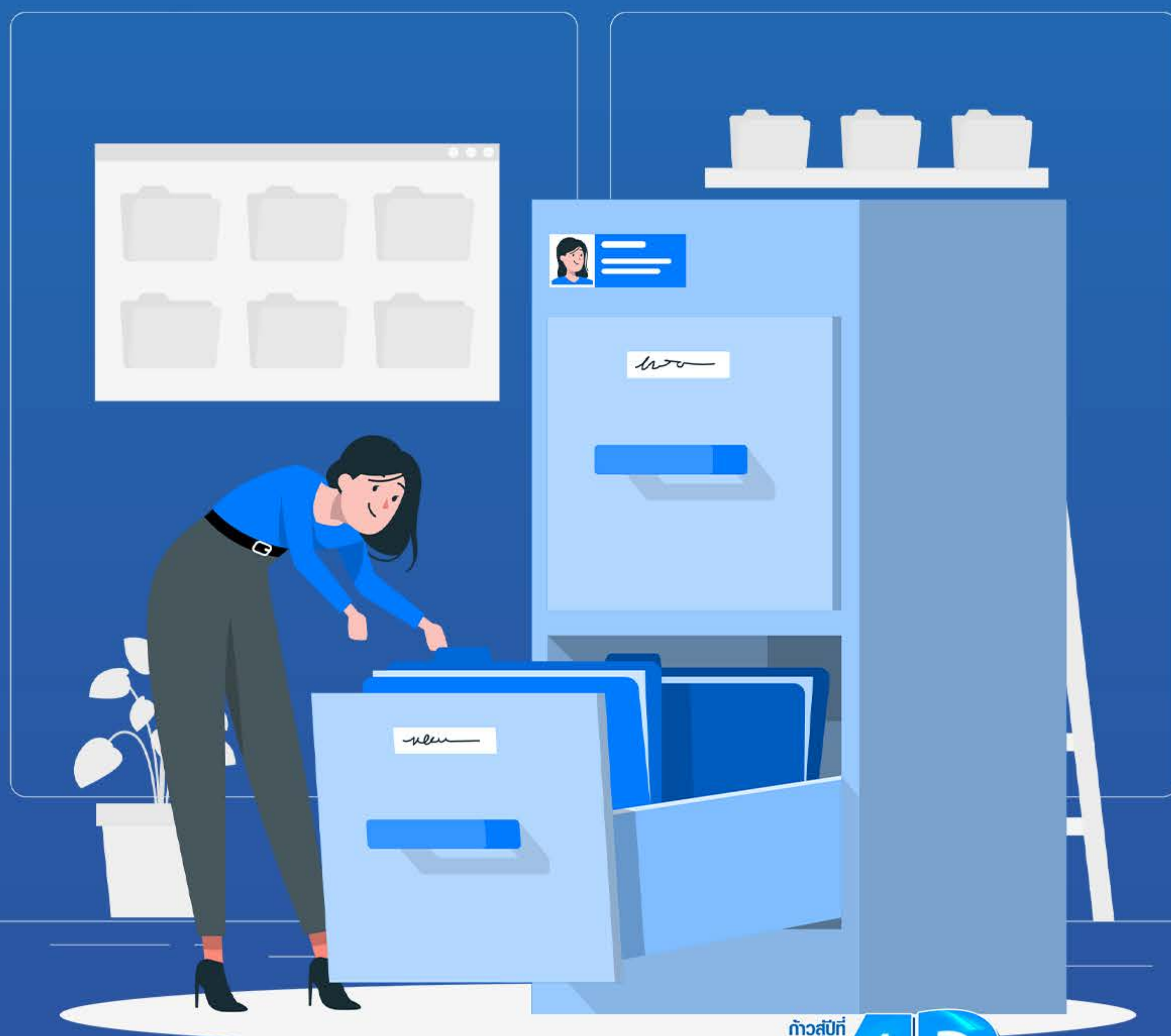


มาตรการป้องกัน การรั่วไหลข้อมูลส่วนบุคคล Generic Measure



ทำสุปที่

43rd ปี
PWA

01

ห้ามทำสำเนาเอกสาร ระบุตัวตนลูกค้าโดยไม่จำเป็น

เช่น บัตรประชาชน หรือ passport ไม่ว่าจะด้วยวิธีการ Xerox, Scan File, Email, Save File, Download, Print, ถ่ายรูปด้วยมือถือ เว้นแต่เป็นการเก็บเข้าระบบหรือ Storage ของ กปภ. ตามกระบวนการทำงานปกติ หรือ เป็นไปตามหลักเกณฑ์ที่ กปภ. กำหนด



02

จัดทำใบรับส่งเอกสาร หรือ Checklist



สำหรับการรับส่งเอกสารภายในและภายนอกองค์กร รวมถึงระบุประเภทเอกสารที่ต้องขอจากลูกค้า ให้ลูกค้าลงนาม ต้องมีกระบวนการตรวจสอบ ความถูกต้องครบถ้วนของเอกสาร และปิดผนึก ให้เรียบร้อย เพื่อป้องกันการละเมิดหรือส่งรั่วข้อมูล ระหว่างทาง

03

การจัดส่งเอกสาร ผ่านช่องทางต่าง ๆ

- ใส่ซองปิดผนึก ระบุผู้รับให้ชัดเจน
- นำส่งด้วยตนเอง หรือผู้ได้รับมอบหมายจาก กปภ.
โดยส่งถึงลูกค้าเท่านั้น เว้นแต่จะได้รับอนุญาตเป็นกรณี ๆ ไป
- กรณีผู้ให้บริการภายนอก ต้องเป็นผู้ให้บริการที่ กปภ.
กำหนดเท่านั้น
- กรณีส่งผ่านไปรษณีย์ ต้องส่งแบบปิดผนึก ระบุผู้รับ
อย่างเจาะจงและต้องมีมาตรการป้องกันการรั่วไหลของ
ข้อมูลอื่นเพิ่มเติม เช่น การปิดบังข้อมูลสำคัญบางส่วน
หรือใช้ผู้ให้บริการส่งไปรษณีย์ที่ กปภ. กำหนดเท่านั้น
- ต้องมีการติดตามสถานะของการจัดส่ง โดยเฉพาะกรณี
ที่เจ้าของข้อมูลมิได้เป็นผู้รับเอง
- ไม่ควรใช้ Line หรือ Email ส่วนตัว ในการปฏิบัติงาน
หรือการรับทำธุรกรรมใด ๆ ที่มีข้อมูลลูกค้า และข้อมูลลับ
หรือลับมากของ กปภ.

04

จัดทำทะเบียนการให้ข้อมูลลับ หรือลับมาก

เพื่อให้สามารถระบุ ติดตาม ตรวจสอบผู้รับข้อมูลได้



05

ระบุชั้นความลับของเอกสาร

ได้แก่ การจัดทำป้ายเพื่อระบุชั้นความลับที่เอกสาร แฝบ
และจัดเก็บให้สอดคล้องกับแนวทาง หรือมาตรการบริหาร
จัดการข้อมูลตามระดับชั้นความลับ



06

จัดทำทะเบียนบันทึก การทำลายเอกสาร

และข้อมูลตามทะเบียนซึ่งอาจอยู่ในรูปแบบเอกสาร
หรือไฟล์ทะเบียน

07

วิธีการทำลายข้อมูล

- เอกสาร ใช้เครื่องย่อยเอกสารชนิดที่ไม่สามารถนำกลับมาประกอบใหม่หรือฉีกเอกสารก่อนหย่อนลงกล่อง
- ลบข้อมูล หรือทำลายข้อมูลตามประเภทสื่อบันทึกข้อมูล ให้ไม่สามารถกู้คืนข้อมูลกลับมาใช้ได้อีก



PWA CLOUD DRIVE

08

บันทึกไฟล์งานใน PWA CLOUD DRIVE

หรือระบบงานที่บริษัทจัดเตรียมไว้ให้เท่านั้น

- จัดเก็บโดยกำหนดวันที่
- กำหนดสิทธิการเข้าถึงไฟล์ใน Folder หรือข้อมูลในระบบ เฉพาะพนักงานที่เกี่ยวข้อง
- ต้องมีการเข้ารหัส (Encrypt) ด้วยสำหรับข้อมูลลับมาก

09

การส่งไฟล์ข้อมูลลับ

กรณีส่งไฟล์ที่มีข้อมูลลับหรือลับมาก ระหว่างกันภายในองค์กร

- ให้จัดทำเป็น link และส่งให้ผู้ที่ต้องใช้ข้อมูลเข้ามาดูผ่าน link ดังกล่าว
- หากไม่สามารถดำเนินการดังกล่าวได้และต้องส่งเป็นไฟล์ให้ดำเนินการ Encrypt ไฟล์ ก่อนส่งทุกครั้ง โดยขอให้พิจารณาปิดบังข้อมูลบางส่วน (Masking) และส่งเฉพาะบุคคลที่เกี่ยวข้องโดยตรงเท่านั้น กรณีเป็นพัสดุไฟล์ให้ปฏิบัติตามข้อ 1 คือห้ามทำสำเนาหรือบันทึกข้อมูลเก็บไว้หลายแห่งเกินความจำเป็น



10

กรณีมีความจำเป็นต้องใช้ข้อมูล

ให้ย้ายไปเก็บอยู่ใน PWA CLOUD DRIVE

กรณีต้องการเก็บไฟล์งานไว้ใช้ อ้างอิงใน Folder ส่วนตัว

ให้ดำเนินการนำข้อมูลส่วนบุคคลออกก่อน และให้จัดเก็บไว้ตามระยะเวลาที่ฝ่ายงานกำหนดหรือลบทิ้งเมื่อไม่ต้องการใช้งานแล้ว

กรณีมีความจำเป็นต้องบันทึกไฟล์ ที่มีข้อมูลส่วนบุคคล

ออกมาใช้งานบน Drive C, Drive D เช่น กรณีการทำงานบน Microsoft Office Online ให้ทำได้เฉพาะกับกรณีใช้เครื่องคอมพิวเตอร์ของ กปภ. เท่านั้น

เมื่อทำงานเสร็จ

และได้บันทึกไฟล์เข้าไปใน PWA CLOUD DRIVE แล้ว
ต้องลบไฟล์ที่บันทึกไว้ในเครื่องคอมพิวเตอร์ทุกครั้ง
และหมั่นลบไฟล์ที่อยู่ในเครื่องทุกปี