# (ร่าง) มาตรฐานบริการโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย

# บันทึกการปรับปรุงเอกสาร

| ครั้งที่ | วันที่ | รายละเอียด | ผู้ดำเนินการ |
|---|---|---|---|
| 0 | - | เอกสารเริ่มต้น | - |

# คำนำ

ปัจจุบันเทคโนโลยีทางด้านดิจิทัลมีการพัฒนาแบบก้าวกระโดด ทำให้หน่วยงานภาครัฐเร่งพัฒนาบริการทางดิจิทัลให้เข้าถึงประชาชนมากยิ่งขึ้น กอปรกับภัยคุกคามด้านไซเบอร์ที่เกิดขึ้นใหม่ตลอดเวลา ส่งผลให้การบริหารจัดการด้านเทคโนโลยีดิจิทัลมีความซับซ้อนมากขึ้น ในขณะเดียวกันหน่วยงานภาครัฐยังขาดกระบวนการในการบริหารจัดการ IT Infrastructure อย่างมีประสิทธิภาพและเป็นระบบ อีกทั้งบุคลากรภาครัฐมีทักษะและความเชี่ยวชาญไม่เพียงพอในการรับมือกับภัยคุกคามและเทคโนโลยีใหม่ๆ รวมถึงข้อจำกัดของกระบวนการจัดซื้อและการจัดทำงบประมาณ ส่งผลให้ไม่สามารถจัดหาเทคโนโลยีและวิธีการป้องกันภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที นอกจากนี้ค่าใช้จ่ายในการการลงทุนด้านความปลอดภัยทางไซเบอร์มีมูลค่ามากหากแต่ละหน่วยงานเป็นผู้ดำเนินการเอง ดังนั้นเพื่อให้หน่วยงานภาครัฐสามารถให้บริการได้อย่างต่อเนื่อง มีความพร้อมใช้ และมีความมั่นคงปลอดภัย จึงจำเป็นต้องมีมาตรการ แนวทาง ข้อปฏิบัติ และมาตรฐานด้านโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย โดยต้องมีการบังคับใช้และมีการตรวจสอบ เพื่อเป็นการควบคุมคุณภาพให้เกิดประสิทธิภาพและความมั่นคงปลอดภัยอย่างยั่งยืน

โครงสร้างพื้นฐานดิจิทัลที่มีความสำคัญของภาครัฐ ซึ่งใช้ในการดำเนินงานตามภารกิจการให้บริการประชาชน หรือการสนับสนุนการปฏิบัติงานภายในหน่วยงาน มี ๓ องค์ประกอบหลัก คือ ๑) ระบบเครือข่าย ๒) ระบบคลาวด์ และ ๓) ศูนย์ข้อมูล โดยองค์ประกอบเหล่านี้จำเป็นต้องมีความพร้อมใช้ มีความมั่นคงปลอดภัย และดำเนินงานให้สอดคล้องตามมาตรฐานสากล เพื่อให้ระบบบริการของภาครัฐมีความน่าเชื่อถือ สามารถให้บริการแก่ประชาชนได้ตลอดเวลา นอกจากนี้ หน่วยงานภาครัฐสามารถเลือกใช้บริการโครงสร้างพื้นฐานต่างๆ ได้ตามความต้องการและเหมาะสมกับการใช้งานและงบประมาณ รวมถึงต้องมีการพัฒนากระบวนการเพื่อให้เกิดความสะดวกและยืดหยุ่นในการจัดหาบริการจากผู้ให้บริการที่ได้รับการรับรองการดำเนินงานที่มีคุณภาพ อีกด้วย

มาตรฐานฉบับนี้จะมีการจัดแบ่งตามบริการและกระบวนการ เพื่อให้เกิดประสิทธิภาพในการนำไปใช้ โดยมีมาตรฐานต่างๆ ซึ่งเป็นองค์ประกอบดังต่อไปนี้

มาตรฐานบริการเครือข่ายภาครัฐที่มีความมั่นคงปลอดภัย (มรด. 1002)

มาตรฐานบริการคลาวด์ภาครัฐที่มีความมั่นคงปลอดภัย (มรด. 1003)

มาตรฐานบริการศูนย์ข้อมูลภาครัฐที่มีความมั่นคงปลอดภัย (มรด. 1004)

ซึ่งผู้ให้บริการหรือหน่วยงานภาครัฐ สามารถนำมาตรฐานต่างๆ มาประยุกต์ใช้ตามบริการโครงสร้างพื้นฐานดิจิทัลที่มีการให้บริการหรือมีการใช้งาน

# สารบัญ

## 1. ขอบเขต

มาตรฐานบริการโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย เป็นแนวปฏิบัติในการพัฒนาโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัยสำหรับหน่วยงานของรัฐ โดยมาตรฐานนี้จะครอบคลุมถึงบริการด้านโครงสร้างพื้นฐานดิจิทัลซึ่งประกอบด้วย ภาครัฐ รัฐวิสาหกิจ และ เอกชน เพื่อให้หน่วยงานของรัฐได้ใช้บริการโครงสร้างพื้นฐานดิจิทัลภาครัฐมีความมั่นคงปลอดภัย มีคุณภาพ และมีประสิทธิภาพ เป็นไปตามมาตรฐานที่กำหนด ซึ่งเป็นกลไกสำคัญในการส่งมอบบริการที่ดี มีคุณภาพและประสิทธิภาพ ให้แก่ประชาชนต่อไป

## 2. มาตรฐานอ้างอิง

-

## 3. บทนิยาม

3.1 ผู้ให้บริการ (GSI Provider) หมายถึง หน่วยงานที่ผ่านการรับรองตามมาตรฐานบริการ ด้านเครือข่าย ด้านระบบคลาวด์ หรือด้านศูนย์ข้อมูล อย่างใดอย่างหนึ่ง หรือทั้งหมด ซึ่งให้บริการแก่หน่วยงานของรัฐ

3.2 หน่วยงานกลาง (Government Intranet eXchange : GIX) หมายถึง หน่วยงานที่เชื่อมโยงเครือข่ายระหว่างผู้ให้บริการ และเป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลของหน่วยงานรัฐ

3.3 ผู้ตรวจสอบ (GSI Conformity Assessment Body : GCAB) หมายถึง หน่วยงานที่มีหน้าที่ตรวจสอบและรับรองมาตรฐานการให้บริการ

3.4 บริการโครงสร้างพื้นฐานดิจิทัลภาครัฐ หมายถึง บริการด้านเครือข่าย ระบบคลาวด์ และ ศูนย์ข้อมูล อย่างใดอย่างหนึ่ง หรือทั้งหมด ซึ่งให้บริการแก่หน่วยงานของรัฐ

3.5 บัญชีผู้ให้บริการ (GSI Provider List) หมายถึง บัญชีรวบรวมผู้ให้บริการโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีการดำเนินการได้ตามมาตรฐาน และได้รับการรับรองจากผู้ตรวจสอบ

3.6 อินเทอร์เน็ตภาครัฐ (Government Internet) หมายถึง การบริการอินเทอร์เน็ตแก่หน่วยงานของรัฐจากผู้ให้บริการ โดยมีมาตรฐานในการดำเนินการ มีความมั่นคงปลอดภัย เป็นไปตามข้อกำหนด

3.7 อินทราเน็ตภาครัฐ (Government Intranet) หมายถึง การบริการเชื่อมโยงเครือข่ายระหว่างหน่วยงานของรัฐจากผู้ให้บริการ เพื่อใช้ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐ โดยมีมาตรฐานในการดำเนินการ มีความมั่นคงปลอดภัย เป็นไปตามข้อกำหนด

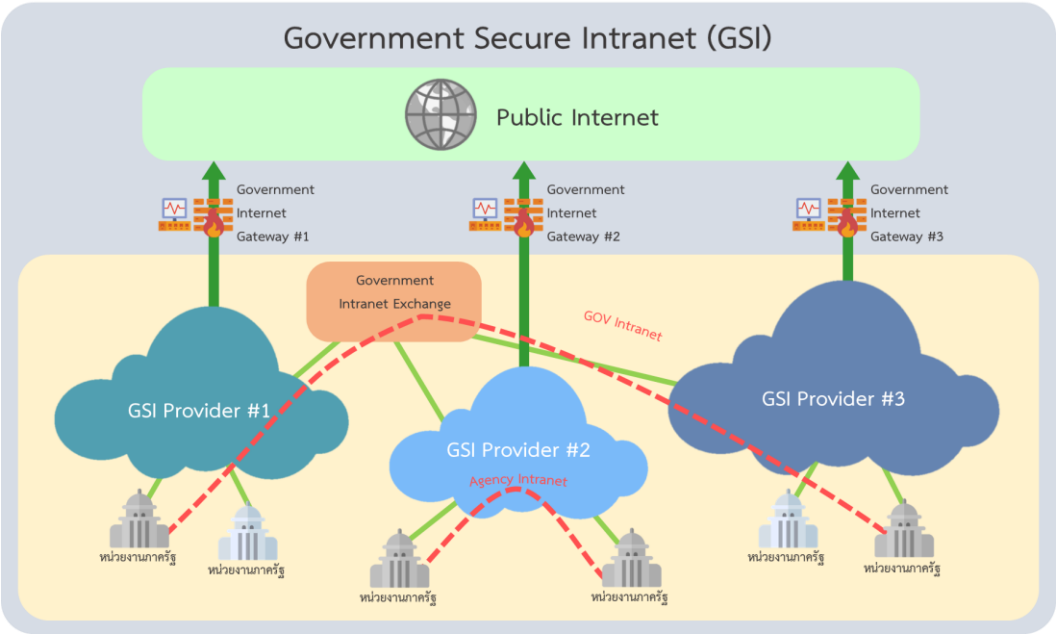
3.8 อินทราเน็ตหน่วยงาน (Agency Intranet) หมายถึง การบริการเครือข่ายระหว่างสาขาหน่วยงานของรัฐ หรือบริการเชื่อมโยงเครือข่ายเฉพาะภารกิจใดๆ จากผู้ให้บริการ เพื่อใช้ในการแลกเปลี่ยนข้อมูลภายในหน่วยงาน หรือแลกเปลี่ยนระหว่างหน่วยงานในภารกิจนั้นๆ โดยมีมาตรฐานในการดำเนินการ มีความมั่นคงปลอดภัย เป็นไปตามข้อกำหนด

## 4. ข้อกำหนดให้ดำเนินการตามมาตรฐาน

เอกสารฉบับนี้จะมีการใช้คำต่างๆ เพื่อบ่งถึงระดับของความจำเป็นและความต้องการในการปฏิบัติตามมาตรฐาน ซึ่งหากในข้อใด กำหนดให้ผู้ขอรับการรับรองต้องดำเนินการอย่างเคร่งครัดจะจะมีข้อความดังนี้ปรากฏอยู่ “จำเป็นต้อง” “ต้อง” “ห้ามมิให้” และ “ห้าม” ส่วนข้อกำหนดใดควรดำเนินการ จะมีข้อความดังนี้ปรากฏอยู่ “ควร” และ “ไม่ควร” ส่วนข้อกำหนดใดถือเป็นส่วนเสริมซึ่งอาจมีการดำเนินการหรือไม่ก็ได้ โดยข้อกำหนดเหล่านี้จะมีข้อความ “อาจ” และ “เพิ่มเติม” ปรากฏอยู่

ข้อกำหนดที่ผู้ขอรับการรับรองต้องดำเนินการอย่างเคร่งครัดนั้น จะมีสัญลักษณ์ “[R]” ส่วนข้อกำหนดที่ควรดำเนินการนั้น จะมีสัญลักษณ์ “[D]” และ ข้อกำหนดส่วนเสริมเพิ่มเติม จะมีสัญลักษณ์ “[O]”

## 5. สถาปัตยกรรมโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย




โครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย มีโครงสร้างหลักในการดำเนินการ ๓ ด้าน คือ ด้านเครือข่าย ระบบคลาวด์ และศูนย์ข้อมูล ซึ่งให้บริการโดยผู้ให้บริการที่ได้รับการรับรองมาตรฐานและได้รับการขึ้นบัญชีผู้ให้บริการเป็นที่เรียบร้อยแล้ว โดยผู้ให้บริการจะต้องได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบพร้อมทั้งมีการกำหนดรอบการทบทวนเพื่อให้เกิดความต่อเนื่องในการดำเนินการ ทั้งนี้ผู้ให้บริการจะต้องดำเนินการเชื่อมโยงเครือข่ายเพื่อรองรับบริการ สำหรับ อินเทอร์เน็ตภาครัฐ อินทราเน็ตภาครัฐ และ อินทราเน็ตหน่วยงาน รวมถึงต้องดำเนินการเชื่อมต่อเครือข่ายไปยังหน่วยงานกลาง เพื่อแลกเปลี่ยนข้อมูลภาครัฐระหว่างผู้ให้บริการด้วย

## 6. ข้อกำหนดทั่วไปของผู้ให้บริการ

6.1. ผู้ให้บริการต้องเป็นหน่วยงานของรัฐหรือเป็นนิติบุคคลซึ่งจดทะเบียนประกอบธุรกิจในประเทศไทย [R]

6.2. ผู้ให้บริการต้องให้บริการโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย อย่างใดอย่างหนึ่งหรือให้บริการทั้งหมด ดังต่อไปนี้ [R]

- การให้บริการเครือข่ายที่มีความมั่นคงปลอดภัยสำหรับหน่วยงานภาครัฐ
- การให้บริการระบบคลาวด์ที่มีความมั่นคงปลอดภัยสำหรับหน่วยงานภาครัฐ
- การให้บริการศูนย์ข้อมูลที่มีความมั่นคงปลอดภัยสำหรับหน่วยงานภาครัฐ

6.3. ผู้ให้บริการต้องปฏิบัติตามและได้รับการตรวจประเมินมาตรฐานบริการโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย ให้สอดคล้องกับบริการตามข้อ ๓.๑ ดังต่อไปนี้ [R]

- บริการเครือข่าย ให้ปฏิบัติตาม มาตรฐานบริการเครือข่ายภาครัฐที่มีความมั่นคงปลอดภัย (DGS 1002)
- ผู้ให้บริการต้องปฏิบัติตามกฎหมายด้านต่างๆ ที่เกี่ยวข้อง โดยเฉพาะ [R]
- กฎหมายที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ
- กฎหมายด้านโทรคมนาคม

6.4. ผู้ให้บริการต้องได้รับการรับรองมาตรฐานสากลในการให้บริการ โดยมีขอบเขตครอบคลุมถึงบริการโครงสร้างพื้นฐานดิจิทัลที่ให้บริการแก่หน่วยงานภาครัฐและใบรับรองมาตรฐานนั้นต้องไม่สิ้นอายุ [R]

- มาตรฐานด้านการให้บริการเทคโนโลยีสารสนเทศ (IT Service Management System: ISO/IEC 20000)
- มาตรฐานด้านการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: ISO/IEC 22301)
- มาตรฐานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISO/IEC 27001)

**7. ข้อกำหนดด้านการบริการ**

7.1. ผู้ให้บริการต้องคิดอัตราค่าใช้บริการไม่เกินกำหนดราคากลาง หรือตามหลักเกณฑ์หรือตามกฎหมายกำหนด โดยมีรูปแบบเป็นการจ่ายค่าบริการตามการใช้งานจริง (Pay-Per-Use) [R]

7.2. ผู้ให้บริการต้องมีระบบสำหรับตรวจสอบ เฝ้าระวัง แจ้งเตือนเพื่อป้องกันปัญหาที่อาจส่งผลกระทบต่อการให้บริการ [R]

7.3. ผู้ให้บริการต้องให้คำปรึกษา รับแจ้งเหตุขัดข้อง ตรวจสอบและแก้ไขปัญหาต่างๆ ต่อผู้ใช้บริการ [R]

7.4. ผู้ให้บริการต้องมีช่องทางในการประสานงานกับผู้ใช้บริการตลอดระยะเวลาการใช้บริการ ๒๔ ชั่วโมงใน ๑ วัน ผ่านช่องทางโทรศัพท์ อีเมล และระบบบริการตนเอง ได้เป็นอย่างน้อย [R]

7.5. ผู้ให้บริการต้องมีระบบบริการตนเองในรูปแบบออนไลน์ (Online Self-Services) สำหรับผู้ใช้บริการ โดยผู้ใช้บริการสามารถตรวจสอบข้อมูลและดำเนินการต่างๆ ได้ [R]

7.5.1. ผู้ใช้บริการสามารถเรียกดูข้อมูลพื้นฐานของหน่วยงาน เช่น ชื่อหน่วยงาน ข้อมูลผู้ประสานงาน และ ช่องทางการติดต่อกับหน่วยงาน เป็นต้น [R]

7.5.2. ผู้ใช้บริการสามารถเรียกดูข้อมูลบริการ เช่น รายละเอียดบริการที่ใช้งาน ระยะเวลาเริ่มต้นและสิ้นสุดบริการ ระดับข้อตกลงในการให้บริการ และ บริการเสริมที่ใช้งาน เป็นต้น [R]

7.5.3. ผู้ใช้บริการสามารถเรียกดูข้อมูลค่าใช้จ่าย เช่น ข้อมูลค่าใช้จ่ายของบริการในปัจจุบันและข้อมูลค่าใช้จ่ายของบริการย้อนหลัง เป็นต้น [R]

7.5.4. ผู้ใช้บริการสามารถเรียกดูข้อมูลด้านความมั่นคงปลอดภัยสารสนเทศ เช่น การโจมตีทางไซเบอร์ ภัยคุกคาม ไวรัส หรือ มัลแวร์ ต่างๆ [R]

7.5.5. ผู้ใช้บริการสามารถดำเนินการขอใช้บริการ เช่น การขอใช้บริการใหม่ และ การขอใช้บริการเสริม เป็นต้น [R]

7.5.6. ผู้ใช้บริการสามารถดำเนินการขอเปลี่ยนแปลงบริการ เช่น การปรับความเร็วสัญญาณอินเทอร์เน็ต หรือ การปรับทรัพยากรสำหรับระบบคลาวด์ เป็นต้น [R]

7.5.7. ผู้ใช้บริการสามารถดำเนินการขอยกเลิกบริการ เช่น การขอยกเลิกบริการปัจจุบัน และการขอยกเลิกบริการเสริม เป็นต้น [R]

7.5.8. ผู้ใช้บริการสามารถดำเนินการแจ้งเหตุขัดข้อง แก้ไขปัญหา พร้อมทั้งติดตามสถานะความก้าวหน้าในการดำเนินการ [R]

7.5.9. ผู้ใช้บริการสามารถดำเนินการเรียกดูรายงานสรุปข้อมูลและการดำเนินการต่างๆ ข้างต้นได้ด้วยตนเอง [R]

7.5.10. ผู้ใช้บริการสามารถดำเนินการอื่นๆ [O]

7.6. ผู้ให้บริการต้องรายงานข้อมูลการใช้งานบริการต่างๆ ตามที่หน่วยงานกลางร้องขอ [R]

## 8. ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

8.1. ผู้ให้บริการต้องมีกระบวนการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของระบบที่ให้บริการเพื่อป้องกันปัญหาที่เกิดจากช่องโหว่บนระบบ [R]

8.2. ผู้ให้บริการต้องมีระบบรักษาความมั่นคงปลอดภัยสารสนเทศ
พร้อมทั้งบุคลากรในการเฝ้าระวังและให้ความช่วยเหลือในกรณีเกิดเหตุ และภัยคุกคามทางไซเบอร์ [R]

## 9. ข้อกำหนดด้านบุคลากร

9.1. บุคลากรที่เกี่ยวข้องกับการให้บริการต้องได้รับใบรับรอง (Certification) ความรู้ความสามารถด้านเทคนิคซึ่งเป็นที่ยอมรับ ในด้านการบริหารจัดการ การปรับแต่งและตั้งค่าระบบการให้บริการ [R]

- ด้านระบบเครือข่าย (Network)
- ด้านระบบคลาวด์ (Cloud)
- ด้านระบบศูนย์ข้อมูล (Data Center)
- ด้านความมั่นคงปลอดภัย (Security)

9.2. บุคลากรที่เกี่ยวข้องกับการให้บริการต้องได้รับการตรวจสอบประวัติอาชญากรรม [R]

9.3. บุคลากรที่เกี่ยวข้องกับการให้บริการต้องลงนามในข้อตกลงไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) ผู้ใช้บริการ ต่อหน่วยงานผู้ให้บริการ [R]

**10. ข้อกำหนดด้านระดับการให้บริการ**

10.1. ผู้ให้บริการต้องดำเนินการให้สอดคล้องกับข้อกำหนดด้านระดับความพร้อมในการให้บริการ (Service Availability) สำหรับการให้บริการโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย [R]

10.2. ผู้ให้บริการต้องดำเนินการให้สอดคล้องกับข้อกำหนดด้านระดับความน่าเชื่อถือในการให้บริการ (Service Reliability) สำหรับการให้บริการโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย [R]

10.3. ผู้ให้บริการควรมีการกำหนดข้อยกเว้นในการให้บริการ (Service Exclusion) สำหรับการให้บริการโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย อย่างชัดเจนและแจ้งให้ทราบทั่วกัน [D]

**11. ข้อกำหนดด้านการตรวจสอบและการรับรอง**

11.1. ผู้ตรวจสอบต้องดำเนินการตรวจประเมินผู้ให้บริการตามมาตรฐานบริการโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัยตามการร้องขอของผู้ให้บริการ และ/หรือ ดำเนินการตรวจประเมินผู้ให้บริการตามระยะควบคุม ไม่เกิน ๑ ปี นับจากวันที่ได้รับการรับรอง [R]

11.2. ผู้ตรวจสอบต้องดำเนินการตรวจสอบเอกสารหลักฐานและข้อมูลเชิงเทคนิคของผู้ให้บริการที่เกี่ยวข้องกับบริการตามมาตรฐาน [R]

11.3. ผู้ตรวจสอบต้องดำเนินการให้การรับรองการดำเนินการตามมาตรฐานของผู้ให้บริการพร้อมทั้งรายงานต่อหน่วยงานกลางเพื่อจัดทำบัญชีผู้ให้บริการ (GSI Provider List) [R]

11.4. ผู้ให้บริการต้องอนุญาตให้ผู้ตรวจสอบสามารถเข้าตรวจสอบกระบวนการทำงาน ระบบงาน สถานที่ อุปกรณ์ และหลักฐานต่างๆ ที่เกี่ยวข้องในการให้บริการ ตามที่หน่วยงานกลางเป็นผู้กำหนด [R]

**12. ข้อกำหนดด้านการคัดเลือกผู้ตรวจสอบและผู้ให้บริการ**

12.1. หน่วยงานกลางต้องดำเนินการคัดเลือกผู้มีคุณสมบัติในการตรวจสอบผู้ให้บริการเพื่อตรวจประเมินตามมาตรฐาน หรือให้ดำเนินการด้านการตรวจประเมินตามมาตรฐานสากล

12.2. หน่วยงานกลางต้องดำเนินการคัดเลือกผู้ให้บริการที่ได้รับการรับรองจากผู้ตรวจสอบแล้วจัดทำบัญชีผู้ให้บริการเพื่อให้หน่วยงานภาครัฐสามารถเลือกใช้บริการจากผู้ให้บริการตามบัญชีดังกล่าว

12.3. หน่วยงานกลางต้องดำเนินการเพิกถอนรายชื่อผู้ให้บริการจากบัญชีผู้ให้บริการหากผู้ให้บริการไม่ได้รับการรับรองจากผู้ตรวจสอบ

**13. ข้อกำหนดด้านการใช้บริการ**

13.1. หน่วยงานของรัฐต้องใช้บริการจากผู้ให้บริการซึ่งได้รับการบันทึกชื่อในบัญชีผู้ให้บริการ

13.2. หน่วยงานของรัฐที่เป็นผู้ใช้บริการต้องมีการตรวจสอบการใช้บริการจากระบบบริการตนเองของผู้ให้บริการ

13.3. หน่วยงานของรัฐที่เป็นผู้ใช้บริการต้องมีการรายงานผลการใช้บริการ การใช้งบประมาณ รวมถึงข้อมูลต่างๆ ให้แก่หน่วยงานกลางทราบ เป็นรายเดือนตามช่วงระยะเวลาการใช้บริการ

# ภาคผนวก

**ภาคผนวก ก. ตัวอย่างแนวทางการจัดทำระบบบริการตนเอง (Online Self-Services)**

1. การขอปรับเปลี่ยนบริการ
    1.1. ผู้ใช้บริการเข้าสู่ระบบบริการตนเองของผู้ให้บริการ
    1.2. ผู้ใช้บริการเลือกหัวข้อ “การปรับเปลี่ยนบริการ” จากช่องทางลัดในส่วนท้ายของแต่ละบริการที่ใช้งานจากผู้ให้บริการ หรือจากรายการหลัก
    1.3. ผู้ใช้งานเลือกปรับปรุงทรัพยากรตามความต้องการ ซึ่งหากการขอปรับปรุงทรัพยากรมากเกินกว่าที่ผู้ให้บริการสามารถให้บริการได้ ต้องมีการแจ้งเตือนอย่างชัดเจน
    1.4. ผู้ใช้บริการส่งคำร้องในการปรับปรุงทรัพยากรไปยังผู้ให้บริการ
    1.5. ผู้ให้บริการดำเนินการตรวจสอบคำร้อง ปริมาณทรัพยากร และค่าใช้จ่าย
    1.6. เมื่อผู้ให้บริการดำเนินการตรวจสอบตามรายการที่ ๑.๕ แล้ว ให้ดำเนินการแจ้งยืนยันการปรับเปลี่ยนทรัพยากรกลับไปยังผู้ให้บริการ โดยประกอบด้วย ผลการร้องขอ การยืนยันปริมาณทรัพยากรที่ต้องการ และค่าใช้จ่ายที่เพิ่มขึ้นหรือลดลง
    1.7. ผู้ใช้บริการต้องทำการยืนยันเพื่อรับทราบการเปลี่ยนแปลงทรัพยากรและค่าใช้จ่าย
    1.8. เมื่อผู้ใช้บริการยืนยันแล้ว ผู้ให้บริการต้องมีการส่งคำร้องเพื่อดำเนินการปรับเปลี่ยนทรัพยากร แจ้งความคืบหน้าของการดำเนินการตลอดจนแจ้งผลการดำเนินการเมื่อดำเนินการแล้วเสร็จให้แก่ผู้ใช้บริการ