สพร./DD

พฤศจิกายน ๒๕๖๕

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัลอยู่ระหว่างการจัดทำ
ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน
มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัลฉบับสมบูรณ์จะมีประกาศโดย
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ร่าง

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล
DGA Community Standard

ว่าด้วยแนวปฏิบัติเชิงเทคนิคกระบวนการทางดิจิทัลภาครัฐ – การดำเนินงานทั่วไป

TECHNICAL GUIDELINES FOR DIGITAL GOVERNMENT PROCESS

สำหรับคณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ชั้น ๑๗ อาคารบางกอกไทยทาวเวอร์ ๑๐๘ ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ ๑๐๔๐๐
หมายเลขโทรศัพท์: ๐ ๒๖๑๒ ๖๐๐๐ โทรสาร: ๐ ๒๖๑๒ ๖๐๑๑ ๐ ๒๖๑๒ ๖๐๑๒

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล

Digital Government Standard

มสพร. [x-xxxx]

DGA [x-xxxx]

ว่าด้วยแนวปฏิบัติเชิงเทคนิคกระบวนการทางดิจิทัลภาครัฐ – การดำเนินงานทั่วไป

TECHNICAL GUIDELINES FOR DIGITAL GOVERNMENT PROCESS

เวอร์ชัน ๑.๐

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักนายกรัฐมนตรี

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล

ว่าด้วยแนวปฏิบัติเชิงเทคนิคกระบวนการทางดิจิทัลภาครัฐ – การดำเนินงานทั่วไป

มสพร. [x-xxxx]

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ชั้น ๑๗ อาคารบางกอกไทยทาวเวอร์ ๑๐๘ ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ ๑๐๔๐๐

หมายเลขโทรศัพท์: ๐ ๒๖๑๒ ๖๐๐๐ โทรสาร: ๐ ๒๖๑๒ ๖๐๑๑ ๐ ๒๖๑๒ ๖๐๑๒

ประกาศโดย

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักนายกรัฐมนตรี

วันที่ กรุณาเลือกวันที่ประกาศ

สารบัญ

คำนำ

ในปัจจุบัน การปฏิบัติหน้าที่โดยหน่วยงานภาครัฐเพื่อการบริหารราชการแผ่นดินและการให้บริการประชาชน มีความจำเป็นต้องอาศัยกระบวนการหรือการดำเนินงานทางดิจิทัลที่มีประสิทธิภาพ ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒ มารตรา ๑๒ (๒) นอกจากนี้ มาตรา ๖ และ มาตรา ๑๙ แห่งพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ กำหนดให้วิธีการทางอิเล็กทรอนิกส์ที่หน่วยงานของรัฐให้บริการประชาชน ต้องมีความสอดคล้องและสามารถเชื่อมโยงถึงกันได้ ดังนั้นสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) จึงได้จัดทำมาตรฐานสำนักงานรัฐบาลดิจิทัล (มสพร.) [๖-๒๕๖๕] ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ – ภาพรวม ขึ้น เพื่อเป็นแนวทางในการจัดทำกระบวนการทางดิจิทัลของหน่วยงานภาครัฐ

ในการนี้ เพื่อให้บรรลุวัตถุประสงค์ข้างต้นและสนับสนุนให้เกิดการพัฒนาบริการภาครัฐที่มีความมั่นคงปลอดภัยและน่าเชื่อถือ จึงจำเป็นต้องทำร่างแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐอีกฉบับหนึ่ง โดยเน้นที่กระบวนการเชิงเทคนิค ให้หน่วยงานภาครัฐสามารถเรียนรู้และนำไปพัฒนากระบวนการทางดิจิทัลที่มีประสิทธิภาพ มีความปลอดภัย สามารถเชื่อมโยงข้อมูล และมีมาตรฐานเป็นไปในแนวทางเดียวกัน อีกทั้งเป็นไปตามกฎหมาย มาตรฐาน แนวปฏิบัติ แนวทางการดำเนินงาน และข้อเสนอแนะที่เกี่ยวข้อง

มาตรฐานสำนักงานรัฐบาลดิจิทัล
ว่าด้วยแนวปฏิบัติเชิงเทคนิคกระบวนการทางดิจิทัลภาครัฐ – การดำเนินงานทั่วไป

๑. ขอบข่าย

(ร่าง) มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ฉบับนี้นำเสนอเนื้อหาเชิงเทคนิคของการจัดทำกระบวนการทางดิจิทัลสำหรับการ “ขออนุญาต” โดยเป็นแนวทางการปฏิบัติสำหรับใช้ภายในสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือเป็นการเสนอแนะแนวปฏิบัติวิธีทางอิเล็กทรอนิกส์เพื่อให้หน่วยงานของรัฐนำไปใช้ได้ ซึ่งมีความสอดคล้องตามระดับความพร้อมที่เหมาะสม โดยตามระดับความพร้อมของหน่วยงานภาครัฐ ได้แก่ ระดับเริ่มต้น (Initial) ระดับมาตรฐาน (Standard) และระดับสูง (Advance) [๑]

แนวปฏิบัติฯ ฉบับนี้เป็นเอกสารฉบับที่ ๑ ซึ่งเป็นส่วนหนึ่งของชุดแนวปฏิบัติเชิงเทคนิคกระบวนการทางดิจิทัลภาครัฐ มีจุดประสงค์เพื่อให้ระบบขออนุญาตที่ให้บริการโดยภาครัฐถูกพัฒนาไปในทิศทางเดียวกัน มีความสอดคล้องทั้งในด้านรูปแบบการให้บริการและเทคโนโลยีที่ใช้เพื่อให้บริการ โดยเน้นในส่วนการดำเนินงานทั่วไป ซึ่งรวมแนวปฏิบัติเชิงเทคนิคที่สามารถนำไปประยุกต์ใช้ได้กับการให้บริการของภาครัฐในทุกรูปแบบ โดยประกอบไปด้วย ๕ กระบวนการหลัก ได้แก่

- การลงลายมือชื่ออิเล็กทรอนิกส์
- การใช้งานเอกสารอิเล็กทรอนิกส์
- การเชื่อมโยงเพื่อแลกเปลี่ยนข้อมูล
- ความมั่นคงปลอดภัยไซเบอร์
- การรักษาความปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล

แนวปฏิบัติฯ ฉบับนี้ มีรูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) ดังนี้

- “ต้อง” (shall) ใช้ระบุสิ่งที่เป็นข้อกำหนด (requirement) ที่ต้องปฏิบัติตาม
- “ควร” (should) ใช้ระบุสิ่งที่เป็นข้อแนะนำ (recommendation)
- “อาจ” (may) ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (permission)

ทั้งนี้ เนื้อหาภายในเอกสารฉบับนี้เป็นเพียงแนวปฏิบัติโดยทั่วไป ไม่สามารถครอบคลุมประเด็นทางกฎหมายหรือปัจจัยแวดล้อมอื่นที่เกี่ยวข้องทั้งหมด ดังนั้น ควรมีการปรึกษากับผู้เชี่ยวชาญทางกฎหมาย และผู้เชี่ยวชาญด้านอื่นที่เกี่ยวข้องก่อนดำเนินการตามรายละเอียดของแนวปฏิบัติฉบับนี้

๒. บทนิยาม

ความหมายของนิยามที่ใช้ในมาตรฐานสำนักงานรัฐบาลดิจิทัลฉบับนี้ มีดังนี้

- “ขออนุญาต” หมายถึง ขอรับใบอนุญาต ขออนุมัติ ขอจดทะเบียน ขอขึ้นทะเบียน ขอแจ้ง ขอจดแจ้ง ขออาชญาบัตร ขอการรับรอง ขอความเห็นชอบ ขอความเห็น ขอให้พิจารณา ขออุทธรณ์ ร้องทุกข์ หรือร้องเรียน ขอให้ดำเนินการ ขอรับเงิน ขอรับสวัสดิการ และขอรับบริการอื่นใดจากหน่วยงานของรัฐ
- “อนุญาต” หมายถึง ออกใบอนุญาต อนุมัติ จดทะเบียน ขึ้นทะเบียน รับแจ้ง รับจดแจ้ง ออกอาชญาบัตร รับรอง เห็นชอบ ให้ความเห็น แจ้งผลการพิจารณา แจ้งผล การดาเนินการ จ่ายเงิน ให้ได้รับสวัสดิการ และให้บริการอื่นใดแก่ประชาชนหรือหน่วยงานของรัฐ
- “หน่วยงานของรัฐ” หมายถึง ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการ ส่วนท้องถิ่น รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานอื่นของรัฐทุกหน่วย แต่ไม่รวมถึงรัฐวิสาหกิจ ที่เป็นบริษัทจำกัดหรือบริษัทมหาชนจำกัด
- “ระบบบริการ” หมายถึง ระบบดิจิทัลที่ให้บริการภาครัฐแก่ผู้ขออนุญาต

๓. สถานะความจำเป็นของกระบวนการทางดิจิทัล

กระบวนการทางดิจิทัลบางกระบวนการเป็นกระบวนการที่ต้องมี (mandatory) และบางกระบวนการเป็นกระบวนการที่อาจมี (optional) หากหน่วยงานของรัฐเห็นสมควรแล้วว่า บริการสำหรับการขออนุญาตหนึ่ง ๆ ไม่จำเป็นต้องมีกระบวนการที่จัดอยู่ในจำพวก “อาจมี” ในตารางด้านบน ให้ข้ามแนวปฏิบัติสำหรับกระบวนการดังกล่าวไป โดยแสดงสถานะของกระบวนการดิจิทัลต่าง ๆ สำหรับกระบวนการในภาพรวมในตารางที่ ๓.๑

ตารางที่ ๓.๑ สถานะความจำเป็นของการดำเนินงานทั่วไปในกระบวนการทางดิจิทัล

กระบวนการ	สถานะความจำเป็น	หมายเหตุ
การลงลายมือชื่ออิเล็กทรอนิกส์	อาจมี	บริการบางประเภทอาจไม่จำเป็นต้องระบุตัวตนของผู้ขออนุญาตและ/หรือผู้อนุญาต ทำให้ไม่ถือว่าเป็นการลงลายมือชื่ออิเล็กทรอนิกส์ ตามมาตรา ๙ แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔
การใช้งานเอกสารอิเล็กทรอนิกส์	ต้องมี	การให้บริการทางดิจิทัลต้องจัดทำหลักฐานการให้บริการในรูปแบบอิเล็กทรอนิกส์
การเชื่อมโยงเพื่อแลกเปลี่ยนข้อมูล	อาจมี	บริการบางประเภทอาจไม่จำเป็นต้องใช้หรือเชื่อมต่อข้อมูลกับหน่วยงานอื่น

กระบวนการ	สถานะความจำเป็น	หมายเหตุ
ความมั่นคงปลอดภัยไซเบอร์	ต้องมี	การให้บริการทางดิจิทัลต้องรักษาความลับของข้อมูล ความสมบูรณ์ของข้อมูล และความพร้อมใช้งาน
การรักษาความปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล	อาจมี	บริการที่ไม่มีการจัดเก็บข้อมูลส่วนบุคคล อาจไม่มีความจำเป็นต้องปฏิบัติตามแนวทางการรักษาความปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล

๔. แนวปฏิบัติการดำเนินงานทั่วไป

๔.๑ การลงลายมือชื่ออิเล็กทรอนิกส์

การลงลายมือชื่ออิเล็กทรอนิกส์เป็นองค์ประกอบสำคัญในการทำให้กระบวนการทางดิจิทัลมีความน่าเชื่อถือ สามารถระบุตัวตนรวมถึงระบุเจตนาในการลงลายมือชื่อของทั้งผู้ขออนุญาตและผู้ให้อนุญาต ในขั้นตอนต่าง ๆ ของกระบวนการอนุญาต เช่น ขั้นตอนการยื่นคำขอ การอนุมัติ และการออกใบอนุญาต

๔.๑.๑ การเลือกประเภทลายมือชื่ออิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์ถูกแบ่งออกเป็น ๓ ประเภท โดยมีคุณสมบัติตาม ขมธอ. ๒๓-๒๕๖๓ หน่วยงานของรัฐสามารถพิจารณาเลือกใช้ประเภทลายมือชื่ออิเล็กทรอนิกส์โดยพิจารณาเลือกประเภทลายมือชื่ออิเล็กทรอนิกส์ได้ ดังนี้

- หน่วยงานของรัฐควรเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ โดยพิจารณาถึงปัจจัยเสี่ยงตามที่กำหนดในหัวข้อ ๕ ใน ขมธอ. ๒๓-๒๕๖๓ ยกตัวอย่างเช่น กฎเกณฑ์ ประเพณี ประเภท ความถี่ และมูลค่าในการทำธุรกรรม
- หน่วยงานของรัฐควรเลือกใช้ประเภทของลายมือชื่ออิเล็กทรอนิกส์ให้เหมาะสมตามระดับความเสี่ยงของธุรกรรม ตามตาราง ๔.๑ ใน มสพร. ๖-๒๕๖๕
- หน่วยงานของรัฐควรเลือกใช้ประเภทของลายมือชื่ออิเล็กทรอนิกส์ตามชนิดของหนังสือราชการตามที่ระบุตามตารางที่ ๓ ใน มสพร. ๗-๒๕๖๕ โดยควรเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓ สำหรับเอกสารที่ถูกส่งออกไปภายนอกหน่วยงาน และอาจเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๑ หรือ ๒ สำหรับเอกสารที่ใช้ภายในหน่วยงาน เป็นต้น

๔.๑.๒ แนวทางการพัฒนาระบบลงลายมือชื่ออิเล็กทรอนิกส์

- ลายมือชื่ออิเล็กทรอนิกส์ต้องมีคุณสมบัติตามมาตรา ๙ แห่ง พ.ร.บ. ด้วยธุรกรรมทางอิเล็กทรอนิกส์ ได้แก่ (๑) สามารถระบุตัวผู้เป็นเจ้าของลายมือชื่อได้ (๒) สามารถแสดงเจตนาของเจ้าของลายมือชื่อ และ (๓) ใช้วิธีการที่เชื่อถือ

- หน่วยงานของรัฐควรกำหนดมาตรการการบรรเทาความเสี่ยงจากการให้บริการลงลายมือชื่ออิเล็กทรอนิกส์ รวมทั้งจัดเก็บหลักฐานการลงลายมือชื่ออิเล็กทรอนิกส์ ตามตารางที่ ๒ ใน ขมธอ. ๒๓-๒๕๖๓
- หน่วยงานของรัฐควรกำหนดมาตรการในการรับมือสถานการณ์ฉุกเฉิน ซึ่งอาจทำให้ระบบลงลายมือชื่ออิเล็กทรอนิกส์ไม่สามารถให้บริการได้ชั่วคราว เช่น การเกิดภัยพิบัติทางธรรมชาติ ในกรณีที่หน่วยงานพิจารณาใช้ลายมือชื่ออิเล็กทรอนิกส์**ประเภทที่ ๒ หรือ ๓** นั้นคือเลือกใช้ลายมือชื่อดิจิทัล (Digital Signature) ระบบลงลายมือชื่ออิเล็กทรอนิกส์มีคุณสมบัติเพิ่มเติมดังต่อไปนี้
    - ลายมือชื่อดิจิทัลต้องมีคุณสมบัติตามมาตรา ๒๖ แห่ง พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ โดยกุญแจส่วนตัวที่ใช้สร้างลายมือชื่อดิจิทัลต้องอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อ และกุญแจสาธารณะต้องสามารถเชื่อมโยงไปยังเจ้าของลายมือชื่อได้
    - หน่วยงานของรัฐควรกำหนดข้อมูลในใบรับรอง (Certificate) และรายการเพิกถอนใบรับรอง (Certificate Revocation List: CRL) ตาม ขมธอ. ๑๕-๒๕๖๐
    - สำหรับลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓ หน่วยงานของรัฐต้องเลือกใช้บริการออกใบรับรอง จากผู้ให้บริการออกใบรับรอง (Certification Authority: CA) ที่มีคุณสมบัติตามมาตรา ๒๘ แห่ง พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และต้องได้รับการรับรองจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ (National Root Certification Authority Of Thailand: NRCA)
    - ในกรณีที่ลายมือชื่อดิจิทัลมีความจำเป็นต้องถูกตรวจสอบในระยะยาว หน่วยงานของรัฐควรพิจารณาใช้การประทับเวลาอิเล็กทรอนิกส์ร่วมด้วย

๔.๑.๓ ข้อเสนอแนะการลงลายมือชื่ออิเล็กทรอนิกส์

- หน่วยงานที่มีความพร้อมใน**ระดับเริ่มต้น**ควรใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๑ เช่น ใช้รูปภาพลายมือชื่อจากการใช้สไตลัสหรือการสแกนภาพลายมือชื่อบนกระดาษ โดยปฏิบัติตามแนวทางการบรรเทาความเสี่ยงและจัดเก็บหลักฐานตามตารางที่ ๒ ใน ขมธอ. ๒๓-๒๕๖๓
- หน่วยงานที่มีความพร้อมใน**ระดับมาตรฐาน**อาจพัฒนาระบบลงลายมือชื่ออิเล็กทรอนิกส์ของตนเอง หรืออาจใช้บริการลงลายมือชื่ออิเล็กทรอนิกส์ของหน่วยงานอื่น โดยควรใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓ ในขั้นตอนการออกใบอนุญาตหรือเอกสารอื่น
- หน่วยงานที่มีความพร้อมใน**ระดับสูง**ต้องใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๓ ในขั้นตอนการออกใบอนุญาตหรือเอกสารอื่น และควรใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๒ เป็นอย่างน้อยในขั้นตอนการอนุมัติ

๔.๒ การใช้งานเอกสารอิเล็กทรอนิกส์

ในปัจจุบัน บริการดิจิทัลของภาครัฐจำนวนมากยังให้บริการในรูปแบบผสม นั้นคือมีองค์ประกอบของบริการที่เป็นดิจิทัล ทว่าใช้งานร่วมกับเอกสารในรูปแบบกระดาษและการดำเนินการแบบดั่งเดิมที่ไม่อยู่ในรูปแบบดิจิทัล อันเนื่องมาจากความไม่พร้อมของผู้ขออนุญาตหรือหน่วยงานที่ให้บริการ รวมถึงข้อจำกัดของกฎหมายและกฎเกณฑ์ซึ่งไม่เอื้อต่อการใช้งานเอกสารในรูปแบบอิเล็กทรอนิกส์

การใช้งานเอกสารอิเล็กทรอนิกส์อย่างมีประสิทธิภาพจะช่วยเพิ่มประสิทธิภาพในการให้บริการประชาชนโดยภาครัฐอย่างมีนัยสำคัญ เช่น ช่วยลดการใช้กระดาษและช่วยประหยัดงบประมาณในการดูแลรักษาเอกสาร ดังนั้น การมาตรฐานการพัฒนาระบบและการใช้งานเอกสารอิเล็กทรอนิกส์จึงมีความสำคัญต่อกระบวนการดิจิทัลภาครัฐในภาพรวมอย่างยิ่ง

๔.๒.๑ มาตรฐานเอกสารอิเล็กทรอนิกส์

ในปัจจุบัน มีการใช้งานเอกสารอิเล็กทรอนิกส์ในหลากหลายรูปแบบ ทั้งในรูปแบบไฟล์เอกสาร รูปภาพนิ่ง รูปภาพเคลื่อนไหว เสียง เป็นต้น หน่วยงานของรัฐสามารถเลือกใช้ประเภทของเอกสารอิเล็กทรอนิกส์ตามความเหมาะสม โดยคำนึงถึงปัจจัยต่าง ๆ เช่น ของลักษณะการใช้งานเอกสาร ประเภทของธุรกรรม ทรัพยากรด้านการเงินหรือบุคคล

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ได้กำหนดมาตรฐานเกี่ยวกับเอกสารอิเล็กทรอนิกส์ไว้ ดังนี้

- ขมธอ. ๑๑-๒๕๖๐ เกี่ยวกับการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ โดยเฉพาะไฟล์เอกสารอิเล็กทรอนิกส์ประเภท Portable Data Format (PDF) โดยหน่วยงานของรัฐอาจเลือกใช้เอกสารอิเล็กทรอนิกส์ประเภทนี้ หากเอกสารถูกจัดทำขึ้นเพื่อให้บุคคลธรรมดาอ่านได้ (human-readable)
- ขมธอ. ๑๔-๒๕๖๐ เกี่ยวกับการใช้ Extensible Markup Language (XML) สำหรับการแลกเปลี่ยนข้อมูล โดยหน่วยงานของรัฐอาจเลือกใช้เอกสารอิเล็กทรอนิกส์ประเภทนี้ หากเอกสารถูกจัดทำขึ้นเพื่อให้ระบบคอมพิวเตอร์อ่าน (machine-readable) หรือใช้สำหรับการแลกเปลี่ยนข้อมูลระหว่างองค์กร
- ขมธอ. ๒๔-๒๕๖๓ เกี่ยวกับเอกสารรับรอง (Verifiable Credential: VC) และ เอกสารสำแดง (Verifiable Presentation: VP) เป็นโมเดลข้อมูล (Data Model) โดยหน่วยงานของรัฐอาจเลือกใช้เอกสารอิเล็กทรอนิกส์ประเภทนี้ หากเอกสารถูกจัดทำขึ้นโดยมีจุดประสงค์เพื่อให้บุคคลธรรมดาจัดเก็บเอกสารดังกล่าวไว้กับตนเองเพื่อใช้ทำธุรกรรมต่อไปในอนาคต เช่น บัตรประจำตัวองค์กร หรือ ใบอนุญาต ทั้งนี้ เอกสารรับรองและเอกสารสำแดงมีคุณสมบัติสำคัญคือสามารถตรวจสอบตัวตนของผู้ออกเอกสารและผู้ถือเอกสาร รวมทั้ง ตรวจสอบความถูกต้องของเอกสารนั้นได้ด้วยกระบวนการทางอิเล็กทรอนิกส์

- ขมธอ. ๒๕-๒๕๖๓ เกี่ยวกับข้อความอิเล็กทรอนิกส์สำหรับใบประมวลผลการศึกษา

ทั้งนี้ การลงลายมือชื่อในเอกสารอิเล็กทรอนิกส์อาจอ้างอิงแนวทางจากมาตรฐานสากล เช่น มาตรฐาน ลายมือชื่ออิเล็กทรอนิกส์ขั้นสูง (Advanced Electronic Signature: AdES) จากสถาบัน European Telecommunications Standards Institute (ETSI)

๔.๒.๒ แนวทางการพัฒนาระบบเอกสารอิเล็กทรอนิกส์

- หน่วยงานของรัฐต้องพัฒนาระบบเอกสารอิเล็กทรอนิกส์ โดยปฏิบัติตามวงจรการใช้งานหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Electronic Certificate Life Cycle) ใน ขมธอ. ๑๑-๒๕๖๐ ซึ่งประกอบไปด้วย ๗ ขั้นตอน (๑) การจัดทำ (๒) การลงลายมือชื่อ (๓) การส่ง/การรับ (๔) การตรวจสอบ (๕) การนำไปใช้งานหรือประมวลผล (๖) การเก็บรักษา (๗) การยกเลิก
- ระบบเอกสารอิเล็กทรอนิกส์ต้องปฏิบัติตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ (ฉบับที่ ๔) พ.ศ. ๒๕๖๔ รวมถึง หลักเกณฑ์การตั้งชื่อ การเก็บรักษา การทำลายเอกสาร การรับและส่งหนังสือ เป็นต้น
- หน่วยงานของรัฐต้องจัดเก็บเอกสารอิเล็กทรอนิกส์ตาม พ.ร.บ. จดหมายเหตุแห่งชาติ พ.ศ. ๒๕๕๖
- ในกรณีที่หน่วยงานของรัฐจำเป็นต้องแปลงเอกสารและข้อความให้อยู่ในรูปของอิเล็กทรอนิกส์ หน่วยงานของรัฐต้องดำเนินตามที่กำหนดในประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.) เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ ซึ่งรวมถึงข้อกำหนดโดยทั่วไปเกี่ยวกับข้อมูลและเมทาดาตาของข้อมูลภาพ เสียง และวิดีทัศน์

๔.๒.๓ ข้อเสนอแนะการใช้งานเอกสารอิเล็กทรอนิกส์

- หน่วยงานที่มีความพร้อมใน**ระดับเริ่มต้น**ควรใช้เอกสารอิเล็กทรอนิกส์รูปแบบ PDF (โดยใช้ร่วมกับลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ ๑ โดยอาจจัดเก็บไฟล์เอกสารอิเล็กทรอนิกส์บนระบบคอมพิวเตอร์ของหน่วยงานเองหรือใช้บริการคลาวน์จากผู้ให้บริการที่น่าเชื่อถือ รวมทั้ง ควรบริหารจัดการเอกสารตลอดวงจรชีวิต (Life Cycle) ด้วยเจ้าหน้าที่ภายในหน่วยงานเอง
- หน่วยงานที่มีความพร้อมใน**ระดับมาตรฐาน**และ**ระดับสูง**อาจจัดเก็บและบริหารจัดการไฟล์เอกสารอิเล็กทรอนิกส์ด้วยระบบอัตโนมัติเพื่อลดโอกาสเกิดความผิดพลาด โดยอาจพัฒนาระบบสารบรรณเพื่อใช้ภายในหน่วยงานเองหรือใช้บริการจากผู้ให้บริการที่น่าเชื่อถือ

๔.๓ การเชื่อมโยงเพื่อแลกเปลี่ยนข้อมูล

เพื่อให้ประชาชนหรือผู้ใช้บริการได้รับการบริการที่สะดวก รวดเร็ว ลดขั้นต่าง ๆ ในการติดต่อกับหน่วยงานราชการ ภาครัฐควรมีการเชื่อมโยงกระบวนการทำงานและข้อมูลอิเล็กทรอนิกส์ภายในหน่วยงาน

หรือข้ามหน่วยงานกันอย่างมีมาตรฐาน มีความรวดเร็ว เชื่อมโยงข้อมูลได้ทุกหน่วยงาน เกิดความสะดวกต่อประชาชนผู้ใช้บริการ

โดย สพร. ได้จัดทำ มรด. ๒-๑:๒๕๖๕ ว่าด้วยกรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (Thailand Government Information eXchange: TGIX) เป็นการพัฒนามาตรฐานและหลักเกณฑ์ เพื่อสร้างและพัฒนากระบวนการทำงานของหน่วยงานภาครัฐให้มีความสอดคล้องเชื่อมโยงกัน โดยเป็นมาตรฐานที่ทำให้หน่วยงานสามารถแลกเปลี่ยนข้อมูล (Data Exchange) แลกเปลี่ยนความหมายของข้อมูล (Meaning Exchange) และเกิดข้อตกลงในขั้นตอนการดำเนินงาน (Process Agreement)

๔.๓.๑ ข้อความอิเล็กทรอนิกส์จำเพาะ

ในกรณีที่ระบบบริการมีการออกหรือแลกเปลี่ยนข้อความอิเล็กทรอนิกส์ หน่วยงานของรัฐต้องจัดทำข้อความดังกล่าวตามกรอบการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (Thailand Government Information eXchange: TGIX) และควรจัดทำข้อความดังกล่าวตามมาตรฐานในตารางที่ ๔.๑

ตารางที่ ๔.๑ มาตรฐานข้อความและการแลกเปลี่ยนข้อความอิเล็กทรอนิกส์

ขอบข่าย	มาตรฐาน
ข้อมูลบุคคล	มสพร. 4-2565
ข้อมูลนิติบุคคล	มสพร. 5-2565
ข้อมูลการนัดหมายหรือเหตุการณ์ใด ๆ สำหรับใส่ในปฏิทิน	RFC 5545
ข้อมูลการติดต่อบุคคลหรือองค์กร	RFC 6350
ข้อมูลผู้ได้รับผลประโยชน์ที่แท้จริง (beneficial ownership)	BODS
ข้อมูลตำแหน่งที่ตั้งทางภูมิศาสตร์	WGS 84 หรือ Indian 1975
มีรูปแบบข้อมูลเป็น HTML	HTML5
มีรูปแบบข้อมูลเป็น PDF	PDF/A
มีรูปแบบข้อมูลเป็นวันที่และเวลาที่คอมพิวเตอร์อ่านได้ (machine-readable)	ISO 8601
มีรูปแบบเป็น Uniform Resource Identifier (URI) อาทิ URL	RFC 3986
มีรูปแบบเป็น Internationalized Resource Identifier (IRI)	RFC 3987
ข้อมูลสัญญา อาทิ สัญญาการจัดซื้อจัดจ้าง	OCDS

๔.๓.๒ แนวทางการพัฒนาระบบเชื่อมโยงเพื่อแลกเปลี่ยนข้อมูล

ในกรณีที่หน่วยงานของรัฐจำเป็นต้องพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลชนิดใดชนิดหนึ่งเป็นการเฉพาะ

- หน่วยงานของรัฐควรสร้างข้อกำหนดทางเทคนิคของชุดข้อมูลร่วม (Core Component Specification) ตามที่กำหนดไว้ใน ขมธอ. ๒๗-๒๕๖๔ ซึ่งรวมถึงการใช้พจนานุกรมชุดข้อมูลร่วม
- ในกรณีที่หน่วยงานของรัฐจำเป็นต้องแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์กับหน่วยงานของรัฐอื่นด้วยข้อความ XML หน่วยงานของรัฐควรจัดทำข้อความ XML ดังกล่าว ตามที่กำหนดไว้ใน ขมธอ. ๑๔-๒๕๖๐
- ในกรณีที่หน่วยงานของรัฐจัดให้มีการเปิดเผยข้อมูลเปิดของภาครัฐในรูปแบบดิจิทัลต่อสาธารณะ หน่วยงานของรัฐต้องดำเนินการตามที่กำหนดไว้ใน มรด.-๑๒๐๐๑:๒๕๖๓ และ มสพร. ๑-๒๕๖๔
- หน่วยงานของรัฐควรจัดทำบัญชีข้อมูล จัดหมวดหมู่ชุดข้อมูล จัดทำเมทาดาตาของชุดข้อมูล จัดทำนโยบายข้อมูล พัฒนาระบบบัญชีข้อมูล และบริหารจัดการระบบบัญชีข้อมูล ตามที่กำหนดไว้ใน มสพร. ๑-๒๕๖๔ ทั้งนี้ หากในการดำเนินการดังกล่าวข้างต้น จำเป็นต้องอาศัยการประเมินคุณภาพข้อมูล หน่วยงานรัฐต้องใช้หลักเกณฑ์การประเมินคุณภาพข้อมูล ตามที่กำหนดไว้ใน มสพร. ๓-๒๕๖๕
- ในกรณีที่หน่วยงานของรัฐใช้ระบบสารบรรณอิเล็กทรอนิกส์ที่จำเป็นต้องมีการแลกเปลี่ยนข้อมูลกับระบบสารบรรณอิเล็กทรอนิกส์อื่น หน่วยงานของรัฐควรจัดให้การแลกเปลี่ยนข้อมูลดังกล่าวเป็นไปตามที่กำหนดไว้ในมาตรฐานการแลกเปลี่ยนข้อมูลระหว่างระบบสารบรรณอิเล็กทรอนิกส์
- หน่วยงานของรัฐควรจัดทำนโยบายการบริหารจัดการข้อมูล ตามที่กำหนดไว้ใน มสพร. ๒-๑:๒๕๖๔ และจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล ตามที่กำหนดไว้ใน มสพร. ๒-๒:๒๕๖๔
- หน่วยงานรัฐควรเข้ารหัสอักขระด้วยชุดรหัส (encoding form) UTF-8

๔.๓.๓ ข้อเสนอแนะการเชื่อมโยงเพื่อแลกเปลี่ยนข้อมูล

หน่วยงานภาครัฐสามารถปรับระบบเข้าสู่มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (TGIX) โดยแบ่งเป็น ๓ กลุ่ม ได้แก่ ผู้ให้บริการแพลตฟอร์มแลกเปลี่ยนข้อมูล (Exchange Platform Provider) ผู้ให้บริการข้อมูล (Data Provider) และผู้ใช้บริการข้อมูล (Data Consumer) โดยหน่วยงานควรปฏิบัติตามข้อเสนอแนะจากกรอบแนวทางเพื่อปรับบริการให้เป็นไปตามมาตรฐานการทำงานร่วมกัน ซึ่งแบ่งได้เป็น ๓ ระดับ ได้แก่ ระดับเทคนิค (Technical) ระดับความหมาย (Semantic) และระดับองค์กร (Organizational)

สามารถสรุปข้อเสนอแนะเบื้องต้น สำหรับหน่วยงานที่ยังไม่ได้พัฒนาระบบดิจิทัลและหน่วยงานที่ดำเนินให้บริการระบบดิจิทัลอยู่ สำหรับมาตรฐานระดับเทคนิคและระดับความหมาย ดังนี้

ตารางที่ ๔.๒ เสนอแนะในการปรับระบบเข้าสู่มาตรฐานฯ สำหรับผู้ให้บริการแพลตฟอร์มแลกเปลี่ยนข้อมูล ผู้ให้บริการข้อมูล และผู้ใช้บริการข้อมูล

สถานะการพัฒนาระบบ	กลุ่มของมาตรฐาน	
	ระดับเทคนิค (Technical)	ระดับความหมาย (Semantic)
ผู้ให้บริการแพลตฟอร์มแลกเปลี่ยนข้อมูล		
หน่วยงานที่ยังไม่ได้พัฒนาระบบดิจิทัล	พิจารณาพัฒนาระบบตามมาตรฐานฯ	พิจารณาสร้าง Adapter ในการแปลงข้อมูลของหน่วยงานให้เข้าสู่มาตรฐานฯ
หน่วยงานที่ดำเนินให้บริการระบบดิจิทัลอยู่	เมื่อถึงวงรอบการใช้งานระบบ พิจารณาสร้างทางเลือกในการเชื่อมต่อตามมาตรฐานฯ	พิจารณาสร้าง Adapter เพื่อสร้างทางเลือกในการให้บริการข้อมูลตามมาตรฐานฯ
ผู้ให้บริการข้อมูล		
หน่วยงานที่ยังไม่ได้พัฒนาระบบดิจิทัล	พิจารณาว่าแพลตฟอร์มที่จะเชื่อมต่อ มีทางเลือกให้เชื่อมต่อตามมาตรฐานหรือไม่ ถ้ามีให้ทำตามมาตรฐานฯ	ติดต่อ สพร. เพื่อพิจารณาประกาศข้อมูลให้เป็นมาตรฐานฯ
หน่วยงานที่ดำเนินให้บริการระบบดิจิทัลอยู่	เมื่อถึงอายุการใช้งานระบบพิจารณาสร้างทางเลือกในการเชื่อมต่อตามมาตรฐานฯ ถ้าแพลตฟอร์มที่เชื่อมต่อมีทางเลือกให้	ติดต่อ สพร. เพื่อพิจารณาประกาศข้อมูลเป็นมาตรฐาน
ผู้ใช้บริการข้อมูล		
หน่วยงานที่ยังไม่ได้พัฒนาระบบดิจิทัล	พิจารณาเชื่อมต่อตามมาตรฐานฯ เป็นอันดับแรก เชื่อมต่อตามข้อกำหนดของแพลตฟอร์มเป็นอันดับที่สอง	พิจารณาเลือกใช้ข้อมูลที่เป็นมาตรฐานฯ ใช้ข้อมูลตามข้อกำหนดของแพลตฟอร์มเป็นทางเลือกที่สอง
หน่วยงานที่ดำเนินให้บริการระบบดิจิทัลอยู่	เมื่อถึงอายุการใช้งานระบบ ให้พิจารณาใช้การเชื่อมต่อตามมาตรฐานฯ เป็นทางเลือกแรก	เมื่อถึงวงรอบการใช้งานระบบให้พิจารณาใช้ข้อมูลตามมาตรฐานเป็นทางเลือกแรก

๔.๔ ความมั่นคงปลอดภัยไซเบอร์

เพื่อให้บริการดิจิทัลจากภาครัฐมีความราบรื่นและได้รับความเชื่อมั่นจากผู้ใช้บริการ หน่วยงานของรัฐมีความจำเป็นต้องคำนึงถึงความมั่นคงปลอดภัยทางไซเบอร์ของบริการ ซึ่งครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) โดยมีความสอดคล้องตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๔.๔.๑ แนวทางการบริหารความมั่นคงปลอดภัยของระบบบริการ

- หน่วยงานภาครัฐต้องดำเนินกระบวนการทางดิจิทัล ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ซึ่งประกอบไปด้วยมาตรฐาน ๑๑ ข้อ เช่น การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ การบริหารจัดการทรัพย์สินสารสนเทศ การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร
- หน่วยงานควรพัฒนาบริการดิจิทัลมีความสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยสากล เช่น ISO/IEC 27001:2013
- ในกรณีที่ระบบบริการจำเป็นต้องมีการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์ หน่วยงานของรัฐควรบริหารความมั่นคงปลอดภัยของบริการดังกล่าว ตามที่กำหนดไว้ใน ขมธอ. ๒๑-๒๕๖๒
- ในกรณีที่ระบบบริการจำเป็นต้องมีองค์ประกอบเข้าข่ายอย่างใดอย่างหนึ่งหรือหลายอย่างดังต่อไปนี้ หน่วยงานของรัฐควรบริหารความมั่นคงปลอดภัยของบริการดังกล่าว ตามที่กำหนดไว้ใน ขมธอ. ๑-๒๕๕๗ และ ขมธอ. ๔-๒๕๕๙ ได้แก่ โปรแกรมสำหรับให้บริการเว็บ (web server software) ระบบบริหารจัดการเว็บไซต์ (content management system: CMS) ระบบฐานข้อมูล (database system) และโปรแกรมประยุกต์บนเว็บ (web application)

๔.๔.๒ ข้อเสนอแนะด้านความมั่นคงปลอดภัยไซเบอร์

เพื่อยกระดับความมั่นคงปลอดภัยทางไซเบอร์ของระบบสารสนเทศ หน่วยงานต้องปฏิบัติตามวิธีการใน “ระดับพื้นฐาน” และอาจปฏิบัติตามวิธีการใน “ระดับกลาง” หรือ “ระดับเคร่งครัด” รายละเอียดตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ดังนี้

- หน่วยงานที่มีความพร้อม**ในระดับเริ่มต้น**ต้องมีการดำเนินการให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยใน**ระดับพื้นฐาน**

- หน่วยงานที่มีความพร้อม**ในระดับมาตรฐาน**ต้องปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยใน**ระดับพื้นฐาน** และควรปฏิบัติเพิ่มเติมตามวิธีการแบบปลอดภัยใน**ระดับกลาง**
- หน่วยงานที่มีความพร้อม**ในระดับสูง**ต้องปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยใน**ระดับพื้นฐาน** และควรปฏิบัติเพิ่มเติมตามวิธีการแบบปลอดภัยใน**ระดับกลาง**และ**ระดับเคร่งครัด**

๔.๕ การรักษาความปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล

การให้บริการทางดิจิทัลของภาครัฐต้องให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล สอดคล้องกับวัตถุประสงค์และหลักการคุ้มครองข้อมูลส่วนบุคคลของไทย โดยเฉพาะ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งมีผลบังคับใช้ในการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในราชอาณาจักร

ทั้งนี้ หน่วยงานของรัฐที่ให้บริการดิจิทัลแก่ประชาชน และมีเหตุต้องเกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล อาทิ ชื่อนามสกุล เลขประจำตัวประชาชน หมายเลขโทรศัพท์ ที่อยู่ เป็นต้น ถือเป็นผู้ควบคุมข้อมูล (Data Controller) โดยอ้างอิงจากมาตรา ๒๔ และ ๓๗ แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และต้องดำเนินการตามกฎหมายคุ้มครองส่วนบุคคล

๔.๕.๑ แนวทางการคุ้มครองข้อมูลส่วนบุคคลของระบบบริการ

- ในกรณีที่ระบบบริการจำเป็นต้องให้ผู้ขออนุญาตที่เป็นบุคคลธรรมดาที่เป็นเจ้าของข้อมูลที่มีอายุครบ ๒๐ ปีบริบูรณ์แล้ว ให้ความยินยอมในการเปิดเผยข้อมูล หน่วยงานของรัฐควรใช้สถาปัตยกรรมระบบการให้ความยินยอม และโครงสร้างข้อมูลการให้ความยินยอม ตามที่กำหนดไว้ใน ขมธอ. ๑๐–๒๕๖๐
- ในกรณีที่การให้บริการเข้าข่ายเหตุการณ์ที่ต้องขอความยินยอม ตามข้อ ๕.๑ ใน ขมธอ. ๒๘–๒๕๖๔ หน่วยงานของรัฐควรดำเนินการ (๑) ขอความยินยอมและการดำเนินการอื่นใดที่เกี่ยวข้อง (๒) แจ้งประกาศความเป็นส่วนตัว (privacy notice) และ (๓) บันทึกการให้ความยินยอม
- ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลภาครัฐ หน่วยงานของรัฐอาจใช้ “เอกสารแม่แบบ” ที่จัดทำโดยหน่วยงานอื่น ในการจัดทำเอกสารของตนเองที่แสดงถึงการดำเนินการตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เช่น เอกสารแม่แบบที่จัดทำโดย สพร.

๔.๕.๒ ข้อเสนอแนะด้านการรักษาความปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล

หน่วยงานสามารถกำหนดกรอบการทำงานเป็นขั้นตอนการปฏิบัติของผู้ควบคุมข้อมูล (Data Controller) ตามมาตรา ๓๗ แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เรื่องหน้าที่ของผู้ควบคุม

ข้อมูลส่วนบุคคล รวมถึงสามารถยกระดับเพื่อการคุ้มครองข้อมูลส่วนบุคคล การเตรียมความพร้อมตามแนวปฏิบัติที่ดี (Best Practices) ที่เสนอแนะโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สามารถสรุปแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลสำหรับหน่วยงานภาครัฐในตารางที่ ๔.๓ ดังต่อไปนี้

ตารางที่ ๔.๓ สรุปข้อเสนอแนะการพัฒนาระบบเพื่อคุ้มครองข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ข้อกำหนดตามกฎหมาย	รายละเอียด
๑. การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	หน่วยงานต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) ในกรณีตามที่กำหนดไว้ในมาตรา ๔๑
๒. การจัดทำประกาศความเป็นความส่วนตัว	หน่วยงานต้องจัดทำประกาศความเป็นความส่วนตัว (Privacy Notice) และแจ้งให้เจ้าของข้อมูลทราบถึงรายละเอียด ก่อนหรือระหว่างการเก็บรวบรวมข้อมูลส่วนบุคคล ตามที่กำหนดไว้ในมาตรา ๒๓
๓. การจัดทำบันทึกรายการกิจกรรมการประมวลผล	หน่วยงานต้องจัดทำบันทึกรายการกิจกรรมการประมวลผล (Records of Processing Activities) อย่างน้อยตามที่ระบุไว้ในมาตรา ๓๙ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบได้
๔. การจัดทำแบบคำขอความยินยอม	เมื่อหน่วยงานมีความจำเป็นต้องใช้ความยินยอมเพื่อการประมวลผลข้อมูล หน่วยงานต้องจัดทำแบบคำขอความยินยอม (Consent Form) โดยมีหลักเกณฑ์ในการขอความยินยอมเป็นไปตามตามมาตรา ๑๙ และมาตรา ๒๐
๕. การจัดทำข้อตกลงการประมวลผล	หน่วยงานต้องจัดทำข้อตกลงการประมวลผล (Data Processing Agreement) กับผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อควบคุมการดำเนินการตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามมาตรา ๔๐ วรรคสาม โดยอย่างน้อยสัญญาต้องมีเงื่อนไขตามที่กำหนดไว้ในมาตรา ๔๐ วรรคหนึ่ง

บรรณานุกรม

[๑] สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). มสพร. ๖-๒๕๖๕ ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ – ภาพรวม. สืบค้นจาก https://standard.dga.or.th/dga-std/5212/