สคส.
สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ.2565

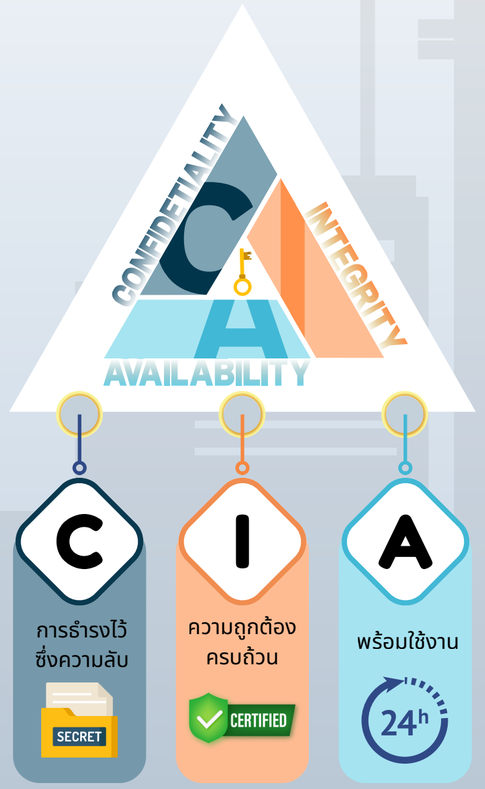
Presented By สำนักตรวจสอบและกำกับดูแล ฝ่ายกำกับการคุ้มครองข้อมูลส่วนบุคคล

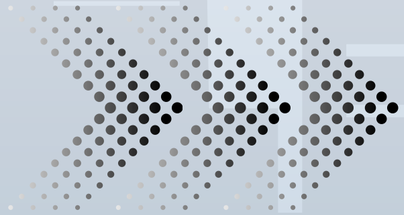
มาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

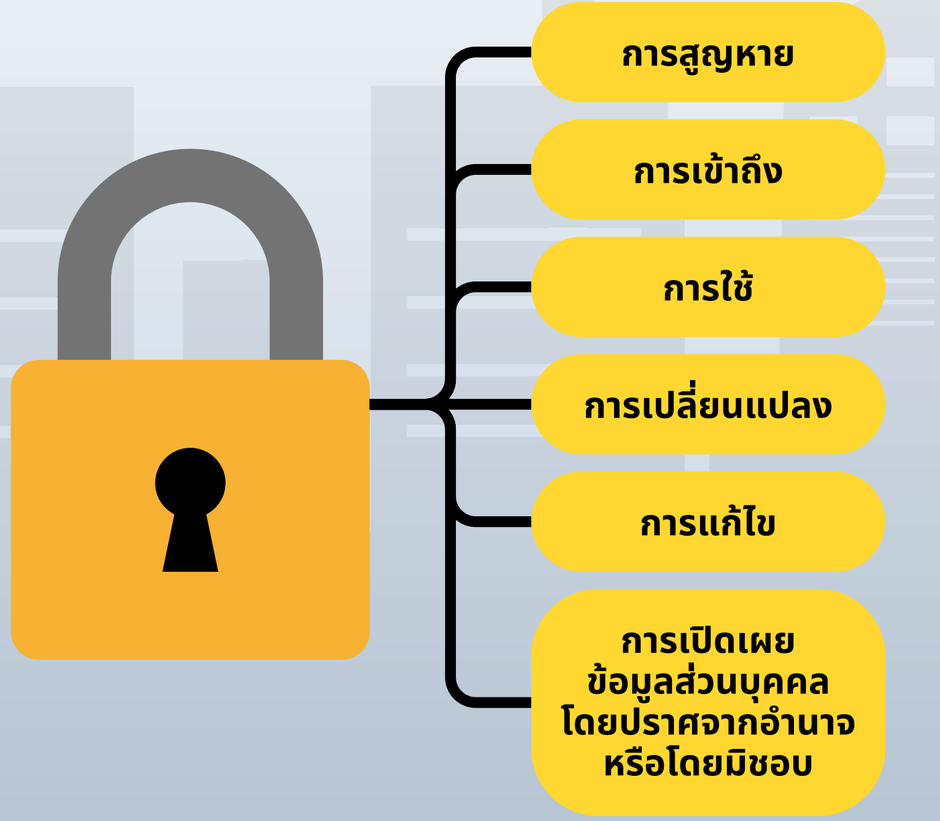
(1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่**เหมาะสม** เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่**เหมาะสม** ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

นิยาม

“ความมั่นคงปลอดภัย”





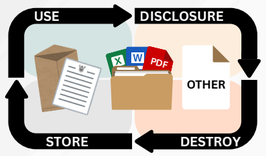


“การธำรงไว้”

ข้อ 4

มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
อย่างน้อยต้องมีการดำเนินการ

7 MEASURE

1


DATA Cycle

2


Measures

3


NIST

4


Security

5

Eletronic Data Processing

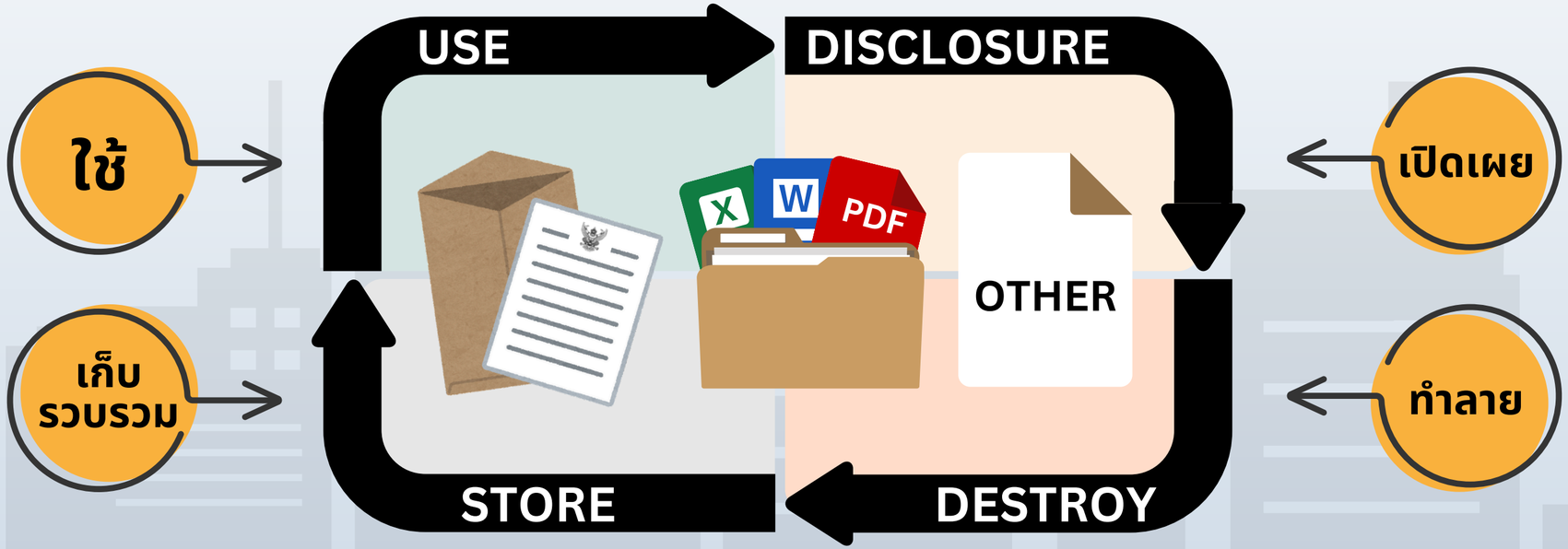
6

Access

7


Privacy and Security awareness

(1) มาตรการรักษาความมั่นคงปลอดภัยต้องครอบคลุม



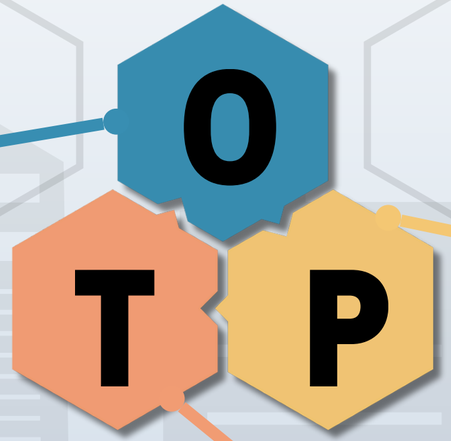
Privacy by design Privacy by default

Remark

การลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นข้อมูลส่วนบุคคลได้

(2)

MEASURES



มาตรการเชิงองค์กร
organizational measures

- นโยบายความเป็นส่วนตัว (Privacy Policy)
- นโยบายการกำหนดสิทธิเข้าถึง (Access Policy)
- การจัดทำข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (DSA : Data Sharing Agreement)

มาตรการเชิงเทคนิค
technical measures

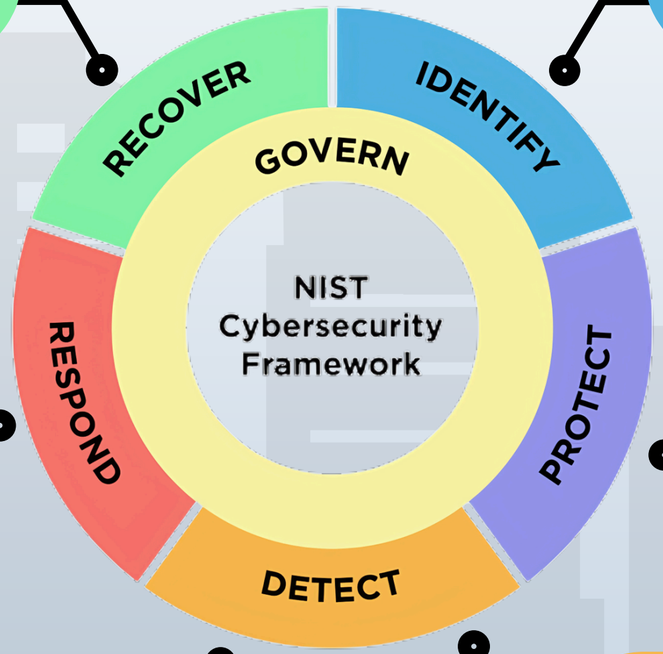
- ระบบป้องกันข้อมูลสูญหาย (DLP : Data Loss Prevention)
- การเข้ารหัสข้อมูล (Data Encryption)
- ตรวจสอบอุปกรณ์ปลายทางและตรวจภัยคุกคาม (EDR : Endpoint Detection and Response)

มาตรการทางกายภาพ
physical measures

- ตู้เซฟนิรภัย/ตู้เก็บเอกสารกันไฟ (Fireproof safe/Document cabinet)
- กล้องวงจรปิด (Closed Circuit Television)
- เซิร์ฟเวอร์สำรอง (Redundant Server)

(3)

NIST Cybersecurity Framework
(version 2.0)



กระบวนการกู้คืนระบบหากถูกโจมตี

ปฏิบัติตามแผนการกู้คืนระบบที่ได้จัดเตรียมไว้อย่างเป็นขั้นตอน
ตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำรองที่ใช้ในการกู้คืน
จัดทำแผนการสื่อสารแจ้งความคืบหน้าให้บุคคลที่เกี่ยวข้องทราบ

การระบุความเสี่ยง

จัดทำรายงานเพื่อระบุความเสี่ยงของอุปกรณ์ต่างๆ
จัดลำดับความสำคัญของสินทรัพย์ภายในองค์กรตามระดับความสำคัญ
และมีกระบวนการจัดการสินทรัพย์ตั้งแต่เริ่มต้นจนวันที่หมดอายุการใช้งาน
(Asset Lifecycle Management – ALM)

การรับมือกับภัยคุกคาม

จัดทำแผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
(Incident Response Plan) อย่างเป็นระบบเพื่อรับมือกับภัยคุกคาม
ที่อาจเกิดขึ้น โดยต้องกำหนดนโยบายและขั้นตอน
รวมถึงระบุหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องอย่างชัดเจน

การป้องกัน

ใช้มาตรการรักษาความปลอดภัย
เพื่อปกป้องระบบการทำงานหรือข้อมูลขององค์กร

การกำกับดูแล

1. กลยุทธ์การจัดการความเสี่ยง (Risk Management Strategy)
2. กำหนดนโยบายและกระบวนการที่ชัดเจน (Policies and Processes)
3. การจัดการสินทรัพย์ (Asset Management)

การตรวจจับ

ต้องมีกระบวนการในการติดตามสินทรัพย์ต่างๆ อย่างต่อเนื่อง
เพื่อตรวจจับสิ่งผิดปกติและสัญญาณที่บ่งชี้ถึงภัยคุกคาม
รวมถึงความสามารถในการวิเคราะห์เหตุการณ์ที่น่าสงสัย
หรืออาจก่อให้เกิดอันตรายอย่างรวดเร็ว

(4)

- การธำรงไว้ซึ่งความลับ CONFIDETIALITY
- ความถูกต้องครบถ้วน INTEGRITY
- สภาพพร้อมใช้งาน AVAILABILITY

“ความมั่นคงปลอดภัย”

ISO 27701:2019 Privacy Information Management CERTIFIED
ระบบบริหารจัดการความปลอดภัยของข้อมูล

ISO 27001:2022 Information Security Management CERTIFIED
ระบบการจัดการข้อมูลส่วนบุคคล

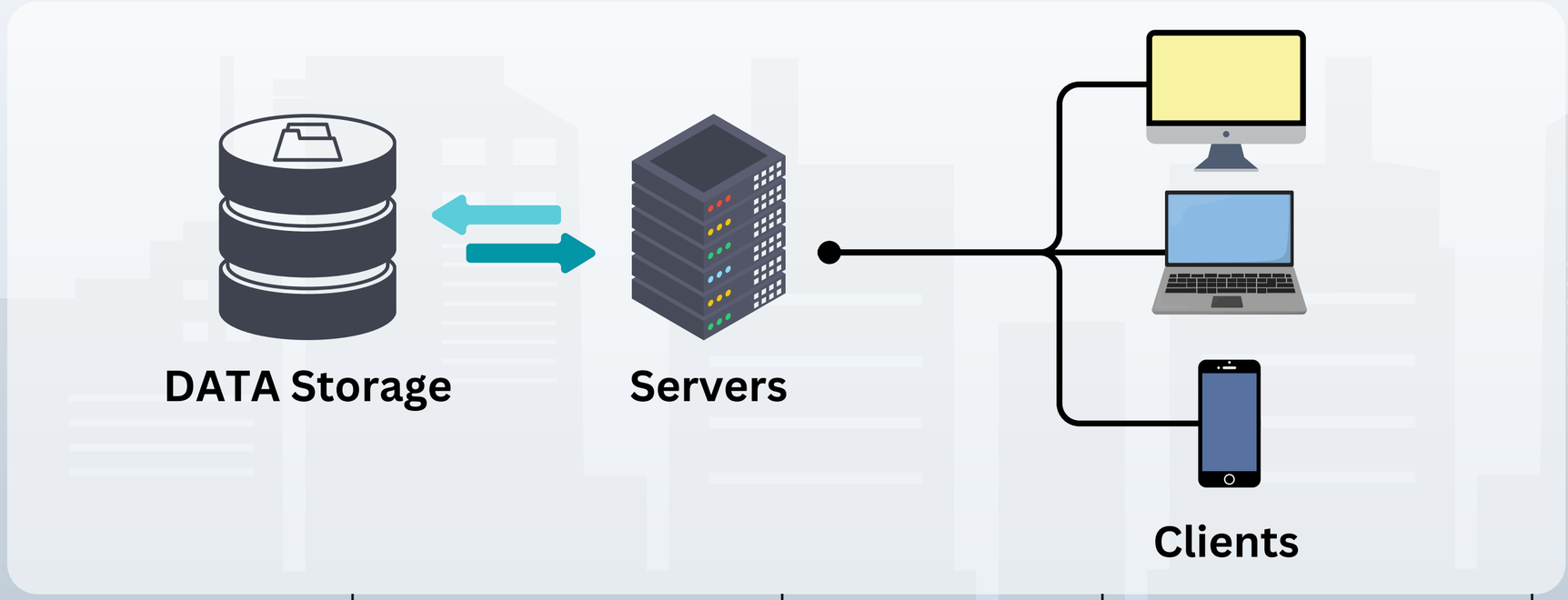
The Open Group Open Certified TOGAF® 9 Certified
Framework สถาปัตยกรรมองค์กรสำหรับการพัฒนาและจัดการกลยุทธ์ไอทีที่ขับเคลื่อนด้วยธุรกิจ

ITIL® Information Technology Infrastructure Library
มาตรฐานการปฏิบัติการจัดการบริการด้านเทคโนโลยีสารสนเทศ

แยกตามปัจจัยทางเทคโนโลยี บริบทสภาพแวดล้อม
มาตรฐานที่เป็นที่ยอมรับสาหรับหน่วยงาน
หรือกิจการในประเภทหรือลักษณะเดียวกัน
หรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม
ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้
และความเป็นไปได้ในการดำเนินการประกอบกัน

(5)

มาตรการรักษาความมั่นคงปลอดภัย ข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์



ควรคำนึงถึง

เพื่อลด
ความเสี่ยง

1
หลักการป้องกันเชิงลึก
(defense in depth)

+

2
มาตรการป้องกันหลายชั้น
(multiple layers of security controls)

(6) ACCESS

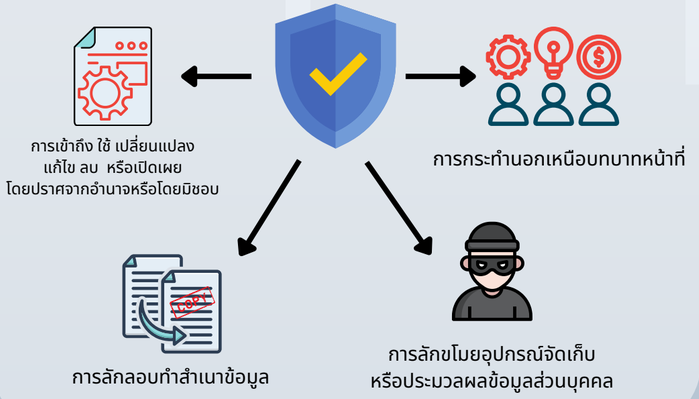
(ก) การควบคุมการเข้าถึง (access control)

1. การพิสูจน์และยืนยันตัวตน
   identity proofing and authentication
2. การอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งาน
   authorization
3. หลักการให้สิทธิเท่าที่จำเป็น
   need-to-know basis
4. หลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น
   need-to-know basis

(ข) การบริหารจัดการการเข้าถึงของผู้ใช้งานที่เหมาะสม (user access management)

- การลงทะเบียนและการถอนสิทธิผู้ใช้งาน
- การจัดการสิทธิการเข้าถึงของผู้ใช้งาน
- การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ
- การบริหารจัดการข้อมูลความลับสำหรับพิสูจน์ตัวตนของผู้ใช้งาน
- การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน
- การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง

(ค) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)



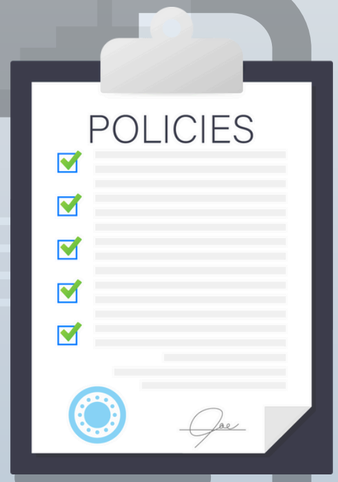
(ง)

การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (audit trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(7)

Privacy and Security awareness

Privacy



Security awareness

Remark

แจ้งให้บุคคลกร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน หรือผู้ที่เกี่ยวข้อง

“รับทราบและถือปฏิบัติ”

ข้อ 5

CAUSE เมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป

ข้อ 5 วรรค 2

เมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็น
ต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยตามวรรคหนึ่ง
เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

RESULT ต้องทบทวนมาตรการการรักษาความมั่นคงปลอดภัย
ตามข้อ 4 (1) - (7)

- P PLAN
- D DO
- C CHECK
- A ACT

ข้อ 6

การจัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล

DPA (Data Processing Agreement)

DPA

DP ต้องมีมาตรการ เป็นไปตามข้อ 4 ด้วย

มาตรา 40 วรรค 3

<u>ประกาศ กคส.</u>
เรื่อง มาตรการรักษาความมั่นคงปลอดภัย ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ข้อ 6

มาตรา 37 (1)

มาตรา 37 (4)

<u>ประกาศ กคส.</u>
เรื่อง หลักเกณฑ์และวิธีการในการแจ้ง เหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

ข้อ 7

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายอื่น ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามกฎหมายนั้น แต่มาตรการรักษาความมั่นคงปลอดภัยดังกล่าวของผู้ควบคุมข้อมูลส่วนบุคคลจะต้องเป็นไปตามมาตรฐานขั้นต่ำที่กำหนดในประกาศนี้ด้วย

Remark

สอดคล้องกับ มาตรา 3
แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

สคส.

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล