(ร่าง) มาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

NECTEC STANDARD

มศอ. ๒๐ XX.๑ – ๒๕๕๑

ระบบเก็บรักษาข้อมูลจราจรคอมพิวเตอร์

เล่ม ๑ ข้อกำหนด

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

กระทรวงวิทยาศาสตร์และเทคโนโลยี

มาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และ
คอมพิวเตอร์แห่งชาติ

ระบบเก็บรักษาข้อมูลจราจรคอมพิวเตอร์

เล่ม ๑ ข้อกำหนด

มศอ. ๒ XX ๕ - ๒๕๕๒

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
กระทรวงวิทยาศาสตร์และเทคโนโลยี
๒๕๕๒

คณะกรรมการวิชาการ

ประธานกรรมการ

นายอาจิน จิรชีพพัฒนา สำนักส่งเสริมอุตสาหกรรมเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

กรรมการ

นายถนัด มานะพันธุ์นิยม สำนักงานคณะกรรมการคุ้มครองผู้บริโภค

พันตำรวจเอกกัลป์ ทังสุพานิช ศูนย์ตรวจสอบและวิเคราะห์การกระทำาความผิดทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ

นายธงชัย แสงศิริ สำนักกำกับการใช้เทคโนโลยีสารสนเทศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

นายณัฐ สกลชัย สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม

นายวิรัตน์ พึ่งสาระ สำนักงานส่งเสริมอุตสาหกรรมซอฟต์แวร์แห่งชาติ (องค์การมหาชน)

นายสมญา พัฒนวรพันธุ์ สำนักข่าวกรองแห่งชาติ สำานักนายกรัฐมนตรี

นายขจร สินอภิรมย์สราญ บริษัท ไอที คอมพาเนี่ยน จำกัด

นายสว่างพงศ์ หมวดเพชร บริษัท ไอที เบเคอรี่ จำกัด สมาคมสมาพันธ์ซอฟต์แวร์โอเพนซอร์ส

นายราเมศวร์ ศิลปพรหม สมาคมสมาพันธ์เทคโนโลยสารสนเทศแห่งประเทศไทย

นายกมล เอื้อชินกุล ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นายบรรจง หะรังษี บริษัท ที-เน็ต จำกัด

กรรมการและเลขานุการ

นายกริช นาสิงห์ขันธุ์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ผู้ช่วยเลขานุการ

น.ส.พลอยรวี เกริกพันธ์กุล กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

นายอรรถนิติ อัศวินนิมิตกุล ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

รายชื่อคณะทำงาน

ที่ปรึกษา

นายพันธ์ศักดิ์ ศิริรัชตพงษ์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นายกว้าน สีตะธนี ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นายโกเมน พิบูลโรจน์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นายบรรจง หะรังษี บริษัท ที-เน็ต จำกัด

คณะทำงานด้านเทคนิค

นายอรรถนิติ อัศวินนิมิตกุล ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นายกริช นาสิงห์ขันธุ์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นายกำธร ไกรรักษ์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นายพุธ นาฑีสุวรรณ บริษัทที-เน็ต จำกัด

นายชวลิต ทินกรสูติบุตร บริษัทที-เน็ต จำกัด

นายปิยวัฒน์ เลื่อนสุคันธ์ บริษัทที-เน็ต จำกัด

นายไตรรัตน์ พุทธรักษา บริษัทที-เน็ต จำกัด

นายศิวพงษ์ นิยมพานิช บริษัทที-เน็ต จำกัด

มาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ระบบเก็บรักษาข้อมูลจราจรคอมพิวเตอร์

เล่ม ๑ ข้อกำหนด

1. ขอบข่าย

มาตรฐานระบบเก็บ รักษาข้อมูลจราจรคอมพิวเตอร์นี้ ครอบคลุมเฉพาะการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการการเข้าสู่ อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ประเภท ๕ (๑) ข ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ และ ประเภท ๕ (๑) ค ผู้ให้บริการเช่าระบบคอมพิวเตอร์หรือให้เช่าบริการโปรแกรมประยุกต์ต่างๆ สำหรับ ประเภท ๕ (๑) ง ผู้ให้บริการร้านอินเตอร์เน็ต นั้นหากมีการใช้งานระบบเก็บรักษาข้อมูลจรารจคอมพิวเตอร์สำหรับผู้ให้บริการ ประเภท ๕ (๑) ข และ ประเภท ๕ (๑) ค ให้ถือว่ามาตรฐานนี้ครอบคลุมเช่นเดียวกัน โดยมาตรฐานนี้ไม่ครอบคลุมถึง ผู้ให้บริการการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ประเภท ๕ (๑) ก ตามภาคผนวก ข ของประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ ซึ่งใช้อำนาจนาจตามมาตรา ๒๖ ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

2. บทนิยาม

1. ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดย อัตโนมัติ

2. ข้อมูลจราจรทาง คอมพิวเตอร์ หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

3. ผู้ให้บริการ หมายความว่า

- **1.** ผู้ให้บริการแก่ บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือเพื่อประโยชน์ของบุคคลอื่น
- **2.** ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

4. ผู้ให้บริการการเข้าสู่อินเทอร์เน็ตหรือผู้ให้บริการให้สามารถติดต่อถึงกัน โดยผ่านระบบคอมพิวเตอร์ ประเภท ๕ (๑) ข ได้แก่ ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ตัวอย่างของผู้ให้บริการเช่น

- **1.** ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ทั้งมีสายและไร้สาย
- **2.** ผู้ประกอบการซึ่ง ให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพัก ห้องเช่า โรงแรม หรือร้านอาหารและเครื่องดื่ม ในแต่ละกลุ่มอย่างใดอย่างหนึ่ง
- **3.** ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กรเช่น หน่วยงานราชการ บริษัทหรือสถาบันการศึกษา

5.ผู้ให้บริการการเข้าสู่อินเทอร์เน็ตหรือผู้ให้บริการให้สามารถติดต่อถึงกัน โดยผ่านระบบคอมพิวเตอร์ ประเภท ๕ (๑) ค ได้แก่ ผู้ให้บริการเช่าระบบคอมพิวเตอร์หรือให้เช่าบริการโปรแกรมประยุกต์ต่างๆ (Hosting Service Provider)
ตัวอย่างผู้ให้บริการเช่น

1.ผู้ให้บริการเช่าระบบคอมพิวเตอร์ (Web Hosting), การให้บริการเช่า Web Server

2.ผู้ให้บริการแลกเปลี่ยนแฟ้มข้อมูล (File Server หรือ File Sharing)

3.ผู้ให้บริการเข้าถึงจดหมายอิเล็กทรอนิกส์ (Mail Server Service Provider)

4.ผู้ให้บริการศูนย์รับฝากข้อมูลทางอินเทอร์เน็ต (Internet Data Center)

6.การพิสูจน์ตัวตน หมายความว่า ขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

1.การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใครเช่น ชื่อผู้ใช้ (username)

2.การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

7.การล็อกอิน หมายความว่า การเข้าใช้งานระบบคอมพิวเตอร์ โดยต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

8.ข้อมูลการล็อกอิน หมายความว่า ข้อมูลที่ใช้ในการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบคอมพิวเตอร์

9.การตรวจสอบความสมบูรณ์และ ความถูกต้องของข้อมูลโดยวิธี hash หมายถึง กรรมวิธีตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูล โดยอาศัยหลักการของการเข้ารหัสลับ (Crytography) ที่ใช้ hash function ที่ถูกออกแบบมาโดยเฉพาะเพื่อใช้ในด้านการรักษาความปลอดภัยของสารสนเทศ เช่น SHA-1,MD5 หรือ CRC32 ซึ่งคุณสมบัติของ hash function เหล่านี้คือ เมื่อนำข้อมูลนำเข้า (input data) มาคำนวณค่ากับ hash function จะได้ผลลัพท์เป็นค่าเฉพาะตัวค่าหนึ่งหรือที่เรียกว่าค่า hash ซึ่งเป็นค่าที่แตกต่างในทุกๆข้อมูลนำเข้าและค่าเฉพาะตัวนี้จะไม่มีโอกาสซ้ำ กันได้ จากคุณสมบัติดังกล่าว hash function จึงถูกนำมาใช้ในการตรวจสอบความถูกต้องของข้อมูลได้ โดยการคำนวณค่า hash แล้วนำค่ามาเก็บไว้ก่อน ที่จะนำข้อมูลไปใช้งานและเมื่อต้องการการตรวจสอบความถูกต้องให้นำข้อมูลนั้น กลับมาคำนวณค่า hash อีกครั้ง ถ้าพบว่าค่า hash มีค่าเดิมจะถือว่าข้อมูลมีความถูกต้องและสมบรูณ์ แต่หากค่า hash มีค่าเปลี่ยนไปไม่เหมือนเดิม แสดงว่าเกิดการเปลี่ยนแปลงของข้อมูลเกิดขึ้น

10.คำย่อในมาตรฐานฉบับนี้

1.ระบบฯ หมายถึง ระบบเก็บรักษาข้อมูลจราจรคอมพิวเตอร์

3. ข้อมูลอ้างอิง

1. ประกาศราชกิจจานุเบกษา, “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”, วันที่ ๑๘ มิถุนายน ๒๕๕๐

2. ประกาศราชกิจจานุเบกษา, “ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐”, วันที่ ๒๓ สิงหาคม ๒๕๕๐

3. หน่วยปฏิบัติการ วิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ และคณะอนุกรรมการด้านความมั่นคง ภายใต้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ในคณะอนุกรรมการธุรกรรมทางอิเล็กทรอนิกส์, “มาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕) ประจำปี ๒๕๕๐”, ISBN: 978-974-229-584-4, พิมพ์ครั้งที่ ๑, ธันวาคม ๒๕๕๐

4. SN ISO/IEC 17799:2005, “Information technology – Security Technique – Code of practice for information security management (ISO/IEC 17799:2005)”, Second Edition, 2005-06-15

5. Chaiyakorn Apiwathanokul, “Computer Time Synchronization Scheme” , http://www.etcommission.go.th/documents/standard/time_sync_server_v1_0.pdf, 3 October 2007

6. ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย ภายใต้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, “แนวทางการจัดเก็บข้อมูลล็อกสำหรับองค์กรเพื่อให้สอดคล้องตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550” , http://www.thaicert.org/paper/auditing/LogImplementationandAuditingGuideline_r2.pdf , ๒๓ สิงหาคม ๒๕๕๐

7. อสมาภรณ์ ฉัตรัตติกรณ์ และ ชวลิต ทินกรสูติบุตร, “การเทียบเวลาด้วย Network Time Protocol ให้สอดคล้องกับ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550” http://www.thaicert.org/paper/basic/NTPandLAW.php, 27 กุมภาพันธ์ 2551
อสมาภรณ์ ฉัตรัตติกรณ์ และ ชวลิต ทินกรสูติบุตร, “คู่มือการใช้บริการ Time Server [ฉบับปรับปรุง]”, http://www.thaicert.org/paper/basic/manualTimeServer.php, 27 กุมภาพันธ์ 2551

8. W3C, "Extended Log File Format", http://www.w3.org/pub/WWW/TR/WD-logfile-960221.html, 19 May 2009

9. IETF Working Groups, "RFC1738 - Uniform Resource Locators (URL)", http://www.ietf.org/rfc/rfc1738.txt, December 1994

10. IETF Working Groups, "RFC1321 - The MD5 Message-Digest Algorithm", http://www.ietf.org/rfc/rfc1321.txt, April 1992

11. IETF Working Groups, "US Secure Hash Algorithm 1 (SHA1)", http://www.ietf.org/rfc/rfc3164.txt, September 2001

12. IETF Working Groups, "The BSD syslog Protocol", http://www.ietf.org/rfc/rfc3174.txt, August 2001

13. Federal Information Processing Standards (FIPS), "FIPS-180-1 SECURE HASH STANDARD", http://www.itl.nist.gov/fipspubs/fip180-1.htm, 1995 April 17

14. Wikipedia, "Cryptographic hash function", http://en.wikipedia.org/wiki/Cryptographic_hash_function, 19 May 2009

4. ข้อมูลจราจรคอมพิวเตอร์ที่ผู้ให้บริการประเภท ๕ (๑) ข และ ประเภท ๕ (๑) ค มีหน้าที่ต้องเก็บรักษา

ตาม ภาคผนวก ข ของประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ ซึ่งใช้อำนาจนาจตามมาตรา ๒๖ ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ได้กำหนดให้ผู้บริการประเภท ๕ (๑) ข และ ประเภท ๕ (๑) ค มีหน้าที่ต้องเก็บรักษาข้อมูลจราจรคอมพิวเตอร์รวม ๖ประเภท และกำหนดรายการข้อมูลที่ต้องจัดเก็บดังนี้

ประเภท ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย

รายการข้อมูลที่ต้องจัดเก็บ

1. ข้อมูลจราจรคอมพิวเตอร์ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่ายหรือ Access Logs

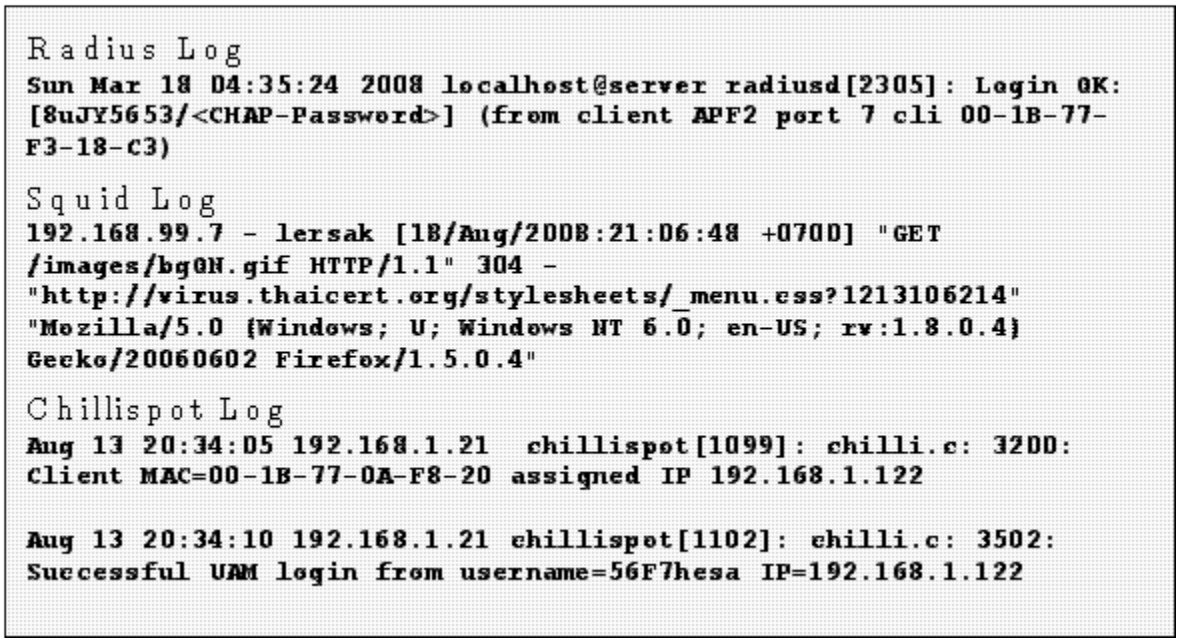
2. ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)

3. ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (User ID)

4. ข้อมูลหมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดโดยระบบผู้ให้บริการ (Assigned IP Address)

5. ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา (Calling Line Identification)

ตัวอย่างข้อมูลจราจร



Radius Log

```
Sun Mar 18 04:35:24 2008 localhost@server radiusd[2305]: Login OK:
[8uJY5653/<CHAP-Password>] (from client APF2 port 7 cli 00-1B-77-
F3-18-C3)
```

Squid Log

```
192.168.99.7 - lersak [18/Aug/2008:21:06:48 +0700] "GET
/images/bgON.gif HTTP/1.1" 304 -
"http://virus.thaicert.org/stylesheets/_menu.css?1213106214"
"Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.8.0.4)
Gecko/20060602 Firefox/1.5.0.4"
```

Chillispot Log

```
Aug 13 20:34:05 192.168.1.21  chillispot[1099]: chilli.c: 3200:
Client MAC=00-1B-77-0A-F8-20 assigned IP 192.168.1.122

Aug 13 20:34:10 192.168.1.21 chillispot[1102]: chilli.c: 3502:
Successful UAM login from username=56F7hesa IP=192.168.1.122
```

ประเภท ข. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)

รายการข้อมูลที่ต้องจัดเก็บ

1. ข้อมูล Log ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการไปรษณีย์อิเล็กทรอนิกส์ (SMTP) ซึ่งได้แก่
    - ข้อมูลหมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID)
    - ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender E-mail Address)
    - ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver E-mail Address)
    - ข้อมูลที่บอกถึงสถานะในการตรวจสอบ (Status Indicator) ซึ่งได้แก่ จดหมายอิเล็กทรอนิกส์ที่ส่งสำเร็จ จดหมายอิเล็กทรอนิกส์ที่ส่งคืน จดหมายอิเล็กทรอนิกส์ทีมีการส่งล่าช้า เป็นต้น
2. ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้ใช้บริการที่เชื่อมต่ออยู่ขณะเข้ามาใช้บริการ (IP Address of Client Connected to Server)
3. ข้อมูลวันและเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of Client Connected to server)
4. ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ที่ถูกเชื่อมต่ออยู่ในขณะนั้น (IP Address of Sending Computer)
5. ชื่อผู้ใช้งาน (User ID) (ถ้ามี)
6. ข้อมูลที่บันทึก การเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือเข้าถึงเพื่อเรียกข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิก โดยยังคงจัดเก็บข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ที่ดึง ไปนั้น ไว้ที่เครื่องให้บริการ หรือ POP3 Log หรือ IMAP4 Log

ตัวอย่างข้อมูลจราจร

```
Sendmail Log
Aug 24 05:18:14 admin@example.com sendmail[1090D]: m70MIE38D1090D:
from=<test@example.com>, size=690, class=0, nrcpts=1,
msgid=<200805242102.m70L24r5010202@example.com>, proto=ESMTP,
daemon=MTA, relay=mail.example.com [14.36.11.2]

Aug 24 05:18:14 admin@example.com sendmail[10202]: m70L24r5010202:
to=lersak@gmail.com, ctladdr=192.168.1.50 (0/0), delay=01:16:10,
xdelay=00:00:00, mailer=relay, pri=30451, relay=[mail.example.com]
[14.36.11.2], dsn=2.0.0, stat=Sent (m70MIE38D1090D Message accepted
for delivery)
```

ประเภท ค. ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล

รายการข้อมูลที่ต้องจัดเก็บ

1. ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องให้บริการโอนแฟ้มข้อมูล
2. ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
3. ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น (IP Source Address)
4. ข้อมลชื่อผู้ใช้งาน (User ID) (ถ้ามี)
5. ข้อมูลตำแหน่ง (Path) และชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการ ส่งขึ้นมาบันทึกหรือดึงให้ข้อมูลออกไป (Path and Filename of Data Object Uploaded or Downloaded)

ตัวอย่างข้อมูลจราจร

```
Microsoft Internet Information Services 5.0 (IIS 5.0) Log
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2007-11-16 10:54:13
#Fields: time c-ip cs-username s-port cs-method cs-uri-stem sc-
status
17:40:30 192.168.1.67 anonymous 21 [139]USER anonymous 331
17:40:30 192.168.1.67 - 21 [139]PASS IEUser@ 530
17:40:41 192.168.1.67 Administrator 21 [140]USER Administrator 331
17:40:41 192.168.1.67 Administrator 21 [140]PASS - 230
```

ประเภท ง. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ

รายการข้อมูลที่ต้องจัดเก็บ

1. ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ให้บริการเว็บ
2. ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ
3. ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น
4. ข้อมูลคำสั่งการใช้งานระบบ

5. ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI: Uniform Resource Identifier) เช่นตำแหน่งของเว็บเพ็จ

ตัวอย่างข้อมูลจราจร

```
W3C Log
192.168.99.7 - lersak [18/Aug/2008:21:06:48 +0700] "GET
/images/bgDIVIDER.gif HTTP/1.1" 304 - "http://www.google.com
/stylesheets/_menu.css?1213106214" "Mozilla/5.0 (Windows; U;
Windows NT 6.0; en-US; rv:1.8.0.4) Geeko/20060602 Firefox/1.5.0.4"

192.168.99.7 - lersak [18/Aug/2008:21:06:48 +0700] "GET
/images/bg0N.gif HTTP/1.1" 304 -
"http://virus.thaicert.org/stylesheets/_menu.css?1213106214"
"Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.8.0.4)
Geeko/20060602 Firefox/1.5.0.4"
```

ประเภท จ. ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)

รายการข้อมูลที่ต้องจัดเก็บ

1. ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครือข่าย (NNTP หรือ Network News Transfer Protocol Log)
2. ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
3. ข้อมูลหมายเลข Port ในการใช้งาน (Protocol Process ID)
4. ข้อมูลชื่อเครื่องให้บริการ (Host Name)
5. ข้อมูลหมายเลขลำดับข้อความที่ได้ถูกส่งไปแล้ว (Posted Message ID)

ตัวอย่างข้อมูลจราจร

```
187.58.96.87, user, 12/1/2007, 14:37:37, NNTPSVC1, NEWS_Server,
134.56.87.11, 2814, 11, 513, 220, 0, article, 6
arl@l#SH#GA.425@serve, microsoft.public.ins

207.46.248.16, <feed>, 4/29/2007, 11:49:10, NNTPSVC1, NEWS_Server,
134.56.87.11, 890, 0, 61, 502, 0, newnews, Access Denied.,
microsoft.public.windows.server.sbs 060101 080000 GMT,
```

ประเภท ฉ. ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ตเช่น Internet Relay Chat (IRC) หรือ Instance Messaging (IM) เป็นต้น

รายการข้อมูลที่ต้องจัดเก็บ

1. ข้อมูลเกี่ยวกับวัน เวลาการติดต่อของผู้ใช้บริการ (Date and Time of Connection of Client to Server)
2. ข้อมูลชื่อเครื่องบนเครือข่าย (Client Hostname and/or IP Address)ข้อมูลหมายเลข Port ในการใช้งาน (Protocol Process ID)
3. หมายเลขเครื่องของผู้ให้บริการที่เครื่องคอมพิวเตอร์เชื่อมต่ออยู่ในขณะนั้น (Destination Hostname and/or IP Address)

ตัวอย่างข้อมูลจราจร

```
1205326745.661 1912 192.168.42.165 TCP_MISS/200 8460 CONNECT
login.live.com:443/ - DIRECT/login.live.com - CMF:40 DCF:20 ERR:0
DEFAULT_CASE-DefaultGroup
```

5. การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์

1. การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ ระบบฯ ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้
    1. เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity)
    2. ระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อ (Media) ที่เก็บข้อมูลจราจรคอมพิวเตอร์ได้
    3. มีระบบการเก็บ รักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้
2. เพื่อให้ข้อมูล จราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริง ระบบต้องตั้งนาฬิกาของระบบฯ ให้ตรงกับเวลาอ้างอิงสากล โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที (ไม่ใช่นาโนวินาที หรือครับ) (มิลลิวินาที ถูกต้องแล้วครับ)

6. วัตถุประสงค์ของระบบเก็บรักษาข้อมูลจราจรคอมพิวเตอร์

1. เพื่อให้ระบบสามารถบันทึกรายละเอียดของข้อมูลจราจรซึ่งมีรายละเอียด เพียงพอที่จะระบุถึงตัวตนผู้กระทำความผิดตามฐานความผิดใน พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ได้
2. เพื่อให้ระบบฯ สามารถแสดงรายละเอียดโดยพื้นฐานทำให้ผู้ใช้งานสามารถเข้าใจได้
3. เพื่อให้ระบบฯ สามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์จากอุปกรณ์หรือระบบต้นทางได้อย่างมั่นคงปลอดภัย
4. เพื่อควบคุมการเข้าถึงระบบฯทั้งในทางกายภาพ (Physical) และทางตรรก (Logical) ให้มีความมั่นคงปลอดภัยในระบบฯ
5. เพื่อให้ระบบฯ สามารถบันทึกข้อมูล ที่แสดงการเข้าถึงหรือใช้งานระบบของผู้ใช้งาน
6. เพื่อป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลจราจรคอมพิวเตอร์ที่ได้จัดเก็บไว้
7. เพื่อสามารถนำข้อมูลจราจรคอมพิวเตอร์ไปใช้ในชั้นศาลได้

7. การแสดงรายละเอียดโดยพื้นฐานของระบบ

1. ระบบฯ ต้องมีการกำหนดหรือแจ้งรายละเอียดต่อไปนี้ ให้ชัดเจนในเอกสารประกอบการขายและคู่มือ
    1. ชื่อระบบ
    2. ข้อกำหนดทางเทคนิคของระบบ เช่น ซีพียู หน่วยความจำที่จำเป็นต้องใช้ เป็นต้น
    3. ขนาดหน่วยความจำสำรองสำหรับเก็บข้อมูลจราจรคอมพิวเตอร์ (เช่น หน่วยความจำของฮาร์ดิสก์ไดรฟ์ เป็นต้น)
    4. ประเภทของผู้ให้บริการที่ระบบฯ สามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์ได้
    5. ประเภทของข้อมูลจราจรคอมพิวเตอร์ที่ระบบฯ สามารถเก็บได้
    6. รายชื่อซอฟต์แวร์ อุปกรณ์ หรือระบบต้นทางใดๆ ที่เป็นแหล่งกำเนิดข้อมูลจราจรคอมพิวเตอร์ที่ระบบฯ สามารถจัดเก็บข้อมูลจราจรจากระบบเหล่านั้นได้
    7. ระบบฯ ต้องสามารถที่จะบ่งชี้ถึงความสามารถในการจัดเก็บของระบบต่อจำนวนผู้ใช้ และระยะ

เวลาจัดเก็บที่สอดคล้องกับพรบ.ฯ เช่นอุปกรณ์นี้รองรับการจัดเก็บจำนวนเหตุการณ์สูงสุดกี่เหตุการณ์ต่อหน่วย เวลา มีขนาดหน่วยจัดเก็บขนาดเท่าไร และมีความสามารถในการเพิ่มพื้นที่จัดเก็บได้หรือไม่ เป็นต้น

9. ขั้นตอนการทำงานหรือการใช้งานของระบบฯ

1. คู่มือการใช้งานและการติดตั้งระบบฯ

1. ระบบฯ ต้องมีคู่มือแสดงขั้นตอนการทำงานหรือการใช้งานระบบ

2. ระบบฯ ต้องมีคู่มือหรือเอกสารแสดงขั้นตอนการติดตั้งระบบตั้งแต่เริ่มต้นจนกระทั่งแล้วเสร็จ

2. ระบบให้ความช่วยเหลือ (Help)

1. ระบบฯ ต้องมีระบบให้ความช่วยเหลือภายในตัวเพื่อให้ผู้ใช้งานสามารถศึกษาและทำความเข้าใจในขั้นตอนการทำงานของระบบฯ ได้

10.การจัดเก็บข้อมูลจราจรคอมพิวเตอร์จากอุปกรณ์หรือระบบต้นทาง

1. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์จากอุปกรณ์หรือระบบต้นทาง

1. ระบบฯ ต้องสามารถระบุประเภทหรือชนิดของข้อมูลที่ต้องการจัดเก็บ ตามบทนิยาม ข้อ 2.6

2. ระบบฯ ต้องสามารถระบุรายชื่อซอฟต์แวร์ อุปกรณ์หรือระบบต้นทางที่จะจัดเก็บข้อมูลจราจรคอมพิวเตอร์

ตัวอย่าง ข้อ 1 และ ข้อ 2 เช่น

ระบบ ก. สามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ในประเภทต่อไปนี้ได้ และสามารถจัดเก็บได้จากอุปกรณ์และซอฟต์แวร ดังต่อไปนี้

ประเภท ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย

1. พร็อกซี่เซิร์ฟเวอร์ squid และ พร็อกซี่เซิร์ฟเวอร์ bluecode

2. อุปกรณ์ที่รองรับการจัดเก็บข้อมูลโดยมาตรฐาน syslog

ประเภท ง. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ

1. เว็บเซอร์เวอร์ Apache

2. เว็บเซอร์เวอร์ Microsoft IIS

3. อุปกรณ์ที่รองรับการจัดเก็บข้อมูลโดยมาตรฐาน syslog

3. ระบบฯ ต้องสามารถตรวจสอบได้ว่าซอฟต์แวร์ อุปกรณ์หรือระบบต้นทางที่จะจัดเก็บข้อมูลจราจรคอมพิวเตอร์ เป็นอุปกรณ์ที่ได้รับอนุญาตแล้ว

4. ระบบฯ ต้องสามารถจำกัดผู้ที่มีสิทธิในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์จากซอฟต์แวร์ อุปกรณ์หรือระบบต้นทาง

5. ระบบฯ ต้องมีมาตรการป้องกันการเข้าถึงข้อมูลจราจรคอมพิวเตอร์ที่มีการส่งผ่านระบบเครือข่ายโดยไม่ได้รับอนุญาต

6. ระบบฯ ต้องสามารถจัดทำรายงานการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ โดยอย่างน้อยประกอบด้วยข้อมูลตามข้อ ๘.๑.๑ และ ๘.๑.๒

7. ระบบฯ ต้องสามารถแสดงข้อผิดพลาดอย่างชัดเจนเพื่อให้ผู้ใช้งานได้รับทราบว่าการจัด เก็บข้อมูลจราจรคอมพิวเตอร์ที่กำหนดให้ระบบฯ ทำนั้นไม่เสร็จสิ้นสมบูรณ์

11.การควบคุมการเข้าถึงระบบฯ

1. การลงทะเบียนผู้ใช้งานของระบบฯ

1. ระบบฯ ต้องสามารถสร้างบัญชีผู้ใช้งานระบบฯ แยกกันและสามารถตรวจสอบได้ว่าบัญชีใดเป็นของใคร

2. ระบบฯ ต้องไม่อนุญาตให้สร้างบัญชีผู้ใช้งานซ้ำซ้อนกัน

2. การจำกัดการเข้าถึงทางกายภาพ

1. อุปกรณ์ต้องมีระบบล็อคทางกายภาพเพื่อป้องกันบุคคลที่ไม่เกี่ยวข้องดำเนินการปรับเปลี่ยนโดยตรงผ่านอุปกรณ์

3. การจำกัดการเข้าถึง

1. ระบบฯ ต้องสามารถจำกัดการเข้าถึงข้อมูลจราจรคอมพิวเตอร์ตามความจำเป็นของผู้ใช้งาน ในการเข้าถึงหรือใช้งานข้อมูลเหล่านั้นโดยทำการกำหนดสิทธิการเข้าถึงให้ เหมาะสม

2. กรณีที่อุปกรณ์รองรับการปรับเปลี่ยนค่าระบบจากทางไกล เช่นมาตรฐาน SNMP หรือ WMI เป็นต้น ต้องสามารถที่จะกำหนดค่าความปลอดภัยในการเข้ารหัสการจราจรระหว่างอุปกรณ์

3. กรณีที่อุปกรณ์รองรับการปรับเปลี่ยนค่าระบบจากพอร์ต บริหารงาน เช่น Console port ระบบต้องมีการตรวจสอบตัวตนก่อนเข้าดำเนินการปรับเปลี่ยนค่า

4. การจัดชั้นความลับในการการเข้าถึง

1. ระบบฯ ต้องสามารถกำหนดหรือจัดชั้นความลับของข้อมูลจราจรคอมพิวเตอร์ที่มีการเข้าถึงโดยผู้ใช้งานในระบบ

2. ระบบฯ ต้องจำกัดผู้ใช้งานให้สามารถเข้าถึงข้อมูลจราจรคอมพิวเตอร์ได้ตามชั้นความ ลับที่ตนมีสิทธิในการเข้าถึงหรือมีความจำเป็นในการใช้งาน

3. ข้อมูลที่อยู่ในระดับชั้นความลับที่เป็นความลับต้องจัดเก็บข้อมูลในรูปแบบการเข้ารหัสที่ไม่สามารถเปิดดูได้โดยตรง

5. การพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบฯ

1. ระบบฯ ต้องมีวิธีการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัยก่อนอนุญาตให้ผู้ใช้งานเข้าใช้ระบบ

12.การบันทึกข้อมูลการเข้าถึงหรือใช้งานระบบฯ

1. การบันทึกข้อมูลการเข้าถึงหรือใช้งานระบบฯ

1. ระบบฯ ต้องสามารถบันทึกข้อมูลที่แสดงกิจกรรมการเข้าถึงหรือใช้งานระบบฯ เพื่อใช้ในการตรวจสอบในภายหลังได้ว่ามีการละเมิดความมั่นคงปลอดภัยเกิดขึ้น หรือไม่

2. การป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลบันทึกการเข้าถึงระบบฯ

1. ระบบฯ ต้องสามารถป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อมูลบันทึกการเข้าถึงระบบโดยไม่ได้รับอนุญาต

3. การตรวจสอบและตั้งนาฬิกาของระบบฯ ให้ตรงกับเวลาอ้างอิงสากล

1. ระบบฯ ต้องสามารถตรวจสอบและตั้งนาฬิกาของระบบฯ ให้ตรงกับเวลาอ้างอิงสากล โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาทีได้ เพื่อให้การบันทึกข้อมูลดังกล่าวมีความถูกต้อง

ตัวอย่าง รายชื่อเซิร์ฟเวอร์ที่ให้บริการข้อมูลเวลาสากลในประเทศไทยและต่างประเทศ

1. สถาบันมาตรวิทยาแห่งชาติ เครื่องเซิร์ฟเวอร์ time1.nimt.or.th หรือ 203.185.69.60, time2.nimt.or.th หรือ 203.185.69.59 และ time3.nimt.or.th หรือ 203.185.69.56
2. กรมอุทกศาสตร์ กองทัพเรือ เครื่องเซิร์ฟเวอร์ time.navy.mi.th หรือ 118.175.67.83
3. ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทยหรือ ThaiCERT เครื่องเซิร์ฟเวอร์ clock.thaicert.org หรือ 203.185.129.186 หรือ 203.185.129.187
4. National Institute of Standards and Technology ประเทศสหรัฐอเมริกา เครื่องเซิร์ฟเวอร์ time.nist.gov หรือ 192.43.244.18

13.การป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลจราจรคอมพิวเตอร์ที่จัดเก็บไว้

1. การตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูลจราจรคอมพิวเตอร์ที่จัดเก็บไว้
    1. ระบบฯ ต้องสามารถตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูลจราจรคอมพิวเตอร์ที่ ได้จัดเก็บไว้ เพื่อเป็นการยืนยันว่าข้อมูลที่จัดเก็บไว้นั้นยังเป็นข้อมูลเดิมที่ไม่มีการ เปลี่ยนแปลงหรือแก้ไขใดๆ
2. การไม่อนุญาตให้เปลี่ยนแปลงแก้ไขข้อมูลจราจรคอมพิวเตอร์ที่จัดเก็บไว้
    1. ระบบฯ ต้องไม่อนุญาตให้เปลี่ยนแปลงแก้ไขข้อมูลจราจรคอมพิวเตอร์ที่ได้จัดเก็บไว้

14.การป้องกันการบุกรุกระบบพื้นฐาน

1. ระบบฯ ต้องมีการควบคุมค่าข้อมูลที่รับจากบุคคลที่ใส่ข้อมูล (Input Validation)
2. ระบบฯ ต้องมีการควบคุมค่าข้อมูลที่ส่งจากระบบสู่ผู้ใช้งาน (Output Validation)
3. หากไปเป็นได้ ระบบฯ ควรมีมาตรการรับมือป้องกันอุปกรณ์เมื่อพบว่าระบบฯสงสัยว่ามีการโจมตีเกิดขึ้น

15.การตรวจสอบ

1. การแสดงรายละเอียดโดยพื้นฐานของระบบ
    1. เมื่อเริ่มต้นใช้งาน ระบบฯ ต้องสามารถแสดงรายละเอียดพื้นฐานของระบบอย่างน้อย ได้แก่
        1. ชื่อระบบ
        2. ข้อกำหนดทางเทคนิคของระบบ เช่น ซีพียู หน่วยความจำที่จำเป็นต้องใช้ เป็นต้น
        3. ขนาดหน่วยความจำสำรองสำหรับเก็บข้อมูลจราจรคอมพิวเตอร์ (เช่น หน่วยความจำของฮาร์ดิสก์ไดรฟ์ เป็นต้น)
        4. ประเภทของผู้ให้บริการที่ระบบฯ สามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์ได้
        5. ประเภทของข้อมูลจราจรคอมพิวเตอร์ที่ระบบฯ สามารถเก็บได้
        6. รายชื่อซอฟต์แวร์ อุปกรณ์หรือระบบต้นทางใดๆ ที่เป็นแหล่งกำเนิดข้อมูลจราจรคอมพิวเตอร์ที่ระบบฯ สามารถจัดเก็บข้อมูลจราจรจากระบบเหล่านั้นได้
    2. ระบบฯ ต้องสามารถที่จะบ่งชี้ถึงความสามารถในการจัดเก็บของระบบต่อจำนวนผู้ใช้ และระยะเวลาจัดเก็บที่สอดคล้องกับพรบ.ฯ เช่นอุปกรณ์นี้รองรับการจัดเก็บจำนวนเหตุการณ์สูงสุดกี่เหตุการณ์ต่อหน่วย เวลา มีขนาดหน่วยจัดเก็บขนาดเท่าไร และมีความสามารถในการเพิ่มพื้นที่จัดเก็บได้หรือไม่ เป็นต้น
2. คู่มือการใช้งานและการติดตั้งระบบฯ
    1. ระบบฯ ต้องมีคู่มือแสดงขั้นตอนการทำงานหรือการใช้งานระบบเพื่อให้ผู้ใช้งานสามารถ เรียนรู้และใช้งานได้อย่างถูกต้อง คู่มือสามารถอยู่ในรูปแบบเอกสารที่เป็นกระดาษหรืออิเล็กทรอนิกส์ก็ได้

2. ระบบฯ ต้องมีคู่มือหรือเอกสารแสดงขั้นตอนการติดตั้งระบบทีละขั้นตอนตั้งแต่ เริ่มต้นจนกระทั่งแล้วเสร็จโดยอาจแสดงตัวอย่างเป็นหน้าจอการติดตั้งทีละหน้า จอเรียงกันไปจนกระทั่งเสร็จสิ้น

3. ระบบให้ความช่วยเหลือ

    1. ระบบฯ ต้องมีระบบให้ความช่วยเหลือภายในตัวเอง กล่าวคือในระหว่างที่ผู้ใช้งานใช้ระบบอยู่และต้องการทราบวิธีการใช้งานหรือ ข้อมูลอื่นๆ ที่เกี่ยวข้องกับระบบ ผู้ใช้งานต้องสามารถร้องขอความช่วยเหลือจากระบบให้ความช่วยเหลือได้

4. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์จากซอฟต์แวร์ อุปกรณ์หรือระบบต้นทาง

    1. ระบบฯ ต้องอนุญาตให้ผู้ใช้งานสามารถระบุหรือเลือกชนิดของข้อมูลที่ต้องการจัดเก็บ ไว้ในระบบ โดยประเภทของข้อมูลนี้จะต้องสอดคล้องกับประเภทของข้อมูลที่ระบบสามารถจัด เก็บ 13.1.1.4 และ 13.1.1.5

    2. ระบบฯ ต้องอนุญาตให้ผู้ใช้งานสามารถระบุซอฟต์แวร์ อุปกรณ์หรือระบบต้นทางที่จะไปนำข้อมูลจราจรคอมพิวเตอร์มาจัดเก็บไว้ในระบบฯ เช่น ชื่อซอฟต์แวร์ อุปกรณ์หรือระบบ ไอพีแอสเดรสของอุปกรณ์หรือระบบ เป็นต้น

    3. ระบบฯ ต้องมีวิธีในการตรวจสอบได้ว่าซอฟต์แวร์ อุปกรณ์หรือระบบต้นทางที่จะไปนำข้อมูลจราจรคอมพิวเตอร์มาจัดเก็บไว้ในระบบฯ ต้องเป็นซอฟต์แวร์ อุปกรณ์หรือระบบที่ได้รับอนุญาตแล้ว กล่าวคือ ถ้ายังไม่ได้ระบุชื่อของซอฟต์แวร์ อุปกรณ์หรือระบบต้นทางที่ต้องการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ก่อน ระบบฯ จะไม่อนุญาตให้ทำการจัดเก็บข้อมูลจากซอฟต์แวร์ อุปกรณ์หรือระบบดังกล่าว

    4. ระบบฯ ต้องมีขีดความสามารถในการจำกัดผู้ที่มีสิทธิในการจัดเก็บข้อมูลจราจร คอมพิวเตอร์จากอุปกรณ์หรือระบบต้นทาง เช่น จะต้องไม่อนุญาตให้ผู้ใช้งานที่ไม่มีสิทธิทำการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ได้

    5. ระบบฯ ต้องมีมาตราการป้องกันเพื่อไม่ให้ข้อมูลจราจรคอมพิวเตอร์ที่มีการส่งผ่าน ระบบเครือข่ายสามารถถูกดักแอบดูหรือดับจับข้อมูลในระหว่างที่มีการเดินทางมา ในระบบเครือข่ายได้ เช่น การป้องกันโดยการใช้การเข้ารหัสข้อมูล เป็นต้น

    6. ระบบฯ ต้องสามารถจัดทำรายงานการนำข้อมูลจราจรคอมพิวเตอร์มาจัดเก็บไว้ในระบบฯ รายงานต้องมีข้อมูลอย่างน้อย ได้แก่ ชนิดของข้อมูลจราจรคอมพิวเตอร์ที่ต้องการจัดเก็บและซอฟต์แวร์ อุปกรณ์หรือระบบต้นทางที่ระบบฯ ไปนำข้อมูลจราจรคอมพิวเตอร์มาจัดเก็บไว้

    7. ระบบฯ ต้องสามารถแสดงข้อผิดพลาดได้อย่างถูกต้องและชัดเจนเพื่อให้ผู้ใช้งานสามารถ ดำเนินการแก้ไขได้ต่อไป เช่น ในกรณีที่ซอฟต์แวร์ อุปกรณ์หรือระบบต้นทางไม่สามารถให้บริการได้ (อาทิ ระบบฯ ไม่สามารถเชื่อมต่อกับอุปกรณ์ต้นทางได้ หรืออุปกรณ์มีปัญหาบางประการในระหว่างที่ยังทำการโอนย้ายข้อมูลยังไม่เสร็จ) ระบบฯ ต้องสามารถแจ้งข้อผิดพลาดได้อย่างถูกต้องเพื่อให้ผู้ใช้งานสามารถทำการแก้ไขได้อย่างถูกต้อง

5. การลงทะเบียนผู้ใช้งานของระบบฯ

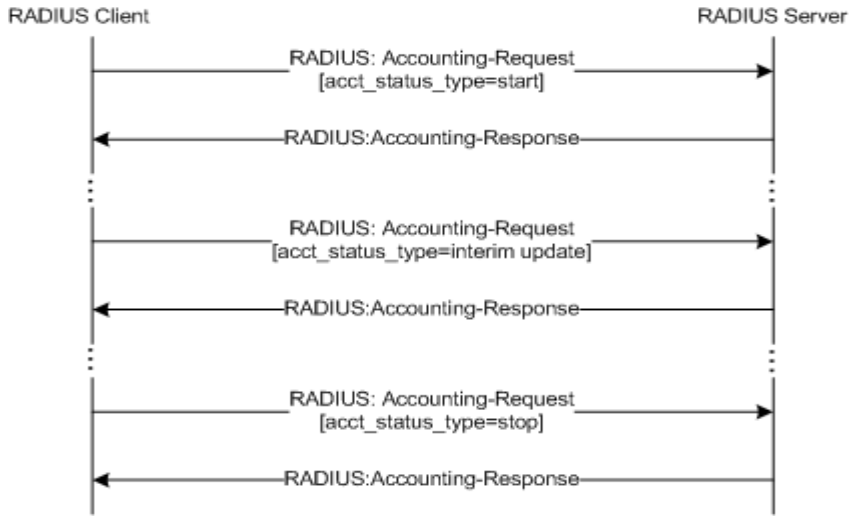
    1. ระบบฯ ต้องสามารถสร้างบัญชีผู้ใช้งานในระบบแยกกันได้ตามการร้องขอเพื่อขอเข้าใช้ระบบ (บัญชีผู้ช้งานแยกออกจากระบบปฏิบัติการ) เช่น บัญชีของผู้ดูแลระบบ บัญชีของผู้ตรวจสอบ เป็นต้น

    2. ระบบฯ ต้องไม่อนุญาตให้สร้างบัญชีผู้ใช้งานที่ซ้ำซ้อนกัน เช่น เมื่อมีความพยายามในการสร้างบัญชีผู้ใช้งานที่เคยสร้างมาแล้ว ระบบฯ ต้องแจ้งเตือนและไม่อนุญาตให้สร้างบัญชีนั้น

    3. ระบบฯ ต้องสามารถบริหารงานสมาชิกได้เช่น การยกเลิก การกำหนดสิทธิ ในการใช้งาน เช่น การกำหนดช่วงเวลาการใช้ หรือ กำหนดสิทธิในการเข้าถึงทรัพยากร ต่าง ๆ ในระบบ

6. การจำกัดการเข้าถึง
    1. อุปกรณ์ต้องมีระบบล็อคเพื่อป้องกันบุคคลที่ไม่เกี่ยวข้องเข้าดำเนินการปรับเปลี่ยนแก้ไขข้อมูลในระดับกายภาพ
    2. อุปกรณ์ที่รองรับการปรับเปลี่ยนค่า หรือข้อมูลจากทางไกลต้องมีการระบุตำแหน่งของเครื่อง และรองรับโพรโตคอลที่มีความปลอดภัย (ดูรายละเอียดเพิ่มเติมจากข้อ 8 ในหัวข้อการพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบฯ)
    3. อุปกรณ์ที่รองรับพอร์ตปรับเปลี่ยนค่าในตัวอุปกรณ์จะต้องรองรับการตรวจสอบตัวตนก่อนเข้าไปดำเนินการปรับเปลี่ยนค่าใดๆในอุปกรณ์เหล่านั้น
    4. จากบัญชีผู้ใช้งาน ต่างๆ ระบบฯ ต้องสามารถกำหนดสิทธิการเข้าถึงข้อมูลจราจรคอมพิวเตอร์จากบัญชีเหล่านั้นได้ โดยต้องให้สิทธิตามความจำเป็นของผู้ใช้งานนั้น เช่น สิทธิของบัญชีผู้ดูแลระบบ สิทธิของบัญชีผู้ตรวจสอบ เป็นต้น
7. การจัดชั้นความลับในการเข้าถึง
    1. ระบบฯ ต้องสามารถกำหนดหรือจัดชั้นความลับของข้อมูลจราจรคอมพิวเตอร์ที่มีการจัด เก็บไว้ในตัวระบบ เช่น ข้อมูลลับ เปิดเผยได้ หรือใช้ภายในเท่านั้น
    2. จากบัญชีผู้ใช้งาน ต่างๆ ระบบฯ ต้องสามารถกำหนดสิทธิการเข้าถึงข้อมูลจราจรคอมพิวเตอร์ตามชั้นความลับของ ข้อมูลที่ตนมีสิทธิในการเข้าถึงหรือความจำเป็นในการใช้งาน
    3. ข้อมูลระดับชั้นความลับต้องมีการเข้ารหัสในการจัดเก็บเพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่เกี่ยวข้อง
8. การพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบฯ
    1. ระบบฯ ต้องมีวิธีการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัยก่อนอนุญาตให้ผู้ใช้งาน เข้าใช้ระบบ การตรวจสอบต้องดูว่าในการล็อกอินเข้าใช้งานระบบฯ ผู้ใช้งานต้องปลอดภัยจากการถูกดักแอบดูข้อมูลการล็อกอินในเครือข่ายโดยผู้ ไม่ประสงค์ดี การพิสูจน์ตัวตนต้องทำงานผ่าน ช่องการในการตรวจสอบโดยระบบต้องแสดงหน้า ในการล็อกอินประกอบด้วย Username และ Password หรือส่วนประกอบในการตรวจสอบเพิ่มเติมเพื่อยืนยันกับระบบสมาชิก ไม่ว่าจะทำงานบนฐานข้อมูล SQL , LDAP, Active Directory, Radius, TACACS+, หรืออื่นๆ โดยอาศัยหลักการพิสูจน์ตัวตนแบบ AAA (Authentication, Authority, Account)
    ตัวอย่างการตรวจสอบการพิสูจน์ตัวตนแบบ RADIUS (Remote Authentication Dial In User Service) เมื่อผู้ใช้งานทำการใช้งานระบบจะบังคับให้ผู้ใช้งานกรอก username, password หลังจากนั้น ข้อมูลจะถูกส่งต่อไปที่ Radius Server เพื่อจะทำการตรวจสอบข้อมูลผู้ใช้ร่วมกับระบบตรวจสอบตัวตนต่างๆในการพิสูจน์ตัวตน และการส่งข้อมูลนั้นควรรักษาความปลอดภัยในการส่ง โดยการใช้โพรโตคอลที่มีความมั่นคงปลอดภัย อาทิ SSL, SSH, HTTPS, หรือมาตรฐานอื่นที่มีการรับรองในระดับสากล (เช่น IPSec, VPN แบบต่างๆ) สำหรับการสื่อสารข้อมูลบนเครือข่ายในระหว่างที่ผู้ใช้งานทำการล็อกอินเข้าสู่ระบบฯ เป็นต้น
    2. ระบบฯ ต้องมีวิธีการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัยก่อนอนุญาตให้ผู้ใช้งาน เข้าใช้ระบบ รวมไปถึงมาตรการรักษาความปลอดภัยในการส่งข้อมูล สำหรับการสื่อสารข้อมูลบนเครือข่ายในระหว่างที่ผู้ใช้งานทำการล็อกอินเข้า สู่ระบบฯ จะต้องใช้โพรโตคอลการสื่อสารที่มีความมั่นคงปลอดภัย อาทิ SSL, SSH, HTTPS, หรือมาตรฐานอื่นที่มีการรับรองในระดับสากล (เช่น IPSec, VPN แบบต่างๆ) เป็นต้น การพิสูจน์ตัวตนต้องทำงานผ่าน ช่องการในการตรวจสอบโดยระบบต้องแสดงหน้า ในการล็อกอินประกอบด้วย Username และ Password หรือส่วนประกอบในการตรวจสอบเพิ่มเติมเพื่อยืนยันกับระบบสมาชิก ไม่ว่าจะทำงานบนฐานข้อมูล SQL , LDAP, Active Directory, Radius, TACACS+, หรืออื่นๆ โดยอาศัยหลักการพิสูจน์ตัวตนแบบ AAA (Authentication, Authority, Account)

ตัวอย่างการตรวจสอบการพิสูจน์ตัวตนแบบ RADIUS (Remote Authentication Dial In User Service) เมื่อผู้ใช้งานทำการใช้งานระบบจะบังคับให้ผู้ใช้งานกรอก username, password หลังจากนั้น ข้อมูลจะถูกส่งต่อไปที่ Radius Server เพื่อจะทำการตรวจสอบข้อมูลผู้ใช้ร่วมกับระบบตรวจสอบตัวตนต่างๆในการพิสูจน์ ตัวตน (เลือกข้อ 1 หรือ ข้อ 2 ใช้รูปเดียวกัน)



9. การบันทึกข้อมูลการเข้าถึงในการบริหารจัดการหรือใช้งานระบบฯ

1. ระบบฯ ต้องสามารถบันทึกข้อมูลการเข้าถึงหรือใช้งานระบบฯ โดยแสดงกิจกรรมการเข้าถึงหรือใช้งานระบบ เช่น เมื่อมีการเปิดดูข้อมูลจราจรคอมพิวเตอร์ ระบบฯ ต้องบันทึกไว้ว่าบัญชีผู้ใช้งานใดเป็นผู้เปิดดู รวมทั้งวันเวลาที่เปิดดู เป็นต้น
2. ระบบ ต้องสามารถบันทึกข้อมูลแยกกันระหว่าง ระบบ ต่างๆ

10.การป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลบันทึกการเข้าถึงหรือใช้งานระบบฯ

1. ถ้ามีความพยายามในการเปลี่ยนแปลงหรือแก้ไขข้อมูลบันทึกการเข้าถึงระบบระบบฯ ต้องไม่อนุญาตให้ดำเนินการ

11.การตรวจสอบและตั้งนาฬิกาของระบบฯ ให้ตรงกับเวลาอ้างอิงสากล

1. ระบบฯ ต้องสามารถตรวจสอบและตั้งนาฬิกาของระบบฯ ให้ตรงกับเวลาอ้างอิงสากล โดยผิดพลาดได้ไม่เกิน ๑๐ มิลลิวินาทีได้ การตรวจสอบสามารถทำได้โดย เช่น เมื่อมีการเปิดดูข้อมูลจราจรคอมพิวเตอร์ เวลาที่มีการบันทึกลงไปในบันทึกการเข้าถึงหรือใช้งานระบบฯ ต้องมีความถูกต้องตรงตามเวลาอ้างอิงสากล

12.การตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูลจราจรคอมพิวเตอร์ที่จัดเก็บไว้

1. ระบบฯ ต้องมีความสามารถในการตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูลจราจรคอมพิวเตอร์ที่ได้จัดเก็บไว้ เช่น
   ใช้ วิธีการเปรียบเทียบค่า hash จาก hash fuction ที่ใช้เพื่อจุดประสงค์ในด้านความปลอดภัยของสารสนเทศเช่น SHA-1,MD5 หรือ CRC32 เป็นต้น
   กล่าวคือ ภายหลังจากที่ได้นำข้อมูลจราจรคอมพิวเตอร์มาจัดเก็บไว้ในระบบฯ แล้ว ให้คำนวณค่า hash กับ ข้อมูลนั้น และจัดเก็บค่าผลลัพธ์ของการคำนวณไว้ในสถานที่ที่มีความปลอดภัย หลังจากนั้น เมื่อต้องการตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูลที่ได้ จัดเก็บไว้ ให้คำนวณค่า hash กับข้อมูลในระบบฯ นั้นซ้ำอีกครั้งหนึ่ง
   ถ้าผลลัพธ์ที่ ได้ตรงกันกับครั้งแรก แสดงว่า ข้อมูลที่ได้นำมาเก็บนั้นมีความถูกต้อง ถ้าผลลัพธ์ที่ได้ไม่ตรงกัน แสดงว่าข้อมูลมีความไม่ถูกต้องหรือมีการเปลี่ยนแปลงข้อมูลเกิดขึ้น

13.การไม่อนุญาตให้เปลี่ยนแปลงแก้ไขข้อมูลจราจรคอมพิวเตอร์ที่จัดเก็บไว้

1. ระบบฯ ต้องไม่อนุญาตหรือเปิดโอกาสให้ทำการเปลี่ยนแปลงแก้ไขข้อมูลจราจรคอมพิวเตอร์ที่ได้จัดเก็บไว้ในระบบฯ

14.ระบบฯต้องมีการป้องกันการบุกรุกระบบพื้นฐาน ได้แก่

1. การควบคุมค่าข้อมูลที่รับจากบุคคลที่ใส่ข้อมูล (Input Validation)
2. การควบคุมค่าข้อมูลที่ส่งจากระบบสู่ผู้ใช้งาน (Output Validation)
3. มีมาตรการรับมือป้องกันอุปกรณ์เมื่อพบว่าระบบฯสงสัยว่ามีการโจมตีเกิดขึ้น