No	หัวข้อหลักเกณฑ์	2550 2560	2564	ตัวอย่างอุปกรณ์ และประเภทของ Log
5(1) ประเภท ข. ผู้ให้บริการการเข้าถึงระบบเครือข่าย คอมพิวเตอร์ (Access Service Provider)				
1	ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย (แนบท้ายประกาศกระทรวงฯ ข ภาคผนวก ข. ข้อ2 (ก))	✓	✓	Active Directory, Domain Controller, Authentication Server, VPN, Proxy Server, Internet Gateway, DHCP,LDAP Server, อื่น ๆ ที่เกี่ยวข้องกับการเข้าถึงระบบ
2	ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers) (แนบท้ายประกาศกระทรวงฯ - ภาคผนวก ข. ข้อ 2 (ข))	✓	✓	Mail Server, Mail Gateway, SMTP Server
3	ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล (แนบท้ายประกาศกระทรวงฯ - ภาคผนวก ข. ข้อ 2 (ค))	✓	✓	Public FTP Server, Public File Sharing
4	ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ (แนบท้ายประกาศกระทรวงฯ - ภาคผนวก ข. ข้อ 2 (ง))	✓	✓	Public Web Access Log
5	ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (แนบท้ายประกาศกระทรวงฯ - ภาคผนวก ข. ข้อ 2 (จ))	✓	✓	Usenet Web Access Log
6	ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต (แนบท้ายประกาศกระทรวงฯ - ภาคผนวก ข. ข้อ 2 (ฉ))	✓	✓	Firewall Internet (Traffic) Instant Messaging Server
5(2) ประเภท ก. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์ (Content Service Provider)				
1	ข้อมูลรหัสประจำตัวผู้ใช้หรือข้อมูลที่สามารถระบุตัวผู้ใช้บริการได้ หรือเลขประจำตัว (User ID) ของผู้ขายสินค้าหรือบริการ หรือ เลขประจำตัวผู้ใช้บริการ (User ID) และที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้ใช้บริการ	✓	✓	Application Log - User ID, Email
2	บันทึกข้อมูลการเข้าใช้บริการ	✓	✓	Application Log - Date, Time, User ID
3	กรณีผู้ให้บริการเว็บบอร์ด (Web board) หรือผู้ให้บริการบล็อก (Blog)ให้เก็บข้อมูลของผู้ประกาศ (Post) ข้อมูล	✓	✓	Application Log - Post Date-Time, User ID อื่น ๆ

No	หัวข้อหลักเกณฑ์	2550 2560	2564	ตัวอย่างอุปกรณ์ และประเภทของ Log
5(2) ประเภท ค. ผู้ให้บริการดิจิทัล (Digital Service Provider) ที่ใช้เครือข่ายคอมพิวเตอร์ หรือระบบคอมพิวเตอร์เป็นส่วนหนึ่งของการให้บริการ				
1	ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่าย ซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย (Access Logs Specific to Authentication and Authorization Servers) เช่น - TACACS (Terminal Access Controller Access-Control System) - RADIUS (Remote Authentication Dial-In User Service) - DIAMETER (Used to Control Access to IP Routers or Network Access Servers)		✓	Application Log
2	ข้อมูลวัน และเวลาในการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)		✓	Application Log
3	ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (User ID)		✓	Application Log
4	ข้อมูลหมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดให้โดยระบบผู้ให้บริการ (Assigned IP Address)		✓	Application Log
5	ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา (Calling Line Identification)		✓	Application Log
6	ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ของผู้ใช้บริการที่เชื่อมต่ออยู่ขณะเข้ามาใช้บริการ (IP Address of Client Connected to Server)		✓	Application Log
7	ข้อมูลรหัสประจำตัวผู้ใช้หรือข้อมูลที่สามารถระบุตัวผู้ใช้บริการดิจิทัลได้ หรือเลขประจำตัวผู้ใช้บริการ (User ID) และที่อยู่จดหมายอิเล็กทรอนิกส์ หรือ บัญชีโซเชียลมีเดียของผู้ใช้บริการ		✓	Application Log
8	บันทึกข้อมูลการเข้าใช้บริการดิจิทัล		✓	Application Log

No	หัวข้อหลักเกณฑ์	2550 2560	2564	ตัวอย่างอุปกรณ์ และประเภทของ Log
มาตรฐานทั่วไปในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. และตามประกาศฉบับนี้ทั้งหมดต้องประกอบด้วย ก. ข้อมูลบันทึกเหตุการณ์การเข้าใช้งานในระบบคอมพิวเตอร์ (Event Logging) ซึ่งต้องมีมาตรการตรวจสอบกำกับดูแล (Control) ข้อมูลจราจรทางคอมพิวเตอร์ให้ระบบคอมพิวเตอร์สามารถให้ข้อมูลเก็บรักษาข้อมูล หรือตรวจสอบข้อมูลการใช้งานของผู้ใช้บริการ ข้อยกเว้นของระบบคอมพิวเตอร์ที่บันทึกข้อมูลคอมพิวเตอร์ไม่ได้ รายละเอียดเปอร์เซ็นต์ ความผิดพลาดของระบบคอมพิวเตอร์และข้อมูลภัยคุกคามทางไซเบอร์ของระบบคอมพิวเตอร์ ซึ่งมี รายละเอียดดังนี้				
1	ข้อมูลที่สามารถระบุตัวตนของผู้ใช้บริการ (ID of Users)		✓	User Name, User ID - (AD, PAM)
2	รายละเอียดของการใช้ข้อมูลของผู้ใช้บริการในระบบคอมพิวเตอร์ (Activities of the system)		✓	All User Activity - (Firewall, OS, App)
3	วัน เวลา และรายละเอียดเหตุการณ์สำคัญที่เกี่ยวข้องกับกิจกรรมของผู้ใช้งาน หรือผู้ใช้บริการ เช่น การล็อคอินเข้าออกระบบคอมพิวเตอร์ (Log-on and Log-off)		✓	Date, Time
4	ข้อมูลที่สามารถระบุหมายเลขของเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ (System ID) สถานที่ในการเข้าออกระบบคอมพิวเตอร์ (Location) และอุปกรณ์ที่ใช้เชื่อมต่อคอมพิวเตอร์ให้คอมพิวเตอร์สามารถเข้าถึงระบบคอมพิวเตอร์ได้ (Device recognition)		✓	IP/MAC Address, Device ID/Location - (EDR)
5	รายละเอียดบันทึกการเข้าถึงและการพยายามเข้าถึงระบบคอมพิวเตอร์ทั้งในส่วนที่เข้าถึงระบบคอมพิวเตอร์ได้ และส่วนที่ระบบคอมพิวเตอร์ปฏิเสธการเข้าถึง (Records of attempts to access the system successfully as well as rejected ones)		✓	Access All (Success, Failure) - (AD, OS)
6	บันทึกรายละเอียดข้อมูลคอมพิวเตอร์ที่มีการเข้าถึงแหล่งข้อมูล (Successful and unsuccessful data records and other attempts to access resources)		✓	Computer Name, OS Version - (EDR)
7	รายละเอียด ประเภทของแอพพลิเคชัน และการใช้งานในระบบคอมพิวเตอร์ (The application and use of systems utilities)		✓	Application Using - (EDR)
8	แฟ้มข้อมูล และประเภทของข้อมูลคอมพิวเตอร์ที่ถูกเข้าถึงในระบบคอมพิวเตอร์ (Accessed files and access kinds)		✓	File Server Access - (Object Access, FIM)
9	ตำแหน่งที่อยู่ของระบบเครือข่ายคอมพิวเตอร์ (Network Addresses) และโปรโตคอลหลักที่ใช้ (Protocols)		✓	Network Address, Protocols - (Firewall)
10	รายละเอียดมาตรการการป้องกันภัยคุกคามทางไซเบอร์ เช่น รายละเอียดการใช้โปรแกรมป้องกันไวรัสคอมพิวเตอร์ ระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ที่ทำให้ระบบทำงาน และถูกระงับการใช้งาน (protective mechanisms such as anti-virus and intrusion detection systems are activated and deactivated as required)		✓	Antivirus - (EPP)
11	รายละเอียดธุรกรรมที่ทำผ่านแอพพลิเคชันต่างๆ โดยผู้ใช้บริการ (Transaction records done in applications by users)		✓	Application/Transaction - (App Log, DAM)