แนวทางการบริหารจัดการระบบสารสนเทศเพื่อการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ

Guidelines for Information Systems Management to Protect Personal Information of Government Agencies

ดร.อรรถพล ป้อมสถิตย์[1]
Auttapon Pomsathit[1]

Received : May 16, 2020
Revised : July 9, 2020
Accepted : July 12, 2020

บทคัดย่อ

ตามที่รัฐบาลเห็นความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล จึงได้ผลักดันพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคลจนสามารถประกาศใช้ในเดือนพฤษภาคมปี 2562 ซึ่งหน่วยงานของรัฐที่มีหน้าที่กำกับดูแลการให้บริการต่างๆ ผ่านระบบสารสนเทศต้องมีการกำหนดแนวทางและระเบียบในการจัดระบบการสำรวจ การจัดเก็บ การประมวล การใช้ประโยชน์ การพัฒนาระบบข้อมูลสารสนเทศ บริการสื่อสารของหน่วยงานในสังกัดและเป็นศูนย์ข้อมูลสารสนเทศเพื่อการบริหาร จึงทำให้การคุ้มครองข้อมูลส่วนบุคคลจึงเป็นหนึ่งในหน้าที่ในการป้องกันไม่ให้ข้อมูลส่วนบุคคลของทั้งบุคลากรภายในและผู้ใช้บริการถูกทำลาย ครอบคลุมไปถึงการกำหนดสิทธิของผู้ใช้ในระบบคอมพิวเตอร์และระบบอินเทอร์เน็ตซึ่งเป็นสื่อกลางในการสื่อสารต่อผู้ใช้บริการ

อีกทั้งในการบริหารจัดการระบบสารสนเทศเพื่อการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐเป็นการดำเนินการทั้งในส่วนนโนบาย และการดำเนินการจัดการด้านสารสนเทศ ที่จะต้องให้ความสำคัญในการรักษาความปลอดภัยข้อมูลด้วยการเข้ารหัสข้อมูล และเพิ่มกระบวนการรักษาความปลอดภัยในการให้บริการสารสนเทศผ่านเว็บไซต์ หรือแอพลิเคชัน แต่เนื่องจากการคุ้มครองข้อมูลส่วนบุคคลของผู้รับบริการเป็นภารกิจใหม่และมีมาตรฐานที่ซับซ้อนที่ไม่เคยปฏิบัติมาก่อนและมาตรการดังกล่าวส่งผลกระทบกว้างขวางต่อผู้ให้บริการและผู้รับบริการ ดังนั้นจึงมีความจำเป็นที่ต้องประเมินสถานการณ์และแนวการดำเนินงานที่หน่วยงานของรัฐปฏิบัติอยู่แล้ว และหามาตรการที่เหมาะสมสอดคล้องตามกฎหมายใหม่ที่จะประกาศใช้กับหน่วยงานทั่วประเทศตามลำดับ

คำสำคัญ: ข้อมูลส่วนบุคคล ระบบสารสนเทศ นโยบายความเสี่ยง และองค์กร

[1]ผู้ช่วยศาสตรจารย์ วิทยาลัยเทคโนโลยีสารสนเทศและการสื่อสารมหาวิทยาลัยรังสิต
Assistant Professor, College of Information and Communication Technology. Rangsit University
E-mail: auttapon.p@rsu.ac.th

Abstract

As the government consider importance of protecting personal information Therefore pushing the Personal Data Protection Act until it can be promulgated in May 2019, in which government agencies responsible for overseeing services through information systems, guidelines and regulations for establishing surveying systems, storing, processing and utilization must be established. Information system development communication service of the agency under and the information center for administration. Therefore, protection of personal information is one of the duties to prevent personal information of both internal personnel and service users. Covers the determination of user rights in computer systems and internet systems, which is a medium of communication to clients.

In addition, the management of information systems for the protection of personal information of government agencies is carried out both in policies and policies. And the implementation of information management ,that must give importance to data security with data encryption and increase the security process in providing information services via the website or mobile application. However, because the protection of personal information of clients is a new mission and has a complex standard that has never been implemented before, such measures have a profound effect on service providers and clients. Therefore, it is necessary to assess the situation and operational guidelines that government agencies already practice and find appropriate measures in accordance with the new law to be announced to agencies nationwide respectively.

Keyword: personal information, information system, risk policy, and organization

1. บทนำ

ตามที่สหภาพยุโรปได้ออก GDPR (General Data Protection Regulation) เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคล บังคับใช้เมื่อ 25 พฤษภาคม พ.ศ.2561 ซึ่งนอกจากมีผลบังคับใช้แก่การส่งข้อมูลภายในประเทศสมาชิกสหภาพยุโรปแล้ว ผู้ประกอบการและหน่วยงานรัฐในไทยที่ต้องติดต่อรับส่งข้อมูลส่วนบุคคลของประชาชนในประเทศที่เป็นสมาชิกสหภาพยุโรป (Cross-Border Data Transfer Issues) ก็ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอด้วย ที่สำคัญกว่านั้นคือความน่าเชื่อถือในมาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศมีผลกระทบต่อการค้าระหว่างประเทศ และการทำธุรกิจระหว่างประเทศ หากประเทศไทยไม่มีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลย่อมทำให้เสียโอกาส

และความเชื่อมั่นจากกลุ่มประเทศในสหภาพยุโรป และอาจรวมไปถึงประชาคมโลกที่กำลังตื่นตัวเรื่องการป้องกันข้อมูลส่วนบุคคล

หน่วยงานต่าง ๆ ซึ่งมีหน้าที่กำกับดูแลการให้บริการประชาชนอย่างมีประสิทธิภาพและจัดเก็บข้อมูลพื้นฐานเพื่อการบริหารและพัฒนาประเทศ จึงเป็นสิ่งสำคัญที่ต้องรู้ขอบเขตของการเข้าถึงข้อมูลส่วนบุคคล มีระบบควบคุมการเข้าถึงข้อมูลส่วนบุคคล มีระบบยืนยันตัวตนของผู้ขอเข้าถึงข้อมูลส่วนบุคคลรวมไปถึงต้องมีการกำหนดนโยบายสำหรับบุคคลภายในองค์กรที่ต้องเกี่ยวข้องกับการใช้งานข้อมูลส่วนบุคคลที่ได้รับการยินยอมจากเจ้าของข้อมูลแล้ว เนื่องจากมีข้อบังคับต่าง ๆ ที่หากละเมิดแล้ว จะมีผลให้เกิดโทษอาญาโทษทางปกครอง ซึ่งมีโทษปรับมากถึง 5 ล้านบาท อีกทั้งในอนาคตสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะออกระเบียบข้อบังคับ แนวทางด้านความมั่นคงปลอดภัยไซเบอร์ให้กับองค์กรต่าง ๆ ที่ต้องใช้ข้อมูลส่วนบุคคล (รวมถึงองค์กรที่ไม่ได้ใช้ข้อมูลส่วนบุคคล) ดังนั้นองค์กรควรปรับตัวและพัฒนาให้มีมาตรฐานด้านการคุ้มครองข้อมูลส่วนบุคคล

ในการจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลโดยอ้างอิงตามพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 [1-3] เพื่อเป็นการสร้างความตระหนักให้หน่วยงานในองค์กรรัฐที่มีการใช้ข้อมูลส่วนบุคคลจากประชาชน จะต้องแจ้งเหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัตินี้ เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ อีกทั้งในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หน่วยงานที่ดูแลข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ ซึ่งแนวทางในการดำเนินการทั้งหมดควรมีการบังคับใช้กับหน่วยงานเพื่อให้ประชาชนผู้ใช้บริการได้รับประโยชน์สูงสุดในการใช้บริการด้านสารสนเทศ

ในการให้ความคุ้มครองข้อมูลส่วนบุคคลในปัจจุบันจะปรากฏการให้ความคุ้มครองในสองลักษณะใหญ่ กล่าวคือ การให้ความคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นหลักทั่วไป ซึ่งเป็นการกำหนดหลักการการให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปที่สามารถนำมาปรับใช้ได้กับทุก ๆ กรณีที่เกี่ยวข้องกับการให้ความคุ้มครองข้อมูลส่วนบุคคล และการให้ความคุ้มครองข้อมูลส่วนบุคคลเฉพาะเรื่องหรือเฉพาะกรณี โดยจะเจาะจงเฉพาะกรณีของข้อมูลส่วนบุคคลที่ได้รับความคุ้มครอง เช่น การให้ความคุ้มครองข้อมูลส่วนบุคคลอันเนื่องมาจากการใช้บริการด้านการสื่อสารและโทรคมนาคม หรือการให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ทำธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น

การให้ความคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยนั้น [4] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 มาตรา 35 วรรค 3 ซึ่งกำหนดให้ความคุ้มครองไว้ว่า “บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงหาประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน อีกทั้งยังมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ที่ได้มีการบัญญัติให้ความคุ้มครองสิทธิข้อมูลส่วนบุคคลไว้ทั่วไป

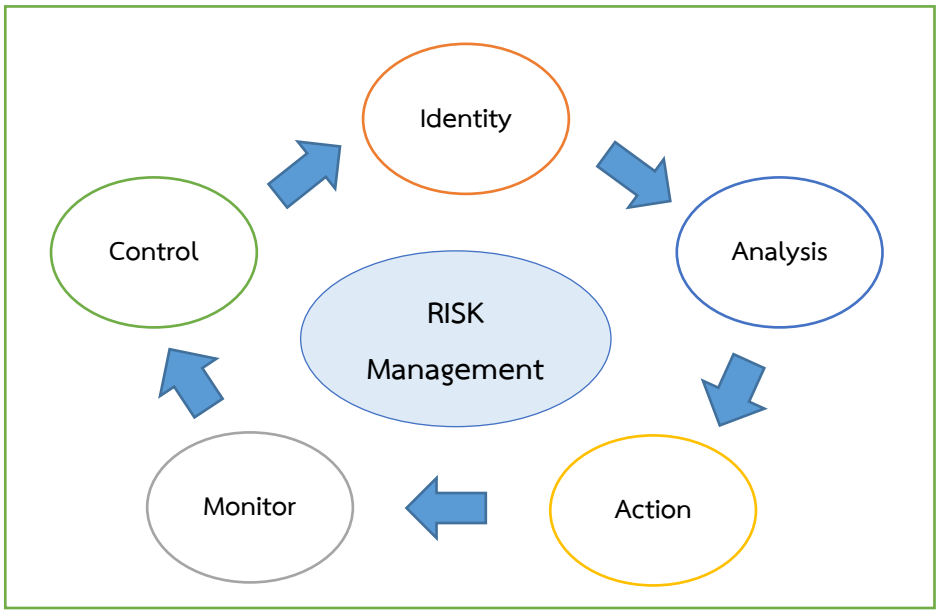
2. ข้อควรคำนึงในการคุ้มครองข้อมูลส่วนบุคคลต่อหน่วยงานให้บริการ

ข้อมูลส่วนบุคคลที่นำมาจัดเก็บไว้ในระบบฐานข้อมูลนั้นอาจมีระดับของความสำคัญแตกต่างกันไป กลุ่มข้อมูลบางกลุ่มอาจเป็นความลับสุดยอดห้ามเผยแพร่เด็ดขาด แต่ข้อมูลบางกลุ่มก็เป็นความรู้ทั่วไปสามารถเปิดเผยได้ ดังนั้นจึงมีการพัฒนาเทคนิคที่นำมาใช้ในการให้ความความปลอดภัยแก่ข้อมูลในระบบฐานข้อมูลที่มีผู้ใช้หลาย ๆ คน ระบบจัดการฐานข้อมูลต้องทำหน้าที่ดูแลว่ากลุ่มผู้ใช้กลุ่มใดได้รับอนุญาตให้เข้าใช้ข้อมูลส่วนใดได้บ้าง

จากรูปที่ 1 การรักษาความปลอดภัยฐานข้อมูลไม่ใช่เพียงแค่การติดตั้งระบบรักษาความปลอดภัยเท่านั้น แต่จะรวมถึงการวิเคราะห์และบริหารความเสี่ยงที่ประกอบด้วยภัย คุกคาม (Threat) ทั้งจากคนภายในองค์กรและคนภายนอกองค์กร และช่องโหว่หรือ จุดอ่อน (Vulnerability) การกำหนด การบังคับใช้นโยบาย (Policy) และการเฝ้าระวัง เหตุการณ์อยู่ตลอดเวลา (Monitoring) นั่นคือต้องมีมาตรการหรือการควบคุมความปลอดภัยที่มีประสิทธิภาพ ประกอบด้วย นโยบาย วิธีปฏิบัติ และกระบวนการขององค์กรในการรักษาข้อมูลให้มีความถูกต้องและน่าเชื่อถือ

2.1 นโยบาย

นโยบายของหน่วยงานมีผลสำคัญยิ่งต่อการรักษาความปลอดภัยของข้อมูล นโยบายขององค์กรจะต้องมุ่งเน้นที่วัตถุประสงค์และการทำงานที่ดี องค์กรจำเป็นต้องมีการกำหนดนโยบายด้านความปลอดภัยให้ชัดเจน โดยมีกฎระเบียบ ข้อบังคับ และหน้าที่ความรับผิดชอบ [5] และวิธีปฏิบัติให้บุคลากรใช้เป็นหลักในการทำงาน รวมทั้งการติดตาม ตรวจสอบการปฏิบัติตามกฎระเบียบที่วางไว้อย่างเคร่งครัดและสม่ำเสมอ เช่น กำหนดให้แน่นอนว่าระบบรักษาความปลอดภัยใครเป็นผู้ปฏิบัติ ใช้กับส่วนใดบ้าง ในระบบมีวิธีการปฏิบัติอย่างไร ใครสามารถเข้าถึงข้อมูลส่วนใดได้บ้าง ใครมีสิทธิที่จะเปลี่ยนแปลงแก้ไขข้อมูลนั้น



รูปที่ 1 นโยบายการรักษาความปลอดภัยของข้อมูล

2.2 สถานภาพของระบบการรักษาความปลอดภัย

จะต้องมีการตรวจสอบสถานภาพของระบบการรักษาความปลอดภัยในปัจจุบันอยู่ในระดับใด และต้องการปรับปรุงหรือเปลี่ยนแปลงอย่างไรบ้าง ความต้องการในการใช้ข้อมูลที่ปลอดภัยและคำแนะนำจากส่วนต่าง ๆ ที่ใช้งานภายในระบบการแจกงานไปสู่เจ้าหน้าที่ที่รับผิดชอบ มีตารางเวลาที่กำหนดว่าส่วนใดของระบบจะต้องปรับปรุงอะไรบ้าง ณ เวลาใด มีการจัดทำแผนฉุกเฉินเพื่อให้องค์กรสามารถดำเนินการต่อไปได้เมื่อมีวิกฤตการณ์เกิดขึ้น บุคลากรที่เกี่ยวข้องควรจะคุ้นเคยกับแผนเหล่านี้และมีการทดสอบให้มั่นใจว่าสามารถใช้งานได้

2.3 การจัดการความเสี่ยงของความเป็นส่วนตัวและความเสี่ยงขององค์กร

การกระทำใด ๆ ต่อข้อมูลส่วนบุคคลที่มีปัญหาจะต้องสามารถประเมินผลกระทบที่ควรจะเกิดขึ้น ซึ่งการประเมินผลกระทบที่เป็นความเสี่ยงของข้อมูลความเป็นส่วนตัวและความเสี่ยงขององค์กรร่วมกัน โดยบุคคลไม่ว่าจะเป็นคนเดียวหรือกลุ่มจะได้รับผลกระทบโดยตรงจากปัญหาอันเป็นผลมาจากปัญหาด้านความปลอดภัยข้อมูลส่วนบุคคลจากประสบการณ์ในแต่ละบุคคล โดยหน่วยงานอาจจะประสบกับผลกระทบต่าง ๆ เช่น ค่าใช้จ่ายที่ไม่ปฏิบัติตาม การยกเลิกการให้บริการ สิ่งที่อันตรายจากภายนอกของหน่วยงาน หรือวัฒนธรรมภายในซึ่งผลกระทบขององค์กร สิ่งเหล่านี้สามารถเป็นตัวขับเคลื่อนสำหรับการตัดสินใจเพิ่มงบประมาณในการจัดสรรทรัพยากรเพื่อเสริมสร้างความแข็งแกร่งทางด้านเทคโนโลยีสารสนเทศในการรักษาความเป็นส่วนตัวและเพื่อช่วยให้องค์กรนำความเสี่ยงด้านความเป็นส่วนตัวเข้ามามีส่วนร่วมกับความเสี่ยงอื่น ๆ ที่กำลังจัดการในระดับภาพรวมขององค์กร จากรูปที่ 2 จะแสดงถึงความสัมพันธ์ระหว่างความเสี่ยงด้านความเป็นส่วนตัวและความเสี่ยงขององค์กร

รูปที่ 2 ความสัมพันธ์ระหว่างความเสี่ยงด้านเป็นส่วนตัวและความเสี่ยงขององค์กร

การจัดการความเสี่ยงด้านความเป็นส่วนตัวเป็นกลุ่มของกระบวนการระหว่างองค์กรที่ช่วยให้เข้าใจว่าระบบสารสนเทศและบริการ อาจจะสร้างปัญหาให้กับบุคคลและวิธีการพัฒนาระบบสารสนเทศในการแก้ปัญหาที่มีประสิทธิภาพเพื่อจัดการกับความเสี่ยงดังกล่าว โดยการประเมินความเสี่ยงด้านความเป็นส่วนตัวเป็นกระบวนการย่อย ๆ สำหรับการระบุ การประเมิน การจัดลำดับความสำคัญ และตอบสนองต่อความเสี่ยงด้านความเป็นส่วนตัวที่เฉพาะเจาะจง [6-7] ซึ่งการประเมินความเสี่ยงด้านความเป็นส่วนตัวจะเป็นกระบวนการย่อย โดยทั่วไปการประเมินความเสี่ยงด้านความเป็นส่วนตัวควรจัดทำข้อมูลที่สามารถช่วยให้หน่วยงานสามารถชั่งน้ำหนักประโยชน์ของการประมวลผลของข้อมูลกับความเสี่ยง และเพื่อกำหนดการตอบสนองต่อปัญหาที่เหมาะสม สำหรับการระบุปัญหา การประเมินผล การจัดลำดับความสำคัญ และการตอบสนองต่อความเสี่ยงด้านความเป็นส่วนตัว โดยหน่วยงานอาจเลือกที่จะตอบสนองต่อความเสี่ยงด้านความเป็นส่วนตัวในรูปแบบต่าง ๆ ซึ่งขึ้นอยู่กับผลกระทบต่อองค์กรประกอบด้วยวิธี

- การลดความเสี่ยง (เช่น องค์กรอาจจะสามารถใช้มาตรการทางเทคนิคและ/หรือนโยบายเกี่ยวกับ ระบบหรือบริการที่ลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้)
- การโอนถ่ายหรือแบ่งปันความเสี่ยง (เช่น สัญญาเป็นวิธีการแบ่งปันหรือโอนถ่ายความเสี่ยงให้องค์กรอื่น ๆ การประกาศความเป็นส่วนตัว และกลไกการยินยอมจากผู้ใช้บริการเป็นวิธีการแบ่งปันความเสี่ยงด้วยตัวบุคคล)
- การหลีกเลี่ยงความเสี่ยง (เช่น หน่วยงานอาจกำหนดว่าความเสี่ยงนั้นมีมากกว่าผลประโยชน์และการสละสิทธิ์หรือยกเลิกการประมวลผลข้อมูล) หรือ
- การยอมรับความเสี่ยง (เช่น องค์กรอาจจะพิจารณาว่าปัญหาของแต่ละบุคคลมีน้อยหรือไม่ที่น่าจะเกิดขึ้น ดังนั้นถ้าผลประโยชน์มีมากกว่าความเสี่ยงและไม่จำเป็นต้องลงทุนทรัพยากรเพื่อลดผลกระทบ)

3. การควบคุมความปลอดภัยข้อมูล

ปัจจุบันภัยคุกคามฐานข้อมูลมาจากหลายทางและยังส่งผลต่อระบบคอมพิวเตอร์ร้ายแรงขึ้น การควบคุมความปลอดภัยจึงถูกนำมาพิจารณาตั้งแต่ช่วงแรกของการพัฒนาระบบ เช่น การควบคุมการเข้าถึง (Access Control) การยืนยันตัวบุคคล (Authentication) และการให้อำนาจหน้าที่ (Authorization) เพื่อระบุตัวบุคคลที่ติดต่อหรือทำธุรกรรมร่วมด้วย การตรวจสอบ (Auditing) การสร้างข้อมูลให้เป็นความลับหรือการเข้ารหัสข้อมูล (Encryption) การควบคุมความถูกต้องสมบูรณ์ (Integrity Controls) การสำรองข้อมูล (Backups) และ ความปลอดภัยแอพลิเคชัน (Application Security) เป็นต้น

3.1 การควบคุมการเข้าถึง (Access Control) ข้อมูล

สิ่งสำคัญในการสร้างระบบรักษาความปลอดภัยในระบบฐานข้อมูล คือการควบคุมการเข้าถึงข้อมูล เป็นการกำหนดสิทธิในการเข้าถึงฐานข้อมูล การกำหนดการใช้ข้อมูลโดยกำหนดสิทธิหรือการยืนยันตัวบุคคล ในการเข้าถึงฐานข้อมูลเฉพาะผู้ที่เกี่ยวข้อง หรือ ทำการเข้ารหัสฐานข้อมูลโดยใช้อัลกอริธึมที่มีความปลอดภัยสูง กำหนดว่าใครบ้างที่สามารถเข้าไปใช้ได้ ผู้ที่จะเข้ามาใช้ระบบฐานข้อมูลได้จะต้องได้รับการอนุญาตก่อน และเมื่อเข้าระบบได้แล้วผู้ใช้งานนั้นจะสามารถทำอะไรกับข้อมูลได้บ้างก็จะขึ้นอยู่กับการให้สิทธิ (Authorization) ของผู้บริหารฐานข้อมูล

3.2 การยืนยันตัวบุคคล [8] และการให้อำนาจหน้าที่เป็นระบบรักษาความปลอดภัยขั้นแรกที่นิยมใช้กันมากที่สุดในปัจจุบัน เช่น

3.2.1 การกำหนดรหัสผ่านและรหัสการเข้าใช้ (User Name and Password) การเข้ารหัสข้อมูลเป็นพื้นฐานสำคัญในการรักษาความปลอดภัยฐานข้อมูล ผู้ใช้จะมีรหัสเฉพาะของตนควรกำหนดรหัสที่ยากต่อการถอดรหัส หลักการพื้นฐานควรกำหนดรหัสให้มีความยาวไม่น้อยกว่า 8 ตัวอักษร และควรให้มีการผสมระหว่างตัวอักขระพิเศษและตัวเลข ไม่ควรนำเอาคำศัพท์ในพจนานุกรมหรือใช้ชื่อ วัน เดือน ปีเกิด หมายเลขโทรศัพท์เพราะรหัสเหล่านี้ง่ายต่อการถอดรหัสหรือทำการเข้ารหัสข้อมูลโดยใช้อัลกอริธึมที่มีความปลอดภัยสูงและควรเปลี่ยนรหัสเมื่อใช้ไปได้ระยะเวลาหนึ่งรหัสผ่าน

3.2.2 การใช้บัตรสมาร์ทการ์ด (Smart Card) ผู้ใช้จะต้องมีบัตรสำหรับเข้าระบบคอมพิวเตอร์ บัตรนี้จะคล้ายกับบัตร ATM (Automatic Teller Machine) และต้องป้อนรหัสส่วนตัว (Personnel Identification Number หรือ PIN) หรือการใช้บัตรกุญแจ (Key Card) หรือบัตรผ่านทาง (Badge) ซึ่งเป็นวัตถุครอบครอง (Possessed Object) เพื่อผ่านทางเข้าไปใช้ระบบหรือข้อมูลที่เก็บในคอมพิวเตอร์เป็นรูปแบบที่นิยมกันมากในปัจจุบัน

3.2.3 การใช้การตรวจสอบจากร่างกายมนุษย์ (Biometric) เช่น ม่านตา หรือเรตินา (Retina) เสียง หรือ ลายนิ้วมือ ตรวจสอบผู้มีสิทธิก่อนเข้าสู่ระบบ การตรวจสอบในลักษณะนี้จะต้องนำลักษณะของผู้ที่ต้องการเข้าไปใช้ฐานข้อมูลไปเปรียบเทียบกับลักษณะข้อมูลของผู้ใช้ที่มีอยู่ในเครื่องคอมพิวเตอร์ ถ้าตรงกันจึงจะมีสิทธิเข้าไปใช้ข้อมูลได้

3.3 การตรวจสอบ (Auditing)

เป็นการตรวจสอบผู้ที่เข้ามาติดต่อกับระบบ โดยใช้ซอฟต์แวร์ในการตรวจสอบ โดยบันทึกข้อมูลของการเข้ามาใช้งานทุกครั้งไว้ใน Log Files โปรแกรมจะทำการบันทึกทั้งวันที่ เวลา บุคคลที่เข้ามาใช้งาน สามารถทำการตรวจสอบข้อมูลย้อยหลังได้ ปัจจุบันมีซอฟท์แวร์ที่ใช้เป็นเครื่องมือรักษาความปลอดภัยในระบบที่กำลังเริ่มใช้อย่างแพร่หลาย ได้แก่ ระบบไฟร์วอลล์ (Firewall) ซึ่งเป็นซอฟท์แวร์ทำหน้าที่เสมือนกับกำแพงกันไฟไม่ให้ลุกลามขยายตัวหากมีไฟไหม้เกิดขึ้น

การติดตามตรวจสอบและสรุปการใช้งานฐานข้อมูลอยู่เสมอ อย่างน้อยเดือนละครั้ง โดยเน้นส่วนข้อมูลสำคัญ เช่น ผู้ใช้เป็นใคร หมายเลข IP เข้าบ่อยแค่ไหน และทำอะไรไปบ้าง ทำสำเร็จหรือไม่ เพื่อตรวจสอบพฤติกรรมที่อาจจะผิดปกติไปจากเดิม ไม่ว่าระบบเครือข่ายจะมีฮาร์ดแวร์หรือซอฟท์แวร์ที่ดีเพียงใดในการปกป้องระบบเครือข่าย สิ่งที่สำคัญอย่างยิ่งก็คือผู้ใช้งานในระบบจะต้องคอยช่วยสอดส่องดูแลและป้องกันไม่ให้ตนเองเป็นช่องทางผ่านของแครกเกอร์ ทั้งนี้ไม่มีระบบเครือข่ายใดที่ปลอดภัยร้อยเปอร์เซ็นต์จากแครกเกอร์

3.4 การสร้างข้อมูลให้เป็นความลับ (Encryption)

การเข้ารหัสข้อมูลโดยพื้นฐานแล้วจะเกี่ยวข้องกับวิธีการทางคณิตศาสตร์เพื่อใช้ในการป้องกันข้อมูลหรือข้อความตั้งต้นที่ต้องการส่งไปถึงผู้รับ ข้อมูลตั้งต้นจะถูกแปรเปลี่ยนไปสู่ข้อมูลหรือข้อความอีกรูปแบบหนึ่งที่ไม่สามารถอ่านเข้าใจได้โดยใครก็ตามที่ไม่มี Key สำหรับเปิดดูข้อมูลนั้น เรียกกระบวนการในการแปรรูปของข้อมูลตั้งต้นว่า "การเข้ารหัสข้อมูล" (Encryption) และกระบวนการในการแปลงข้อความที่ไม่สามารถอ่าน และทำความเข้าใจให้กลับไปสู่ข้อความดั้งเดิมว่าการถอดรหัสข้อมูล (Decryption) โดยมีอัลกอริทึมที่ใช้ในการสร้างรหัสลับต่าง ๆ ดังรูปที่ 3

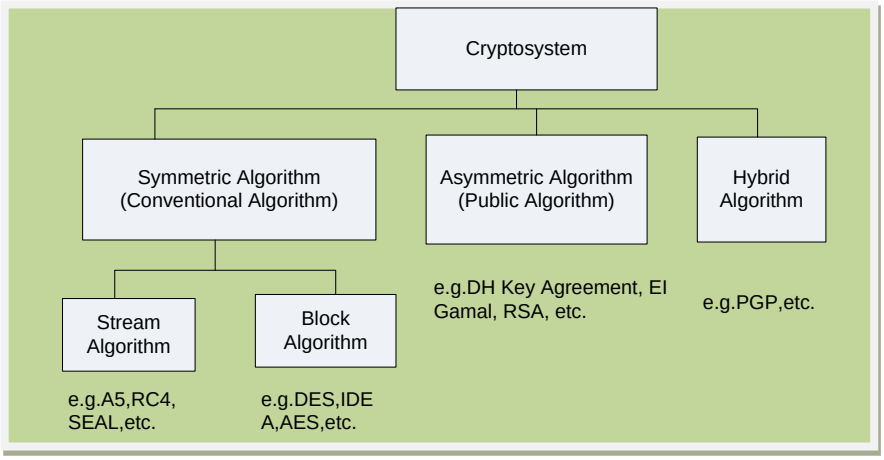
ข้อกำหนดทั่วไปของระบบการเข้ารหัส

ระบบการเข้ารหัสลับใด ๆ จะต้องมีคุณสมบัติเป็นไปตามข้อกำหนดทั่วไปของระบบการเข้ารหัสลับ 3 ข้อ เพื่อที่จะเป็นที่ยอมรับในการนำไปใช้งานในทางปฏิบัติ ข้อกำหนดเหล่านั้นคือ

1. อัลกอริทึมที่ใช้ในการเข้าและถอดรหัสลับต้องมีประสิทธิภาพในทุก ๆ รูปแบบของ Key ที่เป็นไปได้ เช่น ถ้า Key ที่ใช้ในการเข้าและถอดรหัสลับมีขนาด 8 บิต จำนวนรูปแบบของ Key ที่เป็นไปได้ทั้งหมดจะเท่ากับ 28 หรือ 256 รูปแบบ ในการใช้งานอัลกอริทึมในระบบการเข้ารหัสลับไม่ว่าจะใช้ Key รูปแบบใด ระดับความปลอดภัยของข้อความรหัสที่ได้จากการใช้ Key รูปแบบนั้นต้องคงที่ ไม่เปลี่ยนแปลงเมื่อเทียบกับระดับความปลอดภัยของข้อความรหัสที่ได้จากการใช้ Key รูปแบบอื่น ๆ

2. ระบบต้องมีความง่ายต่อการนำไปใช้งาน ข้อกำหนดนี้บ่งชี้ถึงความสามัญ (Simple) ในการคำนวณหา Key โดยวิธีการแปลงแบบผกผันได้ (Invertible Transformation) ซึ่งจะมีประโยชน์เมื่อนำมาใช้ในกระบวนการถอดรหัสลับ นอกจากนี้ความหมายของข้อกำหนดนี้ยังครอบคลุมไปถึงระยะเวลาที่ใช้ในการเข้าและถอดรหัสลับ กล่าวคือ อัลกอริทึมที่ใช้ในการเข้าและถอดรหัสลับ ไม่ควรมีความซับซ้อนและใช้เวลาในการประมวลผลมากเกินไป เนื่องจากในทางปฏิบัติผู้ใช้งานมักทำการเข้าและถอดรหัสลับข้อมูลในเวลาที่ทำการส่งหรือรับข้อมูลนั้น ๆ ส่งผลให้ระบบที่มีความซับซ้อนสูงจะทำให้มีการติดต่อสื่อสารแบบเวลาจริง (Real-Time Communication) ไม่ได้

3. ความปลอดภัยของระบบควรขึ้นอยู่กับการเป็นความลับของ Key เท่านั้น ไม่ขึ้นกับการเป็นความลับของอัลกอริทึมที่ใช้ในการเข้าและถอดรหัสลับ ข้อกำหนดนี้บ่งชี้ว่าระบบการเข้ารหัสลับที่ดีไม่ควรเกิดจุดอ่อนเพียงเพราะว่าผู้โจมตีรู้และเข้าใจถึงวิธีการหรืออัลกอริทึมที่ใช้ในการเข้าและถอดรหัสลับ



รูปที่ 3 ประเภทอัลกอริทึมที่ใช้ในการสร้างรหัสลับ

3.5 การทำสำเนาข้อมูล (Data Copy Setting)

กรณีที่ข้อมูลอยู่ในแผ่นบันทึกอาจทำสำเนาข้อมูลทั้งแผ่นโดยใช้คำสั่ง Copy แต่ถ้าข้อมูลอยู่ในจานแม่เหล็กชนิดแข็งหรือกรณีที่มีข้อมูลเป็นจำนวนมากจะทำสำเนาโดยการใช้คำสั่ง Backup ลงบนแผ่นบันทึกหรือในเทปแม่เหล็ก ทั้งนี้ในการใช้งานจริงในการรักษาความปลอดภัยของฐานข้อมูลมักจะเป็นการนำเทคนิคต่าง ๆ หลายเทคนิคมาประยุกต์ใช้งานร่วมกันเพื่อให้ระบบความปลอดภัยนั้นมั่นคงและเชื่อถือได้

3.6 การควบคุมความถูกต้องหรือความคงสภาพของข้อมูล (Integrity Controls)

หมายถึง การที่ระบบจัดการฐานข้อมูลจะจัดการกับข้อมูล (เมื่อมีการใช้คำสั่งเพิ่ม ลบ หรือแก้ไขข้อมูล) เพื่อให้แน่ใจว่าข้อมูลในฐานข้อมูลมีความถูกต้องน่าเชื่อถือตามกฎ/เงื่อนไขและข้อตกลง (Integrity Rules) ที่ได้กำหนดไว้ตั้งแต่ต้น กฎดังกล่าวเป็นกฎระเบียบที่กำหนดขึ้นในขั้นตอนการออกแบบฐานข้อมูลเพื่อรักษาให้ข้อมูลในฐานข้อมูลมีความถูกต้อง ส่วนการควบคุมความถูกต้องของข้อมูลจะเป็นขั้นตอนที่เกิดขึ้นเมื่อนำฐานข้อมูลไปใช้งานแล้ว

3.7 การสำรองข้อมูล (Backups)

เป็นการคัดลอกแฟ้มข้อมูลเพื่อทำสำเนาและหลีกเลี่ยงความเสียหายที่อาจจะเกิดขึ้น ถ้าข้อมูลเกิดการเสียหายหรือสูญหาย โดยสามารถนำข้อมูลที่สำรองไว้มาใช้งานได้ทันที การสำรองข้อมูลทำได้หลายวิธี เช่น

3.7.1 ใช้โปรแกรม System Restore ซึ่งเป็นโปรแกรมหนึ่งในการสำรองและเรียกข้อมูลกลับคืน

3.7.2 สำรองข้อมูลด้วยอุปกรณ์ฮาร์ดแวร์ เช่น ฮาร์ดดิสก์แบบติดตั้งภายนอกผ่านพอร์ต USB เทปแบ็กอัพ ซิปไดรฟ์ (Zip Drive) และ เครื่องบันทึก DVD/CD เป็นต้น

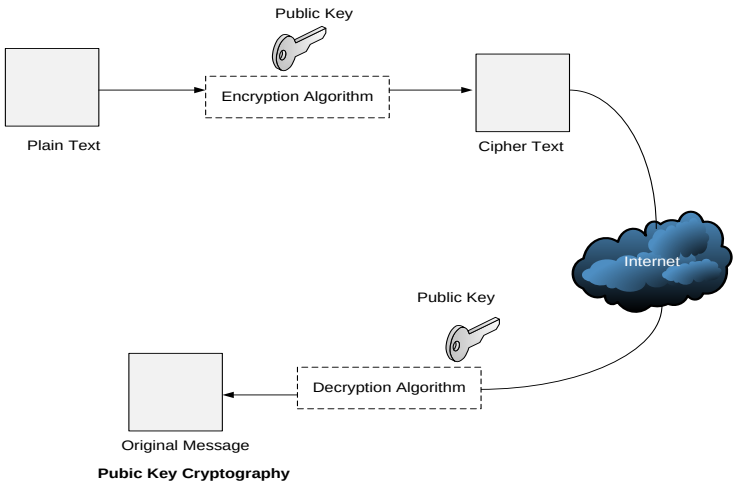
3.7.3 ใช้โปรแกรมสำรองข้อมูล (Backup Program) เช่น โปรแกรม Symantec NetBackup, Norton Ghost, Microsoft DPM เป็นต้น

3.7.4 การสำรองข้อมูลบนระบบเครือข่ายแบบคลาวด์ (Cloud) เช่น Apple iCloud, Google Drive, One Drive, Dropbox เป็นต้น

ทั้งนี้ระบบที่มีผู้ใช้เป็นจำนวนมากจำเป็นอย่างยิ่งที่จะต้องมีการควบคุมการเรียกใช้ข้อมูลเพื่อป้องกันผู้ที่ไม่มีอำนาจในการเรียกใช้ข้อมูลนำข้อมูลจากฐานข้อมูลมาใช้ อันอาจจะเกิดผลเสียกับระบบฐานข้อมูลได้ ระบบบริหารจัดการข้อมูลจะกำหนดสิทธิในการเข้าถึงข้อมูลและมอบอำนาจการเข้าถึงข้อมูลตลอดจนเรียกคืนอำนาจจากผู้ใช้ในระบบได้ด้วยการใช้คำสั่งภาษา SQL การยืนยันตัวบุคคลเป็นระบบรักษาความปลอดภัยขั้นแรกที่นิยมใช้กันมากที่สุด ในปัจจุบันเพื่อให้มั่นใจได้ว่าผู้ที่จะเข้าระบบได้นั้นจะต้องเป็นผู้ที่มีสิทธิจริง ๆ ผู้ใช้งานแต่ละคนจะต้องป้อนรหัสผ่านจึงจะมีสิทธิเข้าถึงข้อมูลได้ การยืนยันตัวบุคคลโดยคำสั่ง SQL เป็นการกำหนดรหัสผ่านให้แก่ผู้ใช้แต่ละคนในการจัดการข้อมูลในตารางหรือวิว

3.8 การรักษาความปลอดภัยในการให้บริการผ่านเว็บไซต์

การสื่อสารอย่างปลอดภัยในการให้บริการผ่านเว็บไซต์โดยโพรโทคอล HTTPs คือการทำงานระหว่างไคลแอนต์และเซิร์ฟเวอร์ โดยการอนุญาตให้มีกระบวนการพิสูจน์ตัวตนร่วมกับการใช้งานลายเซ็นดิจิทัลสำหรับการรักษาความถูกต้องของข้อมูลและการเข้ารหัสข้อมูลเพื่อป้องกันความเป็นส่วนตัวระหว่างการสื่อสารข้อมูลโพรโทคอล SSLหรือ TLS ที่อนุญาตให้สามารถเลือกวิธีการในการเข้ารหัส วิธีสร้างไดเจสต์ และลายเซ็นดิจิทัล ได้อย่างอิสระก่อนการสื่อสารจะเริ่มต้นขึ้น โดยจากรูปที่ 4 โพรโทคอล HTTPs มีการเข้ารหัสข้อมูลแบบ Asymmetric Encryption ที่จะแบ่ง Key ออกเป็นชุดละ 2 ดอกคือ Public Key สำหรับ Encrypt ที่จะแจกให้ผู้ร้องขอ และ Private Key สำหรับการ Decrypt ข้อมูลกลับมาเป็นเหมือนเดิม ซึ่งเจ้าของไม่สามารถให้ผู้อื่น ในการเริ่มการเชื่อมต่อก็จะมีการแลกกุญแจเพื่อสร้างกุญแจดอกเดียวที่ใช้แค่ใน Session นั้น ๆ เพื่อให้มั่นใจว่าเว็บไซต์ที่เข้าเป็นของจริง ต่อจากนั้นจะมีการตรวจสอบ Certificate โดยจะอ่านไปตาม CA เพื่อยืนยันว่า Certificate นี้มีตัวตนอยู่จริง และไม่ถูกยกเลิกนั่นเอง จากทั้งหมดนี้จุดประสงค์มีเพียง 2 อย่างเท่านั้นคือ การทำให้ข้อมูลที่ส่งไปจะมีแค่ผู้รับเท่านั้นที่อ่านได้ และ มั่นใจได้ว่าผู้ที่ติดต่อด้วยคือตัวจริงไม่ใช่ตัวปลอม



รูปที่ 4 แสดงการรักษาความปลอดภัยของ HTTPs

Digital Certification คือใบรับรองว่าเว็บที่สื่อสารอยู่ด้วยนั้นคือเว็บที่ต้องการจะสื่อสาร ไม่ใช่การปลอมตัวมา ซึ่งกระบวนการออก Certificate นี้ ก็ต้องการความน่าเชื่อถือได้ นั่นคือ Certificate Authority (CA) โดยใน Certificate จะมี Digital Signature ของ CA รับรองอยู่ ซึ่ง Certificate Authority (CA) ก็คือองค์กรที่ทำหน้าที่ออก Certificate ซึ่งการจะออก Certificate ได้จะต้องตรวจสอบก่อนว่าผู้ที่ขอเป็นใครเชื่อถือได้จริงหรือไม่ เพราะถ้าข้อมูลที่ไม่ถูกต้อง CA นั้นก็จะสูญเสียความน่าเชื่อถือไป

ขั้นตอนการขอใบรับรอง

1. ผู้ให้บริการ สร้าง Certificate Signing Request (CSR) และส่ง Public Key ของตัวเองไปให้ CA CA ตรวจสอบและยืนยันความถูกต้อง
2. CA ออกใบรับรองให้ โดยเนื้อหาประกอบด้วย ข้อมูลของผู้ให้บริการ, Public Key ที่ส่งมา, และรับรองด้วย Digital Signature ของ CA
3. ผู้ให้บริการเอาใบรับรองนั้นไปใช้แสดงตัวเวลามีคนสื่อสารด้วย

4. สรุปการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ

การคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน ซึ่งเข้าไปมีบทบาทมากบ้างน้อยบ้างตามแต่ศักยภาพของหน่วยงาน ด้านการบริหารงาน และการจัดกิจกรรมร่วมกับหน่วยงานภายนอกหรือหน่วยงานภายใน และข้อมูลได้แสดงให้เห็นถึงปัญหาหลักคือเนื่องจากเป็นเรื่องที่ใหม่สำหรับการป้องกันข้อมูลส่วนบุคคล ซึ่งจากการเข้าสัมภาษณ์บุคลากรส่วนภูมิภาคที่มีส่วนเกี่ยวข้องกับงานด้านสารสนเทศนั้น [9] สิ่งสำคัญคือการสร้างความตระหนัก และรับรู้ว่าข้อมูลส่วนบุคคลใดที่หน่วยงานของรัฐได้จัดเก็บมาจากหลากหลายช่องทาง อาทิ ข้อมูลบัตรประชาชน ผู้ที่ดูแลและจัดเก็บข้อมูลจะต้องให้ความสำคัญในรักษาความลับของข้อมูล และต้องพร้อมที่จะเรียกข้อมูลนั้น ๆ เพื่อทำลายหรือเปลี่ยนแปลงตามที่เจ้าของข้อมูลต้องการ

4.1 ความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ

การให้ความคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยนั้น รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 มาตรา 35 วรรค 3 ซึ่งกำหนดให้ความคุ้มครองไว้ว่า “บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงหาประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน อีกทั้งยังมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ที่ได้มีการบัญญัติให้ความคุ้มครองสิทธิข้อมูลส่วนบุคคลไว้ทั่วไป

ทั้งนี้ในการให้บริการประชาชนอย่างมีประสิทธิภาพและจัดเก็บข้อมูลพื้นฐานเพื่อการบริหารและพัฒนาประเทศและยังเป็นหน้าที่และความรับผิดชอบของหน่วยงานคือการกำหนดแนวทางและระเบียบในการจัดระบบ การสำรวจ การจัดเก็บ การประมวล การใช้ประโยชน์ การพัฒนาระบบข้อมูลสารสนเทศบริการสื่อสารของหน่วยงานในสังกัด จึงทำให้การเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคลสามารถทำได้โดยง่าย สะดวก และรวดเร็ว อันจะลดโอกาสซึ่งความเดือดร้อน รำคาญ หรือความเสียหายในกรณีที่มีการนำไปแสวงหาประโยชน์หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมหรือแจ้งล่วงหน้า หรืออย่างน้อยการให้บริการประชาชนในรูปแบบต่างๆ ผ่านเว็บไซต์ ควรมีการทำ Digital Certification

เพื่อรับรองตัวตน และมีตราประทับยืนยันความถูกต้อง จากองค์กรที่สังคมเชื่อถือ และมีการใช้ HTTPs เพื่อความปลอดภัยในการสื่อสารข้อมูล

4.2 ข้อเสนอแนะ

หน่วยงานรัฐที่มีการจัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการ ไม่ว่าจะเป็นทางเว็บไซต์ App สื่อ Social Media หรือ สื่อดิจิทัลอื่น ๆ ควรเตรียมตัวและจัดทำดังนี้

4.2.1 ในกรณีที่มีการให้แจ้งการเปลี่ยนแปลงวัตถุประสงคหรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูล ทราบและขอความยินยอมก่อนทุกครั้งตามวิธีการและภายในกำหนดเวลาที่ประกาศ เช่น การแจ้งล่วงหน้าให้เจ้าของข้อมูลทราบก่อน 15 วัน โดยการส่งทางจดหมายอิเล็กทรอนิกส์ หรือประกาศไว้ในหน้าแรกของ เว็บไซต์เว้นแต่กฎหมายจะกำหนดไว้เป็นอย่างอื่น

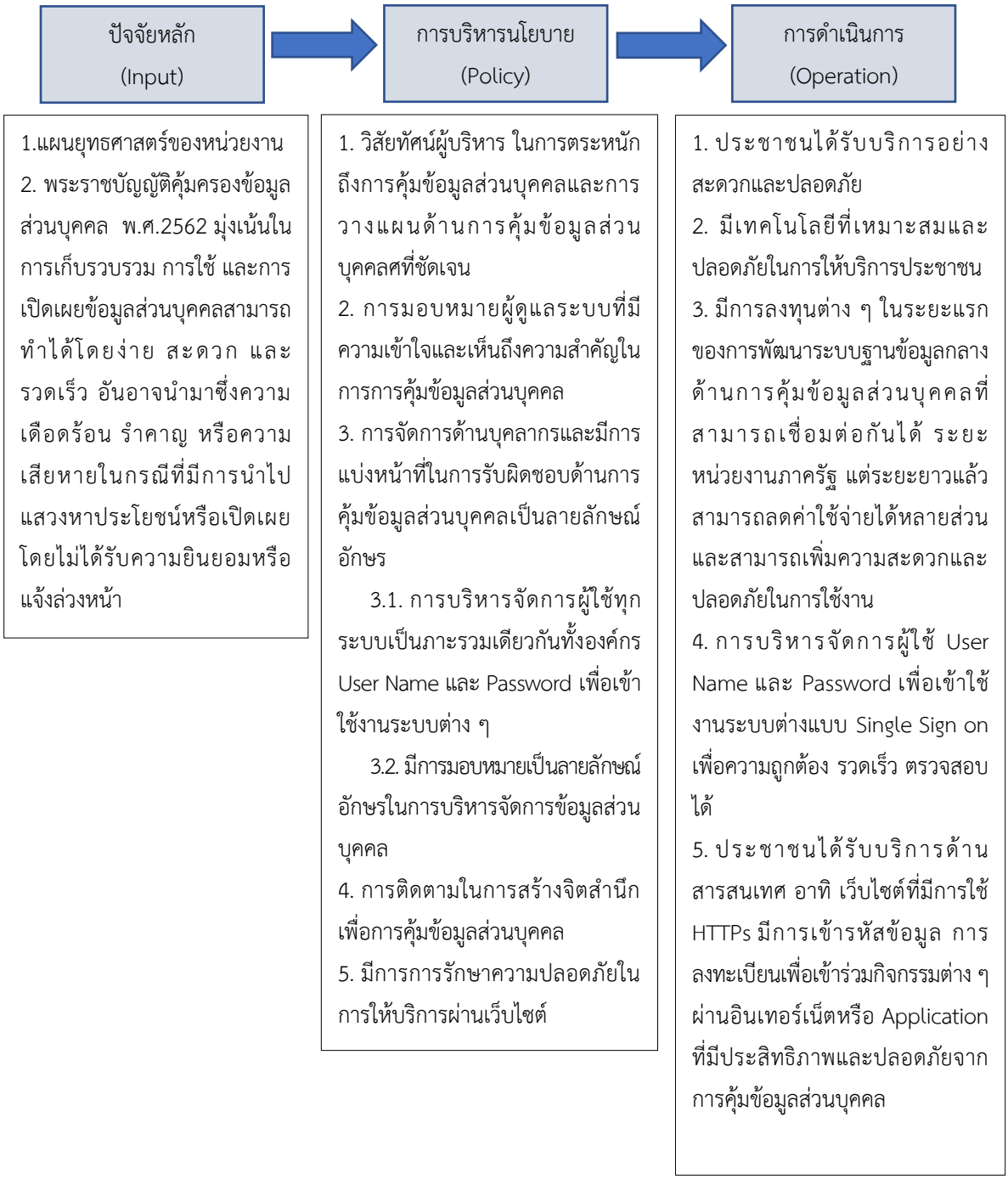
4.2.2 ให้หน่วยงานของรัฐระบุบนเว็บไซต์สำหรับการใช้คุกกี้ที่เชื่อมโยงกับข้อมูลส่วนบุคคลว่าผู้ใช้บริการจะใช้คุกกี้เพื่อวัตถุประสงค์และประโยชน์ใด และให้สิทธิที่จะไม่รับการต่อเชื่อมคุกกี้ได้

4.2.3 มีหน้าในเว็บไซต์ App หรือสื่อดิจิทัลอื่น ๆ โดยมีการเข้ารหัสข้อมูล และมีการรักษาความปลอดภัยการเข้าใช้งานด้วยโพรโทคอล HTTPs โดยจะระบุวัตถุประสงค์ของการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนตัว ในภาษาที่เข้าใจง่ายและตรงไปตรงมา สำหรับคนที่มีเว็บไซต์อยู่แล้วอาจจะคุ้นเคยกับหน้า ‘นโยบายความเป็นส่วนตัว’ (Privacy Policy) ที่จะมีเนื้อหาบางส่วนใกล้เคียงกัน สามารถนำปรับมาใช้ได้แต่ต้องใช้ข้อความที่สั้น ๆ เข้าใจง่าย ๆ มากกว่า

4.2.4 ทุกครั้งที่ให้ผู้ใช้งานลงทะเบียนหรือกรอกข้อมูลส่วนบุคคล ควรมีตัวเลือกแบบ Checkbox ให้ผู้ใช้งานกดเลือกเพื่อยืนยันความยินยอมจากเจ้าของข้อมูลและมี Link เพื่อกดเข้าดูรายละเอียดหน้าวัตถุประสงค์ของการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนตัว

4.2.5 มีช่องทางติดต่อและมีหน้ารายละเอียดระบุว่า หากผู้ใช้งานต้องการที่จะติดต่อเพื่อขอตรวจสอบหรือขอรับสำเนาข้อมูลส่วนบุคคลเกี่ยวกับตน ต้องติดต่อหาหน่วยงานอย่างไร โดยอาจจะเพิ่มปุ่ม ‘ติดต่อเพื่อขอตรวจสอบข้อมูลส่วนบุคคล’ ใน Footer หรือหน้า Contact Us ในเว็บไซต์หรือ App

4.2.6 มีช่องทางให้ผู้ใช้งานเจ้าของข้อมูลแจ้งขอยกเลิกความยินยอมที่เคยให้ไปและลบข้อมูลส่วนบุคคลที่ตัวเองเป็นเจ้าของออกจากระบบการจัดเก็บของแบรนด์และธุรกิจ โดยอาจจะเป็น Link ‘ยกเลิกความยินยอมจัดเก็บและใช้งานข้อมูลส่วนบุคคล’ เพื่อเข้าหน้าเว็บที่มีรายละเอียดวิธีการแจ้งความต้องการดังกล่าว



รูปที่ 5 แนวทางการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ

เอกสารอ้างอิง

[1] คณาธิป ทองรวีวงศ์. การนำหลักกฎหมายลักษณะละเมิดความเป็นอยู่ส่วนตัว (Privacy tort) กรณีการเปิดเผยเรื่องราวส่วนตัวต่อสาธารณะมาปรับใช้เพื่อคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของผู้ถูกเผยแพร่ข้อมูลทางเว็บไซต์เครือข่ายสังคม. บทบัณฑิตย์. มิ.ย. 2556;69(2).

[2] คณาธิป ทองรวีวงศ์. มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของผู้ถูกดักฟังการสื่อสารข้อมูล. วารสารกระบวนการยุติธรรม. ม.ค.-เม.ย. 2556;6(1).

[3] คณาธิป ทองรวีวงศ์. มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของแขกที่มาพักในโรงแรม. บทบัณฑิตย์. มี.ค. 2555;68(1):53-86.

[4] ธนัท สุวรรณปริญญา. ปัญหาทางกฎหมายเกี่ยวกับ การคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ กรณีศึกษา : การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของธนาคาร สถาบันการเงิน และผู้ประกอบธุรกิจบัตรเครดิตในประเทศไทย [สารนิพนธ์ปริญญามหาบัณฑิต]. กรุงเทพฯ: มหาวิทยาลัยกรุงเทพ; 2550.

[5] ธาริณี มณิรอด. ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล [วิทยานิพนธ์ปริญญามหาบัณฑิต]. กรุงเทพฯ: มหาวิทยาลัยธุรกิจบัณฑิตย์; 2559.

[6] ภาระวี ปุณเสรีพิพัฒน์. มาตรการทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ : ศึกษากรณีการใช้คุกกี้บนอินเทอร์เน็ต. วารสารนิติศาสตร์ มหาวิทยาลัยนเรศวร. พ.ค. 2557;7(1).

[7] อธิพร สิทธิธีรรัตน์. ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์. [วิทยานิพนธ์ปริญญามหาบัณฑิต]. กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์; 2558.

[8] ปิยะบุตร บุญอร่ามเรือง, พีรพัฒ โชคสุวัฒนสกุล, ปิติ เอี่ยมจำรูญลาภ, ชวิน อุ่นภัทร, ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล. Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูล ส่วนบุคคล. กรุงเทพฯ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย; 2562.

[9] NIST privacy framework: a tool for improving privacy through enterprise risk management [Internet]. Maryland: National Institute of Standards and Technology; [cited 2019 Sep 6]. Available from: https://www.nist.gov/privacy-framework

[10] กรมสรรพสามิต [อินเทอร์เน็ต]. กรุงเทพฯ: กรม; [สืบค้นเมื่อวันที่ 15 พ.ค. 2563]. จาก: https://www.excise.go.th

[11] สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ. [อินเทอร์เน็ต]. ปทุมธานี: สวทช.; [สืบค้นเมื่อวันที่ 10 พ.ค. 2563]. จาก: http://www.nstda.or.th