THAI GDPR Compliance:

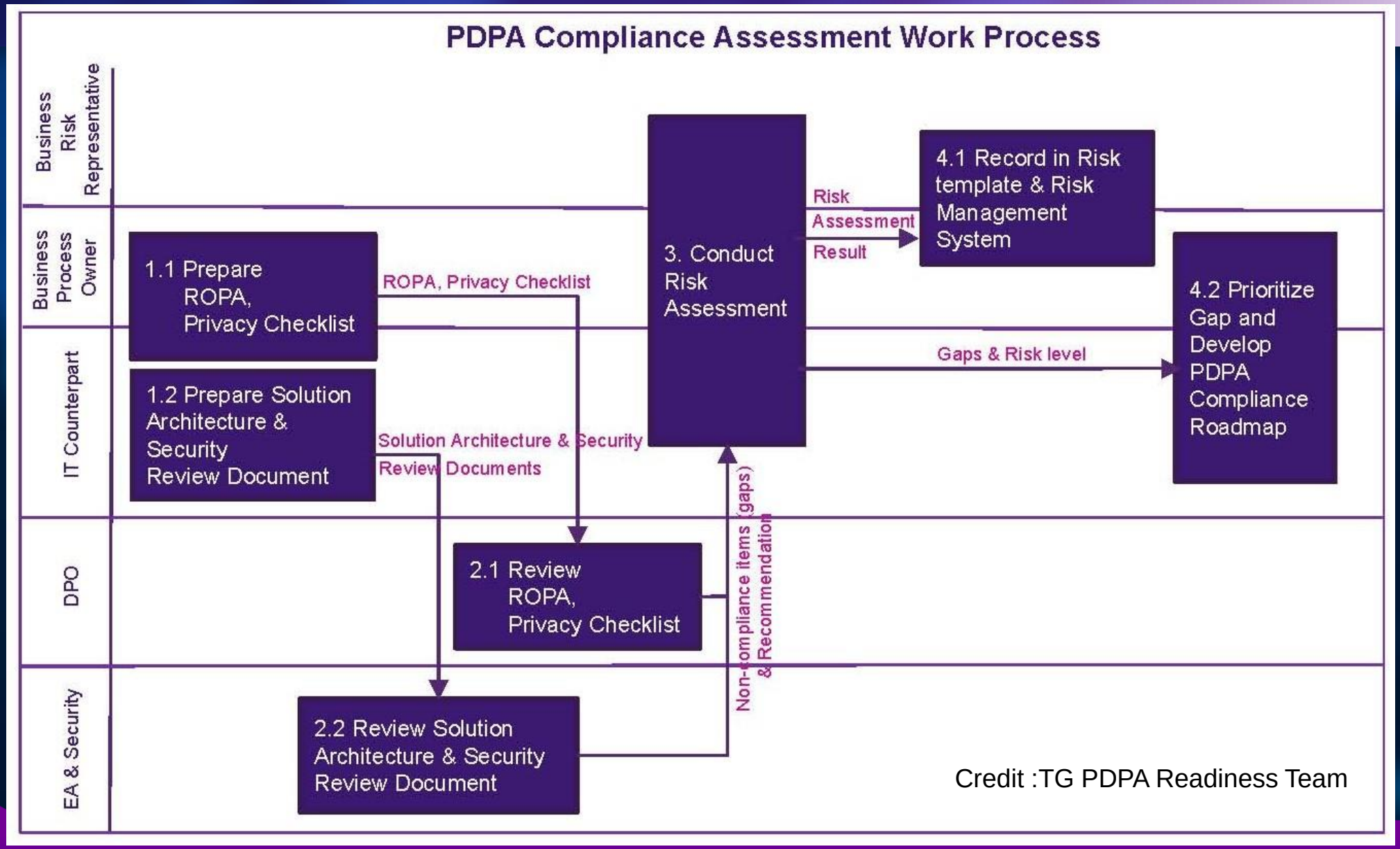
ทำอย่างไรเมื่อข้อมูลส่วนบุคคลรั่วไหล

ดร.สิทธินัย จันทรานนท์
หัวหน้าฝ่าย สังกัดฝ่ายกำกับการปฏิบัติตามกฎเกณฑ์องค์กร
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

15 ธันวาคม 2564

ปรับปรุง 10 ธันวาคม 2564

เทคนิคและวิธีการตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลฯและผู้ประมวลผลข้อมูลฯ



Credit :TG PDPA Readiness Team

วิธีการรักษาความมั่นคงปลอดภัย

Data Protection

- Identify
  - Assessment System that Store Sensitive data
- Protect
  - Network Firewall
  - Hostbase Firewall
  - Data Security (Budget Request Process)
    - Encryption : File Sharing , Database
    - Tokennization : Application level
- Detect

  SIEM

  SOC Team
- Respond

  TG-CIRT Team
- Recovery

  Backup

Credit :TG CIRT Team

GDPR: การแจ้งการละเมิดข้อมูลส่วนบุคคล ไปยังหน่วยงานกำกับดูแล (A33-34)

Data Breach (CIA)

ความลับ ความแม่นยำถูกต้อง ความพร้อมใช้งาน

แจ้งการละเมิดไปยังหน่วยกำกับดูแลที่มีอำนาจโดยไม่ชักช้าโดยไม่มีเหตุผล และเป็นไปได้ ภายใน 72 ชั่วโมงหลังจากได้รับทราบว่ามีการละเมิด

เมื่อการละเมิดข้อมูลส่วนบุคคลน่าจะมีผลกระทบความเสี่ยงงสูงต่อสิทธิและเสรีภาพของบุคคลธรรมดา ผู้ควบคุม จะต้องแจ้งสื่อสารไปยังเจ้าของข้อมูลโดยไม่ช้าพร้อมด้วยการเยียวยา

หรือหากขนาดของการละเมิดเกี่ยวข้องกับการดำเนินการที่ไม่ได้สัดส่วนในกรณีดังว่านั้น จะต้องแจ้งให้สาธารณะชนหรือใช้วิธีการอื่นที่คล้ายคลึงกันแทน

ในอัน ที่จะทำให้เจ้าของข้อมูลได้รับทราบด้วยวิธีการอันมีประสิทธิภาพอันคล้ายกัน

PDPA: การแจ้งการละเมิดข้อมูลส่วนบุคคลไป ยัง สคส. ม 37(4)

Data Breach (CIA)

ความลับ ความแม่นยำถูกต้อง ความพร้อมใช้งาน

แจ้งการละเมิดไปยังสคส. โดยไม่ชักช้า ภายใน 72 ชั่วโมง หลังจากได้รับทราบว่ามีการละเมิด เว้นแต่ไม่มีความเสี่ยง

เมื่อการละเมิดข้อมูลส่วนบุคคลน่าจะมีผลกระทบความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุม จะต้องแจ้งไปยังเจ้าของข้อมูลพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า

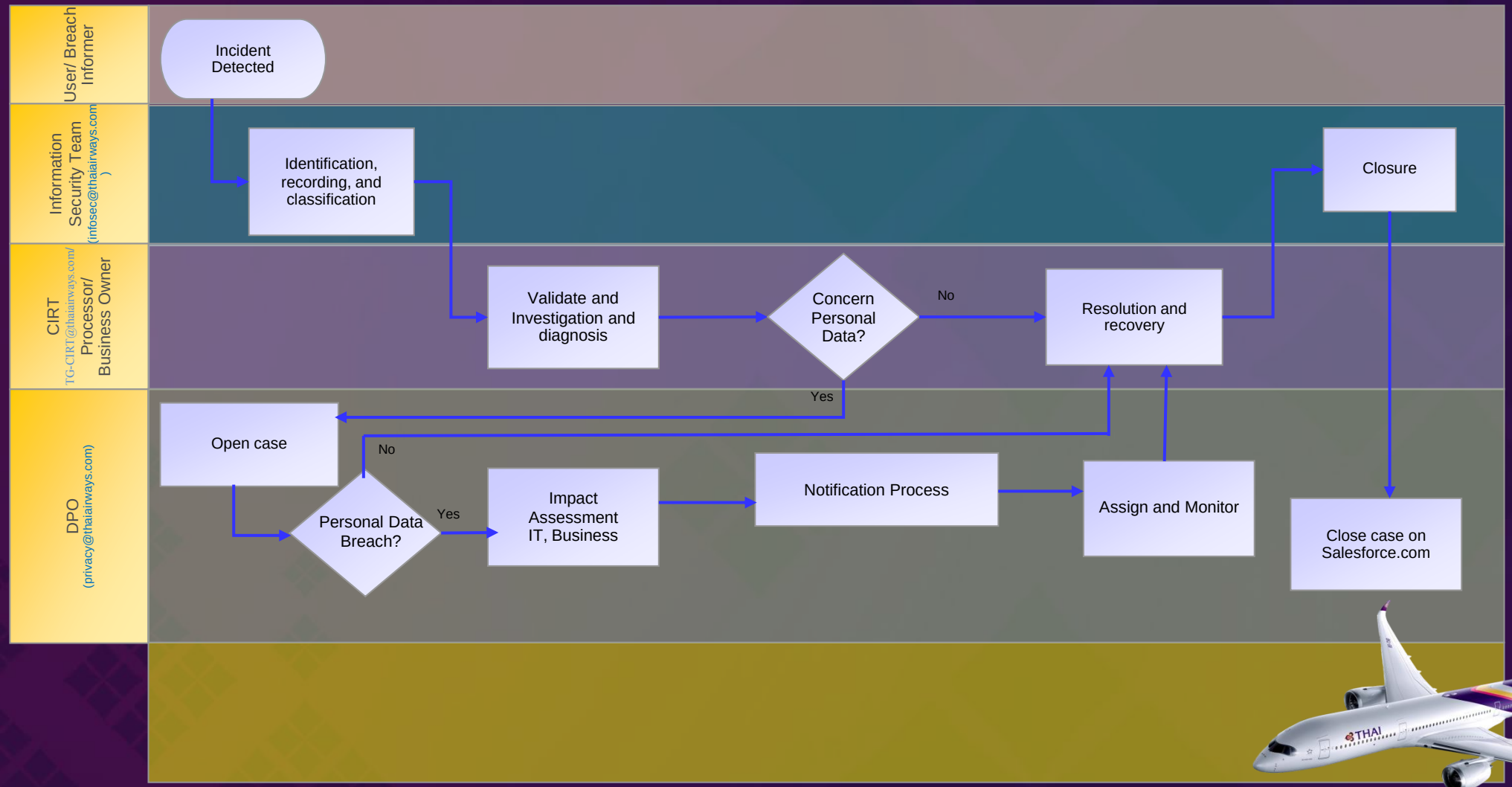
วิธีการแจ้งเป็นไปตามหลักเกณฑ์ที่คณะ กรรมการกำหนด

การแจ้งเหตุข้อมูลส่วนบุคคลรั่วไหล

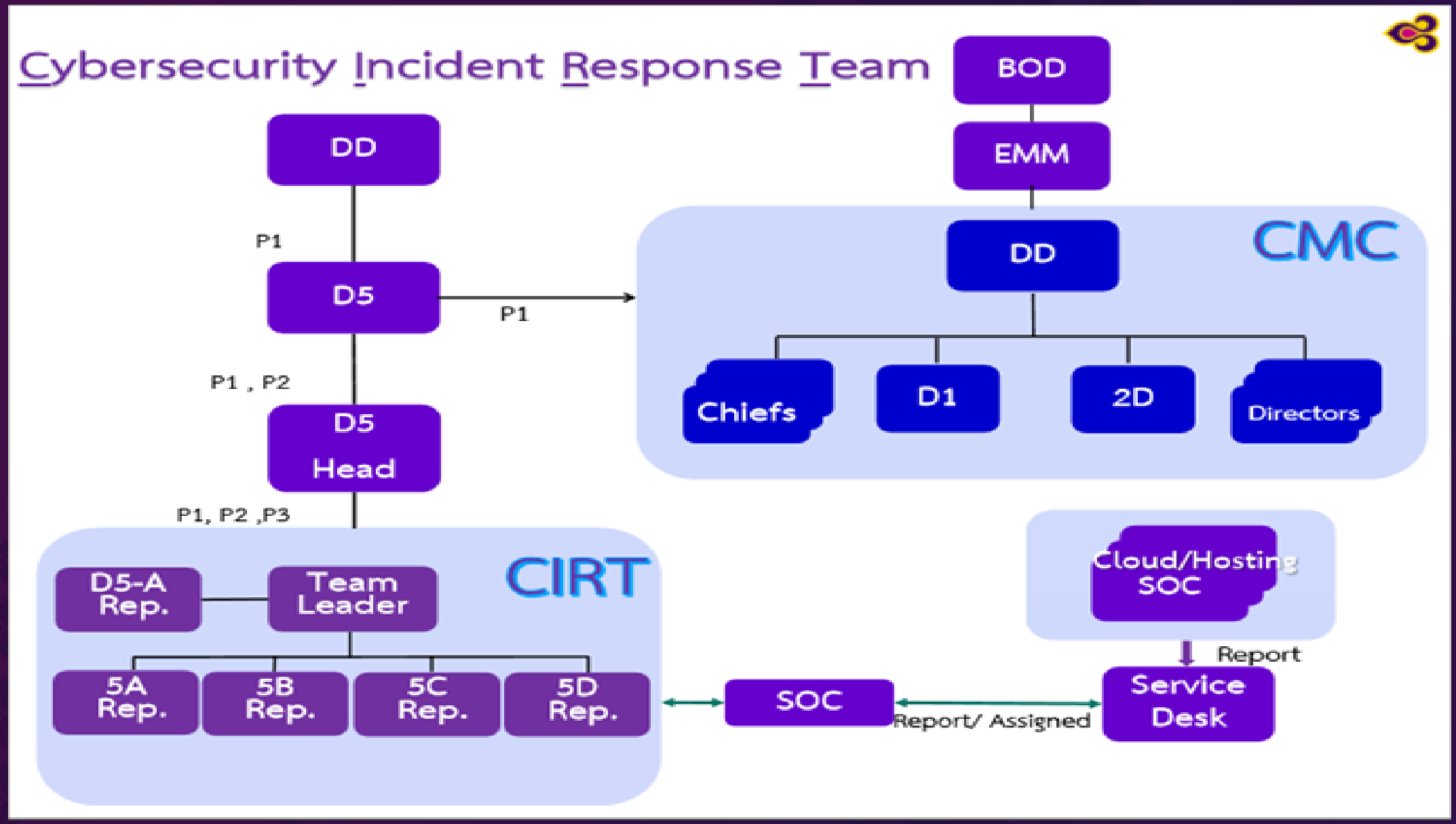
- จัดเตรียมกระบวนการ และช่องทางในการแจ้งการรั่วไหล/ละเมิด
- สื่อสารให้ทั่วทั้งองค์กร
- จัดเตรียม แบบตัวอย่างการแจ้ง (Template)
- ซักซ้อมวิธีการ ในแต่ละพฤติการณ์

Data Breach Process Flow

Credit :TG PDPA Readiness Team



Credit :TG CIRT Team



เทคนิคและวิธีการบริหารจัดการกรณีที่ข้อมูลส่วนบุคคลรั่วไหลหรือถูกละเมิด

Credit :TG CIRT Team

Data Breach Process

Channel / Business Users

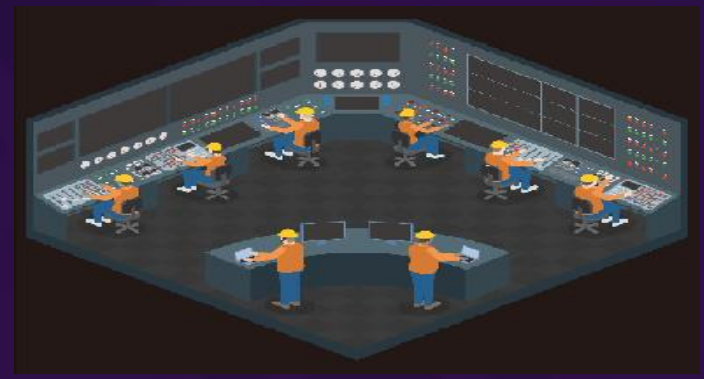
Customer(s)

Contact
email: infosec@thaiairways.com
Tel : 02

Contact DPO
email: privacy@thaiairways.com

Service Desk

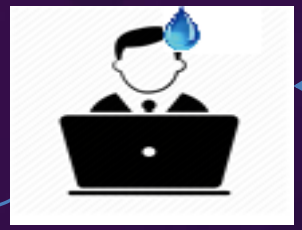
SOC
(Security Operation Center)



Security Monitoring

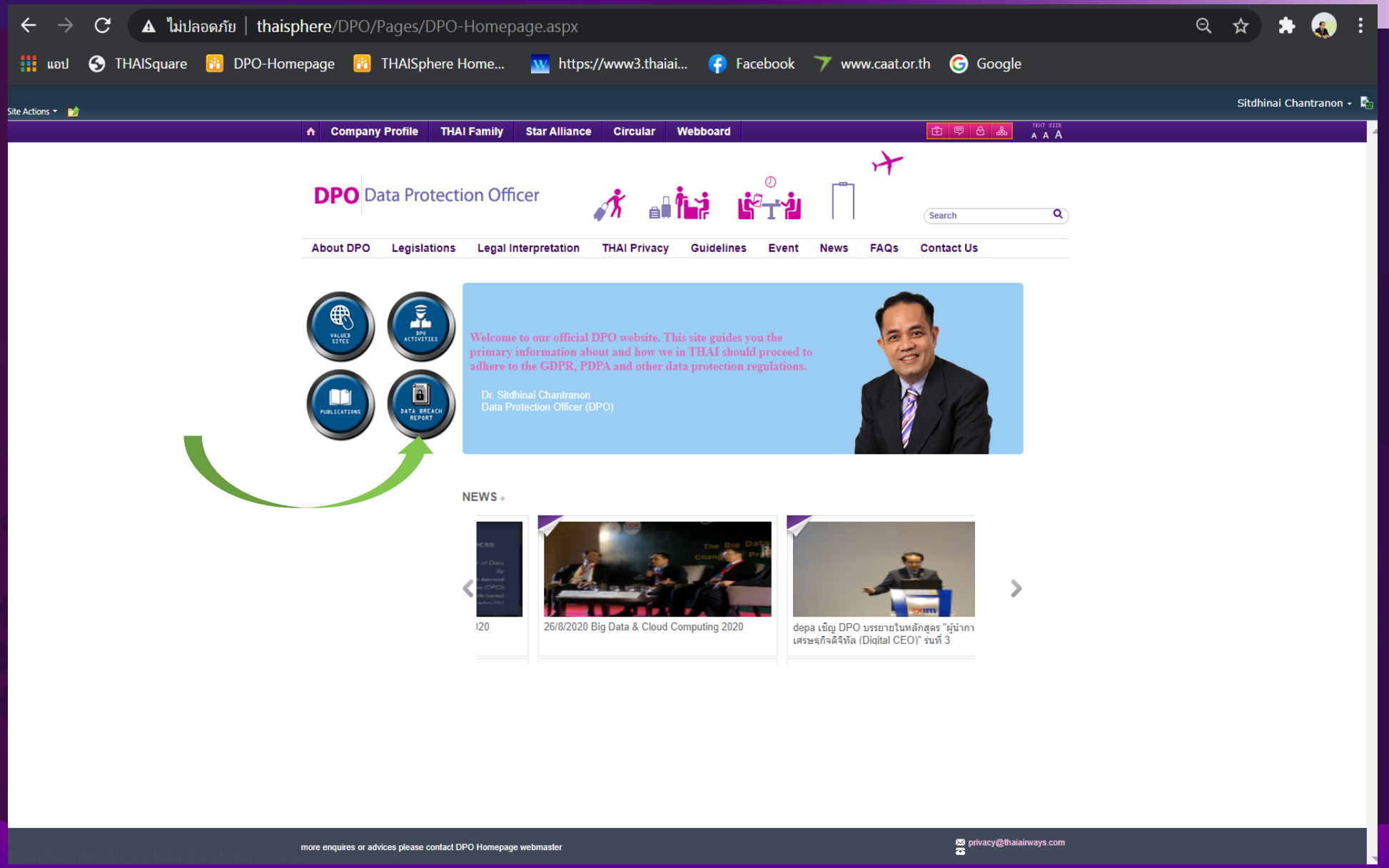
Within 72 Hours

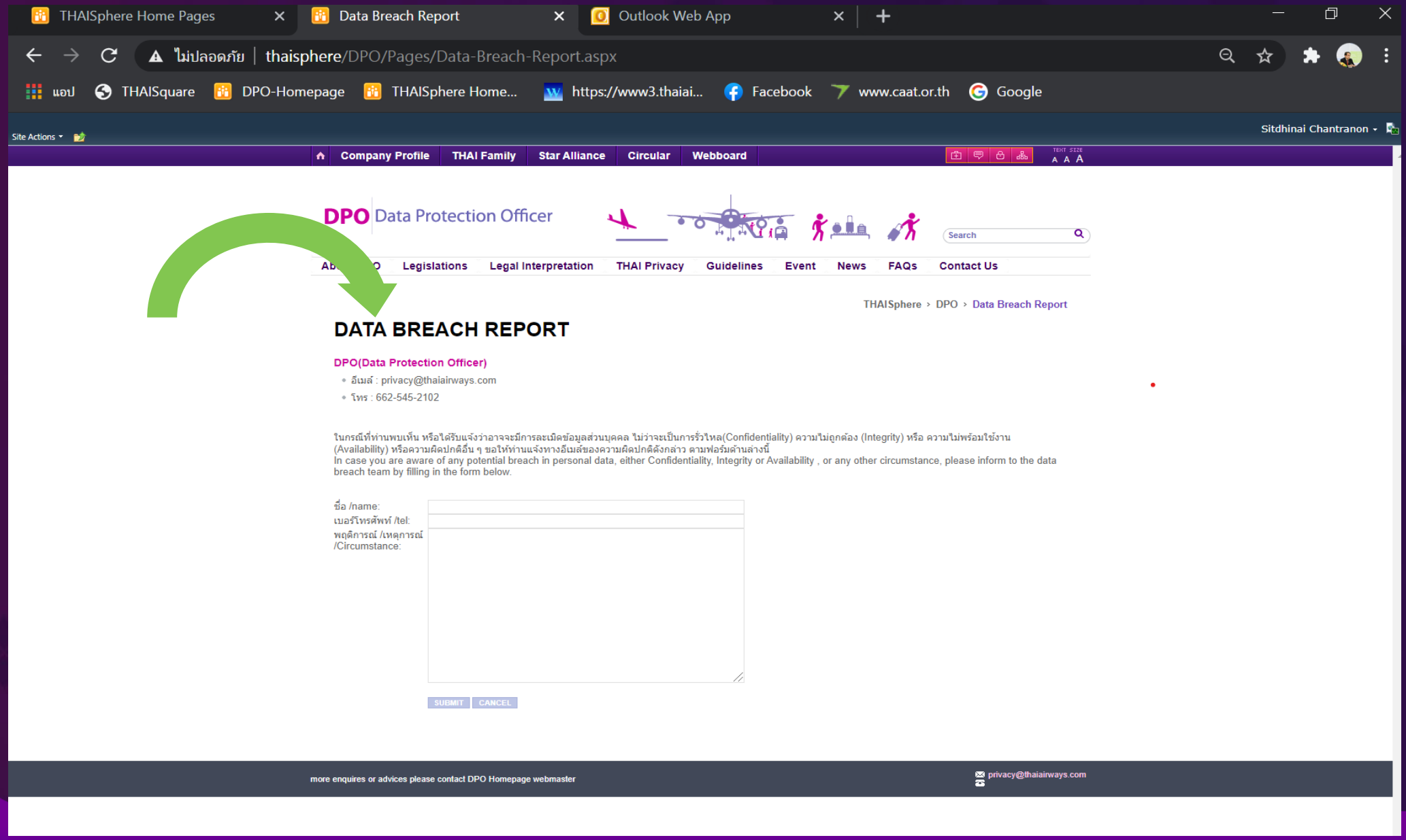
DPA
Data Protection Authority



Business
Concerned

Personal Data Breach




THAISphere Home Pages
Data Breach Report
Outlook Web App
ไม่ปลอดภัย | thaisphere/DPO/Pages/Data-Breach-Report.aspx
แอป
THAISquare
DPO-Homepage
THAISphere Home...
https://www3.thaiai...
Facebook
www.caat.or.th
Google
Site Actions
Sitdhinai Chantranon
Company Profile
THAI Family
Star Alliance
Circular
Webboard
DPO Data Protection Officer
Search
Legislations
Legal Interpretation
THAI Privacy
Guidelines
Event
News
FAQs
Contact Us
THAISphere › DPO › Data Breach Report
DATA BREACH REPORT
DPO(Data Protection Officer)
อีเมล์ : privacy@thaiairways.com
โทร : 662-545-2102
ในกรณีที่ท่านพบเห็น หรือได้รับแจ้งว่าอาจจะมีการละเมิดข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการรั่วไหล(Confidentiality) ความไม่ถูกต้อง (Integrity) หรือ ความไม่พร้อมใช้งาน (Availability) หรือความผิดปกติอื่น ๆ ขอให้ท่านแจ้งทางอีเมล์ของความผิดปกติดังกล่าว ตามฟอร์มด้านล่างนี้
In case you are aware of any potential breach in personal data, either Confidentiality, Integrity or Availability , or any other circumstance, please inform to the data breach team by filling in the form below.
ชื่อ /name:
เบอร์โทรศัพท์ /tel:
พฤติการณ์ /เหตุการณ์ /Circumstance:
SUBMIT
CANCEL
more enquires or advices please contact DPO Homepage webmaster
privacy@thaiairways.com

Case Study: เหตุการณ์ข้อมูลรั่วไหลของการบินไทย

24 กุมภาพันธ์ 2564

- มีการส่งอีเมล์ แจ้งการออก Travel Voucher แทน EMD โดยจากการแจ้งนั้น มีการส่งอีเมล์ผิดไปยังลูกค้ารายอื่นซึ่งไม่ใช่เจ้าของ Voucher ประกอบด้วยลูกค้าหลายสัญชาติ

  - ได้ดำเนินการเรียกประชุมผู้เกี่ยวข้องเพื่อดำเนินการแจ้งขอโทษลูกค้าและส่ง Voucher ที่ถูกต้องพร้อมทั้งแจ้งหน่วยกำกับดูแลใน EU ไปแล้ว 9 ประเทศ ได้รับการตอบรับ 4 ประเทศ และปิดคดี 3 ประเทศ และแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแล้ว

Case Study: เหตุการณ์ข้อมูลรั่วไหลของการบินไทย

28 กุมภาพันธ์ 2564

- ฝ่ายกฎหมายของ Star Alliance ได้นำส่งรายงานของ CEO ของ Star Alliance ซึ่งส่งถึงตัวแทนฝ่ายบริหารของสายการบินสมาชิกว่า ได้รับแจ้งจาก SITA ว่าพบการรั่วไหลของข้อมูลซึ่งกระทบต่อสมาชิก Star Alliance จากการติดต่อทราบว่าเป็นข้อมูลลูกค้า ROP ของ การบินไทย รวมอยู่ด้วย

  - DPO ได้มีการประชุมกับ Star Alliance และผู้เกี่ยวข้อง เนื่องจากการรั่วไหลของข้อมูลเกิดจากสายการบินอื่นและข้อมูลที่รั่วไหลเป็นข้อมูลพื้นฐาน มิใช่ข้อมูลอ่อนไหวมิได้กระทบต่อสิทธิของลูกค้ามากนัก สายการบินอื่น เป็น Controller ข้อมูลมีหน้าที่ในการแจ้งหน่วยงานกำกับ ส่วนบริษัทฯ ดำเนินการแจ้งลูกค้าทางอีเมล์และหน้าเวปไซต์ และเฝ้าติดตามการแลกไมล์สะสมอย่างใกล้ชิดยังไม่พบความผิดปกติ

    ทั้งสองเหตุการณ์ยังไม่มีการร้องเรียนเป็นตัวเงิน

การดำเนินงานของรอยัล ออร์คิด พลัส เกี่ยวกับการรั่วไหลของข้อมูลที่เกิดขึ้นในระบบ SITA

Credit :TG ROP Team

- การแจ้งข่าวสารให้กับสมาชิกผ่านทางเว็บไซต์ของการบินไทย thaiairways.com และ รอยัล ออร์คิด พลัส thaiairways.com/rop

ROYAL ORCHID PLUS | English | Contact Us | FAQs | THAI | ENROLL NOW! | LOG IN

Home | About Royal Orchid Plus | Status & Benefits | Earn Miles | Spend Miles | Promotions

HOME » SITA Data Breach Incident

Important Notice on the Data Breach Incident at SITA Passenger Service System

Need Help? Ask me here

Quick Links

Book a flight

Thai Airways has been notified of the data breach incident at one of the third-party IT service providers, SITA Passenger Service System (US) Inc. (SITA PSS), which operates passenger processing systems for global airlines. This data security incident involves certain passenger data stored in the SITA PSS which is used to support airline operations. Data transferred among Star Alliance Airlines via passenger service systems is necessary to recognize membership tier status of frequent flyer members, in order to ensure that premium customers are recognized across the Alliance and relevant benefits are provided to them during travel.

Thai Airways was initially informed on 28 February, 2021 that data breach incident was found on 24 February, 2021. Then, Thai Airways received a completed list of data from SITA on 9 March, 2021.

Although Thai Airways does not adopt the SITA PSS, this data breach on the SITA PSS server has affected Star Alliance airline members. Please note that only necessary information has been shared between Thai Airways and Star Alliance partner airlines, and is limited to the membership number, name, and tier status. Thai Airways does not share any other personal data of Royal Orchid Plus members to SITA PSS. Thus, please rest assured that your encrypted PIN (Personal Identification Number), mileage balance of your Royal Orchid Plus account, contact information, passport number, and birthdate are safe from this incident. There is no need for you to take any action in this matter.

If you have any concerns about this data breach incident with SITA PSS or would like to know our measures regarding data security, please feel free to contact Thai Airways' Data Protection Officer at privacy@thaiairways.com or if you are residing in EU countries, contact our representative at EU.Representative@thaiairways.com. For your membership account enquiries, please contact Royal Orchid Plus member service directly, here.

ข้อมูลในระบบบริการผู้โดยสารของ SITA ที่ส่งผลกระทบกับข้อมูลของสมาชิก

ตามที่การบินไทยได้รับแจ้งข่าวเหตุการณ์การรั่วไหลของข้อมูลที่เกิดขึ้นกับระบบของ SITA Passenger Service System (US) Inc. (SITA PSS) ซึ่งเป็นหนึ่งในองค์กรที่ดำเนินงานด้านระบบบริการผู้โดยสารให้กับสายการบินต่างๆ ทั่วโลกและ เหตุการณ์ครั้งนี้ได้ส่งผลกระทบต่อข้อมูลของผู้โดยสารบางส่วน เนื่องจากการดำเนินงานของสายการบินพันธมิตรในกลุ่มสตาร์ อัลไลแอนซ์ นั้นมีการถ่ายโอนข้อมูลระหว่างสายการบินผ่านระบบบริการผู้โดยสาร SITA PSS เพื่อให้กลุ่มสายการบินสมาชิกสตาร์อัลไลแอนซ์ ได้รับทราบระดับสถานภาพสมาชิกของผู้โดยสารและสามารถมอบบริการและสิทธิประโยชน์ให้กับสมาชิกในระหว่างการเดินทางได้ตามข้อตกลงของสายการบิน

ทางการบินไทยได้รับแจ้งเบื้องต้นในวันที่ 28 กุมภาพันธ์ 2564 ว่า SITA ได้ตรวจพบการรั่วไหลของข้อมูลดังกล่าวในวันที่ 24 กุมภาพันธ์ 2564 และทางการบินไทยได้รับรายงานข้อมูลที่สมบูรณ์จาก SITA ในวันที่ 9 มีนาคม 2564

แม้ว่าการบินไทยจะมิได้ใช้ระบบ SITA PSS แต่การรั่วไหลของข้อมูลที่เกิดขึ้นในระบบของ SITA PSS ครั้งนี้ได้มีผลกระทบต่อสายการบินในกลุ่มสตาร์ อัลไลแอนซ์ รวมถึงการบินไทยด้วย ซึ่งผลกระทบที่เกิดขึ้นกับข้อมูลสมาชิกรอยัล ออร์คิด พลัส ได้แก่ หมายเลขสมาชิก ชื่อ-นามสกุล ระดับสถานภาพสมาชิกเท่านั้น บริษัทฯ จึงขอเรียนให้ท่านมั่นใจได้ว่า รหัสประจำตัวสมาชิก (PIN) ไมล์สะสมในบัญชีสมาชิก รายละเอียดการติดต่อ หมายเลขหนังสือเดินทาง รวมถึง วันเดือนปีเกิดของท่าน ได้ถูกเก็บรักษาอย่างปลอดภัยและไม่ได้รับผลกระทบจากเหตุการณ์ในครั้งนี้ ท่านจึงไม่จำเป็นต้องดำเนินการเพิ่มเติมใดๆ

บริษัทฯ จึงเรียนมาเพื่อแจ้งให้ท่านทราบถึงเหตุการณ์ดังกล่าว แม้ว่าเหตุการณ์การรั่วไหลข้อมูลในครั้งนี้จะเกิดขึ้นจากองค์กรภายนอกก็ตาม หากท่านมีข้อกังวลใดๆ เกี่ยวกับเหตุการณ์การรั่วไหลของข้อมูลที่เกิดขึ้นกับระบบ SITA PSS ครั้งนี้ หรือมีความประสงค์ที่จะได้รับข้อมูลเพิ่มเติมทางด้านความปลอดภัยของข้อมูล กรุณาติดต่อเจ้าหน้าที่ DPO (Data Protection Officer) ของการบินไทยทางอีเมล privacy@thaiairways.com หรือ หากท่านพำนักอยู่ที่ประเทศกลุ่มสมาชิกสหภาพยุโรป สามารถติดต่อตัวแทนของการบินไทยที่ EU.Representative@thaiairways.com รวมถึงหากท่านมีความประสงค์ในการสอบถามข้อมูลสมาชิก รอยัล ออร์คิด พลัส เพิ่มเติม กรุณาติดต่อฝ่ายบริการสมาชิกรอยัล ออร์คิด พลัส คลิกที่นี่

กระบวนการในการจัดการการละเมิดข้อมูล

- Inspect - ตรวจสอบคำร้องจากผู้แจ้ง เช่นเจ้าของ หรือผู้ประมวลผล พร้อมพยานหลักฐานที่เกี่ยวข้อง เช่น ข้อความภาพบันทึก หรือสำเนาบันทึกหน้าจอที่อ้างว่าเป็นเหตุละเมิด
- Identity Authentication – พิสูจน์ยืนยันตัวตนเจ้าของข้อมูลโดยขอพยานหลักฐานเพิ่มเติม
- Initial Investigate-ไต่สวนข้อเท็จจริงเบื้องต้น วิเคราะห์จนทราบว่าเป็นการละเมิดที่เข้าข่ายต้องรายงาน และวิเคราะห์ผลกระทบต่อเจ้าของข้อมูล
- Report - ดำเนินการรายงาน ต่อหน่วยงานกำกับดูแล ภายใน 72 ชั่วโมง นับตั้งแต่ได้รับทราบชัดแจ้งว่าเป็นการละเมิดที่แท้จริง /รับคำแนะนำจากหน่วยงานกำกับดูแล
- Inform - แจ้งเจ้าของข้อมูล ในกรณีที่อาจมีผลกระทบ
- Remedy- พร้อมด้วยมาตรการในการเยียวยา

กระบวนการในการจัดการการละเมิดข้อมูล

- ระหว่าง ผู้ควบคุม — ผู้ควบคุม

  จะต้องตกลงกันว่า จะดำเนินการอย่างไรในกรณีที่มีการละเมิด

- ระหว่าง ผู้ควบคุม - ผู้ประมวลผล

  หน้าที่เป็นไปตามสัญญาการประมวลผลข้อมูลที่ผู้ประมวลผล จะต้องแจ้งการละเมิดให้ผู้ควบคุม ทราบ เพื่อ ผู้ควบคุมแจ้งและประสานการละเมิด(การรายงานแทน สามารถกระทำได้โดย เป็นไปตามสัญญา)

- หากเป็นการละเมิดชนิดเดียวกันแจ้งพร้อมกันได้ หากเป็นการละเมิดที่ต่างกัน อาจต้องแจ้งแยกกัน
- การละเมิดที่ไม่ก่อให้เกิดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล ไม่จำเป็นต้องรายงาน

ข้อมูลสำคัญที่ต้องรายงานหน่วยงานกำกับ (DPA)

- ลักษณะของการละเมิด จำนวน และปริมาณของข้อมูลและเจ้าของข้อมูล
- ข้อมูลการติดต่อ DPO หรือผู้ที่สามารถให้ข้อมูลเพิ่มเติม
- แนวโน้มผลกระทบของการละเมิด
- มาตรการที่ได้ดำเนินการหรือจะดำเนินการเพื่อลดผลกระทบของการละเมิด
- การรายงานสามารถกระทำเป็นขั้น ๆ ได้ เพื่อขอรับคำแนะนำและแก้ไขคำร้องในเวลาต่อมา
- หากไม่สามารถรายงานภายใน 72 ชม. จะต้องแจ้งเหตุผลของการชักช้า

การแจ้งเจ้าของข้อมูล (Data Subject)

- กรณีที่มีผลกระทบต่อสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล
- ต้องกระทำโดยไม่ชักช้า
- ข้อมูลที่ต้องแจ้ง
  - ลักษณะของการละเมิด
  - ข้อมูลการติดต่อ DPO หรือผู้ที่สามารถให้ข้อมูลเพิ่มเติม
  - แนวโน้มผลกระทบของการละเมิด
  - มาตรการที่ได้ดำเนินการหรือจะดำเนินการเพื่อลดผลกระทบของการละเมิด
- หากไม่สามารถดำเนินการได้ อาจกระทำในลักษณะของการแจ้งผ่านสื่อสาธารณะ (social media, website)
- จดบันทึกเหตุการณ์การละเมิดไว้เป็นหลักฐาน
- DPO ให้คำแนะนำในการปกป้องคุ้มครองข้อมูลและเป็นผู้ประสานงานกับหน่วยกำกับดูแล (DPA)

การบินไทย ห่วงใยในลูกค้า ช่วยกันรักษา ปกป้องข้อมูลส่วนบุคคล

Best Practice
PDPA Award 2020

THAI
Smooth as silk