



แนวทางการจัดทำนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

ภายใต้พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 6 บัญญัติว่า “ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือ ข้อเท็จจริง ที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าจะโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลด้วย” โดยให้มีสาระสำคัญอย่างน้อย ต้องประกอบด้วย 2 ส่วน ได้แก่

ส่วนที่ 1 : นโยบายการคุ้มครองข้อมูลส่วนบุคคล

การจัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคล มีวัตถุประสงค์เพื่อเป็นการแจ้งให้กับผู้ใช้ บริการธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐกับหน่วยงานได้ทราบว่า หน่วยงานมีแนวทางในการบริหารจัดการ ข้อมูลส่วนบุคคลของผู้ใช้บริการซึ่งเป็นเจ้าของข้อมูลอย่างไร เพื่อให้ผู้ใช้บริการทราบและสามารถตัดสินใจได้ว่า สมควรให้ข้อมูลส่วนบุคคลของตนหรือไม่ เพื่อให้สอดคล้องเป็นไปตามประกาศคณะกรรมการธุรกรรมทาง อิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 ในส่วนของนโยบายฯ จะต้องมีส่วนหลักที่เป็นสาระสำคัญอย่างน้อย 8 ข้อ ดังนี้

1. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด
2. คุณภาพของข้อมูลส่วนบุคคล
3. การระบุวัตถุประสงค์ในการเก็บรวบรวม
4. ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้
5. การรักษาความมั่นคงปลอดภัย
6. การเปิดเผยเกี่ยวกับการดำเนินการแนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล
7. การมีส่วนร่วมของเจ้าของข้อมูล
8. ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

ส่วนที่ 2 : แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

การทำแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล มีวัตถุประสงค์เพื่อเป็นการประกาศให้กับ บุคลากรในหน่วยงานปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ ทั้งนี้ แนวปฏิบัติต้องแสดงถึงขั้นตอนและวิธีการดำเนินการเพื่อให้บุคลากรซึ่งเป็นผู้ปฏิบัติสามารถปฏิบัติได้อย่างถูกต้อง เพื่อให้สอดคล้องเป็นไปตามประกาศคณะกรรมการฯ จะต้องมีส่วนหลักที่เป็นสาระสำคัญในแนวปฏิบัติ อย่างน้อย 9 ข้อ ดังนี้

1. ข้อมูลเบื้องต้น
2. การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล
3. การแสดงระบุมความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น
4. การรวมข้อมูลจากที่มาจากหลายแห่ง
5. การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล
6. การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ
7. การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน
8. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
9. การติดต่อกับเว็บไซต์

ในแนวปฏิบัติฯ บางข้อที่หน่วยงาน

- มีการดำเนินการ ให้ระบุเนื้อหาเพิ่มเติมไว้ในนโยบาย โดยระบุเป็นข้อ ต่อจากนโยบายข้อ 8
- ไม่มีการดำเนินการ ให้ระบุไว้ในแนวปฏิบัติข้อนั้นว่า “- ไม่มี -”

หมายเหตุ

1. กรณีที่หน่วยงานได้รับเครื่องหมายการค้าจากหน่วยงานหรือองค์กรอื่นที่ทำหน้าที่ออกเครื่องหมายการค้า (Trust Mark) ในเรื่องของการคุ้มครองข้อมูลส่วนบุคคล ให้หน่วยงานของรัฐนั้นแสดงนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการรับรองจากหน่วยงานหรือองค์กรที่ออกหรือรับรองเครื่องหมายการค้าดังกล่าวต่อคณะกรรมการฯ ด้วย

เครื่องหมายการค้า (Trust Mark) ตามความในวรรคแรกหมายถึง เครื่องหมายที่รับรองว่าหน่วยงานดังกล่าวมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งออกโดยหน่วยงานหรือองค์กรที่จัดตั้งโดยชอบด้วยกฎหมายเพื่อทำหน้าที่ในการตรวจสอบและรับรองการออกเครื่องหมายการค้าให้กับผู้ขอรับการรับรอง

2. กรณีที่มีการปรับปรุงนโยบาย ให้ระบุวัน เวลา และปี ที่มีการปรับปรุงหรือเปลี่ยนแปลงนโยบายดังกล่าวไว้ด้วย

3. เพื่อความสะดวกในการปรับแก้ไขประกาศนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานในอนาคต หน่วยงานควรจัดทำนโยบายและแนวปฏิบัติแยกออกจากกัน

4. ในกรณีที่หน่วยงานมีระบบสารสนเทศที่ให้บริการธุรกรรมทางอิเล็กทรอนิกส์หลายระบบงาน โดยแต่ละระบบงานนั้นวิธีปฏิบัติในบางเรื่องอาจมีความแตกต่างกัน ในกรณีที่มีการให้บริการหลายระบบงาน ซึ่งแต่ละระบบงานอาจมีข้อปฏิบัติที่มีความแตกต่างกัน หน่วยงานควรมีการกำหนดแนวปฏิบัติของแต่ละระบบงานโดยอาจจะกำหนดไว้เป็นระเบียบข้อบังคับแนบท้ายประกาศฉบับนี้ได้

ตารางที่ 1 คำแนะนำการจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

ที่	ประกาศคณะกรรมการฯ	คำแนะนำ	เนื้อหาควรปรากฏใน	
			แนวนโยบาย	แนวปฏิบัติ
ข้อ 1	ให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ จัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษร โดยให้มีสาระสำคัญอย่างน้อย ดังนี้	<p>การจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล ต้องมีรายละเอียดอย่างน้อย ดังนี้</p> <ol style="list-style-type: none"> (1) การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด (2) คุณภาพของข้อมูลส่วนบุคคล (3) การระบุวัตถุประสงค์ในการเก็บรวบรวม (4) ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้ (5) การรักษาความมั่นคงปลอดภัย (6) การเปิดเผยเกี่ยวกับการดำเนินการแนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล (7) การมีส่วนร่วมของเจ้าของข้อมูล (8) ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล 		
(1)	การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด การจัดเก็บรวบรวมข้อมูลส่วนบุคคลให้มีขอบเขตจำกัด และใช้วิธีการที่ชอบด้วยกฎหมายและเป็นธรรม และให้เจ้าของข้อมูลทราบหรือได้รับความยินยอมจากเจ้าของข้อมูลตามแต่กรณี	<ol style="list-style-type: none"> 1. ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หน่วยงานควรระบุว่าเป็นไปตามกฎหมายใด และต้องระบุวิธีการที่ได้มาซึ่งข้อมูลส่วนบุคคล โดยให้เจ้าของข้อมูลรู้เห็น รับรู้ หรือได้รับความยินยอมจากเจ้าของข้อมูล 2. ในกรณีที่การเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อใช้ในการดำเนินการตามกฎหมาย เช่น หน่วยงานมีการประกาศแบบคำร้อง/คำขอต่างๆ หน่วยงานสามารถดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลตามแบบนั้นได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูล เนื่องจากการดำเนินงานตามกฎหมายของหน่วยงานอยู่แล้ว ทั้งนี้ หน่วยงานสามารถแจ้งให้กับผู้บริการทราบว่า การเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวเป็นไปตามแบบคำร้อง/คำขอ เลขที่ใด เรื่องอะไร เป็นต้น สำหรับข้อมูลส่วนบุคคลที่หน่วยงานต้องการเก็บรวบรวมนอกเหนือจากแบบดังกล่าวข้างต้น หน่วยงานต้องแจ้งให้ทราบว่ามีการเก็บข้อมูลอะไรเพิ่มเติม ใช้เพื่อการใด ซึ่งจะต้องแจ้งให้เจ้าของข้อมูล รับรู้และได้รับความยินยอม 	✓	-
(2)	คุณภาพของข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บให้เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานของรัฐตามกฎหมาย	<ol style="list-style-type: none"> 1. หน่วยงานควรคำนึงถึงการเก็บรวบรวมและจัดเก็บข้อมูลส่วนบุคคลนั้น ต้องเป็นไปตามกฎหมาย / อำนาจหน้าที่ของหน่วยงานที่กำหนดไว้ และรวมถึงการนำไปใช้ที่สำคัญ 2. ข้อมูลส่วนบุคคลที่จัดเก็บจะต้องคำนึงถึงความถูกต้องสมบูรณ์ และทำให้เป็นปัจจุบันและทันสมัยอยู่เสมอ เช่น (1) มีวิธีการตรวจสอบความถูกต้องของข้อมูลก่อนที่มีการจัดเก็บและนำไปประมวลผล (2) มีช่องทางสำหรับให้ผู้ใช้บริการสามารถปรับปรุงแก้ไขข้อมูลส่วนบุคคลของตน (ตัวอย่างเช่น การตรวจสอบการกรอกข้อมูลเลขบัตรประชาชนครบ 13 หลักหรือไม่ การตรวจสอบการกรอก e-Mail เป็นไปตามรูปแบบ name@host.domain หรือไม่ เป็นต้น 	✓	-

ที่	ประกาศคณะกรรมการฯ	คำแนะนำ	เนื้อหาควรปรากฏใน	
			แนวนโยบาย	แนวปฏิบัติ
(3)	การระบุวัตถุประสงค์ในการเก็บรวบรวม ให้บันทึกวัตถุประสงค์ของการเก็บรวบรวมข้อมูล ส่วนบุคคล ในขณะที่มีการรวบรวมและจัดเก็บ รวมถึง การนำข้อมูลนั้นไปใช้ในภายหลัง และหากมีการ เปลี่ยนแปลงวัตถุประสงค์ของการเก็บรวบรวมข้อมูล ให้จัดทำบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐาน	1. หน่วยงานต้องกำหนดวัตถุประสงค์ให้ชัดเจนว่า มีการรวบรวม จัดเก็บ ใช้ ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ใด	✓	-
		2. กรณีที่มีการเปลี่ยนแปลงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล หน่วยงานควรจัดทำบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐาน		
(4)	ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้ ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ ปรากฏในลักษณะอื่นใดซึ่งข้อมูลส่วนบุคคลที่ไม่ สอดคล้องกับวัตถุประสงค์ของการรวบรวมและจัดเก็บ ข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือเป็นกรณีที่มีกฎหมายกำหนดให้กระทำได้	1. หน่วยงานต้องแสดงถึงเจตนาการไม่นำไปเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดต่อผู้อื่นที่มีได้เกี่ยวข้อง	✓	-
		2. หน่วยงานจะต้องระบุให้ทราบในกรณีที่มีการบังคับให้เปิดเผยข้อมูลตามกฎหมาย / คำสั่งศาล (กรณีที่มีกฎหมายกำหนดให้กระทำได้ ให้มีการระบุกฎหมายที่เกี่ยวข้องนั้นด้วย)		
(5)	การรักษาความมั่นคงปลอดภัย ให้มีมาตรการในการรักษาความมั่นคงปลอดภัย ของข้อมูลส่วนบุคคลอย่างเหมาะสม เพื่อป้องกันการ สูญหาย การเข้าถึง ทำลาย ใช้ แปรแปลง แก้ไขหรือ เปิดเผยข้อมูลโดยมิชอบ	1. หน่วยงานต้องระบุมตรการ / วิธีการ ในการรักษาความมั่นคงปลอดภัยที่เหมาะสมในการคุ้มครองข้อมูลส่วนบุคคลเพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปรแปลง แก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ	✓	-
		2. ให้เชื่อมโยงกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานด้วย **หมายเหตุ ดูเพิ่มเติม ตารางที่ 2 มาตรการสำหรับการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลที่ควรคำนึง		
(6)	การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และ นโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล ให้มีการเปิดเผยการดำเนินการ แนวปฏิบัติ และ นโยบายที่เกี่ยวกับข้อมูลส่วนบุคคลและจัดให้มีวิธีการ ที่สามารถตรวจสอบความมีอยู่ ลักษณะของข้อมูลส่วน บุคคลวัตถุประสงค์ของการนำข้อมูลไปใช้ ผู้ควบคุม และสถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคล	1. หน่วยงานต้องระบุวิธีการเปิดเผยนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล	✓	-
		2. หน่วยงานต้องระบุวิธีการที่ให้ผู้ให้บริการสามารถตรวจสอบความมีอยู่ลักษณะของข้อมูลส่วนบุคคล / วัตถุประสงค์ของการนำข้อมูลไปใช้ / ผู้ควบคุมและสถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคล ได้		

ที่	ประกาศคณะกรรมการฯ	คำแนะนำ	เนื้อหาควรปรากฏใน	
			แนวนโยบาย	แนวปฏิบัติ
(7)	<p>การมีส่วนร่วมของเจ้าของข้อมูล ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งถึงความมีอยู่หรือรายละเอียดของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลเมื่อได้รับคำร้องขอภายในระยะเวลาอันสมควรตามวิธีการในรูปแบบ รวมถึงค่าใช้จ่าย(ถ้ามี) ตามสมควร</p> <p>ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธที่จะให้คำชี้แจงหรือให้ข้อมูลแก่เจ้าของข้อมูล ผู้สืบทิต์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ ตามกฎหมายให้ผู้ควบคุมข้อมูลจัดทำบันทึกคำคัดค้านการจัดเก็บ ความถูกต้อง หรือการกระทำใดๆ เกี่ยวกับข้อมูลของเจ้าของข้อมูลไว้เป็นหลักฐาน</p>	<p>1. หน่วยงานต้องระบุถึงวิธีการ / รูปแบบ และระยะเวลา ในการยื่นคำร้องขอรายละเอียดของข้อมูลส่วนบุคคลของเจ้าของข้อมูล รวมถึงค่าใช้จ่าย (ถ้ามี) และระบุให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งถึงความมีอยู่หรือรายละเอียดของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลเมื่อได้รับคำร้องขอดังกล่าวภายในระยะเวลาอันสมควร</p>	✓	-
		<p>2. หน่วยงานต้องระบุนำมิให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธที่จะให้คำชี้แจงหรือให้ข้อมูลแก่เจ้าของข้อมูล ผู้สืบทิต์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ ตามกฎหมาย และให้ผู้ควบคุมข้อมูลจัดทำบันทึกคำคัดค้านการจัดเก็บ ความถูกต้อง หรือการกระทำใดๆ เกี่ยวกับข้อมูลของเจ้าของข้อมูลไว้เป็นหลักฐาน</p>	✓	-
(8)	<p>ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล ให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติตามมาตรการที่กำหนดไว้ข้างต้นเพื่อให้การดำเนินงานตามแนวนโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานของประกาศฉบับนี้</p>	<p>1. หน่วยงานต้องแสดงให้เห็นถึงการกำหนดให้มีผู้ควบคุมข้อมูลส่วนบุคคลที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลนี้</p> <p>2. ให้เชื่อมโยงกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานด้วย</p>	✓	-

ที่	ประกาศคณะกรรมการฯ	คำแนะนำ	เนื้อหาควรปรากฏใน	
			แนวนโยบาย	แนวปฏิบัติ
ข้อ 2	ให้หน่วยงานของรัฐจัดทำข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการและให้มีรายการอย่างน้อย ดังนี้	<ul style="list-style-type: none"> - แนวปฏิบัติต้องแสดงถึงขั้นตอนและวิธีการดำเนินการให้บุคลากรในหน่วยงานปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการได้อย่างถูกต้อง - ควรเขียนแนวปฏิบัติ แยกออกจากนโยบายฯ 		
(1)	ข้อมูลเบื้องต้น ประกอบด้วย (ก) ชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคลว่าเป็นของหน่วยงานใด	ต้องมีชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคลว่าเป็นของหน่วยงานใด	-	✓
	(ข) รายละเอียดขอบเขตของการบังคับใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานของรัฐรวบรวม จัดเก็บ หรือการใช้ตามวัตถุประสงค์	- ให้ระบุ “รายละเอียดขอบเขตของการบังคับใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานของรัฐรวบรวม จัดเก็บ หรือการใช้ตามวัตถุประสงค์”	-	✓
	(ค) ให้แจ้งการเปลี่ยนแปลงวัตถุประสงค์หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบและขอความยินยอมก่อนทุกครั้งตามวิธีการและภายในกำหนดเวลาที่ประกาศ เช่น การแจ้งล่วงหน้าให้เจ้าของข้อมูลทราบก่อน 15 วัน โดยการส่งทางจดหมายอิเล็กทรอนิกส์หรือประกาศไว้ในหน้าแรกของเว็บไซต์ เว้นแต่กฎหมายจะกำหนดไว้เป็นอย่างอื่น การขอความยินยอมจากเจ้าของข้อมูลนั้น ให้มีความชัดเจนว่าหน่วยงานของรัฐขอรับความยินยอมเพื่อวัตถุประสงค์ใด	- ให้ระบุ “ให้แจ้งการเปลี่ยนแปลงวัตถุประสงค์หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบและขอความยินยอมก่อนทุกครั้งตามวิธีการและภายในกำหนดเวลาที่ประกาศ เช่น การแจ้งล่วงหน้าให้เจ้าของข้อมูลทราบก่อน ๑๕ วัน โดยการส่งทางจดหมายอิเล็กทรอนิกส์หรือประกาศไว้ในหน้าแรกของเว็บไซต์ เว้นแต่กฎหมายจะกำหนดไว้เป็นอย่างอื่นการขอความยินยอมจากเจ้าของข้อมูลนั้น ต้องให้มีความชัดเจนว่าหน่วยงานขอรับความยินยอมเพื่อวัตถุประสงค์ใด”	-	✓

ที่	ประกาศคณะกรรมการฯ	คำแนะนำ	เนื้อหาควรปรากฏใน	
			แนวนโยบาย	แนวปฏิบัติ
2)	<p>การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล ให้หน่วยงานของรัฐที่ทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเก็บรวบรวมข้อมูลผ่านทางเว็บไซต์หรือผ่านรูปแบบของการกรอกข้อความทางกระดาษแล้วนำมาแปลงข้อความเข้าระบบอิเล็กทรอนิกส์หรือจัดเก็บโดยวิธีอื่น ให้แสดงรายละเอียดของการรวบรวมข้อมูลเป็นชนิด ประเภท รวมถึงข้อมูลที่จะไม่จัดเก็บ และข้อมูลที่รวบรวมและจัดเก็บนั้นจะนำไปใช้ตามวัตถุประสงค์ใด โดยลักษณะหรือด้วยวิธีการที่ทำให้เจ้าของข้อมูลได้ทราบ ทั้งนี้ การรวบรวมและจัดเก็บข้อมูลนั้น ให้ทำเป็นประกาศหรือแจ้งรายละเอียดให้เจ้าของข้อมูลทราบ</p> <p>ให้หน่วยงานของรัฐที่จัดบริการผ่านทางเว็บไซต์ แสดงรายละเอียดของการรวบรวมข้อมูลผ่านทางเว็บไซต์ของหน่วยงานนั้น รวมถึงการใช้ข้อมูลซึ่งอย่างน้อยต้องระบุว่าอยู่ในส่วนใดของเว็บไซต์ หรือในเว็บเพจใดที่มีการรวบรวมและจัดเก็บข้อมูล และให้มีรายละเอียดอย่างแจ้งชัดถึงวิธีการในการรวบรวมและจัดเก็บข้อมูล เช่น การจัดเก็บโดยให้มีการลงทะเบียน หรือการกรอกแบบสอบถาม เป็นต้น</p> <p>ให้หน่วยงานของรัฐรวบรวม จัดเก็บและใช้ข้อมูลส่วนบุคคลจัดทำรายละเอียดดังต่อไปนี้</p>	<p>1. ข้อมูลที่หน่วยงานจะไม่จัดเก็บ จะต้องแจ้งให้เจ้าหน้าที่ผู้ปฏิบัติทราบ ซึ่งตัวอย่างข้อมูลที่หน่วยงานอาจจะไม่มีการจัดเก็บ เช่น เลขบัตรเครดิต ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ เป็นต้น</p> <p>2. กรณีที่หน่วยงานมีการเก็บรวบรวมข้อมูลส่วนบุคคลตามแบบคำร้อง / คำขอ ที่หน่วยงานประกาศกำหนดไว้ หน่วยงานสามารถแจ้งให้เจ้าหน้าที่ผู้ปฏิบัติทราบว่าจัดเก็บตามแบบคำร้อง / คำขอ เลขที่ใด เรื่องอะไร</p> <p>กรณีที่หน่วยงานไม่มีจัดบริการผ่านทางเว็บไซต์(ตามวรรคสองของประกาศฯ) ให้ระบุ “ – ไม่มี – พร้อมระบุเหตุผลประกอบ (ตัวอย่างเช่น ...<i>(ชื่อหน่วยงาน)</i>... ไม่มีการจัดบริการเก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ เป็นต้น)”</p> <p>และหน่วยงานไม่ต้องจัดทำ 2 (2) (ก) - (จ)</p>	-	✓
	<p>(ก) การติดต่อระหว่างหน่วยงานของรัฐ ให้หน่วยงานของรัฐซึ่งจะติดต่อไปยังผู้ใช้บริการ ด้วยวิธีการทางอิเล็กทรอนิกส์บอกกล่าวให้ผู้ใช้บริการทราบล่วงหน้า ทั้งนี้ ผู้ใช้บริการอาจแจ้งความประสงค์ให้ติดต่อโดยวิธีการอื่นได้</p>	<p>กรณีที่หน่วยงานไม่มีการติดต่อไปยังผู้ใช้บริการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้ระบุ “ – ไม่มี – พร้อมระบุเหตุผลประกอบ (ตัวอย่างเช่น ...<i>(ชื่อหน่วยงาน)</i>... ไม่มีการติดต่อไปยังผู้ใช้บริการด้วยวิธีการทางอิเล็กทรอนิกส์ เป็นต้น)”</p> <p>- ถ้ามี ให้ระบุ “ว่าหน่วยงานจะติดต่อไปยังผู้ใช้บริการด้วยวิธีการทางอิเล็กทรอนิกส์โดยวิธีการใด และการบอกกล่าวให้ผู้ใช้บริการทราบล่วงหน้า”</p> <p>- ถ้ามี ให้ระบุ “ในกรณีที่ผู้ใช้บริการอาจแจ้งความประสงค์ให้ติดต่อโดยวิธีการอื่นได้”</p>	-	✓

ที่	ประกาศคณะกรรมการฯ	คำแนะนำ	เนื้อหาควรปรากฏใน	
			แนวนโยบาย	แนวปฏิบัติ
	(ข) การใช้คุกกี้ (Cookies) ให้หน่วยงานของรัฐระบุบนเว็บไซต์สำหรับการใช้คุกกี้ที่เชื่อมโยงกับข้อมูลส่วนบุคคลว่าผู้ใช้บริการจะใช้คุกกี้เพื่อวัตถุประสงค์และประโยชน์ใด และให้สิทธิที่จะไม่รับการต่อเชื่อมคุกกี้ได้	กรณีที่หน่วยงานไม่มีเว็บไซต์ที่ให้บริการ หรือมีเว็บไซต์ที่จัดให้บริการแต่ไม่มีการใช้คุกกี้ที่เชื่อมโยงกับข้อมูลส่วนบุคคล ให้ระบุ ว่า “- ไม่มี - พร้อมระบุเหตุผลประกอบ (ตัวอย่างเช่น เว็บไซต์ของ...(ชื่อหน่วยงาน)... ไม่มีการใช้คุกกี้ เป็นต้น)” - ถ้ามีการใช้คุกกี้ “ให้ระบุสิทธิที่จะไม่รับการต่อเชื่อมคุกกี้ได้ด้วย”	-	✓
	(ค) การเก็บข้อมูลสถิติเกี่ยวกับประชากร (Demographic Information) ให้หน่วยงานของรัฐมีเว็บไซต์สำหรับการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากร เช่น เพศ อายุ อาชีพ ที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ ระบุถึงวิธีการรวบรวมและจัดเก็บข้อมูลดังกล่าวไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลด้วย และให้ชี้แจงวัตถุประสงค์ของการใช้ข้อมูลดังกล่าว รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลนั้นด้วย	ในแนวนโยบาย ให้หน่วยงานวัตถุประสงค์ของการใช้ข้อมูลดังกล่าว รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลนั้นด้วย ไว้ในนโยบายข้อที่ 3 “การระบุวัตถุประสงค์ในการเก็บรวบรวม” กรณีที่หน่วยงานไม่มีเว็บไซต์ที่มีการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากร ที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ - หน่วยงานไม่ต้องระบุรายละเอียดดังกล่าวไว้ในนโยบาย ในแนวปฏิบัติ ให้หน่วยงานระบุ ถึง - วัตถุประสงค์ของการใช้ รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลข้อมูลสถิติเกี่ยวกับประชากร ที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ - ให้เชื่อมโยงกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานด้วย กรณีที่หน่วยงานไม่มีเว็บไซต์ที่มีการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากร ที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ - หน่วยงานไม่ต้องระบุรายละเอียดดังกล่าวไว้ในนโยบายข้อ 3 - หน่วยงานต้องระบุในแนวปฏิบัติ ว่า “- ไม่มี - พร้อมระบุเหตุผล (ตัวอย่างเช่น ...(ชื่อหน่วยงาน)... ไม่มีเว็บไซต์สำหรับการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากร” / เว็บไซต์ของ...(ชื่อหน่วยงาน)...ไม่มีการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากร ที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ เป็นต้น”	✓ (ถ้ามี)	✓

ที่	ประกาศคณะกรรมการฯ	คำแนะนำ	เนื้อหาควรปรากฏใน	
			แนวนโยบาย	แนวปฏิบัติ
	(ง) บันทึกผู้เข้าชมเว็บ (Log Files) ให้หน่วยงานของรัฐซึ่งจัดบริการเว็บไซต์ที่มีการเก็บบันทึกการเข้าออกโดยอัตโนมัติ เช่น หมายเลขไอพี (IP Address) เว็บไซต์ที่เข้าออกก่อนและหลัง และประเภทของโปรแกรมบราวเซอร์ (Browser) ที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลซึ่งระบุตัวบุคคลได้ ระบุวิธีการรวบรวมและจัดเก็บข้อมูลดังกล่าวไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล และให้ชี้แจงวัตถุประสงค์ของการใช้ รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลนั้นด้วย	<p>ในแนวนโยบาย</p> <p>ให้หน่วยงานชี้แจงวัตถุประสงค์ของการใช้ รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลนั้นด้วย ไว้ในนโยบายข้อที่ 3 “การระบุวัตถุประสงค์ในการเก็บรวบรวม”</p> <p>กรณีที่หน่วยงานไม่มีเว็บไซต์ที่ให้บริการ หรือมีเว็บไซต์ที่จัดให้บริการ แต่ไม่มีการเก็บบันทึกการเข้าออกโดยอัตโนมัติที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลซึ่งระบุตัวบุคคลได้</p> <ul style="list-style-type: none"> - หน่วยงานไม่ต้องระบุรายละเอียดดังกล่าวไว้ในนโยบาย 	✓ (ถ้ามี)	✓
	<p>ในแนวปฏิบัติ</p> <p>ให้หน่วยงานระบุ ถึง</p> <ul style="list-style-type: none"> - วัตถุประสงค์ของการใช้ รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลเข้าออกโดยอัตโนมัติ ที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลซึ่งระบุตัวบุคคลได้ - ให้เชื่อมโยงกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานด้วย <p>คำแนะนำ</p> <p>กรณีที่หน่วยงานไม่มีเว็บไซต์ที่ให้บริการ หรือมีเว็บไซต์ที่จัดให้บริการ แต่ไม่มีการเก็บบันทึกการเข้าออกโดยอัตโนมัติที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลซึ่งระบุตัวบุคคลได้</p> <ul style="list-style-type: none"> - หน่วยงานไม่ต้องระบุรายละเอียดดังกล่าวไว้ในนโยบาย - หน่วยงานต้องระบุในแนวปฏิบัติ ว่า “- ไม่มี - พร้อมระบุเหตุผล (ตัวอย่างเช่น เว็บไซต์ของ...(ชื่อหน่วยงาน)... ไม่มีการเก็บบันทึกการเข้าออกโดยอัตโนมัติที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลซึ่งระบุตัวบุคคลได้ เป็นต้น)” 			
	(จ) ให้หน่วยงานของรัฐระบุข้อมูลที่มีการจัดเก็บผ่านทางเว็บไซต์ว่าเป็นข้อมูลที่ประชาชนมีสิทธิเลือกกว่า “จะให้หรือไม่ให้” ก็ได้ และให้หน่วยงานของรัฐจัดเตรียมช่องทางอื่นในการติดต่อสื่อสารสำหรับผู้ใช้บริการที่ไม่ประสงค์จะให้ข้อมูลผ่านทางเว็บไซต์	ให้หน่วยงานระบุข้อมูลที่มีการจัดเก็บผ่านทางเว็บไซต์ ว่า เป็นข้อมูลที่ประชาชนมีสิทธิเลือกกว่า “จะให้หรือไม่ให้” ก็ได้ และให้ระบุช่องทางอื่นในการติดต่อ สำหรับผู้ให้บริการที่ไม่ประสงค์จะให้ข้อมูลผ่านทางเว็บไซต์	-	✓

ที่	ประกาศคณะกรรมการฯ	คำแนะนำ	เนื้อหาควรปรากฏใน	
			แนวนโยบาย	แนวปฏิบัติ
(3)	<p>การแสดงระบุมความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น</p> <p>การเก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ของหน่วยงานของรัฐและเว็บไซต์ดังกล่าวที่มีการเชื่อมโยงให้ข้อมูลแก่หน่วยงานหรือองค์กรอื่น ให้หน่วยงานของรัฐแสดงไว้อย่างชัดเจนถึงชื่อผู้เก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ หรือชื่อผู้มีสิทธิในข้อมูลที่ได้มีการเก็บรวบรวม (Data Subject) และชื่อเป็นผู้มีสิทธิเข้าถึงข้อมูลดังกล่าวทั้งหมด รวมถึงประเภทของข้อมูลที่จะใช้ร่วมกับหน่วยงานหรือองค์กรอื่นๆ ตลอดจนชื่อผู้มีหน้าที่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้ผู้ใช้บริการทราบ</p> <p>ให้หน่วยงานของรัฐแจ้งให้ผู้ใช้บริการทราบและให้ความยินยอมล่วงหน้าก่อนทำการเปลี่ยนแปลงการเชื่อมโยงข้อมูลตามวาระแรกกับหน่วยงานหรือองค์กรอื่น</p>	<p>ในแนวนโยบาย</p> <p>ให้หน่วยงานระบุชื่อผู้เก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ หรือชื่อผู้มีสิทธิในข้อมูลที่ได้มีการเก็บรวบรวม (Data Subject) และชื่อเป็นผู้มีสิทธิเข้าถึงข้อมูลดังกล่าวทั้งหมด รวมถึงประเภทของข้อมูลที่จะใช้ร่วมกับหน่วยงานหรือองค์กรอื่นๆ ตลอดจนชื่อผู้มีหน้าที่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ หน่วยงานสามารถระบุเป็นชื่อส่วนงานที่กำกับดูแลในเรื่องดังกล่าว หรือ ระบุเป็นชื่อผู้รับผิดชอบ ตามแต่กรณี ตามที่หน่วยงานได้มีการกำหนดไว้</p> <p>กรณีที่หน่วยงานไม่มีการเชื่อมโยงให้ข้อมูลแก่หน่วยงานหรือองค์กรอื่น</p> <ul style="list-style-type: none"> - หน่วยงานไม่ต้องระบุเรื่องนี้ไว้ในนโยบายฯ - หน่วยงานต้องระบุในแนวปฏิบัติว่า “ ไม่มี – พร้อมระบุเหตุผลประกอบ (ตัวอย่างเช่น เว็บไซต์ของ...(ชื่อหน่วยงาน)... ไม่มีการเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น เป็นต้น)” 	✓ (ถ้ามี)	✓
		<p>ในแนวปฏิบัติ</p> <p>ต้องกำหนดให้มีการระบุชื่อผู้เก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ หรือชื่อผู้มีสิทธิในข้อมูลที่ได้มีการเก็บรวบรวม (Data Subject) และชื่อเป็นผู้มีสิทธิเข้าถึงข้อมูลดังกล่าวทั้งหมด รวมถึงประเภทของข้อมูลที่จะใช้ร่วมกับหน่วยงานหรือองค์กรอื่นๆ ตลอดจนชื่อผู้มีหน้าที่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล และต้องกำหนดให้มีการแจ้งให้ผู้ใช้บริการทราบและให้ความยินยอมล่วงหน้าก่อนทำการเปลี่ยนแปลงการเชื่อมโยงให้ข้อมูลแก่หน่วยงานหรือองค์กรอื่น</p> <p>กรณีที่หน่วยงานไม่มีการเชื่อมโยงให้ข้อมูลแก่หน่วยงานหรือองค์กรอื่น</p> <ul style="list-style-type: none"> - หน่วยงานไม่ต้องระบุเรื่องนี้ไว้ในนโยบายฯ - หน่วยงานต้องระบุในแนวปฏิบัติว่า “ ไม่มี – พร้อมระบุเหตุผลประกอบ (ตัวอย่างเช่น เว็บไซต์ของ...(ชื่อหน่วยงาน)... ไม่มีการเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น เป็นต้น)” 		

ที่	ประกาศคณะกรรมการฯ	คำแนะนำ	เนื้อหาควรปรากฏใน	
			แนวนโยบาย	แนวปฏิบัติ
(4)	การรวมข้อมูลจากที่มาหลาย ๆ แห่ง ให้หน่วยงานของรัฐที่ซึ่งได้รับข้อมูลมาจาก ผู้ให้บริการเว็บไซต์ และจะนำไปรวมเข้ากับข้อมูลของ บุคคลดังกล่าวที่ได้รับจากที่มาแห่งอื่น ระบุไว้ใน นโยบายคุ้มครองข้อมูลส่วนบุคคลถึงเจตนารมณ์การ รวมข้อมูลดังกล่าวด้วย เช่น เว็บไซต์ได้รับข้อมูลที่เป็น ชื่อและที่อยู่ของการส่งจดหมายอิเล็กทรอนิกส์จาก ผู้ให้บริการโดยการกรอกข้อมูลตามแบบสอบถามผ่านทาง เว็บไซต์ และจะนำข้อมูลดังกล่าวไปรวมเข้ากับข้อมูล เกี่ยวกับประวัติของผู้ให้บริการที่ได้รับจากที่มาแห่งอื่น	<p>ในแนวนโยบาย</p> <p>ให้หน่วยงานแสดงเจตนาของการรวบรวมข้อมูลส่วนบุคคลจากผู้ให้บริการผ่านทางเว็บไซต์ที่ให้บริการ และนำข้อมูล ส่วนบุคคลนั้นไปรวมกับข้อมูลส่วนบุคคลที่ได้รับจากแห่งอื่นๆ นั้น เพื่ออะไร</p> <p>กรณีที่หน่วยงานไม่มีการรับข้อมูลส่วนบุคคลจากผู้ให้บริการผ่านทางเว็บไซต์ที่ให้บริการ และนำข้อมูลส่วนบุคคลนั้นไปรวมกับ ข้อมูลส่วนบุคคลที่ได้รับจากแห่งอื่นๆ หน่วยงานไม่ต้องระบุเรื่องนี้ไว้ในนโยบาย</p>	✓ (ถ้ามี)	✓
		<p>ในแนวปฏิบัติ</p> <p>ต้องกำหนดให้มีการแสดงเจตนาของการรวบรวมข้อมูลส่วนบุคคลจากผู้ให้บริการผ่านทางเว็บไซต์ที่ให้บริการ และนำข้อมูล ส่วนบุคคลนั้นไปรวมกับข้อมูลส่วนบุคคลที่ได้รับจากแห่งอื่นๆ นั้น เพื่ออะไร ไว้ในแนวนโยบายในการคุ้มครองข้อมูลส่วนบุคคล</p> <p>กรณีที่หน่วยงานไม่มีการรับข้อมูลส่วนบุคคลจากผู้ให้บริการผ่านทางเว็บไซต์ที่ให้บริการ และนำข้อมูลส่วนบุคคลนั้นไป รวมกับข้อมูลส่วนบุคคลที่ได้รับจากแห่งอื่นๆ ให้ระบุว่า “ – ไม่มี – พร้อมระบุเหตุผลประกอบ (ตัวอย่างเช่น ...(ชื่อหน่วยงาน)... ไม่มี การนำข้อมูลส่วนบุคคลซึ่งได้รับจากผู้ให้บริการผ่านทางเว็บไซต์ไปรวมเข้ากับข้อมูลของบุคคลที่ได้รับจากที่มาแห่งอื่น)”</p>		
(5)	การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล ให้หน่วยงานของรัฐระบุไว้ในนโยบายการ คุ้มครองข้อมูลส่วนบุคคลด้วยว่ามีบุคคลอื่นที่จะเข้าถึง หรือใช้ข้อมูลที่หน่วยงานนั้นได้เก็บรวบรวมมาผ่านทาง เว็บไซต์ด้วย และให้ระบุไว้ด้วยว่าการให้เข้าถึง ใช้ หรือเปิดเผยข้อมูลดังกล่าวสอดคล้องกับข้อกำหนด ตามกฎหมายของหน่วยงานของรัฐที่ดำเนินการ ดังกล่าว	<p>ในแนวนโยบาย</p> <p>ให้หน่วยงานระบุว่า หน่วยงานได้มีการอนุญาตให้เข้าถึง ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล กับหน่วยงานใดหรือบุคคลใดบ้าง และสอดคล้องกับข้อกำหนดตามกฎหมายของหน่วยงานที่มีหน้าที่ในการดำเนินการดังกล่าวอย่างไร</p> <p>กรณีที่หน่วยงานไม่มีการให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคลไม่ต้องระบุเรื่องนี้ไว้ในนโยบาย</p>	✓ (ถ้ามี)	✓
		<p>ในแนวปฏิบัติ</p> <p>ต้องกำหนดให้มีการระบุไว้ในนโยบายในการคุ้มครองข้อมูล โดยให้ระบุว่า หน่วยงานได้มีการให้เข้าถึง ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคล กับหน่วยงานใดหรือบุคคลใดบ้าง และสอดคล้องกับข้อกำหนดตามกฎหมายของหน่วยงานที่มีหน้าที่ในการดำเนินการ ดังกล่าวอย่างไร</p> <p>กรณีที่หน่วยงานไม่มีการให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล ให้ระบุว่า “ – ไม่มี – พร้อมระบุเหตุผลประกอบ (ตัวอย่างเช่น ...(ชื่อหน่วยงาน)... ไม่มีการให้บุคคลอื่นเข้าถึงหรือใช้ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมมา เป็นต้น)”</p>		

ที่	ประกาศคณะกรรมการ	คำแนะนำ	เนื้อหาควรปรากฏใน	
			แนวนโยบาย	แนวปฏิบัติ
(6)	<p>การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ให้บริการ</p> <p>ให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่ประสงค์จะนำไปดำเนินการอื่นนอกเหนือไปจากวัตถุประสงค์ของการรวบรวมข้อมูลส่วนบุคคลตามที่ระบุไว้ เช่น การรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลที่ไม่จำเป็น หรือการเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลอื่น ระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลถึงสิทธิของผู้ใช้บริการที่จะเลือกว่า จะให้หน่วยงานของรัฐรวบรวม จัดเก็บหรือไม่ให้จัดเก็บ ใช้หรือไม่ให้ใช้ และเปิดเผยหรือไม่เปิดเผยข้อมูลดังกล่าว</p> <p>การให้ผู้ให้บริการใช้สิทธิเลือกตามวรรคแรกให้รวมถึงการให้สิทธิเลือกแบบที่หน่วยงานของรัฐจะต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลนั้นก่อน และการให้สิทธิเลือกแบบที่ให้สิทธิแก่ผู้ใช้บริการในการปฏิเสธไม่ให้มีการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่เก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวข้างต้นแล้วเท่านั้น ทั้งนี้ การให้สิทธิเลือกต้องกระทำให้สมบูรณ์ก่อนที่เว็บไซต์จะทำการติดต่อกับผู้ใช้บริการในครั้งแรก และหากเป็นการใช้สิทธิเลือกแบบห้ามไม่ให้มีการใช้ข้อมูลส่วนบุคคลต่างไปจากวัตถุประสงค์เดิม หน่วยงานเจ้าของเว็บไซต์ต้องระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ให้บริการได้รับทราบถึงวิธีการของการส่งการติดต่อครั้งที่สองของเว็บไซต์ด้วย</p>	<p>ในนโยบาย</p> <p>ให้หน่วยงานระบุถึงสิทธิของผู้ใช้บริการ สำหรับในกรณีที่หน่วยงานมีความประสงค์จะนำข้อมูลส่วนบุคคลของผู้ใช้บริการไปใช้เพื่อวัตถุประสงค์อย่างอื่นที่แตกต่างหรือที่นอกเหนือจากที่ได้ระบุไว้ โดยหน่วยงานต้องระบุ ดังนี้</p> <ul style="list-style-type: none"> - หน่วยงานจะขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลก่อน - หน่วยงานให้สิทธิกับผู้ใช้บริการสามารถปฏิเสธ “ไม่ให้” มีการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่เก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวข้างต้นแล้วเท่านั้น <p>ทั้งนี้ หน่วยงานต้องระบุรายละเอียดให้ผู้บริการทราบว่า หากต้องการใช้สิทธิ “ให้หรือไม่ให้” ผู้ใช้บริการจะต้องดำเนินการอย่างไร กรณีที่ผู้ใช้บริการเลือกสิทธิห้ามไม่ให้ใช้ข้อมูลส่วนบุคคลนอกเหนือวัตถุประสงค์ที่ได้ระบุไว้ในครั้งแรก หน่วยงานต้องระบุช่องทางการติดต่อให้ผู้บริการทราบว่า หากจะติดต่อกับเว็บไซต์ในครั้งต่อไปจะมีวิธีการอย่างไร</p> <p>กรณีที่หน่วยงานไม่มีความประสงค์จะนำข้อมูลส่วนบุคคลของผู้ใช้บริการไปใช้เพื่อวัตถุประสงค์อย่างอื่นที่แตกต่างหรือที่นอกเหนือจากที่ได้ระบุไว้ หน่วยงานไม่ต้องระบุเรื่องนี้ไว้ในนโยบาย</p>	<p>✓ (ถ้ามี)</p>	<p>✓</p>
		<p>ในแนวปฏิบัติ</p> <p>ให้หน่วยงานระบุถึงสิทธิของผู้ใช้บริการ สำหรับในกรณีที่หน่วยงานมีความประสงค์จะนำข้อมูลส่วนบุคคลของผู้ใช้บริการไปใช้เพื่อวัตถุประสงค์อย่างอื่นที่แตกต่างหรือที่นอกเหนือจากที่ได้ระบุไว้ โดยหน่วยงานต้องระบุ ดังนี้</p> <ul style="list-style-type: none"> - หน่วยงานจะขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลก่อน - หน่วยงานให้สิทธิกับผู้ใช้บริการสามารถปฏิเสธ “ไม่ให้” มีการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่เก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวข้างต้นแล้วเท่านั้น <p>ทั้งนี้ หน่วยงานต้องระบุรายละเอียดให้ผู้บริการทราบว่า หากต้องการใช้สิทธิ “ให้หรือไม่ให้” ผู้ใช้บริการจะต้องดำเนินการอย่างไร กรณีที่ผู้ใช้บริการเลือกสิทธิห้ามไม่ให้ใช้ข้อมูลส่วนบุคคลนอกเหนือวัตถุประสงค์ที่ได้ระบุไว้ในครั้งแรก หน่วยงานต้องระบุช่องทางการติดต่อให้ผู้บริการทราบว่า หากจะติดต่อกับเว็บไซต์ในครั้งต่อไปจะมีวิธีการอย่างไร</p> <p>กรณีที่หน่วยงานไม่มีความประสงค์จะนำข้อมูลส่วนบุคคลของผู้ใช้บริการไปใช้เพื่อวัตถุประสงค์อย่างอื่นที่แตกต่างหรือที่นอกเหนือจากที่ได้ระบุไว้</p> <ul style="list-style-type: none"> - หน่วยงานต้องระบุไว้ในแนวปฏิบัติว่า “ไม่มี - พร้อมระบุเหตุผลประกอบ - หน่วยงานไม่ต้องระบุเรื่องนี้ไว้ในนโยบาย 		

ที่	ประกาศคณะกรรมการฯ	คำแนะนำ	เนื้อหาควรปรากฏใน	
			แนวนโยบาย	แนวปฏิบัติ
(7)	<p>การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน</p> <p>ให้หน่วยงานของรัฐกำหนดวิธีการที่ผู้ใช้บริการเว็บไซต์สามารถเข้าถึงและแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลเกี่ยวกับตนเองที่หน่วยงานของรัฐรวบรวมและจัดเก็บไว้ในเว็บไซต์ให้ถูกต้อง</p>	<p>ให้หน่วยงานของรัฐกำหนดวิธีการที่ผู้ใช้บริการเว็บไซต์สามารถเข้าถึงและแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลเกี่ยวกับตนเองที่หน่วยงานของรัฐรวบรวมและจัดเก็บไว้ในเว็บไซต์ให้ถูกต้อง</p>	-	✓
(8)	<p>การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล</p> <p>ให้หน่วยงานของรัฐซึ่งรวบรวมข้อมูลส่วนบุคคลผ่านทางเว็บไซต์ จัดให้มีวิธีการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บไว้ให้เหมาะสมกับการรักษาความลับของข้อมูลส่วนบุคคล เพื่อป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวโดยมิชอบ รวมถึงการป้องกันการกระทำใดที่จะมีผลทำให้ข้อมูลไม่อยู่ในสภาพพร้อมใช้งาน ซึ่งหน่วยงานของรัฐพึงดำเนินการ ดังนี้</p> <p>(ก) สร้างเสริมความสำคัญในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงานด้วยการเผยแพร่ข้อมูลข่าวสาร ให้ความรู้จัดสัมมนา หรือฝึกอบรมในเรื่องดังกล่าวให้แก่บุคลากรในองค์กรเป็นประจำ</p>	<p>**หมายเหตุ ดูเพิ่มเติม ตารางที่ 2 มาตรการสำหรับการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลที่ควรคำนึง</p> <p>กรณีที่หน่วยงานมีเอกสารรายละเอียดมาตรการการสร้างเสริมความสำคัญในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงานอยู่แล้ว หน่วยงานสามารถอ้างอิงไปยังเอกสารฉบับนั้นได้</p> <p>- ให้เชื่อมโยงกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานด้วย</p>	-	✓
	<p>(ข) กำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของบุคลากร พนักงานหรือลูกจ้างของตนในแต่ละลำดับชั้นให้ชัดเจน และให้มีการบันทึก รวมทั้งการสำรองข้อมูลของการเข้าถึงหรือการเข้าใช้งานข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด</p>	<p>กรณีที่หน่วยงานมีเอกสารรายละเอียดการกำหนดสิทธิและข้อจำกัดสิทธิให้กับบุคลากรที่เกี่ยวข้องในการเข้าถึงข้อมูลส่วนบุคคลแต่ละลำดับชั้นอยู่แล้ว หน่วยงานสามารถอ้างอิงไปยังเอกสารฉบับนั้นได้</p> <p>- ให้เชื่อมโยงกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานด้วย</p>	-	✓
	<p>(ค) ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือของระบบสารสนเทศทั้งหมดอย่างน้อยปีละ 1 ครั้ง</p>	<p>กรณีที่หน่วยงานมีเอกสารรายละเอียดการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือของระบบสารสนเทศทั้งหมดอยู่แล้ว หน่วยงานสามารถอ้างอิงไปยังเอกสารฉบับนั้นได้</p> <p>- ให้เชื่อมโยงกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานด้วย</p>	-	✓

ที่	ประกาศคณะกรรมการฯ	คำแนะนำ	เนื้อหาควรปรากฏใน	
			แนวนโยบาย	แนวปฏิบัติ
	(ง) กำหนดให้มีการใช้มาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ให้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจนอยู่แล้ว หน่วยงานสามารถอ้างอิงไปยังเอกสารฉบับนั้นได้	กรณีที่หน่วยงานมีเอกสารรายละเอียดมาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ให้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน เช่น หมายเลขบัตรเดบิต หรือบัตรเครดิต หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวบุคคล เชื้อชาติ ศาสนา ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ เป็นต้น	-	✓
	(จ) ควรจัดให้มีมาตรการที่รอบคอบในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีโดยใช้วิธีการโดยเฉพาะและเหมาะสม	กรณีที่หน่วยงานมีเอกสารรายละเอียดการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีอยู่แล้ว หน่วยงานสามารถอ้างอิงไปยังเอกสารฉบับนั้นได้	-	✓
(9)	การติดต่อกับเว็บไซต์ เว็บไซต์ซึ่งให้ข้อมูลแก่ผู้ให้บริการในการติดต่อกับหน่วยงานของรัฐ ต้องจัดให้มีทั้งข้อมูลติดต่อไปยังสถานที่ทำการงานปกติและข้อมูลติดต่อผ่านทางออนไลน์ด้วย ข้อมูลติดต่อที่หน่วยงานของรัฐควรจะระบุเอาไว้ อย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้ (ก) ชื่อและที่อยู่ (ข) หมายเลขโทรศัพท์ (ค) หมายเลขโทรสาร (ง) ที่อยู่จดหมายอิเล็กทรอนิกส์	-	-	✓

ที่	ประกาศคณะกรรมการฯ	คำแนะนำ	เนื้อหาควรปรากฏใน	
			แนวนโยบาย	แนวปฏิบัติ
ข้อ 3	<p>ให้หน่วยงานของรัฐจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลภายใต้หลักการตามข้อ 1 และข้อ 2 สำหรับหน่วยงานของรัฐที่ได้รับทรัพย์สินจากหน่วยงานหรือองค์กรอื่นที่ทำหน้าที่ออกทรัพย์สิน (Trust Mark) ให้หน่วยงานของรัฐนั้นแสดงนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการรับรองจากหน่วยงานหรือองค์กรที่ออกหรือรับรองทรัพย์สินดังกล่าว ต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วย</p> <p>ทรัพย์สิน (Trust Mark) ตามความในวรรคแรก หมายถึง เครื่องหมายที่รับรองว่าหน่วยงานดังกล่าวมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งออกโดยหน่วยงานหรือองค์กรที่จัดตั้งโดยชอบด้วยกฎหมายเพื่อทำหน้าที่ในการตรวจสอบและรับรองการออกทรัพย์สินให้กับผู้ขอรับการรับรอง</p>	-	-	-
ข้อ 4	<p>ให้หน่วยงานของรัฐกำหนดชื่อเรียกนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ให้ชัดเจน และในกรณีที่มีการปรับปรุงนโยบาย ให้ระบุวัน เวลา และปี ซึ่งจะมีการปรับปรุงหรือเปลี่ยนแปลงนโยบายดังกล่าวไว้ด้วย</p>	-	✓	-

**** หมายเหตุ**

- สำหรับมาตรการที่กำหนดไว้ในนโยบายเกี่ยวกับมาตรการการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลว่าจะมีการดำเนินการอย่างไรที่จะป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ ให้กับผู้ใช้บริการทราบและมั่นใจในบริการของหน่วยงานนั้น ให้หน่วยงานนำมาตรการดังกล่าวมาระบุขั้นตอนการปฏิบัติไว้ในแนวปฏิบัติด้วย ทั้งนี้ หากมาตรการดังกล่าวหน่วยงานได้มีเอกสารรายละเอียดเป็นข้อปฏิบัติ / แผนปฏิบัติในการดำเนินการดังกล่าวอยู่แล้ว หน่วยงานสามารถอ้างอิงไปยังเอกสารฉบับนั้นได้ ตัวอย่างเช่น มาตรการป้องกันการทำลายข้อมูลส่วนบุคคล โดยให้ไปเป็นไปตามวิธีปฏิบัติในประกาศ.....(ชื่อหน่วยงาน)... เรื่อง ...(ชื่อเอกสารที่ต้องการอ้างอิง)..... หน้าที่..... ถึงหน้าที่..... ในหัวข้อ(ระบุชื่อหัวข้อ)..... เป็นต้น

- ดูเพิ่มเติม ตารางที่ 2 มาตรการสำหรับการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลที่ควรคำนึง

ตารางที่ 2 มาตรการสำหรับการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลที่ควรคำนึง

ข้อกำหนด	มาตรการที่ควรคำนึง
การป้องกันการสูญหายข้อมูลส่วนบุคคลโดยมิชอบ	<ul style="list-style-type: none"> - กระบวนการสำรองข้อมูลส่วนบุคคล ประกอบด้วย ข้อมูลที่สำรอง ความถี่ในการสำรอง สื่อที่ใช้ สถานที่เก็บ วิธีการเก็บรักษา และการนำไปใช้งาน - ความถี่ในการสำรองข้อมูลส่วนบุคคล - ความถี่ในการทดสอบข้อมูลที่เก็บสำรองไว้อย่างสม่ำเสมอ - การจัดการ Malicious code และ mobile code
การป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ	<ul style="list-style-type: none"> - การแยกระบบที่มีข้อมูลส่วนบุคคลที่สำคัญ - การจัดลำดับชั้นความลับของข้อมูลส่วนบุคคลในระบบสารสนเทศ - วิธีการรับส่ง ประมวลผล และจัดเก็บข้อมูลส่วนบุคคลที่เป็นความลับตามระดับความสำคัญ - การเข้าถึงระบบปฏิบัติการ - การเข้าถึงระบบเครือข่าย
การป้องกันการทำลายข้อมูลส่วนบุคคลโดยมิชอบ	<ul style="list-style-type: none"> - กระบวนการพิจารณาเพื่อทำลายข้อมูลส่วนบุคคล - รอบความถี่ในการทำลายข้อมูลส่วนบุคคล - ระบุผู้ที่มีหน้าที่ในการทำลายข้อมูลส่วนบุคคล - วิธีการทำลายสื่อบันทึกข้อมูลทั้งชนิดถาวร และการนำกลับมาใช้ใหม่
การป้องกันการใช้ข้อมูลส่วนบุคคลโดยมิชอบ	<ul style="list-style-type: none"> - การลงทะเบียนพร้อมแจ้งวัตถุประสงค์การใช้งาน - การยืนยันตัวบุคคลตามรหัสผ่านที่ได้รับอนุญาต
การป้องกันการแปลงข้อมูลส่วนบุคคลโดยมิชอบ	<ul style="list-style-type: none"> - การแปลงข้อความเข้ารหัสระบบอิเล็กทรอนิกส์
การป้องกันการแก้ไขข้อมูลส่วนบุคคลโดยมิชอบ	<ul style="list-style-type: none"> - ข้อจำกัดในการแก้ไขข้อมูลส่วนบุคคลเท่าที่จำเป็น - ระบุผู้ที่ทำหน้าที่ในการแก้ไขข้อมูลส่วนบุคคล - บันทึกรายละเอียดการปรับแก้ไขข้อมูลส่วนบุคคล เช่น การอนุมัติจากผู้มีอำนาจ การประมวลผล การบันทึกการแก้ไขเปลี่ยนแปลง และการแจ้งผู้ที่ได้รับผลกระทบจากการเปลี่ยนแปลงทราบ
การป้องกันการเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ	<ul style="list-style-type: none"> - การแลกเปลี่ยนข้อมูลทั้งภายในและภายนอกหน่วยงาน - การกำหนดสัญญาการรักษาความลับของข้อมูลส่วนบุคคล

ข้อกำหนด	มาตรการที่ควรคำนึง
การบันทึกผู้เข้าชมเว็บไซต์ (Log Files)	1) กรณีการเข้า-ออกโดยอัตโนมัติ <ul style="list-style-type: none"> - บันทึกและจัดเก็บข้อมูลการขออนุญาตเข้าใช้ระบบ - บันทึกและจัดเก็บข้อมูลการเข้า-ออก ของผู้มีสิทธิเข้าใช้ข้อมูลส่วนบุคคล - รายละเอียดข้อมูลที่ใช้ในการเก็บ 2) กรณีการแลกเปลี่ยนข้อมูล ระหว่างหน่วยงาน <ul style="list-style-type: none"> - บันทึกและจัดเก็บข้อมูลการขออนุญาตเข้าใช้ระบบ - บันทึกและจัดเก็บข้อมูลการเข้า-ออก ของผู้มีสิทธิในการแลกเปลี่ยนข้อมูล ระหว่างหน่วยงาน - รายละเอียดการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล - ระบุรายละเอียดข้อมูลที่ใช้ในการจัดเก็บ
การสร้างเสริมความสำคัญในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงานด้วยการเผยแพร่ข้อมูลข่าวสาร ให้ความรู้ จัดสัมมนา หรือฝึกอบรมในเรื่องดังกล่าวให้แก่บุคลากรในองค์กรเป็นประจำ	<ul style="list-style-type: none"> - การอบรม เพิ่มพูนความรู้แก่บุคลากรเก่าและใหม่อย่างสม่ำเสมอ - กระบวนการลงโทษทางวินัย เพื่อลงโทษบุคลากรที่ฝ่าฝืน ละเมิดนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล
การกำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของบุคลากร พนักงาน หรือลูกจ้างของตนในแต่ละลำดับชั้นให้ชัดเจน และให้มีการบันทึกรวมทั้งการทำสำรองข้อมูลของการเข้าถึงหรือการเข้าใช้งานข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด	<ul style="list-style-type: none"> - กระบวนการมอบหมายหรือกำหนดสิทธิ์ - การกำหนดสิทธิตามหน้าที่ความรับผิดชอบและตามความจำเป็น - การเพิกถอนสิทธิ เมื่อมีการลาออก เปลี่ยนตำแหน่ง หรือย้าย - การให้สิทธิพิเศษสำหรับผู้บริหารระดับสูงของหน่วยงาน และระยะเวลาทบทวนสิทธิของผู้บริหาร - การเฝ้าระวังบัญชีที่ได้รับสิทธิพิเศษ
การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์ หรือของระบบสารสนเทศทั้งหมดอย่างน้อยปีละ 1 ครั้ง	<ul style="list-style-type: none"> - กำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรม - ระบุผู้ตรวจสอบภายในหรือผู้ตรวจสอบจากภายนอก
การกำหนดให้มีการใช้มาตรการที่เหมาะสมและเป็น การเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็น	<ul style="list-style-type: none"> - การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งยวด เช่น หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวบุคคล เป็นต้น - การรักษาความมั่นคงปลอดภัยของข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชน

ข้อกำหนด	มาตรการที่ควรคำนึง
<p>ข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจนควรจัดให้มีมาตรการที่รอบคอบในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีโดยใช้วิธีการโดยเฉพาะและเหมาะสม</p>	<p>ซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ เช่น เชื้อชาติ ศาสนา ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ เป็นต้น</p> <ul style="list-style-type: none"> - การรักษาความมั่นคงปลอดภัยของข้อมูลที่อาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพ ของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน เช่น หมายเลขบัตรเดบิต หรือบัตรเครดิต เป็นต้น
<p>มาตรการที่รอบคอบในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีโดยใช้วิธีการโดยเฉพาะและเหมาะสม</p>	<ul style="list-style-type: none"> - การรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลซึ่งอายุไม่เกินสิบแปดปี
