**แบบฟอร์มแนวคิดของโครงการจัดหา[[1]](#footnote-1)ระบบโปรแกรมคอมพิวเตอร์**

**(Application and Digital Solution)**

**ประกอบการเสนอโครงการจัดหาระบบคอมพิวเตอร์ กระทรวงสาธารณสุข**

***โปรดให้ข้อมูลให้ครบทุกข้อ และใส่เครื่องหมาย*** [✓] ***ในข้อที่เลือกข้อ***

**ชื่อหน่วยงาน**…………………………………………………………………**รหัสหน่วยงาน (5 หลัก)** ………………….................. **สังกัด**.......................................................................................................................................................................

**ชื่อระบบ/Application** .......................................................................................................................................

...............................................................................................................................................................................

**1. กรอบการพิจารณา**

**1.1 ข้อมูลทั่วไปของโครงการ** ประกอบด้วย

 1.1.1 สรุปสาระสำคัญ/รายละเอียดของการจัดหาระบบ ....................................................................

...............................................................................................................................................................................

...............................................................................................................................................................................

 1.1.2 วัตถุประสงค์ของการพัฒนาระบบ ...............................................................................................

 1.1.3 เป้าหมายของโครงการ (Goal) …....................................................................................................

1.1.4 ผลลัพธ์ที่ต้องการ (Outcomes) …................................................................................................

1.1.5 ผลผลิต ของโครงการ (Output) …................................................................................................

1.1.6 ตัวชี้วัดผลสัมฤทธิ์ของโครงการ (KPI) …..........................................................................................

**1.2 ขอบเขตของโครงการ**

[ ] กระบวนงานภายในหน่วยงาน เช่น Queue, HIS , Back Office เป็นต้น

[ ] กระบวนงานระหว่างหน่วยงาน (เช่น ระบบ Refer ส่งผู้ป่วยรักษาต่อเนื่อง)

[ ] กระบวนงานนอกหน่วยงาน เช่น การดูแลในชุมชน ดูแลที่บ้าน ดูแลรายบุคคลนอกโรงพยาบาล,

 การทำ survey, Screening

[ ] กระบวนงานอื่นๆ เช่นบริการ การเชื่อมโยงข้อมูลสุขภาพ (โปรดอธิบายรายละเอียด)......................

...............................................................................................................................................................................

...............................................................................................................................................................................

**1.3 ผู้มีส่วนได้เสีย (Stakeholder) หรือผู้ที่ได้รับผลกระทบ** (โปรดระบุรายละเอียด)

 [ ] หน่วยงานภายใน (ในสังกัดเดียวกัน)...........................................................................................................

 [ ] หน่วยงานภาคนอก (นอกสังกัด) ................................................................................................................

 [ ] ภาคส่วนอื่น (เช่น ภาคเอกชน) .................................................................................................................

 [ ] ภาคประชาสังคม ......................................................................................................................................

**2. มิติของการพิจารณาลงทุนระบบโปรแกรมคอมพิวเตอร์**

หลักการตาม Public Service Governance Framework ที่หน่วยงานควรพิจารณาเพื่อให้การลงทุนระบบโปรแกรมคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพ และเป็นประโยชน์ต่อหน่วยงานอย่างยั่งยืน แบ่งเป็น 3 ระยะ

**2.1 ระยะที่ 1** **การพัฒนาระบบ (Development phase)**

**2.1.1 Environment (ปัจจัยหรือสิ่งแวดล้อม) ของการพัฒนา**

 - OS (ระบบปฏิบัติการที่ใช้ในการพัฒนา เช่น Linux, Windows, IOS, Android ........................

 - Database (เช่น MySQL, PostgreSQL)....................................................................................

 - Development Tool (เช่น ภาษาหรือเครื่องมือที่ใช้ในการพัฒนา, Framework)......................

- เมื่อส่งมอบ ผลิตภัณฑ์ แล้วต้องมีภาระค่าใช้จ่ายผูกพันอีกกี่ปี................... จำนวนเงิน……….บาท

- เงื่อนไขและระยะเวลารับประกันรวมถึงการ Update ระบบ.…...............................................…

- SLA[[2]](#footnote-2) ในการแก้ไข update ระบบ…………....................................................................……………

 **2.1.2 ต้นทุนในการพัฒนาระบบ (Development cost)**

ให้แสดงรายละเอียดในแบบบัญชีราคากลางงานจัดหาระบบแบบได้กรรมสิทธิ์ ประกอบด้วย ค่าใช้จ่ายบุคลากรที่ใช้ในการพัฒนาระบบ, ค่าใช้จ่ายครุภัณฑ์คอมพิวเตอร์ที่ใช้ในการพัฒนาระบบ, ค่าใช้จ่ายซอฟต์แวร์และเครื่องมือที่ใช้ในการพัฒนาระบบ, ค่าที่ปรึกษาโครงการ หรือผู้เชี่ยวชาญเฉพาะทางที่ใช้ในการจัดหาระบบ, ค่าใช้จ่ายที่เกิดขึ้นทุกเดือนตลอดระยะเวลาโครงการ, ค่าใช้จ่ายอื่นๆ ที่ใช้ในการดำเนินโครงการ

**2.2. ระยะที่ 2** **การติดตั้งใช้งานระบบ (Implementation & Operational Phase)**

2.2.1 หน่วยงานที่เป็นเจ้าของกิจการ (Business Operation) .................................................................

 2.2.2 หน่วยงานที่เป็นผู้ให้บริการระบบ (IT Operation) .........................................................................

 2.2.3 งบประมาณและค่าใช้จ่ายในการดำเนินการ

ให้แสดงรายละเอียดในแบบบัญชีราคากลางงานจัดหาระบบแบบไม่ได้กรรมสิทธิ์ ประกอบด้วย ค่าซอฟต์แวร์ระบบ, ค่าใช้จ่ายบุคลากรที่ใช้ในการให้บริการประกอบการส่งมอบระบบ, ค่าใช้จ่ายครุภัณฑ์คอมพิวเตอร์ประกอบการส่งมอบระบบ, ค่าใช้จ่ายซอฟต์แวร์และเครื่องมือประกอบการส่งมอบระบบ, ค่าใช้จ่ายที่เกิดขึ้นทุกเดือน/ปี ตลอดระยะเวลาโครงการ, ค่าใช้จ่ายอื่นๆ ที่ใช้ในการดำเนินโครงการ

2.2.4 ระบุระยะเวลาของการดำเนินการ…………………ระยะเวลา................ปี.................เดือน...............…...

**2.3 ระยะที่ 3** **การ****บำรุงรักษา (Sustainability & Maintenance phase)**

 **2.3.1 มีแผนการดูแลและพัฒนาต่อเนื่องอย่างไร และโปรดระบุที่มาของแหล่งรายได้ในการหล่อเลี้ยงโครงการนี้** .................................................................................................................................................................

...................................................................................................................................................................................

...................................................................................................................................................................................

...................................................................................................................................................................................

 **2.3.2 มีแผนการพัฒนาต่อยอดการใช้งานระบบหรือไม่**

[ ] มี ภายในระยะ.....ปี ค่าใช้จ่าย..... แหล่งงบประมาณ.......

[ ] ไม่มี

 **2.3.3 มีข้อตกลงในการประกันคุณภาพการบริการอย่างไร**

 SLA ของระบบ………………....................................................................................................................

 **2.3.4 มีแผนรองรับการขยายการบริการที่ Workload เพิ่มขึ้นอย่างไร (Infrastructure scaling up)**

 - ค่า Hardware …………………………………………………………………….………………………………………………

 - ค่า Network……………………………………………………….................…………………………………………….....

 - SLA ของ Infrastructure ……………………………………………………...........………………………………….....

 - System Redundancy…………………………………………………………………...............………………………

 - ค่าบริการรายปี………………………………………………………………………………………..................................

 **2.4 มีแผนการลงทุนซ้ำอย่างไร (Re-Investment) เมื่ออุปกรณ์หมดอายุการใช้งาน**

 2.4.1 ระบุ งบประมาณและแหล่งงบประมาณ รายปี ปีถัดไปจนครบอายุโครงการ………………………………..

 2.4.2 ระบุ ระยะเวลาของการใช้งานตลอดโครงการ……………………………………………………………………………

**2.5 มีแผนการเพิ่มผู้ใช้งานอย่างไร แผนและค่าใช้จ่ายทางการตลาด (Marketing Cost)**

 ค่าใช้จ่ายทางการตลาด (Marketing Cost) รวม ......................................................................................

 2.5.1 แผนการสื่อสารประชาสัมพันธ์…….................................................…………………………………………...

 2.5.2 แผนการเพิ่มจำนวนผู้ใช้…………………………………………….................................................................

 2.5.3 แผนการปรับปรุงประสิทธิภาพ Hardware & Network ให้รองรับกับใช้งาน…………………………….

**2.6 ลิขสิทธิ์และการอ้างสิทธิในระบบ**

ให้แสดงรายละเอียดในแบบฟอร์มการบริหารจัดการสิทธิและผลประโยชน์ที่เกี่ยวข้อง

**3. มิติของการจัดการเรื่องอำนาจหน้าที่และความรับผิดชอบ (Governance) สำหรับภาครัฐ ให้ปฏิบัติตามแนวทางของ พ.ร.บ. บริหารงานและให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562**

 **3.1 หน่วยงานหรือองค์กรที่รับผิดชอบ** (โปรดแสดงหลักฐานอำนาจหน้าที่ตามกฎหมายที่เกี่ยวข้องกับภารกิจ)

3.1.1 หน่วยงานที่เป็นเจ้าของระบบ (System Owner) ..................................................……….………………

3.1.2 หน่วยงานเจ้าของกิจการ​ (Business Owner) …...................................................……….……………….

3.1.3 หน่วยงานรับผิดชอบให้บริการระบบ (Operation Unit) ……………………………………….................……

 **3.2 ผู้รับผิดชอบสูงสุดของหน่วยงานหรือโครงการนี้** (พร้อมแนบหลักฐานคำสั่งและอำนาจหน้าที่ตามกฎหมาย)

 3.2.1 ผู้บริหารหน่วยงานสูงสุด (CEO) ....…………………………………………………………..…..…………….......……

 3.2.2 ผู้รับผิดชอบโครงการสูงสุด (CIO) ....…………………………………………..………………..…………….......……

 **3.3 ผู้ใช้งาน หรือผู้มีส่วนเกี่ยวข้อง**

3.3.1 แจกแจงหน่วยงานที่ใช้งาน (End Point Unit)....…………………………………………..…………….......……

3.3.2 ผู้ใช้งาน (Target User)​ กลุ่ม​เป้าหมายเป็นใคร ระบุ……….........................…………จำนวน…….…….

3.3.3 จำนวน Concurrent User สูงสุดที่ต้องการ…………………....................................................…………

 3.3.4 ผู้เกี่ยวข้องอื่นๆ ..................................................................................................................................

**4. ความสอดคล้องกับกฎหมายดิจิทัลที่เกี่ยวข้อง** อย่างน้อยได้แก่

 **4.1 พ.ร.บ. บริหารงานและให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 เช่น**

 [ ] มีการกำหนดผู้รับผิดชอบสูงสุด (Accountable) ในการบริหารจัดการระบบและมีการกำหนดนโยบายและแนวปฏิบัติที่ชัดเจนในการบริหารจัดการระบบสารสนเทศได้แก่ CEO , CIO, CDO, CISO

 [ ] มีการกำหนดสิทธิ หรือคำสั่งในการมอบหมายสิทธิ หน้าที่ และความรับผิดชอบในการปฏิบัติที่ชัดเจนและมีการตรวจสอบว่าคำสั่งนั้นยังมีผลต่อการปฏิบัติอย่างสม่ำเสมอ

 [ ] มีการกำหนดแนวทางในการบริหารจัดการข้อมูลให้เป็นไปตามรูปแบบที่เหมาะสมตามแนวทางของ Data Governance

**4.2 พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เช่น**

 [ ] มีการดำเนินการตาม "ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.2564"

#  [ ] มีการดำเนินการตาม "นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565 "

#  [ ] มีความพร้อมในการขึ้นทะเบียนสารสนเทศกับหน่วยงานกำกับดูแล

#  ระบุ Regulator ……………………………………………………………………………………………….

#  [ ] มีแนวทางการแจ้งภัยคุกคาม ตามมาตรา 58

#  4.3 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่น

#  [ ] มีแนวทางการจัดทำ Data Flow ตาม Data Lifecycle ของระบบสารสนเทศ

#  [ ] มีแนวทางการจัดทำ ROPA (Record of Processing Activity) ตามมาตรา 39

#  [ ] มีแนวทางการจัดทำ Privacy Notice ตามมาตรา 23

#  [ ] มีการตรวจสอบและแน่ใจว่ามีฐานอำนาจ ตามมาตรา 24 และ 26

#  [ ] มีแนวทางการบริหารจัดการเรื่อง Data Controller, Data Processor ตามมาตรา 6 มีการจัดทำ DPA, DSA และเป็นไปตาม นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของกระทรวงสาธารณสุข

#  [ ] มีการแต่งตั้ง DPO ตามมาตรา 41

#  [ ] มีแนวทางการแจ้งการละเมิดข้อมูลส่วนบุคคล ตามมาตรา 37(4)



 ตัวย่าง Data Flow ตาม Data Lifecycle

**4.4 พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม เช่น**

 [ ] ระบบสารสนเทศที่จะให้บริการ จะมีการดำเนินการเพื่อให้ได้การรับรองมาตรฐาน ISO/IEC 27001, ISO/IEC 27799 เป็นอย่างน้อย

 [ ] มีมาตรฐานในการพิสูจน์ตัวตน ยืนยันตัวตน เป็นไปตามประกาศของ สพธอ.

 [ ] มีการทำธุรกรรมอิเล็กทรอนิกส์ แบบ ปลอดภัยและน่าเชื่อถือ

 [ ] ผู้รับจ้างในการพัฒนา Software จะมีการดำเนินการเพื่อให้ได้การรับรองมาตรฐาน ISO/IEC 29110 เป็นอย่างน้อย

**4.5 พ.ร.บ. ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม เช่น**

 [ ] มีการเก็บรักษาข้อมูลการจราจรทางคอมพิวเตอร์ (Event Log) และ Database Log ไว้อย่างน้อย 90 วัน

**5. มิติของการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection)**

โครงการนี้มีการรวบรวมข้อมูลส่วนบุคคลทั่วไป หรือ ข้อมูลส่วนบุคคลอ่อนไหวหรือไม่ ถ้ามีโปรดแสดงอำนาจหน้าที่ตามกฎหมาย

 **5.1 ผู้รับผิดชอบในการคุ้มครองข้อมูลส่วนบุคคล**

 5.1.1 ผู้ควบคุม​ข้อมูล (Data Controller)​ …………………………..........................................................

 5.1.2 ผู้ประมวลผลข้อมูล (Data Processer)​ ………………………….....................................................

 5.1.3 มีกระบวนการตรวจสอบความพร้อมผู้ประมวลผลข้อมูลอย่างไร……………..……………..............

 5.1.3 มีข้อตกลงการประมวลผล (DPA) หรือไม่ [ ] มี [ ] ไม่มี

 5.1.4 ผู้บริหารข้อมูลระดับสูง (CDO) ....…………………………………………..………......…….....................

 5.1.5 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ....…………………………………………..…………….......…

 **5.2 การจัดการข้อมูลส่วนบุคคลทั่วไป (ตาม ม.24 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)**

 5.2.1 การประมวลผล

 [ ] รวบรวม [ ] ใช้

 [ ] เผยแพร่ ให้กับ ....…………………….................................……………………..…………….......……

 มีข้อตกลงในการเปิดเผยข้อมูล (DSA) หรือไม่? [ ] มี [ ] ไม่มี

 5.2.2 ฐานอำนาจในการดำเนินการ (Lawful Basis**)**

[ ] ใช้ฐานยินยอม

 [ ] ใช้ฐานกฎหมาย โปรดระบุว่าใช้ฐานอำนาจใดตาม ม.24 และโปรดแสดงหลักฐานแห่งอำนาจหน้าที่นั้น………………………………………………........……………………………………………………………………………………………*……………..*

 **5.3 การจัดการข้อมูลส่วนบุคคลอ่อนไหว** (ตาม ม.26 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

 5.3.1 การประมวลผล

 [ ] รวบรวม [ ] ใช้

 [ ] เผยแพร่ ให้กับ ....…………………………………………..……………......

 มีข้อตกลงในการเปิดเผยข้อมูล (DSA) หรือไม่. [ ] มี [ ] ไม่มี

 5.3.2 ฐานอำนาจในการดำเนินการ (Lawful Basis**)**

[ ] ใช้ฐานยินยอม

 [ ] ใช้ฐานกฎหมาย โปรดระบุว่าใช้ฐานอำนาจใดตาม ม.26 และโปรดแสดงหลักฐานแห่งอำนาจหน้าที่นั้น

………………………..………………………………………………………………………………………………..................................

**5.4 มีแผนในการทำลายข้อมูลส่วนบุคคล** [ ] ไม่มี [ ] มี ระบุระยะเวลาที่เก็บไว้ จำนวน................... ปี

**5.5 มีการประเมินความเสี่ยงเกี่ยวกับข้อมูลส่วนบุคคลอย่างไร** (Risk Assessment)......................................................................................................................................................................................

......................................................................................................................................................................................

 **5.6 มีแนวทางการบริหารเพื่อให้มีการปฏิบัติตามกฎเกณฑ์และกฎหมายที่เกี่ยวข้องอย่างไร** (Compliance Management) ..........................................................................................................................................................

......................................................................................................................................................................................

 **5.7 มีมาตรการรับมือเมื่อเกิดการละเมิดหรือข้อมูลส่วนบุคคลรั่วไหลอย่างไร** (Breach Response) .....................................................................................................................................................................................

**6. มิติของการจัดการเรื่อง ความมั่นคงปลอดภัยไซเบอร์**

 **6.1 ผู้รับผิดชอบสูงสุด (CISO)** ....…………………...........................................………………………..…………….......……

 **6.2 การรักษาความมั่นคงปลอดภัยไซเบอร์ดำเนินการโดย**

 [ ] ดำเนินการเอง โปรดระบุทรัพยากรที่ใช้ จำนวนบุคคลากรและสาขาที่เชี่ยวชาญ

.....................................................................................................................................................................................

 [ ] ใช้บริการหน่วยงานภายนอก ระบุ.............................................................................................................

**6.3 มีมาตรฐานความมั่นคงปลอดภัยของระบบอย่างไร**

 มีแนวทางรักษาความมั่นคงปลอดภัยของระบบหรือไม่ อย่างไร

 [ ] มี ระบุ (อย่างน้อย 1 ข้อ)

* เป็นไปตามมาตรฐานของ (ระบุชื่อมาตรฐาน)...............................................
* เป็นไปตามแนวทางของ (ระบุชื่อแนวทาง หรือคำแนะนำ)...........................
* อื่นๆ...............................................................................................................

[ ] ไม่มี

**6.4 มีการประเมินความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร (Risk Assessment)**

.................................................................................................................................................................

.................................................................................................................................................................

**6.5 มีมาตรการรับมือเมื่อถูกโจมตีทางไซเบอร์อย่างไร**

.................................................................................................................................................................

.................................................................................................................................................................

**6.6 มีแผนการบริหารความต่อเนื่องอย่างไร (BCP)**

.................................................................................................................................................................

.................................................................................................................................................................

ลงชื่อ................................................... (หัวหน้าหน่วยงาน)
ตำแหน่ง...............................................
วันที่.....................................................

 *(ประทับตราหน่วยงาน ถ้ามี)*

1. จัดหา หมายรวมถึงการจ้างพัฒนาและการซื้อระบบโปรแกรมคอมพิวเตอร์ ทั้งแบบได้กรรมสิทธิ์ และไม่ได้กรรมสิทธิ์ [↑](#footnote-ref-1)
2. SLA : Service Level Agreement ข้อตกลงระดับการให้บริการ การรักษาระดับคุณภาพการให้บริการ [↑](#footnote-ref-2)