

คำนำ

คนส่วนใหญ่มีระบบคอมพิวเตอร์ใช้ส่วนตัวกันเกือบทุกคน หรือจะพูดว่ามนุษย์ทุกคนในยุคนี้แทบไม่มีใครไม่รู้จักคอมพิวเตอร์ หรือ ระบบคอมพิวเตอร์ ซึ่งในการใช้ระบบคอมพิวเตอร์เพื่อการสื่อสารจะทำให้เกิดข้อมูลคอมพิวเตอร์ และข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งได้แก่ ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่าย ซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ เป็นต้น ข้อมูลดังกล่าวมีประโยชน์ในทางสืบสวนสอบสวนเพื่อทราบตัวตนของผู้ใช้ระบบคอมพิวเตอร์และอาจขยายผลไปถึงการทราบตัวตนผู้กระทำความผิดได้ ข้อมูลดังกล่าวจะจัดเก็บไว้โดยผู้ให้บริการ ซึ่งพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม สามารถเรียกให้ผู้บริการส่งมอบให้ได้เพื่อประโยชน์ในทางสืบสวนสอบสวน โดยกองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ (ปท.) ได้มีการให้บริการเรียกข้อมูลจราจรทางคอมพิวเตอร์ให้แก่พนักงานสอบสวนทั่วราชอาณาจักร เป็นงานที่เข้ามาเป็นจำนวนมากเนื่องจากคดีที่ใช้ระบบคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดมีจำนวนมากขึ้นทุกปีนั่นเอง กลุ่มงาน กสป. เห็นสมควรสรุปขั้นตอนการดำเนินการในกระบวนการดังกล่าวไว้เป็นคู่มือเพื่อประโยชน์ในการทำความเข้าใจงาน กระบวนการและ การนำไปใช้ปฏิบัติ เรียกว่า คู่มือ งานสนับสนุนการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์

กลุ่ม.กสป.

1 กันยายน 2563

สาระสำคัญของงานสนับสนุนการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์

ผู้ปฏิบัติงานต้องมีองค์ความรู้พื้นฐานในการปฏิบัติงานดังกล่าว ดังนี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

(ได้แก่ คอมพิวเตอร์ที่เชื่อมต่อกันหรือไม่ก็ตาม โทรศัพท์เคลื่อนที่ เป็นต้น)

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

(ได้แก่ ไฟล์ข้อความ ไฟล์ภาพ ไฟล์เสียง โปรแกรมคอมพิวเตอร์ เป็นต้น)

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น (ได้แก่ ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่าย ซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย ข้อมูลเกี่ยวกับวันและเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ เป็นต้น)

“ผู้ให้บริการ” หมายความว่า

(1) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

****ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มา ให้แก่บุคคลใด เว้นแต่เพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือเป็นการกระทำความผิดตามคำสั่งหรือที่ได้รับอนุญาตจากศาล**

****พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ**

****ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา 18 และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ**

**ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญา หรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มีได้เกิดขึ้นจากการจงใจมีค้ำมั่นสัญญา ชูเชิญ หลอกลวง หรือโดยมิชอบประการอื่น

**ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวัน แต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

**พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

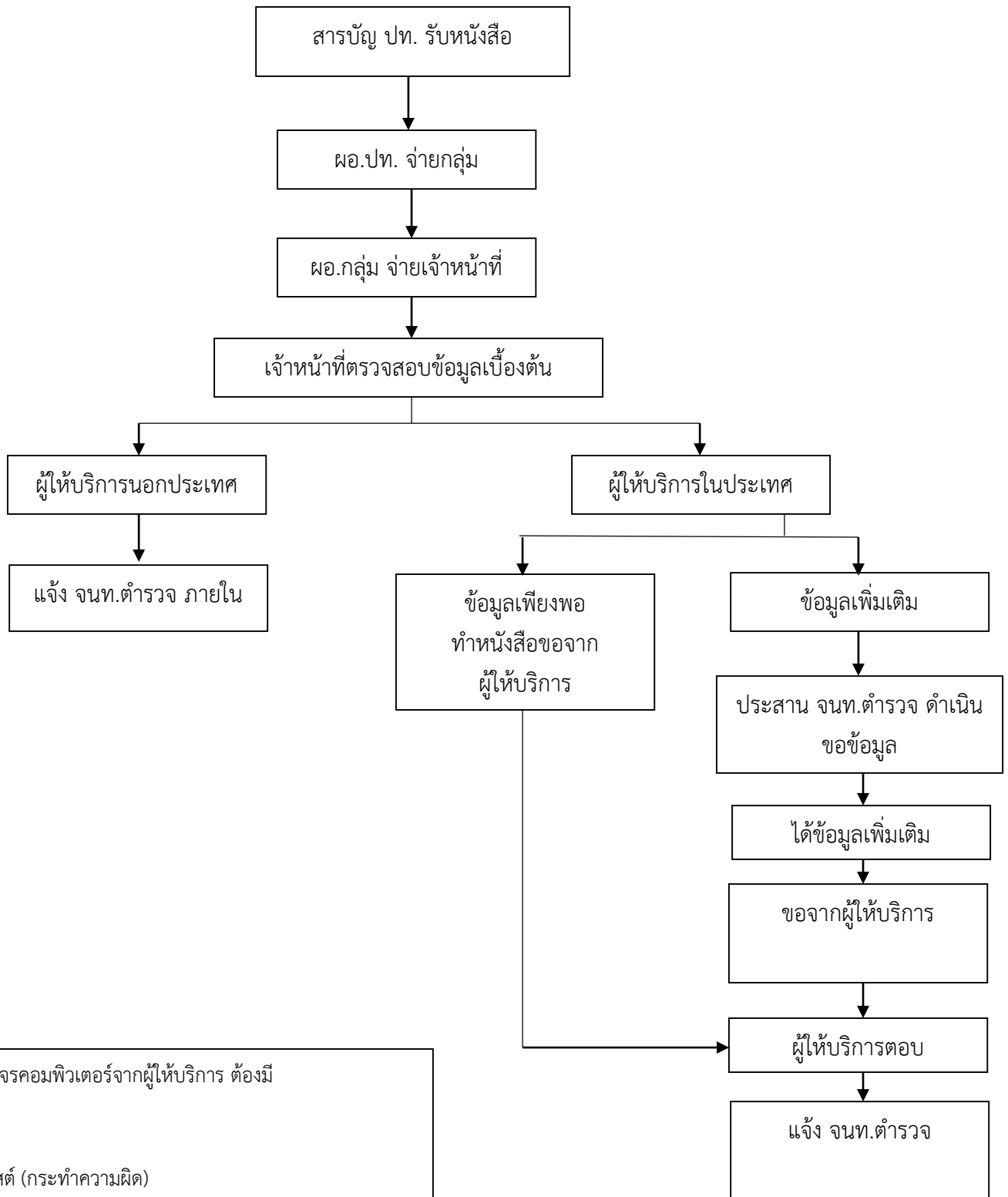
(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มา เพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามกฎหมาย หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

***IP Address (internet Protocal Address) คือ หมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่ายที่ใช้โปรโตคอลแบบ TCP/IP สามารถบอกได้ว่าเครื่องคอมพิวเตอร์ตั้งอยู่ที่ไหน ซึ่งสามารถระบุได้ผ่าน IP address และแน่นอนแต่ละ IP จะไม่ซ้ำกัน เหมือนเลขที่บ้านที่ไม่ซ้ำกัน เพราะถ้าซ้ำการส่งข้อมูลผ่านเครือข่ายก็อาจจะงงได้ว่าต้องส่งข้อมูลไปที่ไหนกันแน่ ซึ่ง IP address จะประกอบไปด้วยตัวเลข 4 ชุด โดยในปัจจุบันมาตรฐานของ IP address คือ IPv4 และ IPv6 โดย IPv4 จะเป็นเลข 32 บิต และ IPv6 เป็นเลข 128 บิต

งานสนับสนุนการตรวจสอบข้อมูลจราจรคอมพิวเตอร์ของเจ้าหน้าที่ตำรวจ



การขอข้อมูลจราจรคอมพิวเตอร์จากผู้ให้บริการ ต้องมี

1. IP Address
2. วัน เวลา ที่โพสต์ (กระทำความผิด)
3. ชื่อเว็บไซต์ที่ใช้ในการกระทำความผิด

หมายเหตุ ผู้ให้บริการต้องจัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ ๙๐ วัน