



EGA
e-Government Agency



มาตรฐานแอปพลิเคชันภาครัฐสำหรับอุปกรณ์เคลื่อนที่
Government Mobile Application Standard
Version 1.0

มาตรฐานแอปพลิเคชันภาครัฐสำหรับอุปกรณ์เคลื่อนที่
Government Mobile Application Standard
Version 1.0



มาตรฐานแอปพลิเคชันภาครัฐสำหรับอุปกรณ์เคลื่อนที่
Government Mobile Application Standard
Version 1.0

ISBN: 978-616-8001-02-8

พิมพ์ครั้งที่ 1 (กันยายน 2558) จำนวนพิมพ์ 1,000 เล่ม

เมื่อนำเนื้อหาในหนังสือเล่มนี้ไปใช้ ควรอ้างถึงแหล่งที่มา
โดยไม่นำไปใช้เพื่อการค้าและยินยอมให้ผู้อื่นนำไปใช้ต่อไปได้

จัดทำโดย

ส่วนมาตรฐาน

ฝ่ายนวัตกรรม

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สโร.)

ชั้น 17 อาคารบางกอกไทยทาวเวอร์

108 ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ

โทรศัพท์ 0 2612 6000

โทรสาร 0 2612 6010-12

<http://www.ega.or.th>

e-Mail: contact@ega.or.th

จัดพิมพ์โดย

บริษัท พี.เอ็ม. มีเดีย พรินท์ จำกัด

1575/1 อาคารชัยสงวน ถนนเพชรบุรีตัดใหม่

แขวงมักกะสัน เขตราชเทวี กรุงเทพฯ 10400

โทรศัพท์ 0 2253 6350-1, 08 1467 8559

โทรสาร 0 2253 6352

e-Mail: pmmediaprint@yahoo.com





> คำนำ

01



กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ พ.ศ. 2554 – 2563 ใน ยุทธศาสตร์ที่ 6 กลยุทธ์ที่ 6.5 “ส่งเสริมให้เกิดชุมชนหรือสังคมเรียนรู้ออนไลน์ และการรวมกลุ่มทางสังคมที่เข้มแข็ง” ได้ มีการกล่าวถึงการส่งเสริมและการพัฒนาการจัดทำเว็บท่า (Portal) ในการเข้าถึงแหล่งข้อมูลความรู้หรือข้อมูลที่เป็นประโยชน์แก่ประชาชน

และสังคม โดยใช้ความร่วมมือและการสนับสนุนของหน่วยงานภาครัฐและภาคเอกชนในการพัฒนาการให้บริการ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สโร.) ได้ให้ความสำคัญในการพัฒนาการให้บริการตามกรอบแนวทางของรัฐบาล จึงได้จัดทำโครงการพัฒนาช่องทางการเข้าถึงข้อมูลและบริการภาครัฐ (Government Access Channels) โดยมุ่งเน้นให้มีระบบการให้บริการในรูปแบบ Mobile Applications แก่ภาครัฐด้วยการจัดตั้งศูนย์กลางของแอปพลิเคชันภาครัฐ (Government Application Center: GAC) ในการรวบรวม Mobile Application ของหน่วยงานภาครัฐเพื่อให้บริการแก่ประชาชนทำให้ประชาชนผู้รับบริการภาครัฐสามารถเข้าถึงได้สะดวก ทุกที่ ทุกเวลา จากอุปกรณ์เคลื่อนที่ (Mobile Devices) ต่าง ๆ ได้

จากที่กล่าวมาข้างต้น สโร. จึงเห็นความสำคัญเป็นอย่างยิ่งในการจัดทำมาตรฐานแอปพลิเคชันสำหรับอุปกรณ์เคลื่อนที่ เพื่อให้การพัฒนา Mobile Application เป็นไปในทิศทางเดียวกัน รวมถึงการกำหนดมาตรฐานเชิงเทคนิคและข้อกำหนดในด้านต่าง ๆ เช่น การคุ้มครองข้อมูลส่วนบุคคล (Privacy Information) การรักษาความมั่นคงปลอดภัย (Security Policy)







หัวข้อ

หน้า

คำนำ

มาตรฐานแอปพลิเคชันสำหรับอุปกรณ์เคลื่อนที่ (MOBILE APPLICATION STANDARD)	1
---	---

1. คุณสมบัติด้านการให้บริการ (APPLICATION FUNCTIONAL REQUIREMENT)	2
--	---

1.1. ลักษณะทั่วไปของแอปพลิเคชัน ส่วนติดต่อผู้ใช้งานและการใช้งานแอปพลิเคชัน (User Interface and Usability)	2
1.1.1. ทั่วไป (General)	2
1.1.2. โครงสร้าง (Structure)	2
1.1.3. การควบคุมการเข้าถึง/และการเปลี่ยนหน้าจอ (Navigation)	3
1.1.4. การรองรับขนาดหน้าจอ (Supported Resolution)	4
1.1.5. ปุ่มและองค์ประกอบที่สัมผัสเพื่อควบคุมได้ (Buttons & Touchable elements)	5
1.1.6. ความสามารถในการอ่านได้ (Readability)	5
1.1.7. ความสอดคล้องกับแอปพลิเคชันอื่น ๆ (Platform Consistency)	7
1.1.8. คุณภาพของภาพและกราฟิก (Visual Quality)	7
1.1.9. การตอบสนองของส่วนรับข้อมูลจากผู้ใช้งาน (Application Speed)	8
1.1.10. การติดต่อกับระบบแม่ข่าย (Acknowledge and Notice)	9
1.1.11. การแสดงข้อความแจ้ง (Notification)	9
1.1.12. ข้อความแจ้งเตือน (Warning) และแสดงข้อผิดพลาด (Error)	10
1.1.13. การแสดงสัญลักษณ์ประจำหน่วยงาน (Symbol)	10
1.1.14. ส่วนการให้ความช่วยเหลือผู้ใช้งาน (Help and Support)	10
1.1.15. การทำงานร่วมกับแอปพลิเคชันภายนอก (Using and Transferring Application)	11
1.1.16. การโทรศัพท์และการส่งอีเมล (Contact Data)	12
1.1.17. การเข้าเว็บไซต์จากภายในแอปพลิเคชัน (Browsing Website in-application)	12



1.1.18. ข้อมูลที่อยู่และตำแหน่งที่ตั้งต่าง ๆ (Location Data)	13
1.1.19. แบบฟอร์มกรอกข้อมูล (Text field)	14
1.1.20. การลงทะเบียนเพื่อสมัครเข้าใช้งานและเพื่อเข้าใช้งาน (User Registration)	16
1.1.21. การใช้สื่อภาพวิดีโอและเสียงต่าง ๆ (Multimedia)	16
1.1.22. การทำงานในโหมดเบื้องหลัง (Background Process)	17
1.2. การรักษาข้อมูลส่วนบุคคล (Privacy)	18
1.2.1. ทั่วไป (General)	19
1.2.2. สิทธิของผู้ใช้งานความเป็นส่วนตัวของผู้ใช้งาน และข้อตกลงในการใช้งาน (User's Right)	19
1.2.3. การเก็บข้อมูลชั่วคราวไว้ในอุปกรณ์ของผู้ใช้งาน (Cache Data, Caching)	20
1.2.4. การเก็บข้อมูลถาวรไว้ในอุปกรณ์ของผู้ใช้งาน (Local Storage)	21
1.2.5. การใช้งานชุดเครื่องมือในการพัฒนาซอฟต์แวร์จากภายนอก (3rd Party Software Development Kit; SDK)	22
1.3. ส่วนติดต่อเพื่อพัฒนาโปรแกรม (Application Programming Interface; API) และการเปิดข้อมูลเพื่อพัฒนาต่อยอด (Open Data)	23
1.3.1. ทั่วไป (General)	23
1.3.2. API เพื่อการเข้าถึงและการแสดงข้อมูลสาธารณะ (Public Contents' Accessing API)	23
1.3.3. API เพื่อเข้าถึงข้อมูลที่จำเพาะเจาะจงเฉพาะผู้ใช้งาน เฉพาะแอปพลิเคชันและ/หรือเฉพาะผู้พัฒนา (Specific Content's Focused API)	25
1.3.4. การเปลี่ยนแปลง API (Changing API)	25
1.3.5. การกำหนดข้อตกลงในการใช้งาน API (API Agreement))	26



1.4. การทดสอบคุณสมบัติของแอปพลิเคชัน (Functional Testing)	27
1.4.1. ทั่วไป (General)	27
1.4.2. การทดสอบส่วนติดต่อกับผู้ใช้งาน (User Interface Testing)	27
1.4.3. การทดสอบการทำงานร่วมกับระบบแจ้งเตือน (Notification System)	28
1.4.4. การทดสอบการทำงานกับระบบเครือข่าย (Network delay and loss of connection)	29
1.4.5. การทดสอบการทำงานกับ API และ/หรือระบบแม่ข่ายข้อมูล (API Testing)	29

1.5. สิทธิและข้อตกลงในการใช้เครื่องมือและองค์ประกอบต่าง ๆ จากภายนอก (3rd Party)	29
1.5.1. ทั่วไป (General)	29
1.5.2. การใช้งานโปรแกรมต่าง ๆ (Developer's Right and Permission)	30
1.5.3. การใช้งานภาพภาพถ่ายภาพกราฟิกเพลงและสื่อต่าง ๆ (Media's Right)	30
1.5.4. การใช้ฟอนต์ (Font)	31
1.5.5. การใช้งาน API และ SDK จากภายนอก (External API/SDK)	32

2. คุณสมบัติด้านความมั่นคงปลอดภัย (SECURITY FUNCTIONAL REQUIREMENT) 33

2.1. ความมั่นคงปลอดภัย (Security)	33
2.1.1. การจัดการข้อมูลที่มีความสำคัญ (Sensitive Information)	32
2.1.2. มาตรการรองรับสำหรับความปลอดภัยเมื่ออุปกรณ์สูญหาย (Security on loss devices)	34
2.1.3. การติดต่อกับระบบแม่ข่ายข้อมูล (Networking)	34
2.1.4. การระบุตัวตนผู้ใช้งาน (Authentication)	35



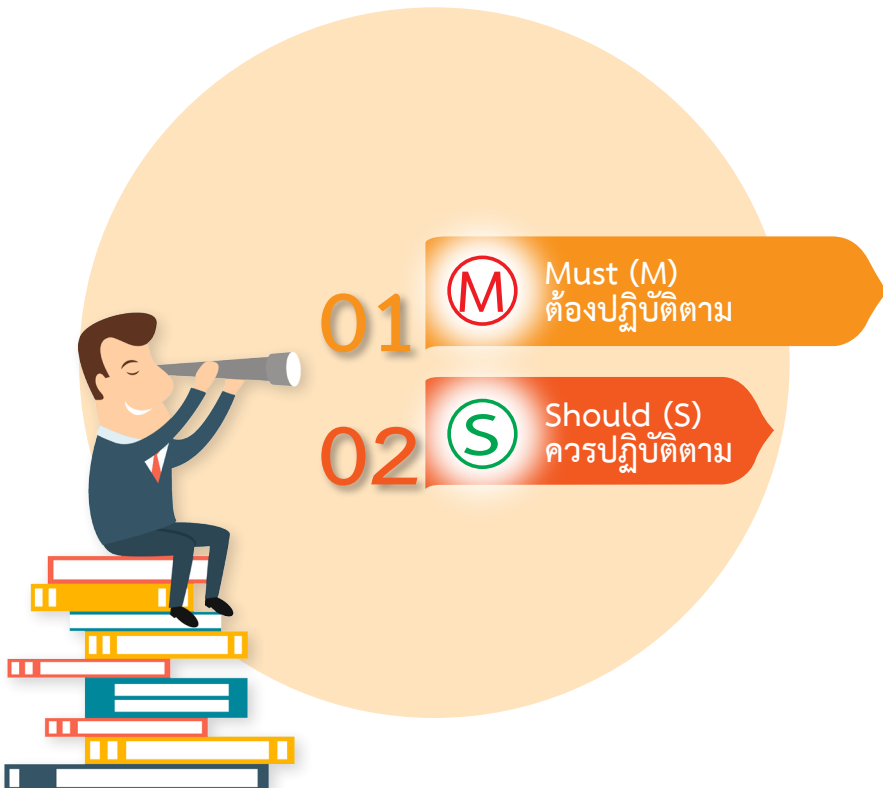




มาตรฐาน แอปพลิเคชันสำหรับอุปกรณ์เคลื่อนที่ (Mobile Application Standard)

02

เพื่อให้แอปพลิเคชันสำหรับอุปกรณ์เคลื่อนที่ (Mobile Application) เป็นไปในทิศทางเดียวกัน ผู้พัฒนาแอปพลิเคชัน ต้องนำมาตรฐานแอปพลิเคชันสำหรับอุปกรณ์เคลื่อนที่ (Mobile Application Standard) ใช้ร่วมกับการพัฒนาแอปพลิเคชันของผู้พัฒนา โดยมีหัวข้อที่เกี่ยวข้องดังต่อไปนี้



1

คุณสมบัติด้านการให้บริการ
(Application Functional Requirement)

1.1.

ลักษณะทั่วไปของแอปพลิเคชัน ส่วนติดต่อผู้ใช้งานและการใช้งานแอปพลิเคชัน
(User Interface and Usability)

1.1.1. ทั่วไป (General)

- A ส่วนติดต่อกับผู้ใช้งานต้องออกแบบโดยยึดถือ User Interface Guideline (UIG) หรือ Human Interface Guideline (HIG) ของแต่ละแพลตฟอร์ม (M)
- B ส่วนติดต่อกับผู้ใช้งาน ผู้พัฒนา ต้องคำนึงถึงความสะดวกในการใช้งาน ความชัดเจนในการทำความเข้าใจ ความคุ้นเคยของผู้ใช้งานจากการใช้งานแอปพลิเคชันของแต่ละแพลตฟอร์ม (M)
- C ต้องมีการแสดง Status Bar เสมอ ไม่ซ่อนจากการแสดงผล นอกเสียจากการซ่อน Status Bar นั้น เป็นประโยชน์ต่อการใช้งานของผู้ใช้งาน โครงสร้าง (M)

1.1.2. โครงสร้าง (Structure)

- A แอปพลิเคชันต้องจัดลำดับความสำคัญของหน้าจอโดยคำนึงถึงความต้องการของผู้ใช้งานหรือรับบริการต่าง ๆ ผ่านแอปพลิเคชันเป็นหลัก (M)
- B แต่ละหน้าจอต้องมีป้ายชื่อกำกับหน้าจออย่างชัดเจน (M)
- C หน้าหลักของแอปพลิเคชันควรแสดงให้เห็นถึงภาพรวมความสามารถหลักของแอปพลิเคชันและมีช่องทางการเข้าถึงความสามารถหลักอย่างชัดเจน (S)



1.1.3. การควบคุมการเข้าถึงและการเปลี่ยนหน้าจอ (Navigation)

- A การออกแบบการเข้าถึงหน้าจอและการเปลี่ยนหน้าจอ ต้องอ้างอิงจาก UIG หรือ HIG ของแต่ละแพลตฟอร์มอย่างเคร่งครัด นอกเสียจากกรณีที่เป็นในเชิงการใช้งาน (M)
- B ใช้สัญลักษณ์ดั้งเดิม (Native Icon) ให้สอดคล้องกับมาตรฐานของระบบ ในการสื่อถึงรูปแบบการทำงานและฟังก์ชันที่เป็นมาตรฐานเช่น การแบ่งปันการเข้าถึงเนื้อหาอยู่เป็นต้น (M)
- C การย้อนกลับไปหน้าจอก่อนหน้านี้ต้องใช้รูปแบบมาตรฐานของแต่ละแพลตฟอร์ม ทั้งรูปแบบลักษณะการทำงาน และการออกแบบส่วนติดต่อผู้ใช้งานบนหน้าจอ (M)



- D. หากแพลตฟอร์มแนะนำให้ใช้ปุ่มย้อนกลับ (Back) ปุ่มดังกล่าวควรอยู่ในตำแหน่งที่เหมาะสม ⑤
- E. ตำแหน่งของปุ่มต่าง ๆ ที่ใช้สำหรับการเข้าถึงเนื้อหาหรือเปลี่ยนหน้าจอที่ถูกกำหนดขึ้นในแต่ละแพลตฟอร์ม ไม่ควรถูกใช้งานเพื่อวัตถุประสงค์อื่น ๆ เช่น ตำแหน่งที่ควรจะเป็นปุ่มย้อนกลับได้ไม่ควรนำปุ่มอื่นวางแทนที่เป็นต้น ⑤



1.1.4. การรองรับขนาดหน้าจอ (Supported Resolution)

- A. ภาพกราฟิกต่าง ๆ ควรจัดเตรียมไว้รองรับทุกระดับความละเอียดของหน้าจออย่างเหมาะสมไม่ก่อให้เกิดการย่อหรือขยายภาพผิดระดับความละเอียดจนสูญเสียความชัดเจน ⑤



1.1.5. ปุ่มและองค์ประกอบที่สัมผัสเพื่อควบคุมได้ (Buttons & Touchable elements)



- A. ปุ่มและองค์ประกอบที่สัมผัสเพื่อควบคุมได้ ต้องมีขนาดไม่เล็กเกินไป M
- B. ปุ่มและองค์ประกอบที่สัมผัสเพื่อควบคุมได้ ต้องถูกปิดสถานะการอนุญาตให้กดเมื่อไม่สามารถกดได้ด้วยเงื่อนไขบางอย่างในขณะนั้น (เช่น ผู้ใช้งานยังกรอกข้อมูลไม่ครบ) และต้องยังคงเห็นปุ่มหรือองค์ประกอบนั้น ๆ ในหน้าจอแต่มีการใช้สีเพื่อแสดงสถานะที่แตกต่างไปอย่างชัดเจน M
- C. ปุ่มและองค์ประกอบที่สัมผัสเพื่อควบคุมได้ ควรมีการแสดงผลตอบรับ เมื่อมีการสัมผัสก่อนที่จะฟังก์ชันที่เกี่ยวข้องจะถูกเรียกใช้งาน S
- D. การใช้ภาพกราฟิกเพื่อประกอบปุ่มและองค์ประกอบที่สัมผัสเพื่อควบคุมได้ ให้เลือกใช้ภาพที่ผู้ใช้งานคุ้นเคยสื่อความหมายได้ชัดเจน S

1.1.6. ความสามารถในการอ่านได้ (Readability)

- A. ขนาดขององค์ประกอบต่าง ๆ ต้องถูกคำนวณให้มีขนาดเหมาะสมกับเนื้อหาไม่ทำให้เนื้อหาถูกตัดโดยไม่จำเป็น เว้นแต่กรณีอยู่ในหน้าจอแสดงรายการที่ผู้ใช้งานสามารถเข้าไปอ่านเนื้อหาต่อได้ในหน้าจอแสดงรายละเอียด M
- B. การจัดวางองค์ประกอบต่าง ๆ ของหน้าจอควรให้ความสำคัญกับความสามารถในการอ่านได้ S



- ๕ หากแอปพลิเคชันรองรับการเปลี่ยนขนาดตัวอักษร ควรมีการคำนวณขนาดขององค์ประกอบต่าง ๆ โดยขึ้นกับขนาดของตัวอักษรที่จะใช้แสดง และมีการคำนวณใหม่เมื่อมีการเปลี่ยนแปลงขนาดตัวอักษร ๕
- ๕ หากแอปพลิเคชันมีการเปลี่ยนหน้าจอโดยอัตโนมัติ ควรกำหนดเวลาให้เหมาะสมสำหรับการอ่านข้อมูลที่จำเป็นบนหน้าจอ ก่อนที่จะทำการเปลี่ยนหน้าจอ ๕





1.1.7. ความสอดคล้องกับแอปพลิเคชันอื่น ๆ (Platform Consistency)

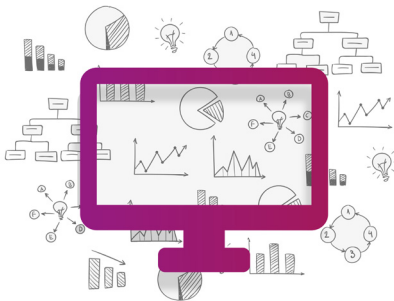
- A การใช้สัญลักษณ์และข้อความต่าง ๆ ต้องสอดคล้องกับ UIG/HIG หรือ สอดคล้องกับแอปพลิเคชันมาตรฐานในแต่ละแพลตฟอร์ม M
- B แอปพลิเคชันไม่ควรเปลี่ยนภาพสัญลักษณ์ของการกระทำที่เป็นมาตรฐานในแต่ละแพลตฟอร์ม (เช่น การส่งอีเมลควรใช้สัญลักษณ์ที่เป็นมาตรฐานในแต่ละแพลตฟอร์มมากกว่ากำหนดเอง) S
- C แอปพลิเคชันไม่ควรเปลี่ยนการกระทำพื้นฐาน (Action) ในแต่ละแพลตฟอร์มที่กำหนดที่มีความเชื่อมโยงกับสัญลักษณ์ (เช่น สัญลักษณ์ที่ใช้สำหรับแบ่งปันข้อมูลไม่ควรถูกกำหนดให้นำไปใช้อย่างอื่น) S

1.1.8. คุณภาพของภาพและกราฟิก (Visual Quality)

- A การแสดงผลของภาพตัวอักษรและองค์ประกอบส่วนติดต่อกับผู้ใช้งานต่าง ๆ ต้องถูกแสดงผลโดยไม่มีการบิดเบี้ยวของอัตราส่วน M
- B การเลือกใช้สีควรคำนึงถึงความสามารถในการอ่านและการมองเห็นของผู้ใช้งานเป็นหลัก ควรหลีกเลี่ยงการใช้ตัวอักษรและสีของพื้นหลังที่รบกวน

ความสามารถในการอ่าน แม้ว่าจะจะเป็นสีประจำของหน่วยงานก็ตาม S

- C สีประจำหน่วยงานสามารถนำมาใช้เป็นสีประจำแอปพลิเคชัน (Application Key Color) ได้ โดยอาจใช้เป็นสีของพื้นหลังหรือสีของตัวอักษร ขึ้นกับความเหมาะสม ทั้งนี้ไม่ควรทำให้ความสามารถในการอ่านลดลง S



1.1.9. การตอบสนองของส่วนรับข้อมูลจากผู้ใช้งาน (Application Speed)

- A. แอปพลิเคชันต้องเตรียมการรองรับหรือการกดปุ่มและองค์ประกอบควบคุมต่าง ๆ บนหน้าจออย่างรวดเร็วและพร้อม ๆ กัน (Input Flooding) เช่น เตรียมปุ่ม Submit ไม่ให้ผู้ใช้งานสามารถกดซ้ำได้เป็นต้น Ⓜ
- B. ทุก ๆ การกระทำ (Action) จากผู้ใช้งานควรมีการแสดงการตอบสนอง (Response) ที่เหมาะสม เช่น การตอบสนองเมื่อมีการกดปุ่มการแสดงสัญลักษณ์เคลื่อนไหวเมื่อผู้ใช้งานสั่งให้โหลดข้อมูลการแสดงผลเคลื่อนไหวตามสถานะการประมวลผล เป็นต้น Ⓢ



1.1.10. การติดต่อกับระบบแม่ข่าย (Acknowledge and Notice)

- A. ในขณะที่ทำการโหลดข้อมูลต้องมีการแสดงสัญลักษณ์ของสถานะ (Indicator) อย่างชัดเจนว่ามีการโหลดข้อมูล (M)
- B. การโหลดข้อมูลจากแม่ข่ายต้องทำใน Background เพื่อไม่ให้เกิดการรบกวนการทำงานของแอปพลิเคชัน และมีการแสดงสัญลักษณ์แสดงสถานะ (Indicator) ที่เหมาะสมในส่วนการติดต่อกับผู้ใช้งาน (M)
- C. หากระบบแม่ข่ายไม่สามารถให้ข้อมูลที่ถูกต้องหรือไม่ทำงาน แอปพลิเคชันต้องมีการตอบสนองที่เหมาะสม เช่น แสดงข้อความแจ้งเตือนให้แก่ผู้ใช้งาน และแอปพลิเคชันต้องไม่ปิดตัวเองโดยเด็ดขาด (M)
- D. หากมีการเชื่อมต่อกับระบบแม่ข่ายข้อมูลควรให้มีการโหลดข้อมูลเป็นช่วง และข้อมูลสามารถโหลดข้อมูลเพิ่มได้เมื่อจำเป็นเช่นเมื่อผู้ใช้งานเลื่อนดูรายการจนสุดเป็นต้น (S)
- E. การโหลดข้อมูลในแต่ละหน้าอาจแยกการโหลดเป็นหลายส่วนเพื่อให้นำข้อมูลที่มีย่อยขนาดเล็กโหลดได้เร็วมาแสดงได้ก่อน (เช่น ข้อความต่าง ๆ) และจากนั้นค่อย ๆ อัปเดตส่วนข้อมูลที่มีขนาดใหญ่ (เช่น รูปภาพ) มาแสดงเพิ่มเติมไปในส่วนต่าง ๆ ที่เตรียมไว้เมื่อโหลดข้อมูลเหล่านั้นเสร็จแล้ว (S)
- F. ควรพิจารณาการเก็บข้อมูลที่โหลดจากแม่ข่ายไว้ชั่วคราวภายในแอปพลิเคชัน (Caching) เพื่อลดการโหลดข้อมูลที่ไม่จำเป็น และทำให้มีการแสดงผลข้อมูลที่ทำการโหลดมาแล้วอย่างรวดเร็วขึ้น (S)

1.1.11. การแสดงข้อความแจ้ง (Notification)

- A. ผู้ใช้งานต้องสามารถปิดการรับข้อความแจ้งเตือนต่าง ๆ ได้ โดยมีช่องทางให้ปิดการแจ้งเตือนได้โดยตรงจากภายในแอปพลิเคชัน ด้วยนอกเหนือจากช่องทางที่มาตรฐานในแต่ละแพลตฟอร์มเตรียมไว้ให้แล้ว (M)



- B. ควรใช้ระบบการส่งข้อความแจ้งเตือน (Notification) ของแต่ละแพลตฟอร์ม ในการส่งข้อความแจ้งเตือนต่าง ๆ ที่สำคัญให้กับผู้ใช้งาน ⑤
- C. การส่งข้อความแจ้งเตือนต่าง ๆ ควรส่งในปริมาณ และความถี่ที่ไม่เป็นการรบกวนผู้ใช้งานยกเว้นเป็นข้อมูลที่เกี่ยวข้องกับผู้ใช้งานโดยตรง เช่น การสนทนาการรับแจ้งเตือนพบสิ่งของหายที่ประกาศไว้เป็นต้น ⑤
- D. การส่งข้อความแจ้งเตือนที่ไม่เกี่ยวข้องกับผู้ใช้งานโดยตรง ควรส่งเมื่อผู้ใช้งานแสดงความจำนงค์ที่จะรับข้อความเหล่านั้น ⑤

1.1.12. ข้อความแจ้งเตือน (Warning) และแสดงข้อผิดพลาด (Error)

- A. การแสดงข้อความแจ้งเตือนและข้อผิดพลาดทั่วไป ควรแสดงโดยใช้ส่วนติดต่อกับผู้ใช้งานปกติ ไม่มีการแสดงกล่องข้อความแยก (Dialog Box) ยกเว้นกรณีที่เป็นข้อผิดพลาดที่สำคัญ หรือเป็นข้อความที่ไม่สามารถแสดงไว้ในส่วนติดต่อกับผู้ใช้งานปกติได้ ⑤
- B. ข้อความที่ใช้ควรแสดงให้ชัดเจนว่าเป็นการเตือนเป็นคำแนะนำหรือเป็นข้อผิดพลาด ⑤
- C. ข้อความที่ใช้แจ้งเตือนข้อผิดพลาด ควรระบุข้อผิดพลาดให้ชัดเจน เข้าใจง่าย และระบุแนวทางแก้ไขเบื้องต้น ⑤

1.1.13. การแสดงสัญลักษณ์ประจำหน่วยงาน (Symbol)

- A. การแสดงสัญลักษณ์ของหน่วยงานให้แสดงได้ในหน้าก่อนเข้าแอปพลิเคชัน (Splash Screen) ⑤

1.1.14. ส่วนการให้ความช่วยเหลือผู้ใช้งาน (Help and Support)

- A. ไม่ควรมีโหมดตัวอย่างการใช้งาน (Tutorial Screen) ที่เป็นภาพนิ่งหลายภาพ และมีการแสดงลูกศรถึงตำแหน่งต่าง ๆ ยกเว้นกรณีที่เป็นจริง ๆ เท่านั้น ⑤
- B. อาจมีหน้าคำถามเกี่ยวกับการใช้งานที่พบบ่อย (Frequency Asked Questions) เพื่อให้ผู้ใช้งานสามารถศึกษารูปแบบการใช้งานบางอย่างเพิ่มเติมได้ ⑤



- ๕. อาจมีการทำ Video Clip ที่มีรูปแบบการใช้งานเบื้องต้นอัปโหลดไว้ในเว็บหน่วยงานหรือเว็บแบ่งปัน Video ออนไลน์ที่เข้าถึงได้ง่าย เพื่อให้ผู้สนใจสามารถเห็นรูปแบบการใช้งานเบื้องต้นได้ก่อนเข้าใช้งานจริง ๕
- ๖. ควรมีช่องทางในการติดต่อผู้พัฒนาหรือผู้ที่มีส่วนเกี่ยวข้องโดยตรงเพื่อตอบคำถามข้อสงสัยในการใช้งานแอปพลิเคชัน ๕



1.1.15. การทำงานร่วมกับแอปพลิเคชันภายนอก

(Using and Transferring Application)

- ๗. ในกรณีที่แอปพลิเคชันต้องทำงานร่วมกับแอปพลิเคชันอื่น ๆ ในระบบปฏิบัติการและยังส่งผลให้มีการเปลี่ยนข้ามไปยังแอปพลิเคชันอื่น ๆ จะต้องทำการถามความประสงค์ของผู้ใช้งานก่อนทำการเปลี่ยนข้ามเสมอ ๓



1.1.16. การโทรศัพท์และการส่งอีเมล

(Contact Data)

- A. แอปพลิเคชันต้องมีการแสดงเบอร์โทรศัพท์และอีเมลที่เกี่ยวข้องกับการบริการต่าง ๆ ของหน่วยงาน ที่สามารถติดต่อได้ (M)
- B. ข้อมูลที่เป็นเบอร์โทรศัพท์ ต้องมีการแสดงผลที่ชัดเจนและสามารถกดเพื่อทำการโทรออก ยกเว้นแอปพลิเคชันทำงานบนอุปกรณ์ที่ไม่สามารถใช้ฟังก์ชันของโทรศัพท์ได้ (M)
- C. การกดเบอร์โทรศัพท์เพื่อทำการโทรออกต้องทำการถามความประสงค์ของผู้ใช้งานเสมอว่าต้องการโทรออกไปยังเบอร์นั้น ๆ จริงหรือไม่ ห้ามทำการโทรทันทีโดยผู้ใช้งานไม่ได้ยืนยันก่อน (M)
- D. ข้อมูลที่เป็นอีเมลต้องมีการแสดงผลที่ชัดเจนและสามารถกดเพื่อทำการส่งอีเมลได้ (M)
- E. การส่งอีเมลจากอีเมลของผู้ใช้งานผู้ใช้งานต้องเห็นข้อความทั้งหมดที่จะส่ง และเป็นผู้ยืนยันการส่งด้วยตัวเองเสมอ ทั้งนี้อาจมีการใส่ข้อความเบื้องต้นในอีเมลแบบอัตโนมัติ เพื่ออำนวยความสะดวกให้ผู้ใช้งานใส่ข้อความเพิ่มเติมได้ (M)



1.1.17. การเข้าเว็บไซต์จากภายในแอปพลิเคชัน

(Browsing Website in-application)

- A. แอปพลิเคชันต้องมีการแสดงที่อยู่ของเว็บไซต์หน่วยงาน (Website URL) และเว็บไซต์บริการต่าง ๆ ที่เกี่ยวข้อง (M)
- B. ข้อมูลลิงก์เว็บไซต์ (Website URL) ต้องมีการแสดงผลที่ชัดเจน และสามารถกดเพื่อเข้าชมเว็บไซต์ได้ (M)



- Ⓒ การเข้าชมเว็บไซต์อาจทำได้โดยอาศัยแอปพลิเคชันสำหรับท่องเว็บ (Web Browser) อื่น ๆ ที่มีอยู่ในเครื่องหรือแสดงผลหน้าเว็บไซต์นั้น ๆ จากภายในแอปพลิเคชันเอง ⑤
- Ⓓ กรณีใช้ Web Browser ภายนอกแอปพลิเคชันควรเรียกถามความประสงค์ในการเปลี่ยนข้ามแอปพลิเคชันจากผู้ใช้งานเสมอ ⑤
- Ⓔ กรณีไม่เปลี่ยนข้ามไปใช้ Web Browser ภายนอกแต่มีการพัฒนาหน้าจอเพื่อแสดงผลหน้าเว็บภายในแอปพลิเคชันควรมีส่วนติดต่อกับผู้ใช้งานเพื่อทำการควบคุมการทำงานของหน้าเว็บเช่นย้อนกลับถัดไปโหลดใหม่อีกครั้งและหยุดการโหลดหน้าเว็บเสมอ ⑤



1.1.18. ข้อมูลที่อยู่และตำแหน่งที่ตั้งต่าง ๆ (Location Data)

- Ⓐ แอปพลิเคชันต้องมีการแสดงข้อมูลที่อยู่ ที่ตั้งหน่วยงาน หรือสถานที่ต่าง ๆ ที่เกี่ยวข้องที่สามารถติดต่อได้ ④
- Ⓑ ข้อมูลที่เป็นที่อยู่หรือตำแหน่งที่ตั้งของหน่วยงานหรือสถานที่ต่าง ๆ ที่เกี่ยวข้องกับสิ่งที่แสดงผลอยู่ต้องพัฒนาให้ทำงานร่วมกับแอปพลิเคชันแผนที่ที่อยู่ในเครื่องได้ ④





- Ⓒ แอปพลิเคชันไม่จำเป็นต้องแสดงพิกัดภูมิศาสตร์ให้ผู้ใช้งานเห็นอย่างชัดเจน ยกเว้นในกรณีที่ช่วยให้ประสบการณ์ผู้ใช้งานดีขึ้นและมีการระบุกรณียกเว้นดังกล่าวอย่างชัดเจน ⑤
- Ⓓ กรณีเปลี่ยนข้ามไปใช้แอปพลิเคชันแผนที่อื่น ๆ ในเครื่อง ควรมีการเรียกถามความประสงค์ของผู้ใช้งานก่อนทุกครั้ง ⑤

1.1.19. แบบฟอร์มกรอกข้อมูล (Text Field)

- Ⓐ แบบฟอร์มกรอกข้อมูลต้องมีการแสดงป้ายชื่ออย่างชัดเจนและป้ายชื่อนี้ควรจะเห็นตลอดเวลา ④
- Ⓑ ข้อมูลที่จำกัดรูปแบบต้องมีการตรวจสอบรูปแบบของข้อมูลที่ใช้งานกรอกเสมอ ④
- Ⓒ ในช่องกรอกข้อมูลที่มีการจำกัดรูปแบบจะต้องมีการแสดงแป้นพิมพ์ที่เหมาะสม เช่น ข้อมูลที่เป็นตัวเลขเท่านั้นควรแสดงแป้นพิมพ์ที่เป็นเฉพาะตัวเลข ④
- Ⓓ ข้อมูลรหัสผ่านต้องถูกแทนที่ด้วยตัวอักขระอื่น (เช่น *) และต้องมีปุ่มแสดงรหัสผ่านที่สามารถแสดงรหัสผ่านที่ถูกซ่อนไว้ เพื่อให้ผู้ใช้งานมองเห็น และยืนยันได้ ④
- Ⓔ ผู้ใช้งานต้องไม่สามารถใส่ข้อมูลที่เป็นไปไม่ได้ (เช่น ต้องไม่สามารถใส่ปีเกิดเป็นปีในอนาคต) ④



- ☒ แบบฟอร์มกรอกข้อมูลควรมีการใช้ร่างข้อมูล (Placeholder Information) ในช่องดังกล่าวเพื่อระบุแบบข้อมูลและ/หรือตัวอย่างข้อมูล ⑤
- ☒ ไม่ควรใช้ร่างข้อมูล(Placeholder Information) แทนการใช้ป้ายชื่อ เพราะร่างข้อมูลจะถูกแทนที่ด้วยข้อมูลจริง และทำให้ไม่รู้ว่าข้อมูลนี้คือข้อมูลสำหรับอะไร ⑤
- ☒ หากผู้ใช้งานทำการปิดหน้าจอกรอกแบบฟอร์มหรือข้อมูลต่าง ๆ และข้อมูลไม่มีการบันทึกไว้ส่งผลให้ผู้ใช้งานต้องกรอกข้อมูลใหม่ควรมีข้อความแจ้งเตือนแสดงให้ผู้ใช้งานทราบและยืนยันการปิดหน้าจอเสมอ ⑤



1.1.20. การลงทะเบียนเพื่อสมัครเข้าใช้งานและเพื่อเข้าใช้งาน (User Registration)

A. แอปพลิเคชันที่ต้องการให้
ผู้ใช้งานลงทะเบียนเพื่อ
ใช้งานต้องทำแบบฟอร์ม
สำหรับลงทะเบียน
โดยอ้างอิงจากส่วนของ
“แบบฟอร์มกรอกข้อมูล”
เป็นหลัก (M)

B. ต้องมีระบบช่วยเหลือ
ในกรณีผู้ใช้งานลิ้มรสผ่าน
จากหน้าจอลงทะเบียน
สำหรับวิธีการช่วยเหลือ

นั้นขึ้นกับหน่วยงาน เช่น อาจจะใช้วิธีการถามคำถามลับ เพื่อตั้ง
รหัสผ่านใหม่ หรือส่งลิงก์สำหรับตั้งรหัสผ่านใหม่ไปยังอีเมลที่ให้ไว้ หรือ
วิธีการอื่นๆ (M)

C. ในแอปพลิเคชันควรมีหน้าจอให้ผู้ใช้งานปรับข้อมูลและตัวเลือกต่าง ๆ
ที่กรอกไปในการลงทะเบียนใช้งานครั้งแรก โดยเป็นหน้าจอที่เข้าถึง
ได้ง่าย (S)



1.1.21. การใช้สื่อภาพวิดีโอและเสียงต่าง ๆ (Multimedia)

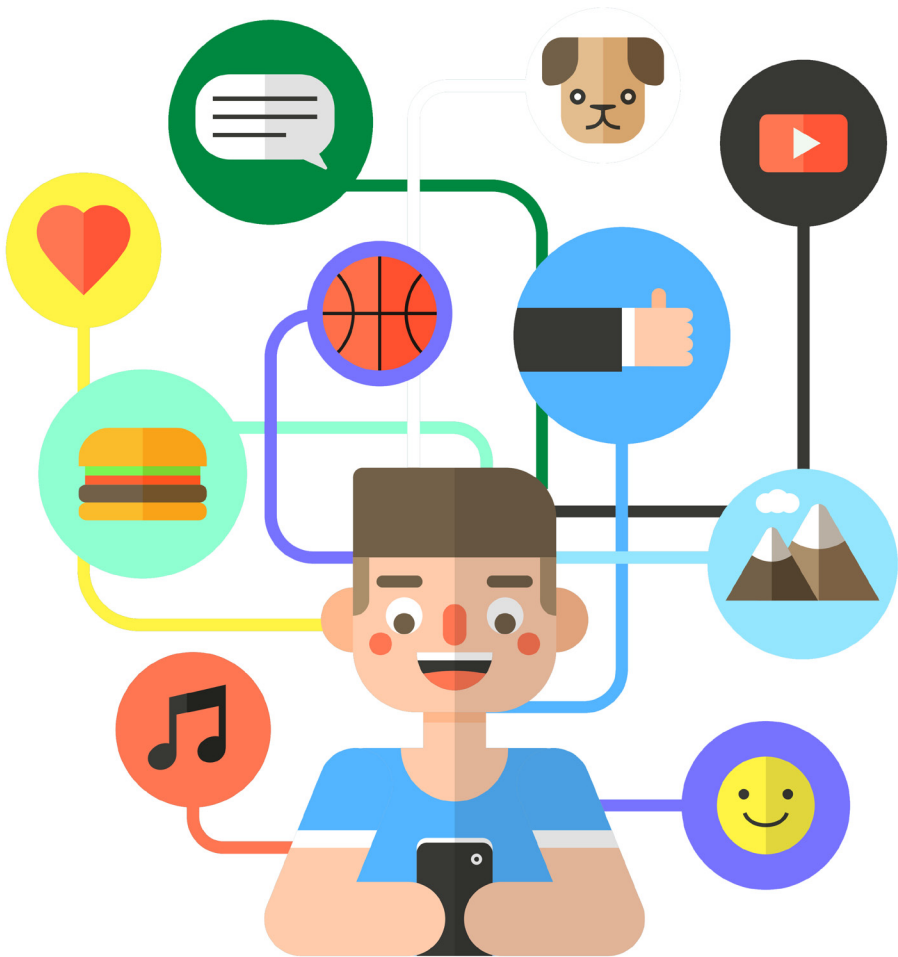
A. แอปพลิเคชันต้องไม่มีการเล่นไฟล์ Video หรือไฟล์ Audio เมื่อเริ่มต้นใช้
งานแอปพลิเคชันอัตโนมัติ (M)

B. การเล่นไฟล์ Video หรือไฟล์ Audio ใด ๆ ต้องเป็นความประสงค์ของ
ผู้ใช้งานเท่านั้น ผู้ใช้งานต้องเป็นผู้กดปุ่มเริ่มเล่นด้วยตัวเอง (M)

C. การแนบไฟล์ Video และไฟล์ Audio ต่าง ๆ ไปกับแอปพลิเคชัน
เพื่อให้ไม่ต้องการดาวน์โหลดภายหลังควรคำนึงถึงขนาดของแอปพลิเคชัน
เป็นสำคัญ ขนาดของแอปพลิเคชันเมื่อดาวน์โหลดครั้งแรกไม่ควรมี
ขนาดใหญ่เกินไป โดยเฉพาะอย่างยิ่งถ้าไฟล์ต่าง ๆ เหล่านั้นอาจไม่ได้ใช้
เป็นประจำ (S)



1.2. การรักษาข้อมูลส่วนบุคคล (Privacy)



1.2.1. ทัวไป (General)

- A เนื้อหาหรือข้อมูลที่แสดงในแอปพลิเคชันต้องไม่ละเมิดกฎหมายที่เกี่ยวข้องกับความเป็นส่วนตัวของบุคคล (M)
- B การเก็บข้อมูลต่าง ๆ ที่เกี่ยวข้องกับความเป็นส่วนตัวของผู้ใช้งานต้องกระทำโดยความยินยอมของผู้ใช้งานเท่านั้น (M)
- C การเก็บข้อมูลต่าง ๆ ที่เกี่ยวข้องกับความเป็นส่วนตัวของผู้ใช้งานต้องเป็นข้อมูลที่เกี่ยวข้องกับการทำงาน และใช้งานแอปพลิเคชันโดยตรงเท่านั้น (M)
- D ข้อมูลที่เกี่ยวข้องกับความเป็นส่วนตัวของผู้ใช้งานต้องไม่ถูกเปิดเผยนอกจากกรณีที่เป็นต่อการใช้งานแอปพลิเคชันโดยตรงและเปิดเผยเป็นการชั่วคราวต่อผู้ที่เกี่ยวข้องกับเท่านั้น (เช่น แอปพลิเคชันที่ระบุตำแหน่งขอความช่วยเหลือที่มีการระบุตัวตนและตำแหน่งจะเปิดเผยตัวตนและตำแหน่งให้แก่เจ้าหน้าที่ที่เกี่ยวข้องในระยะเวลาที่ทำการช่วยเหลือเท่านั้น เป็นต้น) (M)

1.2.2. สิทธิของผู้ใช้งานความเป็นส่วนตัวของผู้ใช้งานและข้อตกลงในการใช้งาน (User's Right)



- A ผู้ใช้งานต้องสามารถเข้าถึงหน้าจอเพื่อแสดงสิทธิในการใช้งาน (User's Right) ความเป็นส่วนตัวของผู้ใช้งาน (User's Privacy) และข้อตกลงในการใช้งาน (Service Agreement หรือ Term of Uses) ได้โดยง่ายจากภายในแอปพลิเคชัน (M)
- B แอปพลิเคชันที่มีการเก็บข้อมูลส่วนบุคคลของผู้ใช้งานต้องระบุในหน้าจอแสดงสิทธิและความเป็นส่วนตัวของผู้ใช้งานให้ผู้ใช้งานทราบอย่างชัดเจนว่ามี การเก็บข้อมูลอะไรบ้าง (M)

- 
- ๕. ผู้ใช้งานต้องสามารถลบหรือแก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้องไม่สมบูรณ์ หรือไม่เป็นปัจจุบันได้ (M)
 - ๖. หากมีการเปลี่ยนแปลงสิทธิ์ของผู้ใช้งาน ความเป็นส่วนตัวของผู้ใช้งาน หรือข้อตกลงในการใช้งานต้องมีการแจ้งผู้ใช้งานให้ทราบอย่างชัดเจนเสมอ (M)
 - ๗. หากแอปพลิเคชันมีการให้ ผู้ใช้งานยอมรับในสิทธิ์ผู้ใช้งาน ความเป็นส่วนตัวของผู้ใช้งาน หรือข้อตกลงในการใช้งานในการลงทะเบียนเข้าใช้งานครั้งแรก และภายหลัง มีการเปลี่ยนแปลงเงื่อนไขดังกล่าวต้องมีการแสดงหน้าจอให้ผู้ใช้งานยอมรับสิทธิ์ที่มีการเปลี่ยนแปลงทุกครั้ง (M)
 - ๘. แอปพลิเคชันต้องมีช่องทางให้ติดต่อผู้เกี่ยวข้องเพื่อสอบถาม หรือตรวจสอบสิทธิ์และการใช้ข้อมูลที่เกี่ยวข้องกับความเป็นส่วนตัวของตัวเองได้ (M)

1.2.3. การเก็บข้อมูลชั่วคราวไว้ในอุปกรณ์ของผู้ใช้งาน (Cache Data, Caching)

- ๑. แอปพลิเคชันจะต้องไม่มีการเก็บข้อมูลใด ๆ ของผู้ใช้งานที่ไม่เกี่ยวข้องกับการทำงานโดยตรงของแอปพลิเคชันแม้ว่าจะเป็นเพียงข้อมูลชั่วคราวก็ตาม (M)
- ๒. แอปพลิเคชันอาจเก็บข้อมูลไว้ในอุปกรณ์ของผู้ใช้งานชั่วคราว (Caching) ควรมีวัตถุประสงค์เพิ่มประสิทธิภาพการทำงานของแอปพลิเคชัน และลดการติดต่อกับระบบแม่ข่ายข้อมูลเท่านั้น (M)
- ๓. เมื่อเข้าสู่โหมดการทำงานเบื้องหลัง แอปพลิเคชันควรมีการบันทึกข้อมูลชั่วคราวที่จำเป็นในการทำงานต่อ เมื่อกลับสู่โหมดการทำงานปกติ (S)

- D. แอปพลิเคชันที่รองรับการลงทะเบียนเป็นเข้าใช้งาน และมีการเก็บข้อมูลเนื้อหาไว้เป็นข้อมูลชั่วคราวต้องระมัดระวังไม่ให้ข้อมูลชั่วคราวที่เก็บไว้ของผู้ใช้งานแต่ละคนปรากฏแก่ผู้ใช้งานคนอื่น ๆ ในเครื่องเดียวกัน ควรใช้วิธีการแยกเก็บข้อมูลชั่วคราวเป็นรายคนหรือลบข้อมูลชั่วคราวเมื่อมีการ Sign out เกิดขึ้นหรือวิธีการอื่น ๆ ที่ให้ผลลัพธ์ถูกต้อง ⑤
- E. แอปพลิเคชันจะไม่มีการเก็บข้อมูลที่อาจเป็นอันตรายต่อความปลอดภัยของผู้ใช้งานเป็นข้อมูลชั่วคราวโดยไม่มีการเข้ารหัสโดยเด็ดขาด เช่น รหัสผ่านต่าง ๆ หรือหมายเลขบัตรเครดิต เป็นต้น ⑤



1.2.4. การเก็บข้อมูลถาวรไว้ในอุปกรณ์ของผู้ใช้งาน (Local Storage)

- A. แอปพลิเคชันอาจมีการเก็บข้อมูลเนื้อหาบางอย่างในลักษณะข้อมูลถาวร ทั้งนี้ให้พิจารณาถึงความจำเป็น และประเภทข้อมูลในการจัดเก็บ ⑤



1.2.5. การใช้งานชุดเครื่องมือในการพัฒนาซอฟต์แวร์จากภายนอก (3rd Party Software Development Kit; SDK)

- A. แอปพลิเคชันที่มีการพัฒนาโดยใช้ชุดเครื่องมือในการพัฒนาซอฟต์แวร์จากภายนอกต้องไม่ขัดต่อนโยบายที่เกี่ยวข้องกับการเก็บข้อมูล ความเป็นส่วนตัวของผู้ใช้งานในแต่ละแพลตฟอร์มและของ SDK นั้น ๆ (M)
- B. ในกรณีที่ SDK ที่นำมาใช้มีการเก็บข้อมูลของผู้ใช้งานและส่งไปยังแม่ข่ายภายนอกผู้พัฒนา ต้องแน่ใจว่าตัว SDK นั้น ๆ ไม่มีการเก็บข้อมูลที่ละเมิด ความเป็นส่วนตัวของผู้ใช้งานและต้องมีการแจ้งให้ผู้ใช้งานทราบถึงการเก็บและการใช้ข้อมูลดังกล่าวเสมอ (M)



1.3. ส่วนติดต่อเพื่อพัฒนาโปรแกรม (Application Programming Interface; API) และการเปิดข้อมูลเพื่อพัฒนาต่อยอด (Open Data)

1.3.1. ทัวไป (General)

- A. แอปพลิเคชันที่มีการติดต่อกับระบบแม่ข่ายข้อมูลต้องมีการพัฒนาส่วนของ API ที่ระบบแม่ข่ายข้อมูลขึ้นมาทำงานควบคู่กันไป ด้วยเสมอ (M)
- B. แอปพลิเคชันที่มีการต่อติดกับระบบแม่ข่ายข้อมูลไม่ว่าจะเป็นการติดต่อเพื่อขอข้อมูลส่งข้อมูลหรือขอให้ระบบแม่ข่ายดำเนินการประมวลผลต้องทำงานผ่าน API เสมอ (M)
- C. API ที่พัฒนาขึ้นควรรับส่งข้อมูลโดยใช้รูปแบบและเทคโนโลยีที่ใช้กันอย่างกว้างขวาง (เป็น De Facto Standard) ในขณะพัฒนา เช่น รับส่งข้อมูลในรูปแบบ JSON ในปัจจุบันเป็นต้น (S)
- D. หน่วยงานเจ้าของข้อมูลควรพิจารณาการใช้งาน API เพื่อส่งข้อมูลให้แอปพลิเคชันต่าง ๆ นำไปใช้งานแทนการดึงข้อมูลจากหน้าเว็บของหน่วยงาน หรือการดึงหน้าเว็บหน่วยงานไปแสดง (S)
- E. หน่วยงานควรสนับสนุนให้มีการใช้งาน API ในการสร้างแอปพลิเคชันอื่น ๆ ต่อยอดให้ข้อมูลมีประโยชน์หลากหลายยิ่งขึ้น มีคุณค่ามากยิ่งขึ้น (S)



1.3.2. API เพื่อการเข้าถึงและการแสดงข้อมูลสาธารณะ (Public Contents' Accessing API)

- A. แอปพลิเคชันที่มีการแสดงข้อมูลสาธารณะ (เช่น ข่าวสารสาธารณะที่สำคัญข้อมูลทางสถิติที่เป็นสาธารณะรายการต่าง ๆ ที่เป็นข้อมูลสาธารณะ) ที่ประชาชนและผู้ใช้งานทั่วไปสามารถเข้าถึงได้ ควรขอข้อมูลดังกล่าว



ไปยัง Public API ของหน่วยงานซึ่ง Public API นี้ควรเปิดให้นักพัฒนาโปรแกรมโดยทั่วไปสามารถเรียกใช้งานได้ โดยอาจจะมีขั้นตอนการขอสิทธิในการใช้งาน ⑤

- B. หน่วยงานควรพิจารณา Public API เพื่อให้นักพัฒนาทั่วไปสามารถนำข้อมูลสาธารณะที่ถูกต้องเชื่อถือได้จากหน่วยงานไปใช้งานได้โดยตรงอย่างมีประสิทธิภาพ ⑤
- C. Public API ควรเข้าถึงได้โดยง่าย มีรูปแบบการรับส่งข้อมูลที่ใช้กันอย่างกว้างขวาง (เป็น De Facto Standard) ในช่วงที่พัฒนาขณะนั้น ⑤
- D. Public API ที่เข้าถึงข้อมูลได้ทันที ไม่ควรมีการละเมิดความเป็นส่วนตัวของผู้ใช้งานภายในระบบ และไม่ควรสามารถเข้าถึงข้อมูลอันเป็นส่วนตัวของผู้ใช้งานได้ ⑤
- E. Public API ต้องมีเอกสารอ้างอิงสำหรับการพัฒนาโปรแกรม (Development Documentation) ที่ระบุถึงรูปแบบการรับส่งข้อมูลโดยละเอียด (API Specification) เพื่อให้นักพัฒนาสามารถนำไปใช้ได้ทันที ⑤



1.3.3. API เพื่อเข้าถึงข้อมูลที่เจาะจงเฉพาะผู้ใช้งานเฉพาะแอปพลิเคชันและ/หรือเฉพาะผู้พัฒนา (Specific Content's Focused API)

- A. แอปพลิเคชันที่มีการเข้าถึงข้อมูลเจาะจงเฉพาะผู้ใช้งานเฉพาะแอปพลิเคชันและ/หรือเฉพาะผู้พัฒนา ควรมีการออกแบบให้ระบุผู้ใช้งานแอปพลิเคชันที่ใช้และ/หรือผู้พัฒนาได้ ⑤
- B. การเข้าถึง API ดังกล่าวควรเป็นไปตามมาตรฐานความปลอดภัยของข้อมูล ควรคำนึงถึงการเข้ารหัสข้อมูลการควบคุมสิทธิ์ในการเข้าถึงข้อมูลและความเป็นส่วนตัวของผู้ใช้งานอย่างเคร่งครัด ⑤

1.3.4. การเปลี่ยนแปลง API (Changing API)

- A. API ควรรองรับหลายเวอร์ชัน (API Versioning) การเปลี่ยนแปลง API ควรคำนึงถึงแอปพลิเคชันที่ใช้งาน API อยู่แล้วจะยังคงต้องใช้งานได้ต่อไปโดยไม่ส่งผลกระทบ ⑤
- B. API ควรมีช่องทางให้นักพัฒนาลงทะเบียนรับข่าวสารของการเปลี่ยนแปลง API ต่าง ๆ ได้ ⑤



1.3.5. การกำหนดข้อตกลงในการใช้งาน API (API Agreement)

- A. ในกรณีที่มีการเปิด Public API ควรมีเว็บไซต์ที่แสดงข้อตกลง และสิทธิในการใช้งาน API อย่างชัดเจน ⑤
- B. ข้อตกลงควรครอบคลุมสิทธิการใช้งาน หรือรูปแบบของแอปพลิเคชันที่ห้ามพัฒนา หรือสามารถพัฒนาได้ รวมถึงเรื่องการเป็นเจ้าของข้อมูล สิทธิ (Disclaimer) และเงื่อนไขต่าง ๆ ที่นักพัฒนาต้องปฏิบัติตาม เช่น การให้เครดิตการอ้างอิงแหล่งที่มาหรือรูปแบบของการนำข้อมูลไปใช้ต่อไปเป็นต้น ⑤



1.4. การทดสอบคุณสมบัติของแอปพลิเคชัน (Functional Testing)

1.4.1. ทัวไป (General)

- A แอปพลิเคชันต้องได้รับการทดสอบอย่างละเอียดถี่ถ้วนโดยการทดสอบต้องครอบคลุมถึงสถานการณ์ต่าง ๆ ที่เกิดขึ้นได้ในการใช้งานจริง (M)
- B แอปพลิเคชันต้องได้รับการทดสอบว่าไม่ปิดตัวเอง (Crash) ในสถานการณ์การใช้งานปกติ (M)
- C แอปพลิเคชันควรได้รับการทดสอบบนอุปกรณ์จริงที่มีรายละเอียดคุณสมบัติของอุปกรณ์ ครอบคลุมกลุ่มเป้าหมายผู้ใช้งาน (S)
- D แอปพลิเคชันควรได้รับการทดสอบบนทุกระบบปฏิบัติการ ที่เป็นกลุ่มเป้าหมายของการนำไปใช้งานจริง (S)
- E แอปพลิเคชันควรทดสอบกับข้อมูลจริงหรือข้อมูลที่จำลองเสมือนในปริมาณข้อมูลที่เหมาะสมกับการนำไปใช้งานจริงเพื่อให้เห็นสภาพของการใช้งานจริง (S)
- F แอปพลิเคชันควรได้รับการทดสอบสถานการณ์จำลองข้อผิดพลาดในการใช้งานที่อาจเกิดขึ้นได้ทั้งหมด (S)

1.4.2. การทดสอบส่วนติดต่อกับผู้ใช้งาน (User Interface Testing)

- A แอปพลิเคชันต้องได้รับการทดสอบในส่วนของ “ลักษณะทั่วไปของแอปพลิเคชัน ส่วนติดต่อกับผู้ใช้งานและการใช้งานแอปพลิเคชัน” ทุกรายการที่เกี่ยวข้อง (M)
- B แบบฟอร์มสำหรับกรอกข้อมูลทุกจุดต้องได้รับการทดสอบความถูกต้องของข้อมูลที่สามารถใส่ได้ทั้งประเภทข้อมูลรูปแบบ ข้อมูลความถูกต้องของข้อมูล และการนำข้อมูลไปใช้งานต่ออย่างถูกต้อง (M)



- ๕. แอปพลิเคชันควรแสดงผลอย่างถูกต้องในกรณีที่ระบบปฏิบัติการแสดงสถานะการทำงานบางอย่างแทรกเข้ามาในบางส่วนของหน้าจอ เช่น Internet Sharing/Tethering ของระบบปฏิบัติการ iOS เป็นต้น ๕
- ๖. แอปพลิเคชันควรได้รับการทดสอบการรองรับการสัมผัสส่วนต่าง ๆ ของหน้าจออย่างรวดเร็ว หรือ Input Flooding ในแต่ละหน้าจอ ๕



1.4.3. การทดสอบการทำงานร่วมกับระบบแจ้งเตือน (Notification System)

- ๗. แอปพลิเคชันที่มีการทำงานร่วมกับระบบแจ้งเตือนต้องได้รับการทดสอบในกรณีมีข้อความเตือน ผู้ใช้งานสามารถเรียกอ่านข้อความผ่านการแจ้งเตือนได้ เมื่อผู้ใช้งานกดข้อความแจ้งเตือนจะสามารถเข้าไปใช้งานแอปพลิเคชันได้และมีการแสดงหน้าจอที่เหมาะสมสอดคล้องกับข้อความแจ้งเตือนที่ได้รับ ๗
- ๘. แอปพลิเคชันควรได้รับการทดสอบสถานะของแอปพลิเคชันทั้งในสถานะทำงานอยู่ (Active) ปิดอยู่แต่อยู่ในฉากหลัง (Inactive, Background) หรือปิดอย่างสมบูรณ์ (Inactive, Closed) เป็นอย่างน้อย ๕



1.4.4. การทดสอบการทำงานกับระบบเครือข่าย (Network delay and loss of connection)

- A แอปพลิเคชันต้องถูกทดสอบว่าสามารถใช้งานได้ดีในขณะที่ระบบเครือข่ายมีปัญหาโดยแสดงข้อความแจ้งผู้ใช้งานอย่างเหมาะสม (M)
- B แอปพลิเคชันที่มีการใช้งานเครือข่ายควรมีการทดสอบการทำงานกับเครือข่ายที่มีความเร็วแตกต่างกัน (S)

1.4.5. การทดสอบการทำงานกับ API และ/หรือระบบแม่ข่ายข้อมูล (API Testing)

- A แอปพลิเคชันต้องได้รับการทดสอบการทำงานร่วมกับ API ที่จำเป็น (M)
- B แอปพลิเคชันต้องได้รับการทดสอบว่าสามารถทำงานได้โดยไม่ผิดพลาดในกรณีที่ API ทำงานผิดพลาด มีการเปลี่ยนแปลงเวอร์ชันหรือสาเหตุอื่น ๆ ส่งผลให้แอปพลิเคชันไม่สามารถให้บริการได้โดยต้องมีข้อความแจ้งเตือนแก่ผู้ใช้งาน (M)

1.5. สิทธิและข้อตกลงในการใช้เครื่องมือและองค์ประกอบต่าง ๆ จากภายนอก (3rd Party)

1.5.1. ทั่วไป (General)

- A ผู้พัฒนาที่มีการใช้เครื่องมือต่าง ๆ เช่น โปรแกรมจากภายนอก (3rd. Party Application Program) ส่วนติดต่อเพื่อพัฒนาจากภายนอก (3rd. Party Application Programming Interface; API) ชุดพัฒนาซอฟต์แวร์จากภายนอก (3rd. Party Software Development Kit; SDK) ต้องได้รับอนุญาตให้ใช้เครื่องมือเหล่านั้นในการพัฒนาแอปพลิเคชันและสามารถแสดงสิทธิในการใช้งานเครื่องมือดังกล่าวได้ (M)
- B แอปพลิเคชัน สามารถมีองค์ประกอบต่าง ๆ จากภายนอก เช่น เพลง ภาพถ่ายภาพกราฟิก ฟอนต์ ต้องได้รับอนุญาตให้ใช้องค์ประกอบเหล่านั้นในการพัฒนาแอปพลิเคชันและสามารถแสดงสิทธิในการใช้งานดังกล่าวได้ (M)



1.5.2. การใช้งานโปรแกรมต่าง ๆ (Developer's Right and Permission)

- A ผู้พัฒนาแอปพลิเคชันจะต้องมีสิทธิ์การใช้งานโปรแกรมทุกตัวที่นำมาใช้งาน และมีจำนวนสิทธิ์ที่เพียงพอสำหรับจำนวนคนในทีมพัฒนาแอปพลิเคชัน (M)
- B สิทธิ์ในการใช้งานต้องครอบคลุมถึงการนำผลงานจากโปรแกรมไปใช้งานจริงรวมถึงการใช้ทำการค้าไม่ใช่เป็นสิทธิ์ทดลองใช้สิทธิ์เพื่อการศึกษาหรือสิทธิ์อื่น ๆ ที่มักไม่อนุญาตให้นำผลงานไปใช้ในวัตถุประสงค์ดังกล่าว (M)



1.5.3. การใช้งานถ่ายภาพกราฟิกเพลงและสื่อต่าง ๆ (Media's Right)

- A ภาพและสื่อทุกอย่างที่นำมาใช้ต้องได้รับอนุญาตจากเจ้าของภาพหรือผู้ถือลิขสิทธิ์เป็นลายลักษณ์อักษรหรือใช้ภาพและสื่อที่มีข้อตกลงในการใช้งานที่อนุญาตให้นำไปใช้ในการพัฒนาแอปพลิเคชันได้ (M)
- B ห้ามนำภาพและสื่อต่าง ๆ มาใช้โดยไม่ได้รับสิทธิ์ไม่ได้รับอนุญาตโดยเด็ดขาดแม้จะให้เครดิตชัดเจนภายในแอปพลิเคชันก็ตาม (M)



- ๕ ในกรณีที่เ็นภาพหรือสื่อที่ทางผู้พัฒนาได้สิทธิ์มาก่อนในการพัฒนาแอปพลิเคชันหรือสร้างสรรค์ผลงานอื่น ต้องตรวจสอบให้แน่ใจว่าสามารถใช้กับการพัฒนาแอปพลิเคชันใหม่ได้ (M)



1.5.4. การใช้ฟอนต์ (Font)

- A ฟอนต์ที่นำมาใช้ต้องได้รับอนุญาตในการใช้งานในแอปพลิเคชันจากเจ้าของฟอนต์หรือผู้ถือลิขสิทธิ์เป็นลายลักษณ์อักษรหรือใช้ฟอนต์ที่มีข้อตกลงในการใช้งานที่อนุญาตให้นำไปใช้ในการพัฒนาแอปพลิเคชันได้ (M)
- B ฟอนต์ที่ผู้พัฒนาได้สิทธิ์ในการใช้งานสำหรับงานสร้างสรรค์อื่น ๆ เช่น สื่อสิ่งพิมพ์จะต้องตรวจสอบให้แน่ใจว่าสามารถนำมาใช้งานในการพัฒนาแอปพลิเคชันได้ (M)





1.5.5. การใช้งาน API และ SDK จากภายนอก (External API/SDK)

- A. แอปพลิเคชันที่มีการพัฒนาโดยการนำส่วนติดต่อเพื่อพัฒนาโปรแกรม (API) หรือชุดพัฒนาซอฟต์แวร์ (Software Development Kit; SDK) จากภายนอกเข้ามาใช้งานจะต้องพิจารณาข้อตกลงในการใช้งาน API และ SDK ต่าง ๆ โดยละเอียด (M)
- B. ข้อตกลงการใช้งาน API และ SDK ที่นำมาใช้งาน ต้องไม่ละเมิดหรือขัดต่อความเป็นเจ้าของลิขสิทธิ์สิทธิ์การใช้งานการเปิดรหัสซอฟต์แวร์หรือส่วนของซอฟต์แวร์ตามที่ระบุไว้ในสัญญาการพัฒนาแอปพลิเคชันของหน่วยงาน (M)
- C. ข้อตกลงการใช้งาน API และ SDK ที่นำมาใช้งานทั้งหมดต้องมีความสอดคล้องกันไม่ขัดแย้งกัน (M)
- D. ผู้พัฒนาต้องแสดงรายการของ API และ SDK ที่นำมาใช้งานทั้งหมด และแสดงข้อตกลงในการใช้งานเสมอ (M)
- E. ผู้พัฒนาต้องทำตามข้อตกลงการใช้งาน API และ SDK ที่นำมาใช้งานอย่างเคร่งครัด (M)

2

คุณสมบัติด้านความมั่นคงปลอดภัย
(Security Functional Requirement)2.1. ความมั่นคงปลอดภัย
(Security)2.1.1. การจัดการข้อมูลที่มีความสำคัญ
(Sensitive Information)

- A. ข้อมูลที่เป็น Sensitive Information ต้องมีการเข้ารหัสเสมอแม้ว่าจะเป็นการเก็บไว้ชั่วคราวในเครื่องของผู้ใช้งานในระบบแม่ข่ายข้อมูลและการส่งข้อมูลผ่านระบบเครือข่ายทั้งหมดเช่นข้อมูลส่วนตัวของผู้ใช้งาน ข้อมูลบัตรเครดิตข้อมูลบัญชีธนาคาร เป็นต้น (M)
- B. เมื่อมีการปิดแอปพลิเคชันต้องพิจารณาไม่ให้เข้าถึงข้อมูลสำคัญ (Sensitive Information) โดยไม่ใส่รหัสผ่านเพื่อยืนยันตัวตนอีกครั้ง แม้ผู้ใช้งานจะยังคงเข้าระบบค้างอยู่ก็ตาม (M)
- C. การแสดงผลต้องมีการแทนข้อมูลจริงด้วยเครื่องหมาย * เสมอโดยแทนทั้งข้อความหรือในกรณีที่ข้อมูลที่ต้องการให้ผู้ใช้งานเห็นบางส่วน ก็จะต้องแทนด้วย * อย่างน้อย 25% ของข้อมูลทั้งหมด (M)

2.1.2. มาตรการรองรับสำหรับความปลอดภัยเมื่ออุปกรณ์สูญหาย (Security on loss devices)

- A ในกรณีที่ระบบรองรับการให้ผู้ใช้งาน 1 คนเข้าสู่ระบบเพื่อใช้งานพร้อมกันได้มากกว่า 1 อุปกรณ์ต้องรองรับการสั่งให้ออกจากระบบพร้อมกันหมดทุกอุปกรณ์ รวมถึงการลบข้อมูลความเป็นส่วนตัวและข้อมูลชั่วคราวทั้งหมดของผู้ใช้งานออกจากเครื่อง (M)

2.1.3. การติดต่อกับระบบแม่ข่ายข้อมูล (Networking)

- A การส่งข้อมูลที่เป็นข้อมูลส่วนตัวของผู้ใช้งานข้อมูลสำคัญ (Sensitive Information) ระหว่างแอปพลิเคชัน และระบบแม่ข่ายข้อมูล ต้องมีการเข้ารหัสข้อมูลเสมอไม่สามารถส่งเป็นข้อความธรรมดา (Plain Text) ได้ (M)
- B การส่งข้อมูลส่วนตัวของผู้ใช้งานต้องทำผ่าน Secure Channel (SSL/TLS) (M)
- C ในการเข้าถึงข้อมูลที่เป็นส่วนตัวของผู้ใช้งานที่เก็บไว้ที่ระบบแม่ข่ายข้อมูล ต้องรับรองว่าเป็นผู้ได้รับอนุญาตในการเข้าถึงเท่านั้น (M)



- D. ต้องพิจารณาข้อมูลสาธารณะ (Public Data) หรือการตอบสนองจาก Public API ที่สามารถเข้าถึงได้จากภายในแอปพลิเคชันโดยไม่มีข้อมูลความเป็นส่วนตัวของผู้ใช้งานและเข้าถึงได้โดยไม่ต้องทำการเข้ารหัสระบบ จึงจะสามารถส่งเป็น Plain Text ที่ไม่ต้องเข้ารหัสได้ (M)

2.1.4. การระบุตัวตนผู้ใช้งาน (Authentication)

- A. แอปพลิเคชันควรรองรับการระบุตัวตนผู้ใช้งานด้วยเทคโนโลยีระบบ ตัวตนแบบใหม่ เช่น OAuth 2.0 แทนการส่งข้อมูลการเข้าใช้งานระบบ (ชื่อบัญชีผู้ใช้งานและรหัสผ่าน) (S)
- B. หากจำเป็นต้องส่งชื่อบัญชีผู้ใช้งานและรหัสผ่านให้จัดการตามวิธีการจัดการข้อมูลที่เป็น Sensitive Information (S)
- C. ควรพิจารณาการระบุตัวตนโดยใช้องค์ประกอบหรือปัจจัยอย่างน้อย 2 อย่าง (2 Factors Authentication) หรือมากกว่านั้น เช่น การทำงานร่วมกับระบบ One-Time Password (OTP) ไปยังหมายเลขโทรศัพท์ที่ได้รับระบุไว้เป็นต้น (S)







> การอ้างอิง

ลำดับ	แหล่งข้อมูล	ประเทศกลุ่ม
1.	Mobile Government แหล่งที่มา : http://www.government.ae/documents/10138/98433/Guidelines_En_mGov_final.pdf	สหรัฐอเมริกาหรับเอมิเรตส์
2.	Enterprise Mobile Application Lifecycle Developing a Process for End to End Mobile Application Development. แหล่งที่มา : http://www.enterprisemanagement360.com/wp-content/files_mf/1341922927entlifecycle.pdf	กลุ่มผู้พัฒนาระดับสากล
3.	Modeling the Mobile Application Development Lifecycle แหล่งที่มา : http://www.iaeng.org/publication/IMECS2014/IMECS2014_pp596-600.pdf	กลุ่มผู้พัฒนาระดับสากล
4.	Smartphone Secure Development Guidelines for App Developers แหล่งที่มา : www.enisa.europa.eu	สหภาพยุโรป

ลำดับ	แหล่งข้อมูล	ประเทศกลุ่ม
5.	Technical Considerations for 5 Vetting 3rd Party Mobile 6 Applications (Draft) แหล่งที่มา : http://csrc.nist.gov/publications/drafts/800-163/sp800_163_draft.pdf	สหรัฐอเมริกา
6.	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components, ISO/IEC 15408-3:2008 แหล่งที่มา : http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413	องค์กรอิสระ
7.	Delivering enterprise information securely on Android, Apple iOS and Microsoft Windows tablets and smart-phones, แหล่งที่มา : http://www.citrix.com/content/dam/citrix/en_us/documents/oth/delivering-enterprise-informati-on-securely.pdf	สหรัฐอเมริกา
8.	The Digital by Default Service Standard แหล่งที่มา : https://www.gov.uk/service-manual/digital-by-default	สหราชอาณาจักร



ลำดับ	แหล่งข้อมูล	ประเทศกลุ่ม
9.	http://en.wikipedia.org/wiki/Iterative_and_incremental_development	สหรัฐอเมริกา
10.	http://www.scrumguides.org/docs/scrumguide/v1/scrum-guide-us.pdf	สหรัฐอเมริกา
11.	http://docs.telerik.com/platform/appbuilder/code-signing-your-app/configuring-code-signing-for-ios-apps/register-app-id	สหรัฐอเมริกา
12.	App Quality Alliance (AQuA) Best Practice Guidelines แหล่งที่มา : http://www.appqualityalliance.org	กลุ่มผู้พัฒนาระดับสากล
13.	Best Practices for Mobile Application Developers. แหล่งที่มา : https://www.cdt.org/files/pdfs/Best-Practices-Mobile-App-Developers.pdf	กลุ่มผู้พัฒนาระดับสากล





สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)(สรอ.)

ชั้น 17 อาคารบางกอกไทยทาวเวอร์

108 ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ 10400