินการและทำงานต่อจนลุล่วง
- (3) เรียกrogateค่าเสียหายอื่นใดอันหากจะพึงมีที่เป็นจำนวนเกินกว่าหลักประกันสัญญา

7.5 กรมการกงสุล กระทรวงการต่างประเทศ อาจเข้าไปดำเนินการและ/หรือว่าจ้างบุคคลอื่นเข้าไปดำเนินการแทน โดยค่าใช้จ่ายทั้งหมดตกเป็นความรับผิดชอบของผู้รับจ้าง และผู้รับจ้างต้องรับผิดชอบค่าใช้จ่ายที่กระทรวงการต่างประเทศต้องจ่ายให้ผู้ควบคุมงาน (เงินเดือน เบี้ยเลี้ยง ค่าที่พัก และค่าล่วงเวลา) หรือค่าจ้างที่ปรึกษาระหว่างที่ผู้รับจ้างปฏิบัติผิดสัญญา

7.6 หากผู้รับจ้างยังไม่สามารถส่งมอบงานตามขอบเขตการส่งมอบงานงวดใด ๆ ให้แล้วเสร็จ ผู้รับจ้างจะต้องชำระค่าปรับให้แก่กรมการกงสุล กระทรวงการต่างประเทศ ตามอัตราที่กำหนดในสัญญาจ้าง นับแต่วันที่ปฏิบัติผิดสัญญาจนถึงวันที่ผู้รับจ้างปฏิบัติถูกต้องสมบูรณ์ตามสัญญา

7.7 หากผู้รับจ้างไม่สามารถดำเนินการส่งมอบงานงวดที่ 1 และงวดที่ 2 ให้แล้วเสร็จภายหลังกำหนดส่งเกินกว่า 30 วัน กรมการกงสุล กระทรวงการต่างประเทศ สามารถบอกเลิกสัญญาจ้างได้

7.8 ในระหว่างที่มีการปรับ หากกรมการกงสุล กระทรวงการต่างประเทศ พิจารณาเห็นว่าผู้รับจ้างไม่อาจแก้ไขหรือปฏิบัติตามสัญญาได้ กรมการกงสุล กระทรวงการต่างประเทศ สามารถใช้สิทธิบอกเลิกสัญญาและใช้สิทธิตามข้อ 7.3 ก็ได้

7.9 กรมการกงสุล กระทรวงการต่างประเทศ สงวนสิทธิในการฟ้องร้องผู้รับจ้างเพิ่มเติมตามฐานความผิดและ/หรือความเสียหายตามจริงได้อีก

8. ระยะเวลาดำเนินโครงการ

ระยะเวลาโครงการ 33 เดือน และระยะเวลาประกันอุปกรณ์ Hardware/Software/license ทั้งหมด

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

9. วงเงินงบประมาณ

จำนวนเงินรวมทั้งสิ้น 150,000,000.00 บาท (หนึ่งร้อยห้าสิบล้านบาทถ้วน) โดยรวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายต่าง ๆ เรียบร้อยแล้ว

10. เงื่อนไขการส่งมอบงานและการจ่ายเงิน

10.1 การส่งมอบงาน

ผู้รับจ้างต้องส่งมอบงานตามเงื่อนไข และขอบเขตงาน ดังนี้

งวดงาน	สิ่งที่ต้องส่งมอบ	อ้างอิง TOR
งวดที่ 1	1.1 ดำเนินการออกแบบ พัฒนา บริหารจัดการ บำรุงรักษา ดูแล ปรับปรุง ปฏิบัติงานที่เกี่ยวข้องกับระบบทั้งหมด ในส่วนที่เกี่ยวกับการออกแบบพัฒนา จัดหาทรัพยากรที่เกี่ยวข้อง ตามขอบเขตของงาน ดังนี้	ข้อ 5
	(1) ส่งมอบแผนการดำเนินงานของโครงการฯ แบบละเอียด	ข้อ 5
	(2) ส่งมอบรายละเอียดการออกแบบระบบ e-Visa ระบบ Mobile Application ระบบคลาวด์ e-Visa ระยะที่ 2 ระบบสารสนเทศทั้งหมดในโครงการ และระบบความมั่นคงและความปลอดภัย	ข้อ 5.3 5.3.5 5.4 และ 5.7
	(3) ส่งมอบแผนการออกแบบ (Drawing) ปรับปรุงศูนย์ปฏิบัติการข้อมูล การตรวจสอบตรา และศูนย์เฝ้าระวังภัยคุกคามทางด้านไซเบอร์และความปลอดภัยของระบบเทคโนโลยีสารสนเทศ (CSOC) พร้อมรายการอุปกรณ์ ภายในศูนย์ปฏิบัติการข้อมูลการตรวจสอบตรา และศูนย์เฝ้าระวังภัยคุกคามทางด้านไซเบอร์และความปลอดภัยของระบบเทคโนโลยีสารสนเทศ (CSOC) กรมการกงสุล	ข้อ 5.5.1 5.5.2 และ 5.7.1.3
	1.2 ส่งมอบรายงานสรุปการดำเนินงานของผู้รับจ้าง ตามขอบเขตของงานที่ส่งมอบในงวดที่ 1	
งวดที่ 2	2.1 ดำเนินการพัฒนา บริหารจัดการ บำรุงรักษา ดูแล ปรับปรุง และ ปฏิบัติงานที่เกี่ยวข้องกับระบบ e-Visa ระบบ Mobile Application และระบบคลาวด์ทั้งหมด ตามขอบเขตของงาน ดังนี้	ข้อ 5
	(1) เปิดใช้งานระบบ e-Visa ระบบ Mobile Application ระบบคลาวด์ e-Visa ระยะที่ 2 ระบบสารสนเทศทั้งหมดในโครงการ และระบบความมั่นคงและความปลอดภัย	ข้อ 5.3 5.3.5 5.4 และ 5.7
	(2) เปิดใช้งานระบบรักษาความปลอดภัยสำหรับเครื่อง Client และระบบการเข้าถึงเครือข่ายแบบ Zero Trust Network Access (ZTNA)	ข้อ 5.8 และ 5.8.1
	(3) เปิดใช้งานระบบ Mail Marketing	ข้อ 5.6
	(4) เชื่อมโยงข้อมูลไปยัง CCDC และหน่วยงานอื่น	ข้อ 5.9
	(5) ส่งมอบงานปรับปรุงศูนย์ปฏิบัติการข้อมูลการตรวจสอบตรา	ข้อ 5.5.1
	(6) ส่งมอบอุปกรณ์ภายในศูนย์ปฏิบัติการข้อมูลการตรวจสอบตรา	ข้อ 5.5.2

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ

	(7) ส่งมอบงานปรับปรุงศูนย์เฝ้าระวังภัยคุกคามทางด้านไซเบอร์และความปลอดภัยของระบบเทคโนโลยีสารสนเทศ (CSOC) กรมการกงสุล พร้อมอุปกรณ์	ข้อ 5.7.1.3
	(8) ส่งมอบลิขสิทธิ์ Software ทั้งหมดในโครงการให้กรมการกงสุล	ข้อ 5.15.5
	(9) ถ่ายโอนข้อมูล (Data Migration) จากระบบ e-Visa ระยะที่ 1มายังระบบ e-Visa ระยะที่ 2	ข้อ 5.15.2.6
	(10) จัดให้มีศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operations Center: CSOC)	ข้อ 5.13.1
	2.2 ส่งมอบ Source Code username และ password ของระบบของระบบ e-Visa ระบบ Mobile Application และระบบสารสนเทศทั้งหมดที่พัฒนาขึ้นในโครงการฯ และโครงสร้างของระบบแอปพลิเคชัน ที่เกี่ยวข้องทั้งหมดในโครงการ	ข้อ 5.2 5.3 5.9 5.10 5.11 และ 5.15
	2.3 จัดการฝึกอบรมผู้ดูแลระบบและเจ้าหน้าที่ของกรมการกงสุล กระทรวงการต่างประเทศหรือบุคคลที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด โดยผู้รับจ้างจัดเตรียมคู่มือการฝึกอบรมในแต่ละหลักสูตรให้ครบถ้วนเพียงพอต่อผู้เข้าฝึกอบรม และผู้รับจ้างเป็นผู้จัดเตรียมสถานที่รับรองการฝึกอบรม ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด ในหัวข้อการฝึกอบรม ดังนี้	ข้อ 5.12
	(1) จัดการฝึกอบรมแก่ผู้ดูแลระบบ จำนวน 2 ครั้ง	ข้อ 5.12
	(2) จัดการฝึกอบรมแก่เจ้าหน้าที่กงสุลในต่างประเทศ แบบออนไลน์ จำนวน 2 ครั้ง	ข้อ 5.12
	(3) จัดการฝึกอบรมแก่เจ้าหน้าที่หน่วยงานภายนอก จำนวน 1 ครั้ง	ข้อ 5.12
	2.4 ส่งมอบสื่อเพื่อการประชาสัมพันธ์ และสื่อที่ใช้ในการอบรม รวมทั้งข้อมูลและการแปลข้อความต่าง ๆ ในโครงการ	ข้อ 5.14
	2.5 ส่งมอบรายงานสรุปการดำเนินงานของผู้รับจ้าง ตามขอบเขตของงานที่ส่งมอบในงวดที่ 2 รวมถึงรายงานระยะเวลาที่ระบบไม่สามารถใช้งานได้	
งวดที่ 3	3.1 บริหารจัดการ บำรุงรักษา ดูแล ปรับปรุง ปฏิบัติงานที่เกี่ยวข้องกับระบบ e-Visa ระบบ Mobile Application และระบบสารสนเทศทั้งหมดตามขอบเขตของงาน ดังนี้	ข้อ 5
	(1) ให้บริการระบบคลาวด์	ข้อ 5.4
	(2) ใช้งานระบบการเข้าถึงเครือข่ายแบบ Zero Trust Network Access (ZTNA)	ข้อ 5.8.1
	(3) ใช้งานระบบ Mail Marketing	ข้อ 5.6
	(4) เชื่อมโยงข้อมูลไปยัง CCDC และหน่วยงานอื่น	ข้อ 5.9
	(5) ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operations Center: CSOC)	ข้อ 5.13.1

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

	3.2 ส่งมอบ Source Code username และ password ของระบบของระบบ e-Visa ระบบ Mobile Application และระบบสารสนเทศทั้งหมดที่พัฒนาขึ้นในโครงการฯ และโครงสร้างของระบบแอปพลิเคชัน ที่เกี่ยวข้องทั้งหมดในโครงการ	ข้อ 5.2 5.3 5.9 5.10 5.11 และ 5.15
	3.3 จัดการฝึกอบรมผู้ดูแลระบบและเจ้าหน้าที่ของกรมการกงสุล กระทรวงการต่างประเทศหรือบุคคลที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด โดยผู้รับจ้างจัดเตรียมคู่มือการฝึกอบรมในแต่ละหลักสูตรให้ครบถ้วนเพียงพอต่อผู้เข้าฝึกอบรม และผู้รับจ้างเป็นผู้จัดเตรียมสถานที่รับรองการฝึกอบรม ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนดในหัวข้อการฝึกอบรม ดังนี้	ข้อ 5.12
	(1) จัดการฝึกอบรมเทคนิคด้านการออกแบบและการบริหารจัดการระบบคลาวด์ จำนวน 1 หลักสูตร	ข้อ 5.12 (4)
	(2) จัดการฝึกอบรมด้านการออกแบบและพัฒนาระบบจำนวน 1 หลักสูตร	ข้อ 5.12 (5)
	3.4 ส่งมอบสื่อเพื่อการประชาสัมพันธ์ และสื่อที่ใช้ในการอบรม รวมทั้งข้อมูลและการแปลข้อความต่าง ๆ ในโครงการ	ข้อ 5.14
	3.5 ส่งมอบรายงานสรุปการดำเนินงานของผู้รับจ้าง ตามขอบเขตของงานที่ส่งมอบในงวดที่ 3 รวมถึงรายงานระยะเวลาที่ระบบไม่สามารถใช้งานได้	
งวดที่ 4	4.1 บริหารจัดการ บำรุงรักษา ดูแล ปรับปรุง ปฏิบัติงานที่เกี่ยวข้องกับระบบ e-Visa ระบบ Mobile Application และระบบสารสนเทศทั้งหมดตามขอบเขตของงาน ดังนี้	ข้อ 5
	(1) ให้บริการระบบคลาวด์	ข้อ 5.4
	(2) ใช้งานระบบการเข้าถึงเครือข่ายแบบ Zero Trust Network Access (ZTNA)	ข้อ 5.8.1
	(3) ใช้งานระบบ Mail Marketing	ข้อ 5.6
	(4) เชื่อมโยงข้อมูลไปยัง CCDC และหน่วยงานอื่น	ข้อ 5.9
	(5) ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operations Center: CSOC)	ข้อ 5.13.1
	4.2 ส่งมอบ Source Code username และ password ของระบบของระบบ e-Visa ระบบ Mobile Application และระบบสารสนเทศทั้งหมดที่พัฒนาขึ้นในโครงการฯ และโครงสร้างของระบบแอปพลิเคชัน ที่เกี่ยวข้องทั้งหมดในโครงการ	ข้อ 5.2 5.3 5.9 5.10 5.11 และ 5.15
	4.3 จัดการฝึกอบรมผู้ดูแลระบบและเจ้าหน้าที่ของกรมการกงสุล กระทรวงการต่างประเทศหรือบุคคลที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด โดยผู้รับจ้างจัดเตรียมคู่มือการฝึกอบรมในแต่ละหลักสูตรให้ครบถ้วนเพียงพอต่อผู้เข้าฝึกอบรม และผู้รับจ้างเป็นผู้จัดเตรียมสถานที่รับรอง	ข้อ 5.12

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

	การฝึกอบรม ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด ในหัวข้อการฝึกอบรม ดังนี้	
	(1) ฝึกอบรมแก่ผู้ดูแลระบบ จำนวน 2 ครั้ง	ข้อ 5.12 (1)
	(2) ฝึกอบรมแก่เจ้าหน้าที่กงสุลในต่างประเทศ แบบออนไลน์ จำนวน 2 ครั้ง	ข้อ 5.12 (2)
	(3) ฝึกอบรมแก่เจ้าหน้าที่หน่วยงานภายนอก จำนวน 1 ครั้ง	ข้อ 5.12 (3)
	(4) ฝึกอบรมเทคนิคด้านการออกแบบและการบริหารจัดการระบบ คลาวด์ จำนวน 1 หลักสูตร	ข้อ 5.12 (4)
	(5) จัดฝึกอบรมด้านการออกแบบและพัฒนาระบบ จำนวน 1 หลักสูตร	ข้อ 5.12 (5)
	4.4 ส่งมอบสื่อเพื่อการประชาสัมพันธ์ และสื่อที่ใช้ในการอบรม รวมทั้งข้อมูล และการแปลข้อความต่าง ๆ ในโครงการ	ข้อ 5.14
	4.5 ส่งมอบรายงานสรุปการดำเนินงานของผู้รับจ้าง ตามขอบเขตของงานที่ ส่งมอบในงวดที่ 4 รวมถึงรายงานระยะเวลาที่ระบบไม่สามารถใช้งานได้	
งวดที่ 5	5.1 บริหารจัดการ บำรุงรักษา ดูแล ปรับปรุง ปฏิบัติงานที่เกี่ยวข้องกับระบบ e-Visa ระบบ Mobile Application และระบบสารสนเทศทั้งหมดตาม ขอบเขตของงาน ดังนี้	ข้อ 5
	(1) ให้บริการระบบคลาวด์	ข้อ 5.4
	(2) ใช้งานระบบการเข้าถึงเครือข่ายแบบ Zero Trust Network Access (ZTNA)	ข้อ 5.8.1
	(3) ใช้งานระบบ Mail Marketing	ข้อ 5.6
	(4) เชื่อมโยงข้อมูลไปยัง CCDC และหน่วยงานอื่น	ข้อ 5.9
	(5) ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operations Center: CSOC)	ข้อ 5.13.1
	5.2 ส่งมอบพร้อมนำเสนอ Source Code username และ password ของ ระบบ e-Visa และระบบ Mobile Application ที่เกี่ยวข้องทั้งหมดใน โครงการ	ข้อ 5.15.2.7
	5.3 จัดการฝึกอบรมผู้ดูแลระบบและเจ้าหน้าที่ของกรมการกงสุล กระทรวง การต่างประเทศหรือบุคคลที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด โดยผู้รับจ้างจัดเตรียมคู่มือการฝึกอบรมในแต่ละหลักสูตรให้ครบถ้วน เพียงพอต่อผู้เข้าฝึกอบรม และผู้รับจ้างเป็นผู้จัดเตรียมสถานที่รับรองการ ฝึกอบรม ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนด ในหัวข้อการฝึกอบรม ดังนี้	ข้อ 5.12
	(1) ฝึกอบรมเทคนิคด้านการออกแบบและการบริหารจัดการระบบ คลาวด์ จำนวน 1 หลักสูตร	ข้อ 5.12 (4)
	(2) จัดฝึกอบรมด้านการออกแบบและพัฒนาระบบ จำนวน 1 หลักสูตร	ข้อ 5.12 (5)
	(3) ฝึกอบรมแก่เจ้าหน้าที่กงสุลในต่างประเทศ แบบออนไลน์ จำนวน 2 ครั้ง	ข้อ 5.12 (2)

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

	(4) ฝึกอบรมแก่เจ้าหน้าที่หน่วยงานภายนอก จำนวน 1 ครั้ง	ข้อ 5.12 (3)
	5.5 ส่งมอบสื่อเพื่อการประชาสัมพันธ์ และสื่อที่ใช้ในการอบรม รวมทั้งข้อมูลและการแปลข้อความต่าง ๆ ในโครงการ	ข้อ 5.14
	5.6 ส่งมอบรายงานสรุปการดำเนินงานของผู้รับจ้าง ตามขอบเขตของงานที่ส่งมอบในงวดที่ 5 รวมถึงรายงานระยะเวลาที่ระบบไม่สามารถใช้งานได้	
งวดที่ 6	6.1 บริหารจัดการ บำรุงรักษา ดูแล ปรับปรุง ปฏิบัติงานที่เกี่ยวข้องกับระบบ e-Visa ระบบ Mobile Application และระบบสารสนเทศทั้งหมดตามขอบเขตของงาน ดังนี้	ข้อ 5
	(1) ให้บริการระบบคลาวด์	ข้อ 5.4
	(2) ใช้งานระบบการเข้าถึงเครือข่ายแบบ Zero Trust Network Access (ZTNA)	ข้อ 5.8.1
	(3) ใช้งานระบบ Mail Marketing	ข้อ 5.6
	(4) เชื่อมโยงข้อมูลไปยัง CCDC และหน่วยงานอื่น	ข้อ 5.9
	(5) ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operations Center: CSOC)	ข้อ 5.13.1
	6.2 ส่งมอบพร้อมนำเสนอ Source Code username และ password ของระบบ e-Visa และระบบ Mobile Application ที่เกี่ยวข้องทั้งหมดในโครงการ	ข้อ 5.15.2.7
	6.3 จัดการฝึกอบรมผู้ดูแลระบบและเจ้าหน้าที่ของกรมการกงสุล กระทรวงการต่างประเทศหรือบุคคลที่กรมการกงสุล กระทรวงการต่างประเทศกำหนด โดยผู้รับจ้างจัดเตรียมคู่มือการฝึกอบรมในแต่ละหลักสูตรให้ครบถ้วนเพียงพอต่อผู้เข้าฝึกอบรม และผู้รับจ้างเป็นผู้จัดเตรียมสถานที่รับรองการฝึกอบรม ตามที่กรมการกงสุล กระทรวงการต่างประเทศ กำหนดในหัวข้อการฝึกอบรม ดังนี้	ข้อ 5.12
	(1) ฝึกอบรมแก่ผู้ดูแลระบบ จำนวน 2 ครั้ง	ข้อ 5.12 (1)
	(2) ฝึกอบรมแก่เจ้าหน้าที่กงสุลในต่างประเทศ แบบออนไลน์ จำนวน 2 ครั้ง	ข้อ 5.12 (2)
	(3) ฝึกอบรมแก่เจ้าหน้าที่หน่วยงานภายนอก จำนวน 1 ครั้ง	ข้อ 5.12 (3)
	(4) จัดการฝึกอบรมด้านการออกแบบและพัฒนาระบบ จำนวน 1 หลักสูตร	ข้อ 5.12 (5)
	6.4 ส่งมอบสื่อเพื่อการประชาสัมพันธ์ และสื่อที่ใช้ในการอบรม รวมทั้งข้อมูลและการแปลข้อความต่าง ๆ ในโครงการ	ข้อ 5.14
	6.5 ส่งมอบรายงานสรุปการดำเนินงานของผู้รับจ้าง ตามขอบเขตของงานที่ส่งมอบในงวดที่ 6 รวมถึงรายงานระยะเวลาที่ระบบไม่สามารถใช้งานได้	

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

10.2 การจ่ายเงิน

10.2.1 การจ่ายเงินงวดที่ 1

จ่ายให้ร้อยละ 10 ของวงเงินตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามข้อ 10.1 ภายในระยะเวลา 5 เดือน นับถัดจากวันลงนามในสัญญา พร้อมทั้งคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว ทั้งนี้ ความเห็นชอบของคณะกรรมการตรวจรับพัสดุ ที่แต่งตั้งโดยกระทรวงการต่างประเทศถือเป็นที่สุด

10.2.2 การจ่ายเงินงวดที่ 2

จ่ายให้ร้อยละ 26 ของวงเงินตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามข้อ 10.1 ภายในระยะเวลา 9 เดือน นับถัดจากวันลงนามในสัญญา พร้อมทั้งคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว ทั้งนี้ ความเห็นชอบของคณะกรรมการตรวจรับพัสดุ ที่แต่งตั้งโดยกระทรวงการต่างประเทศถือเป็นที่สุด

10.2.3 การจ่ายเงินงวดที่ 3

จ่ายให้ร้อยละ 16 ของวงเงินตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามข้อ 10.1 ภายในระยะเวลา 15 เดือน นับถัดจากวันลงนามในสัญญา พร้อมทั้งคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว ทั้งนี้ ความเห็นชอบของคณะกรรมการตรวจรับพัสดุ ที่แต่งตั้งโดยกระทรวงการต่างประเทศถือเป็นที่สุด

10.2.4 การจ่ายเงินงวดที่ 4

จ่ายให้ร้อยละ 16 ของวงเงินตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามข้อ 10.1 ภายในระยะเวลา 21 เดือน นับถัดจากวันลงนามในสัญญา พร้อมทั้งคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว ทั้งนี้ ความเห็นชอบของคณะกรรมการตรวจรับพัสดุ ที่แต่งตั้งโดยกระทรวงการต่างประเทศถือเป็นที่สุด

10.2.5 การจ่ายเงินงวดที่ 5

จ่ายให้ร้อยละ 16 ของวงเงินตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามข้อ 10.1 ภายในระยะเวลา 27 เดือน นับถัดจากวันลงนามในสัญญา พร้อมทั้งคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว ทั้งนี้ ความเห็นชอบของคณะกรรมการตรวจรับพัสดุ ที่แต่งตั้งโดยกระทรวงการต่างประเทศถือเป็นที่สุด

10.2.6 การจ่ายเงินงวดที่ 6

จ่ายให้ร้อยละ 16 ของวงเงินตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามข้อ 10.1 ภายในระยะเวลา 33 เดือน นับถัดจากวันลงนามในสัญญา พร้อมทั้งคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว ทั้งนี้ ความเห็นชอบของคณะกรรมการตรวจรับพัสดุ ที่แต่งตั้งโดยกระทรวงการต่างประเทศถือเป็นที่สุด

11. การรับประกัน

11.1 ผู้รับจ้างจะต้องรักษาซ่อมแซมและแก้ไขข้อขัดข้องที่เกิดขึ้นทั้งหมด อันเนื่องมาจากการบกพร่องชำรุด และเสื่อมสภาพของอุปกรณ์ ระบบเครือข่าย และระบบสารสนเทศ รวมถึงซอฟต์แวร์ต่าง ๆ ที่มีในโครงการฯ ทั้งหมดขณะที่ยังอยู่ในช่วงระยะเวลาการใช้บริการและระยะเวลารับประกัน ซึ่งรวมถึงกรณีการชำรุดจากการใช้งานอุปกรณ์หรือระบบข้างต้นด้วย

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

11.2 ในกรณีที่ผู้รับจ้างไม่สามารถปฏิบัติตามสัญญาทั้งหมดหรือบางส่วนได้ตามข้อกำหนดในข้อที่ 5 จะต้องชำระค่าปรับเป็นรายชั่วโมง ตามเกณฑ์การคำนวณดังนี้

เกณฑ์การคำนวณค่าปรับ

ค่าปรับรายชั่วโมง = (จำนวนชั่วโมงที่เกินเวลาที่กำหนด โดยเศษของชั่วโมงให้คิดเป็น 1 ชั่วโมง) × (ร้อยละ 0.25 × วงเงินในสัญญารายงวด) × ค่าตัวถ่วง (ตามตารางกำหนดตัวถ่วงด้านล่าง)

11.3 กรมการกงสุล กระทรวงการต่างประเทศ ยอมให้อุปกรณ์ ระบบเครือข่าย ระบบสารสนเทศ รวมถึงซอฟต์แวร์ต่าง ๆ ที่มี การใช้งานในโครงการฯ ทั้งหมดขัดข้องภายหลังที่คำนวณด้วยค่าตัวถ่วงแล้ว ได้ไม่เกินเดือนละ 2 ชั่วโมง (ตามเดือนปฏิทิน) หากขัดข้องเกินระยะเวลาดังกล่าว ผู้รับจ้างยินยอม ให้คิดค่าปรับเพิ่มในส่วนที่เกินในอัตราร้อยละ 0.25 ของจำนวนเงินตามสัญญาในงวดงานนั้น ๆ

ตารางกำหนดตัวถ่วงและกรอบระยะเวลาในการแก้ไขของโครงการศูนย์ข้อมูลการตรวจลงตราของไทย (Visa Data Center - VDC) เพื่อจัดทำและดูแลระบบตรวจลงตราอิเล็กทรอนิกส์ (e-Visa) ระยะที่ 2

ลำดับ	รายการ	ค่าตัวถ่วง	ระยะเวลาในการแก้ไข	ขอบเขตงานอ้างอิงจาก TOR
1	ระบบคลาวด์ e-Visa ระยะที่ 2 (e-Visa Cloud System Phase 2)	1.0	10 นาที	ข้อ 5.4 และข้อ 5.19.2
ระบบสารสนเทศและระบบฐานข้อมูล				
2	ระบบ e-Visa	1.0	10 นาที	ข้อ 5.3 และข้อ 5.19.2
3	ระบบ APEC Business Travel Card (ABTC)	1.0	10 นาที	ข้อ 5.3 และข้อ 5.19.2
4	ระบบ Mail Marketing	1.0	10 นาที	ข้อ 5.6 และข้อ 5.19.2
5	ระบบความมั่นคงและความปลอดภัย	1.0	1 ชม.	ข้อ 5.7 และข้อ 5.19.2
6	ระบบการเข้าถึงเครือข่ายแบบ Zero Trust Network Access (ZTNA)	1.0	10 นาที	ข้อ 5.8 และข้อ 5.19.2
7	ระบบสื่อสารเชื่อมโยงข้อมูลกับหน่วยงานอื่น	1.0	10 นาที	ข้อ 5.9 และข้อ 5.19.2
8	ระบบ Web Enquiry	1.0	10 นาที	ข้อ 5.3.3.10 5.10 และข้อ 5.19.2
9	ระบบ Payment	1.0	10 นาที	ข้อ 5.11 และข้อ 5.19.2
10	ระบบสารสนเทศและ Software	1.0	10 นาที	ข้อ 5.13 และข้อ 5.19.2

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

11	ระบบ Mobile Application	1.0	10 นาที	ข้อ 5.3.5.3
ศูนย์ปฏิบัติการข้อมูลการตรวจลงตรา กรมการกงสุล				
12	อุปกรณ์ภายในศูนย์ปฏิบัติการข้อมูลการตรวจลงตรา กรมการกงสุล	1.0	24 ชม.	ข้อ 5.5.2 และข้อ 5.19.2
ระบบสื่อสารเชื่อมโยงข้อมูล				
13	ระบบเชื่อมโยงข้อมูลระหว่างระบบคลาวด์ e-Visa กับศูนย์บริหารข้อมูลกลางกรมการกงสุล (CCDC)	1.0	10 นาที	ข้อ 5.9.2 และข้อ 5.19.2
14	หน่วยงานภายนอก	1.0	10 นาที	ข้อ 5.9.3 และข้อ 5.19.2
ระบบความมั่นคงและความปลอดภัย				
15	เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์มีความรุนแรงระดับ Critical			
	หากผู้รับแจ้งทราบข้อมูลจากระบบหรือช่องทางอื่น ผู้รับแจ้งจะต้องแจ้งให้กรมการกงสุล กระทรวงการต่างประเทศทราบ ภายใน 15 นาที	1.0	15 นาที	
	ตอบสนอง และยับยั้งภัยคุกคาม (Response และ Contain) และจัดทำรายงานผลการตรวจสอบเบื้องต้น	1.0	4 ชม.	
	เก็บหลักฐานและวิเคราะห์เพื่อกำจัดต้นตอของภัยคุกคามให้ออกจากระบบทั้งหมด (Eradication) พร้อมกู้คืนระบบให้กลับมาทำงานปกติ (Recovery) พร้อมจัดทำรายงานเชิงลึก	1.0	24 ชม.	
16	เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์มีความรุนแรงระดับ High			
	หากผู้รับแจ้งทราบข้อมูลจากระบบหรือช่องทางอื่น ผู้รับแจ้งจะต้องแจ้งให้กรมการกงสุล กระทรวงการต่างประเทศทราบ ภายใน 15 นาที	1.0	1 ชม.	
	ตอบสนอง และยับยั้งภัยคุกคาม (Response และ Contain) และจัดทำรายงานผลการตรวจสอบเบื้องต้น	1.0	6 ชม.	
	เก็บหลักฐานและวิเคราะห์เพื่อกำจัดต้นตอของภัยคุกคามให้ออกจากระบบทั้งหมด (Eradication) พร้อมกู้คืนระบบให้กลับมาทำงานปกติ (Recovery) พร้อมจัดทำรายงานเชิงลึก	1.0	48 ชม.	
17	เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์มีความรุนแรงระดับ Medium			

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

	หากผู้รับแจ้งทราบข้อมูลจากระบบหรือช่องทางอื่น ผู้รับแจ้งจะต้องแจ้งให้กรมการกงสุลกระทรวงการต่างประเทศทราบ ภายใน 15 นาที	1.0	2 ชม.	
	ตอบสนอง และยับยั้งภัยคุกคาม (Response และ Contain) และจัดทำรายงานผลการตรวจสอบเบื้องต้น	1.0	12 ชม.	
	เก็บหลักฐานและวิเคราะห์เพื่อกำจัดต้นตอของภัยคุกคามให้ออกจากระบบทั้งหมด (Eradication) พร้อมกู้คืนระบบให้กลับมาทำงานปกติ (Recovery) พร้อมจัดทำรายงานเชิงลึก	1.0	72 ชม.	
18	เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์มีความรุนแรงระดับ Low			
	หากผู้รับแจ้งทราบข้อมูลจากระบบหรือช่องทางอื่น ผู้รับแจ้งจะต้องแจ้งให้กรมการกงสุลกระทรวงการต่างประเทศทราบ ภายใน 15 นาที	1.0	4 ชม.	
	ตอบสนอง และยับยั้งภัยคุกคาม (Response และ Contain) และจัดทำรายงานผลการตรวจสอบเบื้องต้น	1.0	40 ชม.	
	เก็บหลักฐานและวิเคราะห์เพื่อกำจัดต้นตอของภัยคุกคามให้ออกจากระบบทั้งหมด (Eradication) พร้อมกู้คืนระบบให้กลับมาทำงานปกติ (Recovery) พร้อมจัดทำรายงานเชิงลึก	1.0	96 ชม.	
19	ตรวจสอบและจัดทำรายงานในกรณีที่ระบบถูกเจาะหรือข้อมูลรั่วไหล	1.0	15 นาที	หากผู้รับแจ้งทราบข้อมูลจากระบบหรือช่องทางอื่น ผู้รับแจ้งจะต้องแจ้งให้กรมการกงสุลกระทรวงการต่างประเทศทราบ ภายใน 15 นาที
	(1) จัดทำรายงานผลการตรวจสอบเบื้องต้นในกรณีที่ระบบถูกเจาะหรือข้อมูลรั่วไหล	1.0	8 ชม.	
	(2) จัดทำรายงานเชิงลึกจากผลการตรวจสอบหาสาเหตุในกรณีที่ระบบถูกเจาะหรือข้อมูลรั่วไหล	1.0	48 ชม.	
20	การรับมือกับภัยคุกคามทางไซเบอร์กรณีที่ผู้รับแจ้งตรวจพบ หรือ ได้รับรายงานจาก CSOC หรือหน่วยงานภายนอก	1.0	30 นาที	การควบคุมความเสียหายด้วยวิธีการที่เหมาะสมเพื่อป้องกันไม่ให้ความ

ประธานกรรมการ กรรมการ กรรมการ กรรมการ

กรรมการ 3.9 07/5 กรรมการ กรรมการ กรรมการ กรรมการ

				เสียหายกระจาย ออกไปในวงกว้าง (Containment)
	(1) เก็บหลักฐาน วิเคราะห์ และกำจัดต้นตอของ ภัยคุกคามให้ออกจากระบบทั้งหมด (Eradication)	1.0	4 ชม.	
	(2) คืนสภาพระบบให้กลับมาทำงานปกติ (Full Incident Response)	1.0	8 ชม.	
อื่น ๆ				
21	การให้ข้อมูลเพื่อสนับสนุนการใช้งานให้กับ เจ้าหน้าที่ผ่านช่องทาง Voice และ Non-voice (Service Support)	1.0	5 นาที	ต้อง response ภายใน 5 นาที ตลอด 24 ชั่วโมง 7 วัน
22	การแก้ไขปัญหาเชิงเทคนิค การตรวจสอบข้อมูล ระบบให้กับเจ้าหน้าที่ และประสานงานในเชิง เทคนิคกับหน่วยงานต่าง ๆ ที่เกี่ยวข้อง	1.0	4 ชม.	- แก้ไขปัญหา ทางเทคนิค โดยเจ้าหน้าที่ ปฏิบัติการศูนย์ ข้อมูลการตรวจ ลงตรา ตลอด 24 ชั่วโมง 7 วัน - ผู้รับแจ้งสามารถ ขอขยายระยะเวลา เพิ่มได้ เมื่อมีเหตุ สุดวิสัยและต้อง ได้รับความ เห็นชอบจาก กรรมการกงสุล กระทรวงการ ต่างประเทศ

11.4 กรณีระบบไม่สามารถให้บริการได้เกิน 8 ชั่วโมง 36 นาที ต่อปี (โดยผู้รับแจ้งไม่ได้รับความ
ยินยอมจากกรรมการกงสุล กระทรวงการต่างประเทศ) ผู้รับแจ้งยินยอมให้คำนวณค่าปรับและคิดค่าปรับ
เป็นรายชั่วโมง นับจากเวลาที่ระบบไม่สามารถให้บริการได้ ตามเกณฑ์การคำนวณดังนี้

เกณฑ์การคำนวณค่าปรับ

ค่าปรับรายชั่วโมง = ร้อยละ 0.1 ของมูลค่าตามสัญญาจ้าง × จำนวนชั่วโมงที่เกินเวลาที่กำหนด
(8 ชั่วโมง 36 นาที) โดยเศษของชั่วโมงให้คิดเป็น 1 ชั่วโมง

11.5 การรับประกันหลังจากสิ้นสุดสัญญา

ประธานกรรมการ กรรมการ กรรมการ
กรรมการ กรรมการ กรรมการ กรรมการ

ผู้รับจ้างต้องรับประกันว่า software ที่ถูกพัฒนาขึ้นมาทั้งหมดในโครงการตามข้อ 5.3 สามารถทำงานได้เป็นปกติ หลังจากสิ้นสุดสัญญาต่อไปอีก 1 ปี ทั้งนี้ ในกรณีที่ระบบขัดข้องจาก software ที่ถูกพัฒนาขึ้น ผู้รับจ้างต้องดำเนินการแก้ไขทันทีโดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น

12. อัตราค่าปรับ

อัตราค่าปรับหากผู้รับจ้างไม่สามารถทำงานให้แล้วเสร็จตามขอบเขตของงานในเวลาที่กำหนดไว้ในสัญญาในแต่ละงวดงานตามที่กำหนด ผู้รับจ้างจะต้องชำระค่าปรับให้แก่กระทรวงการต่างประเทศเป็นรายวัน อัตราร้อยละ 0.15 (ศูนย์จุดหนึ่งห้า) ของจำนวนเงินราคาค่าจ้างในงวดงานนั้น ๆ

13. อัตราค่าเสียหาย

กรณีข้อมูลสูญหายและไม่สามารถกู้คืนได้ภายใน 12 ชั่วโมงนับจากเวลาที่พิสูจน์ทราบได้ว่าข้อมูลหาย

13.1 ข้อมูลสำรอง ผู้รับจ้างต้องชำระค่าเสียหายโดยคำนวณจากจำนวนสำรองสำรองละ 50,000 บาท โดยข้อมูลทั้งหมดหรือบางส่วนของแต่ละสำรองคิดเป็น 1 สำรอง (1 สำรอง หมายถึง การขอรับการตรวจลงตราของบุคคล 1 คน ใน 1 รายการ) ตามเกณฑ์การคำนวณดังนี้

เกณฑ์การคำนวณค่าเสียหาย

ค่าปรับ = (จำนวนชั่วโมงที่เกินเวลา 12 ชั่วโมง โดยเศษของชั่วโมงให้คิดเป็น 1 ชั่วโมง) × จำนวนสำรอง × 50,000 × ค่าตัวถ่วง (ตามตารางกำหนดค่าตัวถ่วงด้านล่าง)

ตารางกำหนดตัวถ่วงและระยะเวลาในการกู้คืนข้อมูล

ลำดับ	ช่วงระยะเวลาในการกู้คืนข้อมูล	ค่าตัวถ่วง
1	ชั่วโมงที่ 1 - 12	0.01
2	ชั่วโมงที่ 13 - 24	0.03
3	ชั่วโมงที่ 25 - 36	0.10

หมายเหตุ การคำนวณค่าปรับจะคำนวณตามอัตราก้าวหน้า โดยคิดค่าปรับสูงสุด 36 ชั่วโมง หรือ 84,000 บาท ต่อ 1 สำรอง

13.2 ข้อมูลอื่น ๆ ผู้รับจ้างต้องชำระค่าเสียหายโดยคำนวณและคิดค่าปรับเป็นรายชั่วโมงตามเกณฑ์การคำนวณดังนี้

เกณฑ์การคำนวณค่าเสียหาย

ค่าปรับ = (จำนวนชั่วโมงที่เกินเวลา 12 ชั่วโมง โดยเศษของชั่วโมงให้คิดเป็น 1 ชั่วโมง) × 0.01 × วงเงินในสัญญารายงวด × ค่าตัวถ่วง (ตามตารางกำหนดค่าตัวถ่วงด้านล่าง)

ตารางกำหนดตัวถ่วงและระยะเวลาในการกู้คืนข้อมูล

ลำดับ	ช่วงระยะเวลาในการกู้คืนข้อมูล	ค่าตัวถ่วง
1	ชั่วโมงที่ 1 - 12	0.01
2	ชั่วโมงที่ 13 - 24	0.03
3	ชั่วโมงที่ 25 - 36	0.10

หมายเหตุ การคำนวณค่าปรับจะคำนวณตามอัตราก้าวหน้า โดยคิดค่าปรับสูงสุด 36 ชั่วโมง

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

14. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

14.1 ในการพิจารณาผลการยื่นข้อเสนอราคาครั้งนี้ จะพิจารณาโดยใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่นในการพิจารณา (Price Performance)

14.2 การพิจารณาผู้ชนะการยื่นข้อเสนอ จะใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่น โดยพิจารณาให้คะแนนตามปัจจัย และน้ำหนักตามที่กำหนด ดังนี้

14.2.1 ราคาที่เสนอ กำหนดน้ำหนักเท่ากับ ร้อยละ 40

14.2.2 ข้อเสนอด้านเทคนิคหรือข้อเสนออื่น ๆ กำหนดน้ำหนักเท่ากับร้อยละ 60

ได้แก่ ข้อเสนอด้านเทคนิค ร้อยละ 20 และ POC ร้อยละ 40 โดยคุณภาพของข้อเสนอจะต้องสอดคล้องกับการดำเนินโครงการอย่างมีประสิทธิภาพ ละเอียดรอบคอบ มีคุณภาพเป็นประโยชน์สูงสุดแก่ทางราชการ โดยขอสงวนสิทธิ์ในการดัดให้คะแนนรายที่ยื่นข้อเสนอที่ไม่มีความเหมาะสมหรือไม่อยู่ในเกณฑ์คุณภาพที่ไม่ได้มาตรฐาน

ตารางเกณฑ์การให้คะแนนข้อเสนอด้านเทคนิค

คะแนนเต็ม 100 คะแนน คิดเป็นร้อยละ 20 ตามที่ระบุในข้อ 14.2.2

ลำดับ	ข้อพิจารณา	คะแนน
1	ความน่าเชื่อถือ ผลงาน ประสบการณ์ และความมั่นคงของผู้รับจ้าง	40 คะแนน
	1.1 ทุนจดทะเบียนของผู้รับจ้าง - ทุนจดทะเบียน 20 ล้านบาทขึ้นไปแต่ไม่ถึง 40 ล้านบาท ได้ 12 คะแนน - ทุนจดทะเบียน 40 ล้านบาทขึ้นไปแต่ไม่ถึง 60 ล้านบาท ได้ 14 คะแนน - ทุนจดทะเบียน 60 ล้านบาทขึ้นไปแต่ไม่ถึง 80 ล้านบาท ได้ 16 คะแนน - ทุนจดทะเบียน 80 ล้านบาทขึ้นไปแต่ไม่ถึง 100 ล้านบาท ได้ 18 คะแนน - ทุนจดทะเบียนตั้งแต่ 100 ล้านบาทขึ้นไป ได้ 20 คะแนน 1.2 ผลงานของผู้รับจ้าง ผู้รับจ้างต้องเคยมีผลงานประเภทเดียวกัน (งานพัฒนาระบบสารสนเทศ) กับงานที่จ้างในวงเงินไม่น้อยกว่า 20,000,000 บาท ในสัญญาเดียวและเป็นผลงานที่เสร็จสิ้นแล้วไม่เกิน 5 ปี นับถึงวันยื่นเอกสารเสนอราคาพร้อมรับรองสำเนาถูกต้อง โดยผลงานดังกล่าวจะต้องเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับส่วนราชการ หน่วยงานตามกฎหมายว่าด้วยระเบียบบริหารราชการส่วนท้องถิ่น หน่วยงานอื่นซึ่งมีกฎหมายบัญญัติให้ฐานะเป็นราชการบริหารส่วนท้องถิ่น รัฐวิสาหกิจ หรือหน่วยงานเอกชนที่เชื่อถือได้ - วงเงิน 20 ล้านบาทขึ้นไป แต่ไม่ถึง 50 ล้านบาท ได้ 12 คะแนน - วงเงิน 50 ล้านบาทขึ้นไป แต่ไม่ถึง 80 ล้านบาท ได้ 14 คะแนน - วงเงิน 80 ล้านบาทขึ้นไป แต่ไม่ถึง 110 ล้านบาท ได้ 16 คะแนน - วงเงิน 110 ล้านบาทขึ้นไป แต่ไม่ถึง 140 ล้านบาท ได้ 18 คะแนน - วงเงินตั้งแต่ 140 ล้านบาท ขึ้นไป ได้ 20 คะแนน	20 คะแนน 20 คะแนน

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

2	ระบบคลาวด์ e-Visa (กรณีมีการใช้งาน Multi-cloud จะนับคะแนนผู้ให้บริการ Cloud เพียงรายเดียวที่ดีที่สุด)	40 คะแนน
	ผู้ให้บริการ Cloud ที่ผู้ยื่นข้อเสนอเลือกใช้ มีจำนวนภูมิภาค (Region) ที่เปิดให้บริการ - มีจำนวนภูมิภาค (Region) 4 - 10 ได้ 24 คะแนน - มีจำนวนภูมิภาค (Region) 11 - 17 ได้ 28 คะแนน - มีจำนวนภูมิภาค (Region) 18 - 24 ได้ 32 คะแนน - มีจำนวนภูมิภาค (Region) 25 - 31 ได้ 36 คะแนน - มีจำนวนภูมิภาค (Region) 32 ขึ้นไป ได้ 40 คะแนน	
3	การรับประกัน	20 คะแนน
	3.1 การรับประกัน software ระบบที่พัฒนา - เสนอตามที่กำหนดในข้อ 11.5 ได้ 6 คะแนน - เสนอเพิ่มจากที่กำหนดในข้อ 11.5 อีก 1 ปี (รวมเป็น 2 ปี) ได้ 8 คะแนน - เสนอเพิ่มจากที่กำหนดในข้อ 11.5 อีก 2 ปี (รวมเป็น 3 ปี) ได้ 10 คะแนน 3.2 การรับประกัน software hardware และอุปกรณ์ทั้งหมดในโครงการ ตามข้อกำหนดจากเจ้าของผลิตภัณฑ์ - เสนอตามที่กำหนด ได้ 6 คะแนน - เสนอเพิ่มจากที่กำหนด อีก 1 ปี ได้ 8 คะแนน - เสนอเพิ่มจากที่กำหนด อีก 2 ปี ได้ 10 คะแนน	10 คะแนน 10 คะแนน
	คะแนนเต็มรวม	100 คะแนน

14.2.3 ผู้ยื่นข้อเสนอต้องจัดทำตัวอย่างชิ้นงาน (Proof of Concept) แผนการออกแบบสถาปัตยกรรมของระบบ e-Visa และระบบ Mobile Application พร้อมจัดทำระบบต้นแบบ และนำเสนอตัวอย่างชิ้นงานดังกล่าวต่อคณะกรรมการฯ ในวันที่กรรมการกงสุล กระทรวงการต่างประเทศกำหนด โดยโจทย์การทำ PoC จะแจ้งให้ผู้ยื่นข้อเสนอทราบหลังจากผู้ยื่นข้อเสนอยื่นข้อเสนอและได้รับการตรวจสอบคุณสมบัติแล้ว

ตารางเกณฑ์การให้คะแนนตัวอย่างชิ้นงาน (Proof of Concept)
คะแนนเต็ม 100 คะแนน คิดเป็นร้อยละ 40 ตามที่ระบุในข้อ 14.2.2

ลำดับ	รายละเอียด	คะแนน
1	การออกแบบระบบคลาวด์	17 คะแนน
	(1) ออกแบบระบบคลาวด์ตามโจทย์ที่กำหนด	1 คะแนน
	(2) ทดสอบการทำงานของระบบฯ Scenario 1	1 คะแนน

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

ลำดับ	รายละเอียด	คะแนน
	(3) ทดสอบการทำงานของระบบฯ Scenario 2	3 คะแนน
	(4) ทดสอบการทำงานของระบบฯ Scenario 3	7 คะแนน
	(5) ตรวจสอบข้อมูลครบถ้วน สมบูรณ์	5 คะแนน
2	การออกแบบระบบสารสนเทศ	18 คะแนน
	(1) ทดสอบฟังก์ชันการทำงาน Scenario 1	2 คะแนน
	(2) ทดสอบฟังก์ชันการทำงาน Scenario 2	2 คะแนน
	(3) ทดสอบฟังก์ชันการทำงาน Scenario 3	2 คะแนน
	(4) ทดสอบฟังก์ชันการทำงาน Scenario 4	2 คะแนน
	(5) ทดสอบฟังก์ชันการทำงาน Scenario 5	2 คะแนน
	(6) ทดสอบฟังก์ชันการทำงาน Scenario 6	2 คะแนน
	(7) ทดสอบฟังก์ชันการทำงาน Scenario 7	2 คะแนน
	(8) UX/UI ของระบบรับคำร้อง	2 คะแนน
	(9) UX/UI ของระบบพิจารณาผล	2 คะแนน
3	ทดสอบการทำงานของระบบรับคำร้อง	20 คะแนน
	(1) ทดสอบการทำงานของระบบ ได้ถูกต้อง 10 รายการ	20 คะแนน
	(2) ทดสอบการทำงานของระบบ ได้ถูกต้อง 9 รายการ	16 คะแนน
	(3) ทดสอบการทำงานของระบบ ได้ถูกต้อง 8 รายการ	12 คะแนน
	(4) ทดสอบการทำงานของระบบ ได้ถูกต้อง 7 รายการ	8 คะแนน
	(5) ทดสอบการทำงานของระบบ ได้ถูกต้อง 6 รายการ	4 คะแนน
	(6) ทดสอบการทำงานของระบบ ได้ถูกต้องน้อยกว่า 6 รายการ	0 คะแนน
4	ทดสอบการทำงานของระบบพิจารณาผล	40 คะแนน
	(1) ทดสอบการทำงานของระบบ ได้ถูกต้อง 10 รายการ	40 คะแนน
	(2) ทดสอบการทำงานของระบบ ได้ถูกต้อง 9 รายการ	32 คะแนน

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

ลำดับ	รายละเอียด	คะแนน
	(3) ทดสอบการทำงานระบบ ได้ถูกต้อง 8 รายการ	24 คะแนน
	(4) ทดสอบการทำงานระบบ ได้ถูกต้อง 7 รายการ	16 คะแนน
	(5) ทดสอบการทำงานระบบ ได้ถูกต้อง 6 รายการ	8 คะแนน
	(6) ทดสอบการทำงานระบบ ได้ถูกต้องน้อยกว่า 6 รายการ	0 คะแนน
5	การส่งข้อมูลไปยังหน่วยงานภายนอก (จำนวน 10 รายการ)	5 คะแนน
	(1) สามารถส่งข้อมูลได้ถูกต้อง ครบถ้วน สมบูรณ์ 10 รายการ	5 คะแนน
	(2) สามารถส่งข้อมูลได้ถูกต้อง ครบถ้วน สมบูรณ์ 9 รายการ	4 คะแนน
	(3) สามารถส่งข้อมูลได้ถูกต้อง ครบถ้วน สมบูรณ์ 8 รายการ	3 คะแนน
	(4) สามารถส่งข้อมูลได้ถูกต้อง ครบถ้วน สมบูรณ์ 7 รายการ	2 คะแนน
	(5) สามารถส่งข้อมูลได้ถูกต้อง ครบถ้วน สมบูรณ์ 6 รายการ	1 คะแนน
	(6) สามารถส่งข้อมูลได้ถูกต้อง ครบถ้วน สมบูรณ์ ได้ถูกต้องน้อยกว่า 6 รายการ	0 คะแนน
รวมคะแนน		100 คะแนน

14.3 การตัดสินผู้ชนะ จะคำนวณคะแนนจากข้อกำหนดตามข้อ 14.2

14.4 กรรมการจะตัดสินผู้รับจ้างในการประกวดราคา หากผู้รับจ้างมีคุณสมบัติไม่ตรงตามข้อ 4

14.5 ผู้ที่ได้คะแนนรวมสูงสุดถือเป็นผู้ชนะการคัดเลือก

14.6 กระทรวงการต่างประเทศทรงไว้ซึ่งสิทธิที่จะไม่รับราคาต่ำสุด หรือราคาหนึ่งราคาใด หรือราคาที่เสนอทั้งหมดก็ได้ และอาจพิจารณาเลือกจ้างในจำนวนหรือขนาดหรือเฉพาะรายการหนึ่งรายการใด หรืออาจยกเลิกการประกวดราคาจ้าง โดยไม่พิจารณาจัดจ้างเลยก็ได้แต่พิจารณา ทั้งนี้ เพื่อประโยชน์ของทางราชการเป็นสำคัญ และให้ถือการตัดสินของกระทรวงการต่างประเทศเป็นเด็ดขาด ผู้ยื่นข้อเสนอจะเรียกร้องค่าเสียหายใด ๆ มิได้

15. เอกสารที่ผู้ยื่นข้อเสนอต้องยื่น

15.1 ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารยืนยันคุณสมบัติตามข้อ 4

15.2 เอกสารข้อเสนอด้านเทคนิค สำหรับประกอบสำหรับการประเมินตามเกณฑ์การพิจารณาคัดเลือกข้อเสนอ ข้อ 14.2.2

ประธานกรรมการ กรรมการ กรรมการ
 กรรมการ กรรมการ กรรมการ กรรมการ

16. ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติม

กองตรวจลงตราและเอกสารเดินทางคนต่างด้าว

กรมการกงสุล กระทรวงการต่างประเทศ

123 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

โทรศัพท์ 02 203 5000 ต่อ 33309, 33503

โทรสาร 02 575 1066

ไปรษณีย์อิเล็กทรอนิกส์ consular03@mfa.go.th, bundit.b@mfa.go.th

.....

ประธานกรรมการ..... กรรมการ กรรมการ

กรรมการ กรรมการ กรรมการ กรรมการ