



# PDPA CYBER SECURITY



นพ.ศิลา จิรวิกรานต์กุล



# PDPA



# 9 STEP PDPA IN ACTION



# 9 STEP

01

**DATA PROTECTION OFFICER(DPO)**

04

**DATA PROCESSING AGREEMENT(DPA)**

02

**PRIVACY POLICY**

05

**จดหมายแจ้งการละเมิด**

03

**PRIVACY NOTICER**

06

**บันทึกการประมวลผล  
ข้อมูลส่วนบุคคล(ROPA)**

07

**COOKIES CONSENT**

08

**การกำลังรีช่วงเจ้าง่วง  
ข้อมูล**

09

**CONSENT MANAGEMENT**



# PERSONAL DATA PROTECTION ACT

คุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคล เช่น การควบคุมไม่ให้องค์กรนำข้อมูลไปใช้โดยไม่ได้รับความยินยอม



## DATA PROTECTION OFFICER(DPO)

แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีหน้าที่เป็น “ผู้รับผิดชอบ” ให้แน่ใจว่าการประมวลผลข้อมูลขององค์กร ดำเนินการอย่างถูกต้อง



## PRIVACY POLICY

นโยบายการคุ้มครองข้อมูลส่วนบุคคลกำหนดข้อตกลง หรือคำแฉล狞การเกี่ยวกับแนวทางการจัดเก็บ รวบรวม ใช้ หรือเผยแพร่องานข้อมูลส่วนบุคคล กิจกรรมภายในองค์กร หรือหน่วยงานภายนอกที่เกี่ยวข้อง



## PRIVACY NOTICER

การสร้างประกาศชี้แจงการใช้ ข้อมูลส่วนบุคคล คำประกาศถึงเจ้าของข้อมูล ที่องค์กรจะมีการดำเนินการจัดเก็บประมวลผล รักษา และแจ้ง กำหนดการกำลังข้อมูล ส่วนบุคคล



# PERSONAL DATA PROTECTION ACT

คุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคล เช่น การควบคุมไม่ให้องค์กรนำข้อมูลไปใช้โดยไม่ได้รับความยินยอม



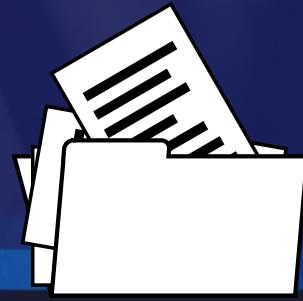
## DATA PROCESSING AGREEMENT(DPA)

สัญญาการกำหนดขอบเขต  
และวัตถุประสงค์ ของข้อตกลง  
การประมวลผลข้อมูลส่วน  
บุคคล



## จดหมายแจ้งการละเมิด

เป็นแบบฟอร์มที่องค์กรต้องเตรียมไว้ในกรณีมีการละเมิด  
ข้อมูลเกิดขึ้น



## บันทึกการประมวลผล ข้อมูลส่วนบุคคล(ROPA)

การจดบันทึกที่บอกร่างแผนก  
ให้ในองค์กร ทำอะไรบ้าง โดย  
มีจุดประสงค์หลักคือ หากการ  
ละเมิดข้อมูลส่วนบุคคลนั้นเกิด  
ขึ้น องค์กรสามารถตรวจสอบ  
กระบวนการได้ และจัดการได้  
อย่างรวดเร็ว



# PERSONAL DATA PROTECTION ACT

คุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคล เช่น การควบคุมไม่ให้องค์กรนำข้อมูลไปใช้โดยไม่ได้รับความยินยอม



## COOKIES CONSENT

ไฟล์ข้อความขอความยินยอมบนเว็บไซต์ เพื่อให้องค์กรสามารถประมวลผลข้อมูลส่วนบุคคลของผู้มา\_rับบริการได้อย่างถูกต้องและสอดคล้องกับ PDPA



## การกำลังสิทธิ์ของเจ้าของข้อมูล

องค์กรจะต้องมีช่องทางที่ผู้มา\_rับบริการสามารถเข้าถึง หรือ ทราบสิทธิ์ของตัวเองได้ง่าย



## CONSENT MANAGEMENT

การที่องค์กร หน่วยงานให้ผู้มา\_rับบริการ ตัดสินใจด้วยตัวเองในการอนุญาตการเก็บข้อมูลต่างๆ โดยไม่ผ่านเก็บข้อมูล หากผู้มา\_rับบริการไม่ยินยอม



# แนวทางการป้องกันการโจนตีข้อมูล ของหน่วยงาน

สำนักงานสาธารณสุข  
จังหวัดบุรีรัมย์



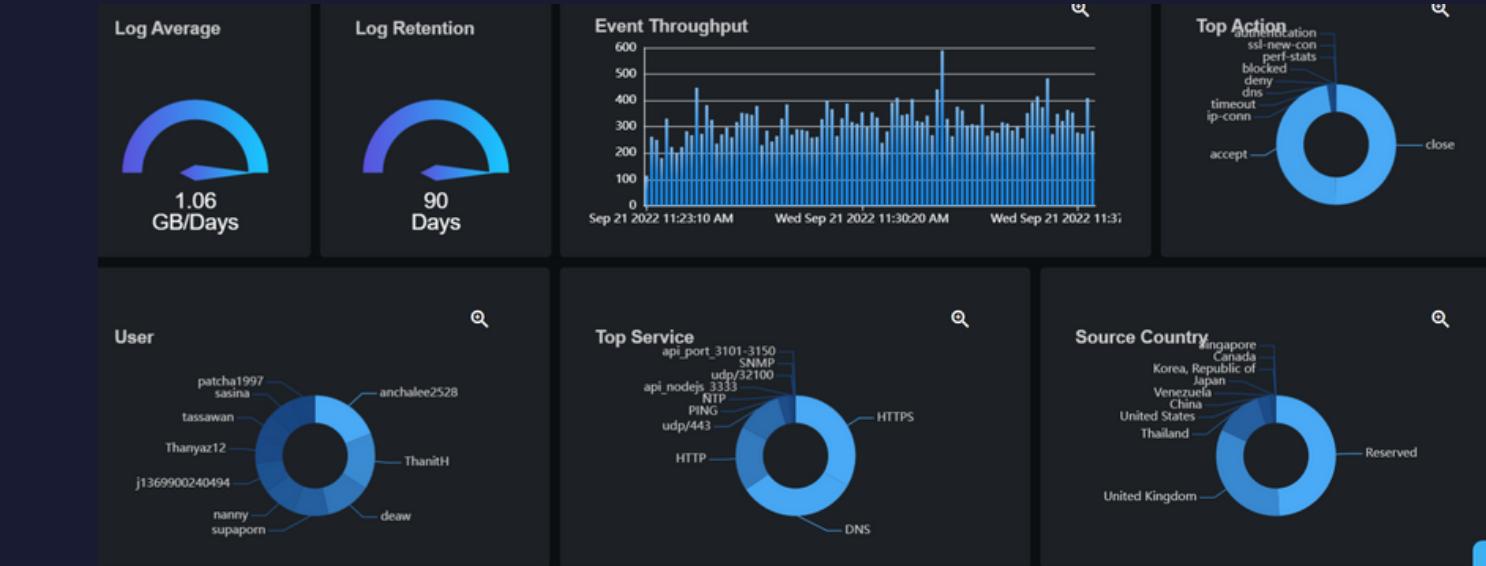
## NEXT GENERATION FIREWALL:ROUTER:SERVER

- 1.ใช้อุปกรณ์ NEXTGENERATION FIREWALL ที่มีลิสต์ไว้ใช้งานในทุกเครือข่าย โดยเปิดใช้งานกรองระดับสูงในทุกฟังก์ชัน ได้แก่ ANTIVIRUS, WEB FILTER, DNS FILTER, APPLICATION CONTROL, INTRUSTION PREVENTION, FILE FILTER, EMAIL FILTER, WEB APPLICATION FIREWALL, SSL/SSH INSPECTER, APPLICATION SIGNATURES, IPS SIGNATURES และ DOS POLICY โดยใช้อุปกรณ์ NEXTGENERATION FIREWALL แยกกันในเครือข่ายบริการเครื่องแม่ข่าย และเครือข่ายบริการภายใต้สำนักงาน
- 2.ปิดกั้นการเข้าถึงเครือข่ายจาก IP ADDRESS ภายนอกประเทศไทย โดยอนุญาตให้เข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายได้จาก IP ADDRESS ของไทยเท่านั้น
- 3.อนุญาตให้เข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายเฉพาะ SERVICE ที่จำเป็นในเครือข่ายนั้นๆ เท่านั้น เช่น อนุญาตเฉพาะ SERVICE HTTPS, MYSQL, FTP เป็นต้น ปิดกั้นการเข้าถึงบริการ MYSQL จากเครือข่ายภายนอก



## NETWORK

1. LOG ANALYZER เพื่อจัดเก็บ LOG และวิเคราะห์/รายงาน พฤติกรรมในเครือข่ายคอมพิวเตอร์
2. ติดตั้ง SSL CERTIFICATE (HTTPS://) ในทุกบริการเว็บไซต์ เพื่อความปลอดภัยและน่าเชื่อถือ ใช้บริการ SSL ของ CLOUDFLARE
3. จดทะเบียนภายใต้ชื่อ \*.MOPH.GO.TH ซึ่งศูนย์เทคโนโลยีสารสนเทศ จะเป็นผู้ดูแลความปลอดภัยในเบื้องต้น ให้แก่หน่วยงานที่ใช้เครือข่าย INTRANET
4. สำรองข้อมูล DATA และ APPLICATION ไปยังส่วนภายนอก ( ผ่านทาง CLIENT ภายใน ไปยัง EXTERNAL HDD/SSD ) ทุกสัปดาห์
5. การเข้าถึงข้อมูล MYSQL ของผู้ดูแล/พัฒนาระบบ ให้เข้าถึงได้ทาง CLIENT ภายในสำนักงานเท่านั้น ภายนอกสำนักงาน ให้ใช้วิธีการรีโมทมายังเครื่อง CLIENT ภายในสำนักงาน หรือใช้ VPN





## SOFTWARE

1. CLIENT ทุกเครื่องภายในสำนักงาน มีการติดตั้งโปรแกรมสแกนไวรัสแบบ CENTRALIZED ANTIVIRUS MANAGEMENT ที่มีการต่อสายลิงค์ทรีรายปี ซึ่งระบบ CENTRALIZED ANTIVIRUS MANAGEMENT สามารถจัดการ/ตรวจสอบ/รายงาน การป้องกันไวรัสของเครื่อง CLIENT ได้ทั้งหมด จึงตัดปัญหาการที่ผู้ดูแลระบบต้องไปดูหรือจัดการโดยตรงที่เครื่อง CLIENT
2. ปรับปรุงระบบ OS ของเครื่อง CLIENT ภายในสำนักงานที่ต่ำกว่า WINDOWS10 ซึ่งไม่มีการสนับสนุนด้านความปลอดภัยแล้ว ให้เป็น WINDOWS10 หรือ WINDOWS11



## GOVERNANCE

1. วอกประการศหน่วยงาน รูปแบบการใช้เว็บไซต์ในสำนักงาน การจำกัดการเข้าถึงเว็บไซต์ที่ไม่เหมาะสม การติดตั้งโปรแกรมด้วยตัวเอง การเชื่อมต่อกับอุปกรณ์ภายนอกที่ไม่ได้รับอนุญาต
2. แต่งตั้งเจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ ( CIRT: CYBER INCIDENT RESPONSE TEAM ) เพื่อประสานงานกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (HEALTH CERT)
3. แต่งตั้งทีมถูข้อมูลฉุกเฉินระดับจังหวัด ประกอบด้วยเจ้าหน้าที่ด้านไอทีของทุกหน่วยงาน เพื่อให้ความช่วยเหลือฉุกเฉินแก่หน่วยงานเครือข่าย ในกรณีข้อมูลสูญหาย/ถูกโจมตี ใช้งานไม่ได้ โดยให้ความเหลือทิ้งในด้านบุคลากร ทรัพยากรต่างๆ ให้สามารถถูข้อมูลหรือเรียกสำรองกลับมาใช้งานได้อย่างรวดเร็ว

# R9 IT TEAM



# THANK YOU

