

ตารางเปรียบเทียบการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามพ.ร.บ.ว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ กับระบบ Softnix Logger มาตรฐานจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

Softnix Logger เป็นระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามมาตรฐาน มคอ.4003.1-2560 ซึ่งได้รับการรับรองจากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) เพื่อให้วิธีการรับข้อมูลจราจรทางคอมพิวเตอร์เป็นไปโดยชอบตามกฎหมายและถูกต้อง

ตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยอาศัยมาตรา ๔ วรรคหนึ่ง แห่งพ.ร.บ.ว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔

ประกาศฯนี้ ผู้ให้บริการประเภท ข้อ ๕(๑) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ตหรือให้สามารถติดต่อถึงกัน โดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามของบุคคลอื่น หรือเพื่อประโยชน์ของบุคคลอื่น มีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

ประเภทของผู้ให้บริการที่กำหนดตามประกาศ :

ผู้ให้บริการ ข้อ๕(๑)	ตัวอย่างของผู้ให้บริการตามกฎหมายกำหนด
ประเภท ข.  ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)	<ol style="list-style-type: none"> <li>1. ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ทั้งมีสายและไร้สาย</li> <li>2. ผู้ประกอบการซึ่งให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพัก ห้องเช่า โรงแรม หรือร้านอาหารและเครื่องดื่ม ในแต่ละกลุ่มอย่างใดอย่างหนึ่ง</li> <li>3. ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการ บริษัทหรือ สถาบันการศึกษา</li> </ol>

ตามประกาศนี้ ข้อ๗(๒) ผู้ให้บริการตามข้อ๕(๑) ข. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามที่กำหนด ตามประเภทชนิดและหน้าที่การให้บริการ ดังนี้

ประเภท	รายการที่กฎหมายกำหนดให้จัดเก็บ	ระบบ Softnix Logger การจัดเก็บตามข้อกำหนด
ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย	1. ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่ายซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย (Access Logs Specific to Authentication and Authorization Servers) เช่น TACACS (Terminal Access Controller Access-Control System) หรือ RADIUS (Remote Authentication Dial-in user Service) หรือ DIAMETER (Used to Control Access to IP Routers or Network Access Servers) 2. ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server) 3. ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (User ID) 4. ข้อมูลหมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดให้โดยระบบผู้ให้บริการ (Assigned IP Address) 5. ข้อมูลที่บ่งบอกถึงหมายเลขสายที่เรียกเข้ามา (Calling Line Identification)	รองรับการจัดเก็บ
ข. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-Mail Server)	1. ข้อมูล Log ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการไปรษณีย์อิเล็กทรอนิกส์ (Simple Mail Transfer Protocol: SMTP Log) ซึ่งได้แก่: - ข้อมูลหมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID) - ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender Email Address) - ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver	รองรับการจัดเก็บ

ประเภท	รายการที่กฎหมายกำหนดให้จัดเก็บ	ระบบ Softnix Logger การจัดเก็บตามข้อกำหนด
	<p>Email Address)</p> <p>- ข้อมูลที่บ่งบองถึงสถานะในการตรวจสอบ (Status Indicator) ซึ่งได้แก่</p> <ul style="list-style-type: none"> <li>- จดหมายอิเล็กทรอนิกส์ที่ส่งสำเร็จ</li> <li>- จดหมายอิเล็กทรอนิกส์ที่ส่งคืน - จดหมายอิเล็กทรอนิกส์ที่มีการส่งล่าช้า เป็นต้น</li> </ul> <p>2. ข้อมูลหมายเลขชุดของอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้ให้บริการที่เชื่อมต่ออยู่ขณะเข้ามาใช้บริการ (IP Address of Client Connected to Server)</p> <p>3. ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client Connected to Server)</p> <p>4. ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ ที่ถูกเชื่อมต่ออยู่ในขณะนั้น (IP Address of Sending Computer)</p> <p>5. ชื่อผู้ใช้งาน (User ID) ถ้ามี</p> <p>6. ข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือการเข้าถึงเพื่อเรียกข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิก โดยยังคงจัดเก็บข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ที่ตั้งไปนั้น ไว้ที่เครื่องให้บริการ [POP3 (Post Office Protocol version3) Log หรือ IMAP4 (Internet Message Access Protocol version4) Log]</p>	<p>รองรับการจัดเก็บ</p>

ประเภท	รายการที่กฎหมายกำหนดให้จัดเก็บ	ระบบ Softnix Logger การจัดเก็บตามข้อกำหนด
ค. ข้อมูลอินเทอร์เน็ต จากการโอนเพิ่มข้อมูล บนเครื่องให้บริการโอน เพิ่มข้อมูล	<ol style="list-style-type: none"> <li>ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่อง ให้บริการโอนเพิ่มข้อมูล</li> <li>ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามา ให้บริการและเครื่องให้บริการ (Date and Time of Connection of Client Connected to Server)</li> <li>ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่อง คอมพิวเตอร์ผู้ใช้ที่เชื่อมต่อ (IP Source Address)</li> <li>ชื่อผู้ใช้งาน (User ID) ถ้ามี</li> <li>ข้อมูลตำแหน่ง (Path) และ ชื่อไฟล์ที่อยู่บน เครื่องให้บริการโอนถ่ายข้อมูลที่มีการ ส่งขึ้นมา บันทึก หรือให้ดึงข้อมูลออกไป (Path and Filename of Data Object Upload or Download)</li> </ol>	รองรับการจัดเก็บ
ง. ข้อมูลอินเทอร์เน็ต บนเครื่องผู้ให้บริการ เว็บ	<ol style="list-style-type: none"> <li>ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ ให้บริการเว็บ</li> <li>ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามา ให้บริการและเครื่องให้บริการ</li> <li>ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่อง คอมพิวเตอร์ผู้ใช้ที่เชื่อมต่ออยู่ในขณะนั้น</li> <li>ข้อมูลคำสั่งการใช้งานระบบ</li> <li>ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URL: Uniform Resource Identifier) เช่น ตำแหน่งของเว็บเพจ</li> </ol>	รองรับการจัดเก็บ
จ. ชนิดของข้อมูลบน เครือข่ายคอมพิวเตอร์ ขนาดใหญ่ (Usenet)	<ol style="list-style-type: none"> <li>ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครือข่าย [ NNTP (Network News Transfer Protocol) Log]</li> <li>ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามา ให้บริการและเครื่องให้บริการ (Date and Time of Connection of Client Connected to Server)</li> <li>ข้อมูลหมายเลข Port ในการใช้งาน (Protocol Process ID)</li> </ol>	รองรับการจัดเก็บ

ประเภท	รายการที่กฎหมายกำหนดให้จัดเก็บ	ระบบ Softnix Logger การจัดเก็บตามข้อกำหนด
	4. ข้อมูลชื่อเครื่องให้บริการ (Host name)	รองรับการจัดเก็บ
	5. ข้อมูลหมายเลขลำดับข้อความที่ได้ถูกส่งไปแล้ว (Posted Message ID)	
จ. ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ Instance Message (IM) เป็นต้น	ข้อมูล Log เช่น ข้อมูลเกี่ยวกับวัน เวลาการติดต่อของผู้ใช้บริการ (Date and Time of Connection of Client to Server) และ ข้อมูลชื่อเครื่องบนเครือข่าย และหมายเลขเครื่องของผู้ให้บริการที่เครื่องคอมพิวเตอร์เชื่อมต่ออยู่ในขณะนั้น (Hostname and IP Address) เป็นต้น	รองรับการจัดเก็บ

นอกจากนี้ประกาศฯ ยังมีข้อกำหนดการจัดเก็บข้อมูลจราจรที่ต้องปฏิบัติ ดังต่อไปนี้:

ประกาศฯ ข้อกำหนดกฎหมาย	ระบบ Softnix Logger การจัดเก็บตามข้อกำหนด
ข้อ ๘ (๑) (๒) (๓) จัดให้มีระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลการอนุญาตเข้าถึงชั้นข้อมูล	รองรับ มีระบบการเข้าใช้งานระบบ 2 ชั้น คือ user / password และรองรับการเข้าด้วยการใช้ OTP
ข้อ ๘ (๕) สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ ข้อมูลในระบบ	รองรับ มีระบบค้นหาข้อมูลจราจรทางคอมฯย้อนหลัง
ข้อ ๙ (๑) ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ใช้วิธีการที่มั่นคงปลอดภัย เก็บในสื่อ (Media) หรืออุปกรณ์คอมพิวเตอร์หรือระบบคอมพิวเตอร์ ที่สามารถรักษา ความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้ เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archiving หรือทำ Data Hashing เป็นต้น	รองรับ ได้รับการตรวจสอบประจำปีจากศูนย์ NECTEC และเป็นระบบ Centralized Log, มีระบบ Data Hashing เพื่อ Integrity, ระบบ Login เข้าใช้เพื่อ Identification และระบบ Archiving

ประกาศฯ ข้อกำหนดกฎหมาย	ระบบ Softnix Logger การจัดเก็บตามข้อกำหนด
<p>ข้อ ๑๑ เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องนำมาใช้ประโยชน์ได้จริง ต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) ให้ตรง กับอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้อง (Clock Synchronization)</p>	<p>รองรับ มีระบบตั้งนาฬิกา Time Server เพื่อ Clock Synchronization เชื่อมเวลามาตรฐานสากล กับอุปกรณ์ที่จัดเก็บข้อมูลจราจรคอมพิวเตอร์</p>
<p>ข้อ ๑๒ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ตามกำหนดระยะเวลา ดังต่อไปนี้</p> <p>(๑) กรณีทั่วไป ให้ผู้ให้บริการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์</p> <p>(๒) กรณีจำเป็นเมื่อมีเหตุอันควรเชื่อได้ว่าการกระทำความผิดตามพระราชบัญญัตินี้ฯ เช่น ความผิดเกี่ยวกับความมั่นคง ก่อการร้าย อาชญากรรมข้ามชาติ หรือความสงบเรียบร้อยของประชาชน ให้พนักงานเจ้าหน้าที่มีคำสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ใช้บริการ เป็นกรณีพิเศษเฉพาะราย ต่อไปอีกคราวละไม่เกินหกเดือนต่อเนื่องกัน แต่ต้องไม่เกินสองปี</p>	<p>รองรับ มีระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ พื้นฐาน 90 วัน และสามารถจัดเก็บได้ถึง 2 ปี ตามขนาดพื้นที่ความจุของ Hard Disk ที่รองรับ</p>

-----