ประเด็นด้านเทคนิค
ในการคุ้มครองข้อมูลส่วนบุคคล

นางสาวรัตนา จรูญศักดิ์สิทธิ์
ผู้อำนวยการกลุ่มงานผลักดันธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ข้อ ๑ (๕)	การรักษาความมั่นคงปลอดภัย
ข้อ ๑ (๘)	ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล
ข้อ ๒ (๒) (ข)	การใช้คุ๊กกี้ (Cookies)
ข้อ ๒ (๒) (ค)	การจัดประเภทข้อมูลส่วนบุคคลในระบบสารสนเทศ
ข้อ ๒ (๒) (ง)	บันทึกผู้เข้าชมเว็บ (Log Files)
ข้อ ๒ (๘)	การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

เงื่อนไขการดำเนินงาน

ข้อกำหนดตามประกาศ	ข้อแนะนำ
ข้อ ๑ (๕) การรักษาความมั่นคงปลอดภัย	ต้องแสดงให้เห็นถึงการกระทำใด ๆ โดยมิชอบกับข้อมูลส่วนบุคคล ดังนี้ • การสูญหายข้อมูลส่วนบุคคลโดยมิชอบ • การเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ • การทำลายข้อมูลส่วนบุคคลโดยมิชอบ • การใช้ข้อมูลส่วนบุคคลโดยมิชอบ • การแปลงข้อมูลส่วนบุคคลโดยมิชอบ • การแก้ไขข้อมูลส่วนบุคคลโดยมิชอบ • การเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

(การระบุข้ออ้างอิง/รายละเอียด)

หัวข้อ	ประเด็นป้องกัน
• การสูญหายข้อมูลส่วนบุคคลโดยมิชอบ	• กระบวนการสำรองข้อมูลส่วนบุคคล ประกอบด้วย ข้อมูลที่สำรองความถี่ในการสำรอง สื่อที่ใช้ สถานที่เก็บ วิธีการเก็บรักษา และการนำไปใช้งาน • ความถี่ในการสำรองข้อมูลส่วนบุคคล • ความถี่ในการทดสอบข้อมูลที่เก็บสำรองไว้อย่างสม่ำเสมอ • การจัดการ Malicious code และ mobile code

(การระบุข้ออ้างอิง/รายละเอียด)

หัวข้อ	ประเด็นป้องกัน
• การเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ	• การแยกระบบที่มีข้อมูล • การจัดลำดับชั้นความลับของข้อมูลส่วนบุคคลในระบบสารสนเทศ ส่วนบุคคลที่สำคัญ • วิธีการรับส่ง ประมวลผล และจัดเก็บข้อมูลส่วนบุคคลที่เป็นความลับตามระดับความสำคัญ • การเข้าถึงระบบปฏิบัติการ • การเข้าถึงระบบเครือข่าย

(การระบุข้ออ้างอิง/รายละเอียด)

หัวข้อ	ประเด็นป้องกัน
• การทำลายข้อมูลส่วนบุคคลโดยมิชอบ	• กระบวนการพิจารณาเพื่อทำลายข้อมูลส่วนบุคคล • รอบความถี่ในการทำลายข้อมูลส่วนบุคคล • ระบุผู้ที่มีหน้าที่ในการทำลายข้อมูล • วิธีการทำลายสื่อบันทึกข้อมูลทั้งชนิดถาวร และการนำกลับมาใช้ใหม่นการทำลายข้อมูลส่วนบุคคล
• การใช้ข้อมูลส่วนบุคคลโดยมิชอบ	• การลงทะเบียนพร้อมแจ้งวัตถุประสงค์การขอใช้งาน • การยืนยันตัวบุคคลตามรหัสผ่านที่ได้รับอนุญาต
•การแปลงข้อมูลส่วนบุคคลโดยมิชอบ	• การแปลงข้อความเข้าระบบอิเล็กทรอนิกส์

(การระบุข้ออ้างอิง/รายละเอียด)

หัวข้อ	ประเด็นป้องกัน
• การแก้ไขข้อมูลส่วนบุคคลโดยมิชอบ	• ข้อจำกัดในการแก้ไขข้อมูลส่วนบุคคลเท่าที่จำเป็น • ระบุผู้ที่หน้าที่ในการแก้ไขข้อมูลส่วนบุคคล • บันทึกรายละเอียดการปรับแก้ไขข้อมูลส่วนบุคคล เช่น การอนุมัติจากผู้มีอำนาจ การประมวลผล การบันทึกการแก้ไขเปลี่ยนแปลง และการแจ้งผู้ที่ได้รับผลกระทบจากการเปลี่ยนแปลงทราบ
•การเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ	• การแลกเปลี่ยนข้อมูลทั้งภายในและภายนอกหน่วยงาน • การกำหนดสัญญารักษาความลับของข้อมูลส่วนบุคคล

เงื่อนไขการดำเนินงาน

ข้อกำหนดตามประกาศ	ข้อแนะนำ
ข้อ ๑ (๘) ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล	ต้องแสดงให้เห็นถึงความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล” โดยเน้นหน้าที่ความรับผิดชอบของผู้ดูแลระบบสารสนเทศในส่วนของข้อมูลส่วนบุคคล

หัวข้อ	ประเด็นพิจารณา
• บุคคลที่เกี่ยวข้อง	• บุคลากรที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในการเข้าถึงข้อมูลในแต่ละระดับชั้นของระบบสารสนเทศ • ผู้ดูแลระบบสารสนเทศในส่วนของข้อมูลส่วนบุคคล

เงื่อนไขการดำเนินงาน

ข้อกำหนดตามประกาศ	ข้อแนะนำ
ข้อ ๒(๒)(ข) การใช้คุ๊กกี้ (Cookies)	ไม่มีประเด็นด้านเทคนิคให้พิจารณา เพียงระบุว่ามีการจัดเก็บข้อมูลหรือไม่

เงื่อนไขการดำเนินงาน

ข้อกำหนดตามประกาศ	ข้อแนะนำ
ข้อ ๒(๒)(ค) การจัดประเภทข้อมูลส่วนบุคคลในระบบสารสนเทศ	ระบุเพิ่ม หัวข้อ “ประเภทข้อมูลส่วนบุคคลในระบบสารสนเทศ” ในเอกสาร Security Policy ภายใต้ ข้อ ๕ (๓)

หัวข้อ	ประเด็นพิจารณา
• ประเภทข้อมูล	• อ้างอิงตาม ประกาศ SP ข้อ ๕ (๓) ประเภทข้อมูล • เพิ่มหัวข้อ “ข้อมูลส่วนบุคคล”

เงื่อนไขการดำเนินงาน

ข้อกำหนดตามประกาศ	ข้อแนะนำ
ข้อ ๒(๒)(ง) บันทึกผู้เข้าชมเว็บ (Log Files)	ต้องแสดงให้เห็นถึงการกระทำด้านเทคนิคในเรื่องต่าง ๆ ดังนี้ • กรณีการเข้า-ออกโดยอัตโนมัติ • กรณีการแลกเปลี่ยนข้อมูลส่วนบุคคลระหว่างหน่วยงาน

(การระบุข้ออ้างอิง/รายละเอียด)

หัวข้อ	ประเด็นพิจารณา
• กรณีการเข้า-ออกโดยอัตโนมัติ	• บันทึกและจัดเก็บข้อมูลการขออนุญาตเข้าใช้ระบบ • บันทึกและจัดเก็บข้อมูลการเข้า-ออก ของผู้มีสิทธิเข้าใช้ข้อมูลบุคคล • รายละเอียดข้อมูลที่ใช้ในการจัดเก็บ
• กรณีการแลกเปลี่ยนข้อมูลส่วนบุคคลระหว่างหน่วยงาน	• บันทึกและจัดเก็บข้อมูลการขออนุญาตเข้าใช้ระบบ • บันทึกและจัดเก็บข้อมูลการเข้า-ออก ของผู้มีสิทธิในการแลกเปลี่ยนข้อมูลส่วนบุคคล ระหว่างหน่วยงาน • รายละเอียดการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล

เงื่อนไขการดำเนินงาน

ข้อกำหนดตามประกาศ	ข้อแนะนำ
ข้อ ๒(๘) การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ข้อ (ก)(ข)(ค)(ง)(จ)	ต้องแสดงให้เห็นถึงการดำเนินงานที่สอดคล้องกับ Security Policy ในประเด็นต่าง ๆ

(การระบุข้ออ้างอิง/รายละเอียด)

หัวข้อ	ประเด็นพิจารณา
ข้อ (ก) สร้างเสริมความสำนึกในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงานด้วยการเผยแพร่ข้อมูลข่าวสาร ให้ความรู้ จัดสัมมนา หรือฝึกอบรมในเรื่องดังกล่าวให้แก่บุคลากรในองค์กรเป็นประจำ	• การอบรม เพิ่มพูนความรู้แก่บุคลากรเก่าและใหม่อย่างสม่ำเสมอ • กระบวนการลงโทษทางวินัย เพื่อลงโทษบุคลากรที่ฝ่าฝืน ละเมิดนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

(การระบุข้ออ้างอิง/รายละเอียด)

หัวข้อ	ประเด็นพิจารณา
ข้อ (ข)กำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของบุคลากร พนักงาน หรือลูกจ้างของตนในแต่ละลำดับชั้นให้ชัดเจน และให้มีการบันทึกรวมทั้งการทำสำรองข้อมูลของการเข้าถึงหรือการเข้าใช้งานข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด	• กระบวนการมอบหมายหรือกำหนดสิทธิ์ • การกำหนดสิทธิตามหน้าที่ความรับผิดชอบและตามความจำเป็น • การเพิกถอนสิทธิ เมื่อมีการลาออก เปลี่ยนตำแหน่ง หรือย้าย • การให้สิทธิพิเศษสำหรับผู้บริหารระดับสูงของหน่วยงาน และระยะการทบทวนสิทธิของผู้บริหาร • การเฝ้าระวังบัญชีที่ได้รับสิทธิพิเศษ

(การระบุข้ออ้างอิง/รายละเอียด)

หัวข้อ	ประเด็นพิจารณา
ข้อ (ค) ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือของระบบสารสนเทศทั้งหมดอย่างน้อยปีละ ๑ ครั้ง	• กำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรม • ระบุผู้ตรวจสอบภายในหรือผู้ตรวจสอบจากภายนอก

(การระบุข้ออ้างอิง/รายละเอียด)

หัวข้อ	ประเด็นพิจารณา
ข้อ (ง)กำหนดให้มีการใช้มาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหายหรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน	มาตรการพิเศษสำหรับข้อมูลดังนี้ • ข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งยวด เช่น หมายเลขประจำตัวประชาชน หรือ หมายเลขประจำตัวบุคคล • ข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชน • ข้อมูลที่อาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของ ผู้เป็นเจ้าของข้อมูล

(การระบุข้ออ้างอิง/รายละเอียด)

หัวข้อ	ประเด็นพิจารณา
ข้อ (จ)ควรจัดให้มีมาตรการที่รอบคอบในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีโดยใช้วิธีการโดยเฉพาะและเหมาะสม	มาตรการพิเศษสำหรับข้อมูลดังนี้ • ข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปี


กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
Ministry of Information and Communication Technology

ขอบคุณ