

ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์
เล่ม ๒ แนวทางในการจัดทำและตรวจสอบ

COMPUTER LOG SYSTEMS

PART 2 : IMPLEMENTATION AND EVALUATION GUIDE

๑. ขอบข่าย

เอกสารนี้ เสนอข้อมูล หลักการ วิธีการ แนวคิด และตัวอย่าง เพื่อเป็นแนวทางในการจัดทำและตรวจสอบ ระบบ เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ให้สอดคล้องและเป็นไปตาม “มาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ เล่ม ๑ ข้อกำหนด”

เอกสารนี้ใช้ได้กับทั้งระบบ ซึ่งอาจหมายถึงหลายหน่วยต่อเชื่อมกันหรือหน่วยเดียว รวมถึงซอฟต์แวร์ประยุกต์ที่ออกแบบมาโดยประสงค์ให้ติดตั้งในระบบคอมพิวเตอร์ เพื่อให้ระบบคอมพิวเตอร์นั้นทำหน้าที่เป็นระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

เอกสารนี้ไม่ครอบคลุมถึง การปรับตั้งค่าต่าง ๆ ของ โปรแกรม ซอฟต์แวร์ประยุกต์ อุปกรณ์เครือข่าย เครื่องและระบบคอมพิวเตอร์อื่น ซึ่งทำหน้าที่ให้บริการใด ๆ ในระบบคอมพิวเตอร์ที่ต่อเชื่อมถึงกัน และมีหน้าที่ต้องส่งข้อมูลจราจรทางคอมพิวเตอร์ที่กำหนด ให้ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

หมายเหตุ ผู้ประกอบกิจการโทรคมนาคม และผู้ประกอบกิจการกระจายภาพและเสียง ที่ให้บริการอื่น ๆ นอกเหนือจากการให้บริการโครงข่ายโทรคมนาคม และการกระจายภาพและเสียง ถูกพิจารณาว่าอยู่ในขอบข่ายของเอกสาร ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาตินี้

เอกสารนี้กำหนดขึ้นโดยใช้ ข้อมูลป้อนกลับจาก**ผู้ใช้** และเอกสารต่อไปนี้เป็นแนวทาง

- มคอ. ๔๐๐๓.๑-๒๕๖๐ มาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ – เล่ม ๑ ข้อกำหนด
- ประกาศราชกิจจานุเบกษา, “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”, วันที่ ๑๘ มิถุนายน ๒๕๕๐
- ประกาศราชกิจจานุเบกษา, “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐”, วันที่ ๒๔ มกราคม ๒๕๖๐
- ประกาศราชกิจจานุเบกษา, “ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐”, วันที่ ๒๓ สิงหาคม ๒๕๕๐

เอกสารนี้เป็นหนึ่งในอนุกรมเอกสารเกี่ยวกับ ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งได้มีการประกาศใช้แล้ว ๒ เล่ม ดังนี้

- มาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ – ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ เล่ม ๑ ข้อกำหนด
- ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ – เล่ม ๒ แนวทางในการจัดทำและตรวจสอบ

๒. บทนิยาม

- ๒.๑ ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งต่อไปในเอกสารศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาตินี้จะเรียกว่า “ระบบ” หมายถึง คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่ทำหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ทั้งนี้หมายถึงซอฟต์แวร์ที่จะติดตั้งในระบบคอมพิวเตอร์เพื่อให้ทำหน้าที่ดังกล่าวข้างต้น

- ๒.๒ **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์คอมพิวเตอร์ ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- ๒.๓ **ข้อมูลจราจรทางคอมพิวเตอร์** หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรือข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
- ๒.๔ **ผู้ให้บริการ** หมายถึง ผู้ซึ่งมีเจตนา
- ๒.๔.๑ ให้บริการแก่ บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือเพื่อประโยชน์ของบุคคลอื่น
- ๒.๔.๒ ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น
- ๒.๕ **ผู้ดูแลระบบ (administrator)** หมายถึง บุคคล หรือกลุ่มบุคคล ที่มีหน้าที่ ดูแลรักษา ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ แต่จะไม่มีสิทธิในการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ และอาจรวมถึงข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่น ๆ ที่เกี่ยวข้อง
- ๒.๖ **ผู้ดูแลข้อมูล** หมายถึง ผู้ที่ได้รับมอบสิทธิจากองค์กร/หน่วยงานในการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ และอาจรวมถึงข้อมูลคอมพิวเตอร์ และข้อมูลอื่น ๆ ที่เกี่ยวข้อง สิทธิในการเข้าถึงข้อมูลจะต้องไม่รวมถึงสิทธิในการแก้ไข เปลี่ยนแปลง ลบ หรือ ทำลายข้อมูล
- ๒.๗ **ผู้ใช้** หมายถึง ผู้ดูแลระบบ หรือผู้ดูแลข้อมูล
- ๒.๘ **การยืนยันตัวบุคคล** หมายถึง ขั้นตอนการขึ้นบ่ง เพื่อยืนยันความถูกต้องของหลักฐานที่ใช้ระบุ (identity) แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง สามารถแบ่งออกได้เป็น ๒ ขั้นตอน คือ การระบุตัวตน และการพิสูจน์ตัวตน
- ๒.๙ **การระบุตัวตน (identification)** หมายถึง ขั้นตอนหรือวิธี ที่ผู้ใช้แสดงเป็นหลักฐานซึ่งตนเอง เช่น ชื่อผู้ใช้ (username)
- ๒.๑๐ **การพิสูจน์ตัวตน (authentication)** หมายถึง ขั้นตอนหรือวิธี การตรวจสอบหลักฐานแวดล้อมเพื่อยืนยันว่าเป็นบุคคลที่กล่าวอ้างจริง
- ๒.๑๑ **การล็อกอิน (log-in)** หมายถึง การเข้าใช้งานระบบคอมพิวเตอร์ โดยต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน
- ๒.๑๒ **ข้อมูลการล็อกอิน (log-in data)** หมายถึง ข้อมูลที่ใช้ในการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบคอมพิวเตอร์
- ๒.๑๓ **บูรณภาพของข้อมูล (data integrity)** หมายถึง ความถูกต้อง เทียบตรง และความสมบูรณ์ของข้อมูล
- ๒.๑๔ **มาตรฐานเล่มที่ ๑** หมายถึง มาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ – เล่ม ๑ ข้อกำหนด
- ๒.๑๕ **พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์** หมายถึง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ

คอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ซึ่งต่อไปในมาตรฐานนี้จะเรียกว่า "พ.ร.บ. ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์"

๓. การประเมินข้อมูลพื้นฐาน

๓.๑ การประเมินองค์กรเพื่อวางแผนในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

การประเมินองค์กรเพื่อวางแผนในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ มีวัตถุประสงค์ ดังนี้

- (๑) เพื่อให้องค์กรได้รับรู้ถึงประเภทของผู้ให้บริการตามความหมายใน พ.ร.บ. ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พร้อมทั้งจำแนกประเภทย่อยของผู้ให้บริการได้
- (๒) เพื่อให้องค์กรสามารถวิเคราะห์และจัดทำบัญชีรายชื่อของเครื่องให้บริการหรือระบบให้บริการที่จำเป็นต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์
- (๓) เพื่อให้องค์กรสามารถเก็บข้อมูลจราจรทางคอมพิวเตอร์ได้ถูกต้องตามที่กฎหมายกำหนด

โดยขั้นตอนการประเมิน แบ่งได้เป็น ๓ ขั้นตอน คือ

- (๑) การประเมินองค์กรเพื่อกำหนดประเภทของผู้ให้บริการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- (๒) การวิเคราะห์และกำหนดระบบให้บริการหรือเครื่องให้บริการที่จำเป็นต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์
- (๓) การวิเคราะห์ปริมาณข้อมูลจราจรทางคอมพิวเตอร์ที่ต้องทำการจัดเก็บเบื้องต้น

๓.๑.๑ การประเมินองค์กรเพื่อกำหนดประเภทของผู้ให้บริการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จากประกาศ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ ได้กำหนดประเภทของผู้ให้บริการซึ่งมีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์แบ่งได้ ดังนี้

- ๓.๑.๑.๑ ผู้ให้บริการ ๕(๑) เป็น ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือเพื่อประโยชน์ของบุคคลอื่น จำแนกได้ ๔ ประเภท ดังนี้

- ก) ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (telecommunication and broadcast carrier)
- ข) ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (access service provider)
- ค) ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่าง ๆ (host service provider)
- ง) ผู้ให้บริการร้านอินเทอร์เน็ต

- ๓.๑.๑.๒ ผู้ให้บริการ ๕(๒) เป็น ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคล (content service provider) ตาม ข้อ ๓.๑.๑.๑ (content service provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอปพลิเคชันต่าง ๆ (application service provider)

ซึ่งผู้ให้บริการทั้ง ๒ ประเภทนั้นมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์แตกต่างกัน ดังนั้นเพื่อให้องค์กรสามารถกำหนดประเภทของผู้ให้บริการขององค์กรได้ จำเป็นต้องพิจารณาประเภทของผู้ให้บริการดังต่อไปนี้

(๑) พิจารณาว່องค์กรจัดอยู่ในประเภทของผู้ให้บริการใด

ที่	ประเด็น	หลักการพิจารณา	ประเภทผู้ให้บริการ
๑	พิจารณาวัตถุประสงค์การให้บริการอินเทอร์เน็ตขององค์กร	ให้บริการอินเทอร์เน็ตแก่บุคคลทั่วไปหรือบุคคลภายในองค์กร	ผู้ให้บริการ ๕(๑)
		ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์แก่บุคคลอื่น	ผู้ให้บริการ ๕(๒)

ตัวอย่าง ผู้ให้บริการ ๕(๑) เช่น

- ผู้ให้บริการอินเทอร์เน็ต (Internet service provider, ISP) ต่าง ๆ ซึ่งเป็นผู้ให้บริการอินเทอร์เน็ตแก่บุคคลทั่วไป
- ผู้ให้บริการเครือข่ายมือถือที่มีการให้บริการอินเทอร์เน็ต
- หน่วยงานราชการหรือองค์กรต่าง ๆ ที่ให้บริการอินเทอร์เน็ต

ตัวอย่าง ผู้ให้บริการ ๕(๒) เช่น

- ผู้ให้บริการ web hosting
- ผู้ให้บริการ application hosting

(๒) พิจารณาว່องค์กรจัดอยู่ในประเภทผู้ให้บริการย่อยใด (เฉพาะในกรณีองค์กรจัดอยู่ในประเภทผู้ให้บริการ ๕(๑))

ที่	ประเด็น	หลักการพิจารณา	ประเภทผู้ให้บริการ
๑	พิจารณาประเภทการให้บริการ	เป็นผู้ประกอบกิจการโทรคมนาคม และการกระจายภาพและเสียง	ผู้ให้บริการ ๕(๑) ก
		เป็นผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์	ผู้ให้บริการ ๕(๑) ข
		เป็นผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่าง ๆ	ผู้ให้บริการ ๕(๑) ค
		เป็นผู้ให้บริการร้านอินเทอร์เน็ต	ผู้ให้บริการ ๕(๑) ง

๓.๑.๒ การวิเคราะห์และกำหนดระบบให้บริการหรือเครื่องให้บริการ ที่จำเป็นต้องเก็บ**ข้อมูลจราจรทางคอมพิวเตอร์**

เพื่อให้สามารถระบุเครื่องให้บริการที่จำเป็นต้องเก็บ**ข้อมูลจราจรทางคอมพิวเตอร์** ผู้ให้บริการควรจัดทำบัญชีรายชื่อของระบบให้บริการหรือเครื่องให้บริการที่จำเป็นต้องเก็บ**ข้อมูลจราจรทางคอมพิวเตอร์** โดยอาศัยขั้นตอนต่อไปนี้

๓.๑.๒.๑ วิเคราะห์ระบบให้บริการหรือเครื่องให้บริการขององค์กร

เมื่อองค์กรได้ทราบถึงประเภทของ**ผู้ให้บริการ**ขององค์กร พร้อมกับได้จำแนกประเภทย่อย ของ**ผู้ให้บริการ**แล้ว จำเป็นต้องมีการวิเคราะห์ ระบบให้บริการหรือเครื่องให้บริการ ที่มีอยู่ทั้งหมดในองค์กร เพื่อให้องค์กรสามารถระบุระบบให้บริการหรือเครื่องให้บริการ ที่เกี่ยวข้องและจำเป็นต้องเก็บ**ข้อมูลจราจรทางคอมพิวเตอร์** โดยการวิเคราะห์ อาศัยหลักการพิจารณา ดังต่อไปนี้

(๑) พิจารณาขอบเขตการให้บริการ

หลักการพิจารณา	การดำเนินการ
๑. ให้บริการเฉพาะภายในองค์กร เข้าถึงได้เฉพาะภายในองค์กร	พิจารณาตามความเหมาะสมและความจำเป็น
๒. ให้บริการเฉพาะภายในองค์กร แต่บุคคลภายนอกสามารถเข้าถึงได้จากอินเทอร์เน็ต	ต้องเก็บ ข้อมูลจราจรทางคอมพิวเตอร์
๓. ให้บริการภายในองค์กร แต่มีการติดต่อสื่อสารกับบุคคลภายนอก	ต้องเก็บ ข้อมูลจราจรทางคอมพิวเตอร์
๔. ให้บริการสาธารณะ	ต้องเก็บ ข้อมูลจราจรทางคอมพิวเตอร์

(๒) พิจารณา**ข้อมูลจราจรทางคอมพิวเตอร์**ที่**ผู้ให้บริการ**แต่ละประเภทต้องทำการจัดเก็บ

(๒.๖) **ผู้ให้บริการ**ประเภท ๕(๑) ข และ ค

ก) ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย

หลักการพิจารณา	การดำเนินการ
๑. ต้องมีการเก็บ ข้อมูลจราจรทางคอมพิวเตอร์ ทุกช่องทางที่มีการเชื่อมต่ออินเทอร์เน็ต	ตรวจสอบช่องทางการเชื่อมต่ออินเทอร์เน็ต ว่าองค์กรมีช่องทางการเข้าสู่อินเทอร์เน็ตทางใดบ้างและในแต่ละช่องทางมีการเก็บ ข้อมูลจราจรทางคอมพิวเตอร์ หรือไม่
๒. รายละเอียดของข้อมูลที่ทำกรจัดเก็บต้องมีครบถ้วนตามข้อกำหนด	ตรวจสอบรายละเอียดของ ข้อมูลจราจรทางคอมพิวเตอร์ ที่จัดเก็บไว้ว่ามีข้อมูลถูกต้องตามข้อกำหนดหรือไม่
๓. ข้อมูลจราจรทางคอมพิวเตอร์ ที่จัดเก็บต้องสามารถระบุตัวตนของผู้ใช้งานได้	ตรวจสอบรายละเอียดของข้อมูลที่ทำกรจัดเก็บไว้ว่าเพียงพอสำหรับการระบุตัวตนของผู้ใช้งานหรือไม่ ตัวอย่าง เช่น ในองค์กรที่มีการใช้งานระบบ NAT (network address translation) จะทำให้หมายเลขไอพี (IP address) ของผู้ใช้งานอินเทอร์เน็ตเป็นหมายเลขเดียวกัน องค์กรจำเป็นต้อง

หลักการพิจารณา	การดำเนินการ
	จัดให้มีมาตรการในการควบคุมผู้ใช้งานเพื่อให้สามารถระบุตัวตนผู้ใช้งานได้ เช่น การจัดทำระบบลงทะเบียนผู้ใช้งาน ในองค์กรที่มีการใช้งานพร็อกซีเซิร์ฟเวอร์ (proxy server) องค์กรจำเป็นต้องจัดให้มีมาตรการในการควบคุมผู้ใช้งาน เพื่อให้สามารถระบุตัวตนผู้ใช้งานได้ เช่น การใช้กลไกการพิสูจน์ตัวตนก่อนเข้าใช้งานอินเทอร์เน็ต

หมายเหตุ การเข้าถึงระบบเครือข่าย หมายถึง การเข้าถึงระยะไกล (remote access) เช่น การเชื่อมโยงผ่านเครือข่ายส่วนตัวเสมือน (virtual private network, VPN), การเข้าถึงเดสก์ท็อประยะไกล (remote desktop), SSH (secure shell)

ข) ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail server)

หลักการพิจารณา	การดำเนินการ
๑. ผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) แก่องค์กร	ถ้ามีการให้บริการโดยผู้ให้บริการภายนอก ผู้ให้บริการภายนอกต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้กับองค์กร
๒. รายละเอียดของข้อมูลที่ทำกรการจัดเก็บต้องมีครบถ้วนตามข้อกำหนด	ตรวจสอบรายละเอียดของข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้ว่ามีข้อมูลถูกต้องตามข้อกำหนดหรือไม่
๓. ต้องมีการเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ ผ่านโปรแกรมจัดการจากเครื่องสมาชิก เช่น POP3, IMAP4	ตรวจสอบว่าเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ ให้บริการการเข้าถึงจดหมายอิเล็กทรอนิกส์แก่สมาชิกด้วยโพรโทคอลประเภทใด เพื่อเก็บข้อมูลจราจรทางคอมพิวเตอร์ของโปรแกรมดังกล่าวด้วย เช่น บริการ POP3, บริการ IMAP4

ค) ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล

หลักการพิจารณา	การดำเนินการ
๑. รายละเอียดของข้อมูลที่ทำกรการจัดเก็บต้องมีครบถ้วนตามข้อกำหนด	ตรวจสอบรายละเอียดของข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้ว่ามีข้อมูลถูกต้องตามข้อกำหนดหรือไม่

ง) ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ

หลักการพิจารณา	การดำเนินการ
๑. รายละเอียดของข้อมูลที่ทำกรการจัดเก็บต้องมีครบถ้วนตามข้อกำหนด	ตรวจสอบรายละเอียดของข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้ว่ามีข้อมูลถูกต้องตามข้อกำหนดหรือไม่

จ) ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)

หลักการพิจารณา	การดำเนินการ
๑. รายละเอียดของข้อมูลที่ทำกรการจัดเก็บต้องมีครบถ้วนตามข้อกำหนด	ตรวจสอบรายละเอียดของข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้ว่ามีข้อมูลถูกต้องตามข้อกำหนดหรือไม่

ฉ) ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ instance messaging (IM)

หลักการพิจารณา	การดำเนินการ
๑. รายละเอียดของข้อมูลที่มีการจัดเก็บต้องมีครบถ้วนตามข้อกำหนด	ตรวจสอบรายละเอียดของข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้ว่ามีข้อมูลถูกต้องตามข้อกำหนดหรือไม่
๒. พิจารณาการให้บริการขององค์กรที่มีอยู่ ว่าเป็นการให้บริการในขอบข่ายการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ตหรือไม่	ถ้าการให้บริการอยู่ในขอบข่าย ให้พิจารณาพอร์ตการสื่อสาร (communication port) และทำการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่พอร์ต (port) ของบริการดังกล่าว

๓.๑.๒.๒ กำหนดและจัดทำบัญชีรายชื่อของระบบให้บริการและ/หรือเครื่องให้บริการ ที่จำเป็นต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์

เมื่อองค์กรสามารถวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการแต่ละประเภทต้องทำการจัดเก็บ ได้แล้ว ควรจัดบัญชีรายชื่อของเครื่องให้บริการที่จำเป็นต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ เพื่อใช้เป็นข้อมูลในการบริหารจัดการของผู้ดูแลข้อมูลจราจรทางคอมพิวเตอร์

๓.๑.๓ การวิเคราะห์ปริมาณข้อมูลจราจรทางคอมพิวเตอร์ที่ต้องทำการจัดเก็บเบื้องต้น

การวิเคราะห์ปริมาณข้อมูลจราจรทางคอมพิวเตอร์ที่ต้องการจัดเก็บ เป็นขั้นตอนส่วนหนึ่งที่ต้องทำการวิเคราะห์ ข้อมูลเบื้องต้น เพื่อที่จะสามารถเลือกระบบเก็บข้อมูลจราจรทางคอมพิวเตอร์ได้อย่างเหมาะสม และสามารถเก็บข้อมูลได้อย่างเพียงพอตามที่กฎหมายกำหนด การวิเคราะห์ปริมาณข้อมูลจราจรทางคอมพิวเตอร์เพื่อหาขนาดหน่วยบันทึกข้อมูลที่ต้องการ อาจใช้การประมาณการขนาดข้อมูลในแต่ละวัน เพื่อประมาณการข้อมูลที่พอเพียงสำหรับการใช้เก็บข้อมูลตามกฎหมายได้ (โดยปกติกฎหมายกำหนดให้เก็บข้อมูล ๙๐ วัน ในกรณีจำเป็น พนักงานเจ้าหน้าที่สามารถสั่งให้เก็บเพิ่มเป็น ๒ ปี หรือ ๗๓๐ วันได้) ซึ่งการคำนวณเบื้องต้นสามารถทำได้หลายวิธี ผลลัพธ์ของการคำนวณ อาจใช้ไม่ได้ในกรณีที่สภาพแวดล้อมการทำงานที่ต่างกัน หรือมีเงื่อนไขอื่น ๆ เข้ามาเกี่ยวข้อง โดยในเอกสารศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาตินี้นำเสนอเพียงแนวคิดเบื้องต้น เพื่อให้สามารถประเมินค่าเบื้องต้นได้ ดังวิธีคำนวณที่จะอธิบายดังต่อไปนี้

- การคำนวณโดยประมาณการจากความเร็วในการเชื่อมต่ออินเทอร์เน็ตขององค์กร
- การคำนวณโดยผลรวมของค่าเฉลี่ยจากข้อมูลจราจรทางคอมพิวเตอร์เดิม

หมายเหตุ การคำนวณแต่ละวิธีอาจเหมาะสมกับองค์กรในแต่ละแบบ แตกต่างกันไป ขึ้นอยู่กับ สภาพแวดล้อมการทำงาน และเงื่อนไขอื่น ๆ ดังนั้นผู้ดูแลระบบขององค์กรจึงควรพิจารณาเลือกวิธีคำนวณให้เหมาะสม

๓.๑.๓.๑ การคำนวณแบบประมาณการจากความเร็วในการเชื่อมต่ออินเทอร์เน็ตขององค์กร

การคำนวณแบบนี้เป็นการประมาณการ (estimation) ที่เหมาะสำหรับองค์กรที่มีความเร็วในการเชื่อมต่ออินเทอร์เน็ตไม่สูง ใช้เพื่อประมาณการหาขนาดหน่วยบันทึกข้อมูลจราจรทางคอมพิวเตอร์ โดยใช้หลักการประมาณค่าขนาดของข้อมูลจราจรทางคอมพิวเตอร์ เป็นร้อยละของจำนวนปริมาณข้อมูลสูงสุดที่สามารถใช้งานได้ (data transfer/second) โดยแสดงข้อมูลสรุปการคำนวณตามตาราง

ความเร็วของการเชื่อมต่ออินเทอร์เน็ต (Mbps)	๑	๓๐	๕๐	๑๐๐	๒๐๐	๕๐๐	๑๐๐๐
ปริมาณข้อมูลใน ๑ วินาที (MB)	๐.๑๒	๓.๕๘	๕.๙๖	๑๑.๙๒	๒๓.๘๔	๕๙.๖๐	๑๑๙.๒๑
ปริมาณข้อมูลใน ๑ นาที (MB)	๗.๑๕	๒๑๔.๕๘	๓๕๗.๖๓	๗๑๕.๒๖	๑๔๓๐.๕๑	๓๕๗๖.๒๘	๗๑๕๒.๕๖
ปริมาณข้อมูลใน ๑ ชั่วโมง (GB)	๐.๔๒	๑๒.๕๗	๒๐.๙๕	๔๑.๙๑	๘๓.๘๒	๒๐๙.๕๕	๔๑๙.๑๐
ปริมาณข้อมูลใน ๑ วัน (GB)	๑๐.๐๖	๓๐๑.๗๕	๕๐๒.๙๑	๑๐๐๕.๘๓	๒๐๑๑.๖๖	๕๐๒๙.๑๔	๑๐๐๕๘.๒๘
ปริมาณข้อมูลใน ๑ เดือน (๓๐ วัน) (TB)	๐.๒๙	๘.๘๔	๑๔.๗๓	๒๙.๔๗	๕๘.๙๔	๑๔๗.๓๔	๒๙๔.๖๘
ปริมาณข้อมูลใน ๓ เดือน (๙๐ วัน) (TB)	๐.๘๘	๒๖.๕๒	๔๔.๒๐	๘๘.๔๐	๑๗๖.๘๑	๔๔๒.๐๑	๘๘๔.๐๓
ปริมาณข้อมูลใน ๑ ปี (๓๖๕ วัน) (TB)	๓.๕๙	๑๐๗.๕๖	๑๗๙.๒๖	๓๕๘.๕๒	๗๑๗.๐๕	๑๗๙๒.๖๑	๓๕๘๕.๒๓
ปริมาณข้อมูลใน ๒ ปี (๗๓๐ วัน) (TB)	๗.๑๗	๒๑๕.๑๑	๓๕๘.๕๒	๗๑๗.๐๕	๑๔๓๔.๐๙	๓๕๘๕.๒๓	๗๑๗๐.๔๖
ประมาณการข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บ (คิดที่ร้อยละ ๑๐ ของปริมาณข้อมูลใน ๙๐, ๓๖๕, ๗๓๐ วัน)							
ข้อมูลจราจรทางคอมพิวเตอร์ ๙๐ วัน (TB)	๐.๐๙	๒.๖๕	๔.๔๒	๘.๘๔	๑๗.๖๘	๔๔.๒๐	๘๘.๔๐
ข้อมูลจราจรทางคอมพิวเตอร์ ๓๖๕ วัน (TB)	๐.๓๖	๑๐.๗๖	๑๗.๙๓	๓๕.๘๕	๗๑.๗๐	๑๗๙.๒๖	๓๕๘.๕๒
ข้อมูลจราจรทางคอมพิวเตอร์ ๗๓๐ วัน (TB)	๐.๗๒	๒๑.๕๑	๓๕.๘๕	๗๑.๗๐	๑๔๓.๔๑	๓๕๘.๕๒	๗๑๗.๐๕
ประมาณการข้อมูลจราจรทางคอมพิวเตอร์ (ปีปกติ ๑๕ เท่า) ที่จัดเก็บ (คิดที่ร้อยละ ๑๐ ของปริมาณข้อมูลใน ๙๐, ๓๖๕, ๗๓๐ วัน)							
ข้อมูลจราจรทางคอมพิวเตอร์ ๙๐ วัน (TB)	๐.๐๑	๐.๑๘	๐.๒๙	๐.๕๙	๑.๑๘	๒.๙๕	๕.๘๙
ข้อมูลจราจรทางคอมพิวเตอร์ ๓๖๕ วัน (TB)	๐.๐๒	๐.๗๒	๑.๒๐	๒.๓๙	๔.๗๘	๑๑.๙๕	๒๓.๙๐
ข้อมูลจราจรทางคอมพิวเตอร์ ๗๓๐ วัน (TB)	๐.๐๕	๑.๔๓	๒.๓๙	๔.๗๘	๙.๕๖	๒๓.๙๐	๔๗.๘๐

หมายเหตุ ค่าปริมาณการใช้ข้อมูลสูงสุดเป็นค่าที่เกิดจากคำนวณโดย ประมาณการจากสมมติฐานว่า การส่งผ่านข้อมูลมีประสิทธิภาพสูงสุด (utilization 100%) โดยไม่คิดค่า overhead และค่าการสูญเสียต่าง ๆ

จากข้อมูลในตารางจะเห็นได้ว่าในองค์กรที่มีความเร็วในการเชื่อมต่ออินเทอร์เน็ตไม่สูง จำนวนผู้ใช้งานน้อย ปริมาณพื้นที่การเก็บข้อมูลจะมีขนาดเล็กเมื่อเทียบกับราคาอุปกรณ์เก็บข้อมูลในปัจจุบัน (ความเร็วอินเทอร์เน็ต 30 Mbps หากคิดที่ร้อยละ ๑๐ ของปริมาณที่จัดเก็บข้อมูลภายใน ๙๐ วัน จะต้องใช้พื้นที่เก็บข้อมูล 2.65 TB)

๓.๑.๓.๒ การคำนวณโดยผลรวมของค่าเฉลี่ยจากข้อมูลจราจรทางคอมพิวเตอร์เดิม

การคำนวณแบบนี้เป็นแบบที่ละเอียดมากกว่าแบบแรก เหมาะสำหรับองค์กรที่มีความซับซ้อนมากขึ้น และแบบนี้อาจต้องมีการจัดทำบัญชีรายชื่อ ระบบให้บริการหรือเครื่องให้บริการที่จำเป็นต้องมีการเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้แล้ว โดยการคำนวณสามารถทำได้ดังนี้

- (๑) คำนวณหาค่าของปริมาณข้อมูลจราจรทางคอมพิวเตอร์ในแต่ละบริการ ซึ่งโดยปกติแล้วบริการโดยทั่วไปจะมีการเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ที่เครื่องให้บริการนั้น ๆ และทำซ้ำในทุกรายการในบัญชีรายชื่อ
- (๒) ในกรณีที่มีการเก็บข้อมูลจราจรทางคอมพิวเตอร์ในแต่ละบริการไว้มากกว่า ๑ วัน เช่น ๑ สัปดาห์ ให้คำนวณเป็นค่าเฉลี่ยแทน
- (๓) คำนวณผลรวมของปริมาณข้อมูลทั้งหมดในทุกบริการในช่วงเวลา ๑ วัน คูณด้วยจำนวนวันที่ต้องการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (เช่น คูณด้วย ๙๐ วัน)
- (๔) ในกรณีที่ไม่สามารถคำนวณหรือตรวจสอบจากข้อมูลจราจรทางคอมพิวเตอร์ได้ในทุกบริการ ให้คำนวณ โดยใช้ปริมาณข้อมูลจราจรทางคอมพิวเตอร์จากเครื่องให้บริการที่มีปริมาณมาก

ที่สุดแทน

- (๕) ในกรณีที่ต้องการข้อมูลโดยหายาที่สุด ให้ใช้วิธีตรวจสอบค่าของปริมาณข้อมูลจราจรทางคอมพิวเตอร์จากเครื่องให้บริการที่คาดว่าจะมีการใช้งานมากที่สุดเป็นตัวตั้งแล้วคูณด้วยจำนวนเครื่องให้บริการแทน แล้วคูณด้วยจำนวนวันที่ต้องการทราบขนาดของหน่วยบันทึกข้อมูลแทน

สรุป

ขนาดของพื้นที่เก็บข้อมูลจราจร	=	ผลรวมของปริมาณข้อมูลทั้งหมดในทุกบริการในช่วงเวลา ๑ วัน x จำนวนวันที่ต้องการทราบ
-------------------------------	---	--

หรือ

ขนาดของพื้นที่เก็บข้อมูลจราจร	=	ปริมาณข้อมูลของเครื่องให้บริการที่มีการใช้งานมากที่สุด x จำนวนเครื่องให้บริการ x จำนวนวันที่ต้องการทราบ
-------------------------------	---	--

๓.๒ หลักการเก็บข้อมูลของระบบเก็บข้อมูลทางจราจรคอมพิวเตอร์

ประเภทของระบบเก็บข้อมูลจราจรทางคอมพิวเตอร์ หากแบ่งตามหลักการจัดเก็บข้อมูลจากระบบให้บริการหรือเครื่องให้บริการ อาจแบ่งได้เป็น ๕ ประเภท

- (๑) แบบที่ใช้หลักการดักจับข้อมูลจากเครือข่าย
- (๒) แบบที่ทำหน้าเป็นเกตเวย์ (gateway) หลักของระบบ
- (๓) แบบที่ใช้โปรแกรมติดตั้งที่ตัวเครื่องให้บริการ เพื่อเก็บข้อมูล
- (๔) แบบที่รองรับการส่งข้อมูลจากเกณฑ์วิธีการสื่อสาร syslog (syslog protocol)
- (๕) แบบผสม

๓.๒.๑ แบบที่ ๑ อุปกรณ์ที่ใช้หลักการดักจับข้อมูลจากเครือข่ายเพื่อจัดเก็บเป็นข้อมูลจราจรทางคอมพิวเตอร์

แบบนี้ใช้ลักษณะการเก็บข้อมูลโดยการดักฟังข้อมูลจราจร แล้วทำการกรองเฉพาะข้อมูลที่ตรงตามกฎ ที่ได้มีการกำหนดค่าไว้

ข้อดี

- สามารถติดตั้งได้ทุกสถานะแวดล้อมการทำงาน ติดตั้งง่าย โดยไม่มีผลกระทบต่อประสิทธิภาพของระบบเครือข่าย
- การติดตั้งสามารถทำได้หลายแบบ เช่น การทำพอร์ตมิเรอร์ (mirror porting) การใช้อุปกรณ์ฮับเน็ตเวิร์ก (hub network) เป็นตัวชั้นกลาง หรือ การแท็ปที่สายโดยตรง

ข้อเสีย

- เนื่องจากวิธีการเก็บข้อมูลด้วยวิธีนี้มีความเสี่ยงในการคัดกรองข้อมูลที่มีความอ่อนไหวทางด้านความ เป็นส่วนตัวของผู้ใช้งาน ดังนั้นการพิจารณาเลือกใช้งาน จำเป็นต้องมีการพิจารณา การออกแบบระบบในส่วนของการเก็บข้อมูล และการคัดกรองข้อมูลโดยละเอียด
- ต้องมีการทำหนังสือแจ้งหรือขอตกลงเพื่อให้พนักงานในองค์กรรับทราบ ว่ามีการบันทึกข้อมูล และให้ทำหนังสือยอมรับ

- ข้อมูลที่อนุญาตให้เก็บได้ต้องเป็นข้อมูลตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และไม่ขัดต่อข้อกำหนดภายใน พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๓.๒.๒ แบบที่ ๒ อุปกรณ์ที่ทำหน้าที่เป็นเกตเวย์ของเครือข่าย (network gateway)

อุปกรณ์แบบนี้ ใช้การเก็บข้อมูลโดยทำตัวเป็นเกตเวย์ของระบบ ข้อมูลจราจรจะถูกส่งผ่านอุปกรณ์แบบนี้ ก่อนถึงจะส่งผ่านไปที่เกตเวย์เดิมอีกครั้ง หรือบางระบบสามารถใช้ทดแทนอุปกรณ์เกตเวย์เดิมได้ และบางครั้งยังมีความสามารถอื่น ๆ เพิ่มเติมลงไปได้ด้วย เช่น การพิสูจน์ตัวตน การกรองเว็บไซต์ที่ไม่เหมาะสม การเก็บข้อมูลการใช้งานเครือข่าย

ข้อดี

- สามารถประยุกต์ใช้ด้านอื่นได้นอกจากเก็บข้อมูลจราจรทางคอมพิวเตอร์ (ขึ้นอยู่กับความสามารถของแต่ละระบบ)

ข้อเสีย

- ในการติดตั้งมีการกระทบกับระบบเครือข่ายเดิม ทั้งในด้านโครงสร้างและในด้านประสิทธิภาพ
- การออกแบบการเก็บข้อมูลโดยไม่เก็บข้อมูลที่กระทบต่อข้อมูลส่วนบุคคล หรือ เทคนิคเฉพาะทางของผู้ผลิต

๓.๒.๓ แบบที่ ๓ แบบที่ใช้โปรแกรมติดตั้งที่ตัวเครื่องให้บริการ

แบบนี้จะมีความทำงานโดย ต้องติดตั้งโปรแกรมที่เครื่องให้บริการหรือระบบที่ต้องการเก็บข้อมูล โดยโปรแกรมจะทำหน้าที่ส่งข้อมูลจราจรทางคอมพิวเตอร์มาให้กับ ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ได้เอง บางระบบเป็นระบบขนาดใหญ่สามารถรองรับจำนวนไคลเอนต์ (client) ได้มากและสามารถนำข้อมูลต่าง ๆ ที่ได้ มาวิเคราะห์เพื่อประโยชน์ด้านอื่น ได้

ข้อดี

- สามารถเก็บข้อมูลจราจรได้จากระบบให้บริการหรือเครื่องให้บริการได้หลายประเภท
- สามารถมีระดับความปลอดภัยที่สูงกว่าเนื่องจากการรับและส่งข้อมูลเป็นแบบรับ-ให้บริการ (client-server) หรือเป็นแบบเฉพาะที่ ผู้ผลิตสามารถออกแบบเองได้
- สามารถนำข้อมูลไปวิเคราะห์เพื่อประโยชน์ด้านอื่นได้

ข้อเสีย

- ราคาค่อนข้างสูงเนื่องจากเป็นระบบที่ต้องการพัฒนาส่วนประกอบต่าง ๆ
- ต้องเข้าไปยุ่งเกี่ยวกับระบบหรือโปรแกรมให้บริการ

๓.๒.๔ แบบที่ ๔ รองรับการส่งข้อมูลจากเครื่องให้บริการโดยตรง (syslog protocol)

ระบบแบบนี้เป็นระบบที่แพร่หลายมากที่สุด รองรับการทำงานที่หลากหลาย มีทั้งระบบที่เป็นโอเพนซอร์ส (open source) สามารถนำไปปฏิบัติ (implement) เองได้ จนถึงระดับวิสาหกิจ (enterprise) ทำงานด้วยมาตรฐาน syslog โดยส่วนมาก โปรแกรมหรือเครื่องให้บริการต่าง ๆ มักรองรับการส่งข้อมูลจราจรทางคอมพิวเตอร์ด้วยมาตรฐานนี้

ข้อดี

- สามารถเก็บข้อมูลจราจรได้ทันทีจากระบบให้บริการหรือเครื่องให้บริการที่รองรับการเก็บข้อมูลแบบ syslog protocol
- ราคาไม่สูงเนื่องจากตัวแกนหลักเป็นโอเพนซอร์ส
- สามารถนำข้อมูลไปวิเคราะห์เพื่อประโยชน์ด้านอื่นได้

ข้อเสีย

- โดยมาตรฐานของ syslog เองไม่รองรับการเข้ารหัสข้อมูล แต่ผู้ใช้งานสามารถเลือกอุปกรณ์ที่รองรับการใช้งานร่วมกับ SSL (secure socket layer) หรือเลือกใช้งานโปรโตคอลที่เทียบเท่ากับ syslog เช่น rsyslog ที่รองรับการส่งข้อมูลแบบเข้ารหัส SSL ได้ทันที

๓.๒.๕ แบบผสม

แบบผสมเป็นแบบที่มีมากที่สุดในท้องตลาด เนื่องจากปัจจุบันการเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยวิธีแบบใดแบบหนึ่งมักไม่ครอบคลุมโปรแกรมให้บริการหรือเครื่องให้บริการทั้งหมด จึงจำเป็นต้องใช้เทคนิคและวิธีการหลายแบบเพื่อให้ครอบคลุม

ข้อดีและข้อเสียของระบบก็จะขึ้นอยู่กับชนิดหรือวิธีที่เลือกใช้ในแต่ละแบบที่ผู้ผลิตเลือก

ข้อดี

- รวมความสามารถของระบบแบบต่าง ๆ ไว้ด้วยกัน

ข้อเสีย

- มีความซับซ้อนในการใช้เนื่องจากมีกรรมวิธีในการเก็บข้อมูลหลายแบบ
- ผู้ใช้งานต้องเป็นผู้เลือกวิธีที่เหมาะสม

๔. แนวทางการจัดทำ

๔.๑ แนวทางการปฏิบัติตามคุณลักษณะและข้อกำหนดต่าง ๆ ตามมาตรฐานเล่มที่ ๑

มาตรฐานเล่มที่ ๑ กำหนดคุณลักษณะและข้อกำหนด เพื่อให้ระบบทำงานได้อย่างถูกต้อง มั่นคงปลอดภัย และเป็นไปตามกฎหมาย โดยคุณสมบัติหรือข้อกำหนดต่าง ๆ อ้างอิงหลักการของมาตรฐาน ISO/IEC 27002 ซึ่งเป็นมาตรฐานของระบบการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ที่ได้มีการประยุกต์เพื่อให้มีความเหมาะสมกับ ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ความเข้มงวดของข้อกำหนดในแต่ละข้อขึ้นอยู่กับความสามารถของระบบ ขนาด และสภาพแวดล้อมการทำงานของระบบที่ต่างกันมาตรฐานต่าง ๆ อาจจำเป็นต้องมีการเพิ่มความเข้มงวด หรือไม่จำเป็นต้องใช้

คุณลักษณะและข้อกำหนดตาม**มาตรฐานเล่มที่ ๑** ไม่ได้กำหนดรายละเอียดทางด้านเทคนิคในเชิงลึก เพื่อให้ผู้จัดทำระบบสามารถเลือกใช้มาตรการที่เหมาะสมกับระบบที่พัฒนาขึ้น และเพื่อให้สะดวกต่อการจัดทำระบบหรือการปฏิบัติตาม ข้อกำหนดของเอกสารนี้ เป็นการสรุปข้อกำหนดของ**มาตรฐานเล่มที่ ๑** เป็น หมวดหมู่ โดยอ้างอิงตามมาตรฐาน ISO/IEC 27002 พร้อมยกตัวอย่างแนวทางการปฏิบัติประกอบเพื่อความเข้าใจมากยิ่งขึ้น ดังรายละเอียดดังต่อไปนี้

๔.๑.๑ หมวด : คุณลักษณะทั่วไป

๔.๑.๑.๑ **ข้อกำหนด:** การแบ่งกลุ่มผู้ใช้งาน เช่น **ผู้ดูแลข้อมูล ผู้ดูแลระบบ** ผู้ใช้งานทั่วไป และการจัดการสิทธิ์

วัตถุประสงค์: เพื่อให้สามารถกำหนดกลุ่มผู้ใช้งาน ซึ่งมีหน้าที่ที่แตกต่างกันออกไป ระบบจำเป็นต้องมีการแบ่งแยกกลุ่มของผู้ใช้งานตามสิทธิ์ที่ได้รับ เช่น

- **ผู้ดูแลข้อมูล** สามารถเข้าถึงข้อมูลได้ แต่จะไม่มี สิทธิ์แก้ไข ดัดแปลง ลบ หรือทำลายข้อมูล
- **ผู้ดูแลระบบ** สามารถจัดการ เพิ่มลบ รายชื่อ ในระบบหรือเครื่องที่ทำการเก็บข้อมูลได้ แต่ไม่สามารถเข้าถึงข้อมูลได้

แนวทางการปฏิบัติ

- การจัดทำระบบลงทะเบียนผู้ใช้งาน เพื่อแยกกลุ่มผู้ใช้งานและระบุตัวตนผู้ใช้งานว่าเป็นบุคคลใด
- การป้องกันการลงทะเบียนผู้ใช้งานที่ซ้ำซ้อนกัน
- การป้องกันการถือครองสิทธิ์ของผู้ใช้งานมากกว่า ๑ กลุ่มผู้ใช้งาน
- การจำกัดจำนวน**ผู้ดูแลข้อมูลและผู้ดูแลระบบ**ให้น้อยที่สุด

๔.๑.๑.๒ **ข้อกำหนด:** การจัดการและควบคุมสิทธิ์ ของกลุ่มผู้ใช้งานและผู้ใช้งานในกลุ่มต่าง ๆ

วัตถุประสงค์: เพื่อให้สามารถควบคุมและจัดการสิทธิ์ ของกลุ่มผู้ใช้งานและผู้ใช้งานในกลุ่มต่าง ๆ ระบบจำเป็นต้องมีการควบคุมสิทธิ์ของกลุ่มของผู้ใช้งานตามสิทธิ์ที่ได้รับ

แนวทางการปฏิบัติ

- การเลือกใช้งานระบบพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย
- การจัดการชั้นความลับของข้อมูล
- การเข้ารหัสข้อมูลที่มีชั้นความลับ เพื่อป้องกันการเข้าถึง

๔.๑.๒ หมวด : คู่มือและข้อแนะนำ

๔.๑.๒.๑ **ข้อกำหนด:** การระบุข้อมูลต่าง ๆ ที่จำเป็นสำหรับการใช้งานระบบ

วัตถุประสงค์: เพื่อให้ผู้ใช้งาน **ผู้ดูแลระบบ** และ**ระบบ**สามารถทำงานได้อย่างถูกต้อง ผู้ผลิตจำเป็นต้อง สร้างเอกสาร คู่มือ หรือ เอกสารการแนะนำวิธีติดตั้ง การใช้งาน การเตรียมการต่าง ๆ เบื้องต้น ทั้งนี้รวมถึง การแก้ไขปัญหาเบื้องต้น ที่เกิดจากการใช้งาน และข้อมูลรายละเอียดที่เกี่ยวกับการแฮช (hash)

ตัวอย่างการดำเนินการ

- เอกสารแนะนำระบบ ความต้องการของระบบ สภาพแวดล้อมการทำงาน ความสามารถ ข้อ จำกัดต่าง ๆ ของ**ระบบ**
- เอกสารคู่มือ การเริ่มการใช้งานอย่างย่อ (quick start) การเตรียมการเบื้องต้น วิธีติดตั้ง การแก้ไขปัญหาเบื้องต้น
- เอกสารคู่มือ แนะนำการเตรียมการ การเลือกและกำหนดพื้นที่ติดตั้ง วิธีติดตั้งซึ่งรวมถึงรูปแบบและวิธีการเชื่อมต่อกับคอมพิวเตอร์เครื่องอื่น การใช้งาน การปรับตั้งค่าต่าง ๆ

การตรวจสอบและการแก้ไขปัญหา ข้อมูลรายละเอียดที่เกี่ยวกับการแฮช และข้อมูลอื่น
ที่จำเป็น โดยละเอียด

๔.๑.๒.๒ **ข้อกำหนด:** เอกสารคู่มือและข้อแนะนำการใช้งาน ต้องจัดทำเป็นภาษาไทย สำหรับคู่มือหรือ
ข้อแนะนำเพิ่มเติมอื่น ที่ใช้ประกอบเพื่อเป็นข้อมูล อนุญาตให้ใช้ภาษาอื่นได้หากไม่เป็นการเพิ่ม
ความเสี่ยงในการใช้งานปกติ

วัตถุประสงค์: เพื่อการสื่อความหมายที่ตรงกัน และสามารถครอบคลุมผู้ใช้งานได้ทุกกลุ่มผู้ใช้งาน
ตัวอย่างการดำเนินการ

- จัดทำเอกสารต่าง ๆ เป็นภาษาไทย

๔.๑.๓ หมวด : การแสดงเครื่องหมายและฉลาก

๔.๑.๓.๑ **ข้อกำหนด:** การแสดงเครื่องหมายหรือข้อความบนเปลือกหุ้มด้านนอกของบรรจุภัณฑ์ และบน
เปลือกหุ้มของบริภัณฑ์หรือระบบ ในลักษณะที่สามารถเห็นได้ง่ายและชัดเจน ประกอบข้อมูลอย่าง
น้อย ดังนี้

- ชื่อแบบรุ่น และชื่อผู้ทำ
- ประเภทของข้อมูลจราจรทางคอมพิวเตอร์ ที่จัดเก็บได้
- คุณสมบัติพื้นฐานที่มีให้ หรือคุณลักษณะพื้นฐานที่ต้องการ ด้านการประมวลผลของระบบ
ได้แก่ แบบรุ่นของหน่วยประมวลผล ขนาดของหน่วยความจำ
- ความสามารถในการจัดเก็บข้อมูล หรือขนาดความจุของฮาร์ดดิสก์หรือสื่ออื่น ๆ ที่ต้องการ

วัตถุประสงค์: เพื่อประโยชน์ในการเลือกใช้งาน ความมั่นใจในการตัดสินใจเลือกระบบที่เหมาะสม
ของผู้ใช้งาน และการแสดงคุณสมบัติ ความสามารถ ชัดความสามารถในการขยายต่อเพิ่ม ของ
บริภัณฑ์หรือระบบ

ตัวอย่างการดำเนินการ

- การจัดทำฉลากระบุข้อมูลที่จำเป็น เช่น

รายละเอียดคุณลักษณะเฉพาะ (detail specification)
ชื่อผลิตภัณฑ์ (product name): ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ แม่นยำ
ชื่อรุ่น (model): เทียงตรง
ประเภทข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บได้ (log category): ตาม พ.ร.บ. ๕(๑) ข และ ค
ข้อมูลจราจรทางคอมพิวเตอร์ที่รองรับ (log support): Syslog , Apache , IIS , MS Windows Event
log เป็นต้น
รายละเอียดฮาร์ดแวร์ (hardware detail)
หน่วยประมวลผล (CPU): ซีพียูสโตร์ 2.4 GHz
หน่วยความจำ (RAM): 2 GB
ฮาร์ดดิสก์ไดรว (HDD): 500 GB

๔.๑.๓.๒ **ข้อกำหนด:** เครื่องหมายหรือข้อความ บนเปลือกหุ้มด้านนอกของบรรจุภัณฑ์ และบนเปลือกหุ้ม
ของบริภัณฑ์ ต้องมีความคงทนต่อการใช้งานตามปกติ และอ่านเข้าใจได้ง่าย

วัตถุประสงค์: เพื่อความสะดวกและคงทนต่อการใช้งานของเครื่องหมายและข้อความ

ตัวอย่างการดำเนินการ

- จัดทำเครื่องหมายหรือข้อความด้วยวัสดุที่คงทน เช่น วัสดุโลหะ
- วัสดุควรยึดติดกับอุปกรณ์ ด้วยอุปกรณ์ที่แข็งแรงไม่หลุดหรือลอกได้ง่าย
- เลือกใช้การพิมพ์ข้อความที่มีความชัดเจนไม่ลบหรือเลือนได้เมื่อโดนน้ำ (กันน้ำได้)

๔.๑.๓.๓ ข้อกำหนด: ระบบต้องแสดงข้อมูลต่อไปนี้ในเอกสารข้อเสนอแนะการติดตั้งระบบ

- ประเภทของข้อมูลจราจรที่จัดเก็บได้ รวมถึงรายละเอียดที่เกี่ยวข้องกัน อาทิ ชื่อและรุ่นของซอฟต์แวร์ประยุกต์ ชื่อและรุ่นของอุปกรณ์หรือบริการหรือระบบต้นทางใด ๆ ที่เป็นแหล่งกำเนิดข้อมูลจราจรทางคอมพิวเตอร์
- คุณลักษณะพื้นฐานที่มีให้ หรือคุณลักษณะพื้นฐานที่ต้องการ ด้านการประมวลผลของระบบ ได้แก่ แบบรุ่นของหน่วยประมวลผล ขนาดของหน่วยความจำ
- ความสามารถในการจัดเก็บข้อมูลที่มีให้ หรือวิธีการคำนวณความสามารถในการจัดเก็บ
- จำนวนผู้ใช้งานสูงสุด และจำนวนเหตุการณ์สูงสุดต่อหน่วยเวลา ที่สามารถรองรับได้
- ความสามารถสูงสุด ที่สามารถขยาย หรือเพิ่มเติมได้ (ถ้ามี)

คำอธิบาย/วัตถุประสงค์: เพื่อให้ผู้ใช้งานสามารถเลือกระบบที่เหมาะสมกับองค์กรหรือหน่วยงาน ผู้ผลิตจำเป็นต้องระบุข้อมูลความสามารถของเครื่อง ตามรายละเอียดที่ข้อกำหนดบังคับ

- ประเภทของข้อมูลจราจรที่จัดเก็บได้ รวมถึงรายละเอียดที่เกี่ยวข้องกัน อาทิ ชื่อและรุ่นของซอฟต์แวร์ประยุกต์ ชื่อและรุ่นของอุปกรณ์หรือบริการหรือระบบต้นทางใด ๆ ที่เป็นแหล่งกำเนิดข้อมูลจราจรทางคอมพิวเตอร์
- ข้อกำหนดนี้ใช้เพื่ออ้างอิงความสามารถในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ตามประเภทของผู้ให้บริการและประเภทของข้อมูลที่ทำกรจัดเก็บ
- คุณลักษณะพื้นฐานที่มีให้ หรือคุณลักษณะพื้นฐานที่ต้องการ ด้านการประมวลผลของระบบ ได้แก่ แบบรุ่นของหน่วยประมวลผล ขนาดของหน่วยความจำ
- ความสามารถในการจัดเก็บข้อมูลที่มีให้ หรือวิธีการคำนวณความสามารถในการจัดเก็บ
- จำนวนผู้ใช้งานสูงสุด และจำนวนเหตุการณ์สูงสุดต่อหน่วยเวลา ที่สามารถรองรับได้
- ความสามารถสูงสุด ที่สามารถขยาย หรือเพิ่มเติมได้ (ถ้ามี)

ข้อกำหนดนี้ใช้เพื่ออ้างอิงความสามารถของระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ความสามารถของฮาร์ดแวร์ ความสามารถในการขยายขีดความสามารถ และความสามารถอื่นๆ ที่ผู้ผลิตต้องการแสดงให้ผู้ใช้งานทราบ

ตัวอย่างการดำเนินการ

ตัวอย่างของข้อความระบุรายละเอียด ประเภท ของข้อมูลจราจรที่จัดเก็บได้ รวมถึงรายละเอียดที่เกี่ยวข้องกัน

ระบบ ก. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ในประเภทต่อไปนี้ได้ และจัดเก็บได้จาก อุปกรณ์และซอฟต์แวร์ ดังต่อไปนี้

ประเภท ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย

๑. พร็อกซีเซิร์ฟเวอร์ squid และ พร็อกซีเซิร์ฟเวอร์ bluecode
๒. อุปกรณ์ที่รองรับการจัดเก็บข้อมูลโดยมาตรฐาน syslog

ประเภท ง. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ

๑. เว็บเซิร์ฟเวอร์ Apache
๒. เว็บเซิร์ฟเวอร์ Microsoft IIS
๓. อุปกรณ์ที่รองรับการจัดเก็บข้อมูลโดยมาตรฐาน syslog

๔.๑.๔ หมวด : ข้อกำหนดของระบบ

๔.๑.๔.๑ ข้อกำหนด: ระบบต้องสามารถเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามประเภทและความสามารถที่ระบุไว้ และต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ได้ต่อเนื่องเป็นเวลาไม่น้อยกว่า ๙๐ วัน

คำอธิบาย/วัตถุประสงค์: การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ไว้ได้ต่อเนื่องเป็นเวลา ๙๐ วัน ถือเป็นข้อบังคับในทางกฎหมาย ทั้งนี้การตรวจสอบไม่สามารถทำได้โดยตรง ขึ้นอยู่กับจำนวนของเครื่องต้นทางที่เป็นแหล่งกำเนิดข้อมูลจราจรทางคอมพิวเตอร์ อย่างไรก็ตาม ข้อกำหนดนี้ไม่สามารถละทิ้งได้ การตรวจสอบจึงอาจทำได้โดยอ้อมดังรายละเอียดบางส่วนตามตัวอย่าง

ตัวอย่างการดำเนินการ

- ระบบต้องรองรับการขยายหน่วยความจำสำหรับบันทึกข้อมูลจราจร เพื่อให้สามารถรองรับการเก็บข้อมูลจราจรได้ ๙๐ วันในสภาวะแวดล้อมใช้งานที่แตกต่างกัน
- ผู้ผลิตทำการประเมินการทำงานเบื้องต้นในสภาวะต่าง ๆ ของระบบ และกำหนดค่าสภาวะแวดล้อมต่างๆ เป็นตัวอย่างเพื่อให้ผู้ใช้งานได้เลือกใช้

๔.๑.๔.๒ ข้อกำหนด: ระบบต้องสามารถปรับตั้งนาฬิกาภายใน ให้ตรงกับเวลาอ้างอิงมาตรฐานระดับชาติ ได้โดยอัตโนมัติ และมีการกำหนดความถี่ในการปรับตั้งค่าอัตโนมัติ โดยพิจารณาจากข้อมูลแวดล้อมที่เกี่ยวข้อง อาทิ ความเสถียรของระบบ

คำอธิบาย/วัตถุประสงค์: เพื่อให้ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ มีเวลาที่ตรงกับมาตรฐานสากลและสามารถใช้อ้างอิงในการวิเคราะห์เหตุการณ์ต่างได้ถูกต้อง

หมายเหตุ	รายชื่อหน่วยงานและเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลาอ้างอิงมาตรฐานระดับชาติ ได้แก่ สถาบันมาตรวิทยาแห่งชาติ ได้แก่ time1.nimt.or.th (203.185.69.60) time2.nimt.or.th (203.185.69.59) time3.nimt.or.th (203.185.69.56) กรมอุทกศาสตร์ กองทัพเรือ ได้แก่ time.navy.mi.th (113.53.247.3) ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ได้แก่ clock.nectec.or.th (203.185.57.115)
-----------------	---

ตัวอย่างการดำเนินการ

- ระบบใช้โพรโทคอล NTP (Network Time Protocol) ในการปรับตั้งค่ากับเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลาอ้างอิงมาตรฐานระดับชาติ

๔.๑.๔.๓ **ข้อกำหนด:** ระบบต้องมีการกำหนดการป้องกันการเข้าถึงระบบโดยผู้ไม่ได้รับอนุญาต ทั้งทางกายภาพและทางอิเล็กทรอนิกส์อย่างเหมาะสม ทั้งนี้อาจหมายรวมถึงข้อแนะนำต่าง ๆ ที่เกี่ยวข้อง โดยอย่างน้อยวิธีใดวิธีหนึ่ง หรือรวมกันต่อไปนี้

- การใช้รหัสผ่านหรือการยืนยันตัวบุคคลหรือวิธีการอื่นที่คล้ายกัน
- การจำกัดรูปแบบและวิธีการเข้าถึง
- การจำกัดจำนวนผู้^๗ใช้
- การจำกัดเวลาการใช้
- การกำหนดช่วงเวลาที่ยอนุญาต
- การกำหนดใช้นโยบายและเทคนิคด้านความมั่นคงปลอดภัยอื่น

หากระบบอนุญาตให้เข้าถึงระยะไกลได้ (remote access) โดยผ่านระบบคอมพิวเตอร์ที่ต่อเชื่อมถึงกันโดยโครงข่าย ภายในองค์กรหรือโครงข่ายสาธารณะ อาจจำเป็นต้องมีมาตรการด้านความมั่นคงปลอดภัย เพิ่มเติมจากที่ระบุไว้ข้างต้น อาทิ

- การใช้เทคนิคการเข้ารหัสข้อมูล
- การจำกัดสิทธิ หรือยกเลิกสิทธิบางประการ
- การกำหนดรูปแบบ หรือเทคนิคการเข้าถึงแบบเฉพาะ

คำอธิบาย/วัตถุประสงค์: เพื่อป้องกันการเข้าถึงระบบโดยผู้ไม่ได้รับอนุญาต ทั้งทางกายภาพและทางอิเล็กทรอนิกส์ ทั้งนี้ระบบอาจจำเป็นต้องใช้กลไกหรือวิธีมากกว่าหนึ่งวิธี เพื่อให้ระบบสามารถป้องกันการเข้าถึงได้อย่างเหมาะสม ที่สภาพแวดล้อมการใช้งาน หรือความสามารถของระบบที่แตกต่างกัน

ตัวอย่างการดำเนินการ

- การใช้รหัสผ่านเพื่อยืนยันตัวบุคคล
- การใช้รหัสผ่านร่วมกับการใช้การพิสูจน์ตัวตนทางชีวมิติ (biometric authentication) เช่น ลายนิ้วมือ ม่านตา ใบหน้า
- การติดตั้งเครื่องไว้ในห้องที่ปิดกั้นมิดชิด มีระบบรักษาความปลอดภัยแน่นอนหนา
- การปิดกั้นฝาเครื่อง (ในกรณีที่ทำได้)
- การกำหนดเวลาใช้งานสำหรับผู้ใช้งานทั่วไป
- การใช้งานโพรโตคอลสื่อสารที่มีการเข้ารหัสในการเข้าถึงระบบจากระยะไกล เช่น HTTPS, SSH
- การสงวนสิทธิ์ในการบริการจัดการบางสิทธิ์ที่ไม่สามารถทำได้ถ้ามีการเข้าถึงจากระยะไกล (local login only)

๔.๑.๔.๔ **ข้อกำหนด:** ระบบต้องสามารถควบคุมและป้องกันการเปลี่ยนแปลงการตั้งค่าต่าง ๆ ของระบบโดยผู้^๗ใช้ได้ สำหรับการตั้งค่าที่อนุญาตให้เปลี่ยนแปลงได้ ต้องสามารถควบคุมและป้องกัน การเปลี่ยนแปลงการตั้งค่า โดยผู้^๗ใช้ที่ไม่เกี่ยวข้องได้

การเปลี่ยนแปลงการตั้งค่าใด ๆ ของระบบ และบัญชีผู้ใช้ ต้องไม่ทำให้คุณสมบัติตามข้อกำหนด ที่ต้องการของเอกสารศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาตินี้ ด้อยลง หรือเสียหาย หรือเกิดความผิดพลาดขึ้น

คำอธิบาย/วัตถุประสงค์: ข้อกำหนดนี้หมายถึง ระบบต้องมีมาตรการการควบคุมสิทธิ์ในการเข้าถึง การเปลี่ยนแปลงการตั้งค่าต่าง ๆ ของระบบโดยผู้ใช้ที่ไม่ได้รับอนุญาต หรือไม่ได้รับสิทธิ์นั้น ๆ เช่น ผู้ใช้งานทั่วไปต้องไม่สามารถเข้าถึงส่วนบริหารจัดการระบบได้ แต่บางระบบไม่ได้มีการป้องกันไว้ ทำให้ผู้ใช้งานสามารถเข้าถึงระบบบริหารจัดการได้ ยกตัวอย่างให้เห็นภาพได้ง่าย เช่น ในกรณีที่ เป็นเว็บแอปพลิเคชัน ถ้าไม่มีการบริหารจัดการช่วงเวลาสื่อสาร (session) ที่เข้มแข็งพอ อาจทำให้ ผู้ใช้บริการสาธารณะ หรือผู้ใช้งานที่ไม่มีสิทธิ์สามารถเข้าถึงหน้าระบบบริหารจัดการได้โดยไม่ต้อง พิสูจน์ตัวตน

ตัวอย่างการดำเนินการ

- ระบบจำเป็นต้องมีการออกแบบให้มีการตรวจสอบสิทธิ์ก่อนกระทำการใด ๆ เพื่อป้องกัน ปัญหาดังกล่าว
- การบริการจัดการช่วงเวลาสื่อสาร สำหรับเว็บแอปพลิเคชันที่ปลอดภัย

๔.๑.๔.๕ ข้อกำหนด: ระบบต้องสามารถระบุและจำแนกตัวบุคคล และบันทึกประวัติการเข้าถึง และใช้งาน ระบบได้ รวมถึงต้องสามารถป้องกันการแก้ไข เปลี่ยนแปลง การปลอมแปลงข้อมูล ที่เกี่ยวข้องเพื่อ การเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาตได้ เทคนิคและวิธีที่ใช้ ในการระบุตัวบุคคลและ ป้องกันการเปลี่ยนแปลง ควรเป็นเทคนิคที่ผ่านการถูกตรวจสอบยืนยันความใช้ได้แล้ว

คำอธิบาย/วัตถุประสงค์:

- เพื่อให้ทำการตรวจสอบย้อนหลังหรือตรวจสอบพฤติกรรมของผู้ใช้งานและ **ผู้ดูแลระบบ**ได้ ระบบจำเป็นต้องมีการจำแนกตัวบุคคลและบันทึกประวัติการเข้าถึงและใช้งานระบบไว้

ตัวอย่างการดำเนินการ

- จัดให้มีการจำแนกตัวบุคคล และบันทึกประวัติการเข้าถึงและใช้งานระบบ

๔.๑.๔.๖ ข้อกำหนด: ระบบควรมีการตรวจสอบความใช้ได้ของข้อมูลอื่น ที่ไม่ใช่ข้อมูลจราจรทาง คอมพิวเตอร์ ที่รับเข้าสู่ระบบ (input validation)

คำอธิบาย/วัตถุประสงค์:

- การโจมตีระบบโดยการส่งข้อมูลอื่นที่ไม่ใช่ข้อมูลจราจรหรือข้อมูลที่ถูกต้องของระบบมีผล ทำให้ระบบสูญเสียความปลอดภัยและอาจทำให้ระบบทำงานผิดพลาดได้

ตัวอย่างการดำเนินการ

- จัดระบบให้มีการตรวจสอบข้อมูลนำเข้า (input validation) โดยเฉพาะอย่างยิ่งในระบบที่มี ช่องทางการเข้าใช้งานผ่านระบบเว็บแอปพลิเคชัน

๔.๑.๔.๗ ข้อกำหนด: ระบบควรจัดให้มีคำอธิบายเพื่อให้ความช่วยเหลือ (help) ในการแก้ไขปัญหา และ ข้อบกพร่องต่าง ๆ ที่มักเกิดขึ้น อย่างเหมาะสมและเพียงพอ

คำอธิบาย/วัตถุประสงค์:

- การแสดงข้อมูลช่วยเหลือ ช่วยลดปัญหาที่จะเกิดในการใช้งานระบบและช่วยอำนวยความสะดวกแก่ผู้ใช้งาน ลดการเกิดข้อผิดพลาดในการทำงาน

ตัวอย่างการดำเนินการ

- จัดทำเมนูให้ความช่วยเหลือในหน้าต่างหลักของโปรแกรม
- จัดทำ tip of the day เมื่อเริ่มต้นใช้งานโปรแกรม
- จัดทำเมนูการใช้งานแบบ wizard เพื่อให้ผู้ใช้งานใหม่สามารถใช้งานได้ง่าย

๔.๑.๕ หมวด: การรับและเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

- ๔.๑.๕.๑ **ข้อกำหนด:** ระบบต้องสามารถรับข้อมูลจราจรทางคอมพิวเตอร์ จากอุปกรณ์ บริการหรือ ระบบต้นทาง ตามที่ระบุได้ อย่างครบถ้วน ถูกต้อง และหากเป็นไปได้ระบบควรมีระบบตรวจสอบ และปฏิเสธข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลอื่นที่ส่งมาจากระบบต้นทาง ที่ไม่ถูกต้องหรือผิดปกติ

คำอธิบาย/วัตถุประสงค์:

- การตรวจสอบข้อมูลที่ได้รับจากอุปกรณ์ต้นทาง นั้นมีผลโดยตรงต่อความถูกต้องของข้อมูลจราจรทางคอมพิวเตอร์ หากไม่มีมาตรการการตรวจสอบ ไม่อาจทำให้ทราบได้ว่าข้อมูลที่ถูกส่งจากต้นทางมีความถูกต้องสมบูรณ์หรือไม่
- การตรวจสอบและปฏิเสธแหล่งต้นทางที่ส่งข้อมูลจราจรทางคอมพิวเตอร์ เป็นสิ่งที่จำเป็นมาก เนื่องจากหากไม่มีการตรวจแหล่งต้นทางอาจเกิดการปลอมแปลงข้อมูลจราจรทางคอมพิวเตอร์ได้

ตัวอย่างการดำเนินการ

- การตรวจสอบความถูกต้องของข้อมูลต้นทางและปลายทางโดยใช้ฟังก์ชันแฮช
- การกำหนดช่วงเวลาการตรวจสอบความถูกต้องที่แน่นอน เช่น รายชั่วโมงหรือรายวัน
- การควบคุมแหล่งต้นทางที่ส่งข้อมูลจราจรทางคอมพิวเตอร์โดยใช้ ไฟร์วอลล์ (firewall)
- การแยกช่องทางสื่อสารสำหรับส่งข้อมูลจราจรทางคอมพิวเตอร์โดยเฉพาะ (management network หรือ logging network)

- ๔.๑.๕.๒ **ข้อกำหนด:** ข้อมูลจราจรทางคอมพิวเตอร์ ที่รับเข้ามาในระบบต้อง

- เก็บในสื่อ (media) ที่สามารถรักษาคุณภาพของข้อมูลได้อย่างเหมาะสมและป้องกันการสูญหาย เสียหาย ถูกลบ ทำลาย แก้ไข ดัดแปลง ทั้งโดยเจตนาและไม่เจตนา
- เข้าถึงได้เฉพาะผู้ดูแลข้อมูล และไม่สามารถเข้าถึงได้โดยผู้ไม่เกี่ยวข้องหรือผู้ไม่ได้รับอนุญาต
- ถูกเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าที่ได้ระบุไว้ และต้องไม่น้อยกว่า ๙๐ วัน

คำอธิบาย/วัตถุประสงค์:

- การรักษาคุณภาพของข้อมูลเป็นเครื่องหมายที่บ่งบอกถึงความถูกต้องและความน่าเชื่อถือของข้อมูล ดังนั้นการเลือกสื่อที่ใช้บันทึกจำเป็นต้องมีการรักษาคุณภาพของข้อมูลให้เหมาะสม

- เช่นเดียวกันกับการรักษา**คุณภาพของข้อมูล** การอนุญาตให้เข้าถึงข้อมูลโดยไม่มีการป้องกันการหรือมาตรการตรวจสอบที่เหมาะสม อาจเป็นเหตุให้สูญเสียความถูกต้องและความน่าเชื่อถือของข้อมูล ทั้งที่เกิดโดยเจตนาและไม่เจตนา
- ระยะเวลาในการเก็บข้อมูลเป็นปัจจัยหนึ่งที่สำคัญ เพื่อให้เกิดประสิทธิภาพในการตรวจสอบกิจกรรมที่เกิดขึ้นจำเป็นต้องมี**ข้อมูลจราจรทางคอมพิวเตอร์**มากพอในช่วงเวลาหนึ่ง อย่างน้อยไม่ต่ำกว่า ๙๐ วัน เพื่อให้เป็นไปตามที่กฎหมายกำหนด

ตัวอย่างการดำเนินการ

- การจัดทำระบบป้องกันการเข้าถึง**ข้อมูลจราจรทางคอมพิวเตอร์** เช่น การพิสูจน์ตัวตนก่อนเข้าถึงข้อมูล การจัดชั้นความลับของข้อมูล การเข้ารหัสข้อมูลที่มีความลับ
- การเลือกใช้สื่อ ที่สามารถรักษา**คุณภาพของข้อมูล**ได้สูง เช่น การเลือกใช้ฮาร์ดดิสก์แบบเรด (RAID) การสำรองข้อมูลลงบนแผ่นซีดีหรือดีวีดีแบบบันทึกได้
- มาตรการการตรวจสอบความถูกต้องของข้อมูลโดยวิธีแฮช
- มาตรการการสำรองข้อมูลโดยสม่ำเสมอ
- มาตรการป้องกันทางกายภาพของตัวเครื่องหรือสภาพแวดล้อมที่ติดตั้งระบบ

๔.๑.๕.๓ **ข้อกำหนด:** ระบบต้องสามารถป้องกันการแก้ไข เปลี่ยนแปลง ลบ ทำลาย**ข้อมูลจราจรทางคอมพิวเตอร์** ข้อมูลการใช้งานระบบ และข้อมูลคอมพิวเตอร์อื่น ๆ ที่เกี่ยวข้อง โดย**ผู้ดูแลข้อมูล** และผู้อื่นที่ไม่เกี่ยวข้องได้ ทั้งโดยเจตนาและไม่เจตนา

คำอธิบาย/วัตถุประสงค์:

- ข้อกำหนดเหล่านี้เป็นสิ่งที่ป้องกันการสูญเสียความถูกต้องและความน่าเชื่อถือของข้อมูลและ**ตัวระบบ** เช่น กรณีวิธีการทำลายข้อมูลส่วนเกินหรือข้อมูลที่ไม่มีความจำเป็น หากไม่มีกรรมวิธีที่ถูกต้องข้อมูลเหล่านี้จะสามารถกู้คืนกลับมาได้ ส่งผลให้ผลกระทบต่อความลับของข้อมูลโดยตรง

ตัวอย่างการดำเนินการ

- การใช้มาตรการป้องกันแบบเดียวกับ**ข้อมูลจราจรทางคอมพิวเตอร์** ในข้อมูลที่เกี่ยวข้องกับระบบอื่น ๆ
- กำหนดกรรมวิธีหรือมาตรการทำลายข้อมูลที่ปลอดภัย สำหรับข้อมูลที่ไม่ได้ใช้งานหรือข้อมูลที่เกิดความจำเป็น

๔.๑.๕.๔ **ข้อกำหนด:** ระบบต้องสามารถตรวจสอบ**ข้อมูลจราจรทางคอมพิวเตอร์**ที่จัดเก็บไว้ได้ รวมถึงการจัดให้มีการเฝ้าระวัง**คุณภาพของข้อมูล**อย่างเหมาะสม

คำอธิบาย/วัตถุประสงค์:

- การรักษา**คุณภาพของข้อมูล**เป็นเครื่องหมายที่บ่งบอกถึงความถูกต้องและความน่าเชื่อถือของข้อมูล ดังนั้นระบบจำเป็นต้องมีกรรมวิธีรักษา**คุณภาพของข้อมูล**และสามารถตรวจสอบได้เองโดยผู้ใช้งานระบบ

ตัวอย่างการดำเนินการ

- การจัดทำระบบตรวจสอบ**คุณภาพของข้อมูล**โดยใช้วิธีแฮช โดยอาจมีการทำแบบอัตโนมัติตามช่วงเวลาหรือ สามารถเลือกทำได้เองจากผู้ใช้งาน

๕. แนวทางการตรวจสอบ

๕.๑ การตรวจสอบคุณลักษณะและข้อกำหนดตามมาตรฐานเล่มที่ ๑

๕.๑.๑ หมวด: คุณลักษณะทั่วไป

๕.๑.๑.๑ ข้อกำหนด: การแบ่งกลุ่มผู้ใช้งาน เช่น ผู้ดูแลข้อมูล ผู้ดูแลระบบ ผู้ใช้งานทั่วไป และการจัดการสิทธิ์

- มีผู้ดูแลระบบ หรือส่วนรับลงทะเบียนผู้ใช้ให้มีสิทธิเป็นผู้ดูแลระบบ ซึ่งมีสิทธิ์ติดตั้ง ตั้งค่า และตรวจสอบการทำงานของระบบได้
- มีผู้ดูแลข้อมูล หรือส่วนรับลงทะเบียนผู้ใช้ให้มีสิทธิเป็นผู้ดูแลข้อมูล ซึ่งมีสิทธิ์เข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ได้ ได้แก่ แสดงข้อมูลจราจรทางคอมพิวเตอร์เมื่อมีเหตุจำเป็นได้ ตรวจสอบความถูกต้องของข้อมูลได้
- ระบบต้องไม่อนุญาตให้กำหนดให้ผู้ใช้มีสิทธิเป็นทั้งผู้ดูแลระบบ และผู้ดูแลข้อมูลพร้อมกัน
- เมื่อลงทะเบียนผู้ใช้ด้วยข้อมูลที่เรียบร้อยแล้ว ระบบต้องไม่อนุญาตให้กระทำซ้ำได้
- ระบบควรมีมาตรการในการจำกัดจำนวนผู้ดูแลข้อมูลและผู้ดูแลระบบให้น้อยที่สุด

๕.๑.๑.๒ ข้อกำหนด: การจัดการและควบคุมสิทธิ์ ของกลุ่มผู้ใช้งานและผู้ใช้งานในกลุ่มต่าง ๆ

- มีการพิสูจน์ตัวตนก่อนเข้าใช้งาน เช่น การใช้ชื่อผู้ใช้ และรหัสผ่าน
- มีการเข้ารหัสข้อมูลในระหว่างการพิสูจน์ตัวตนและการใช้งาน เช่น การใช้งานผ่าน HTTPS การใช้งานผ่าน SSH หรือ VPN
- เมื่อเข้าใช้ระบบด้วยสิทธิ์ของผู้ดูแลระบบ จะไม่สามารถเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ได้ และไม่มีสิทธิในการแก้ไข ทำลายข้อมูลจราจรทางคอมพิวเตอร์ที่กำลังถูกเก็บรักษาได้
- เมื่อเข้าใช้ระบบด้วยสิทธิ์ของผู้ดูแลข้อมูล จะไม่สามารถแก้ไขการตั้งค่าต่าง ๆ ของระบบได้ และไม่สามารถแก้ไข หรือทำลายข้อมูลจราจรทางคอมพิวเตอร์ที่กำลังถูกเก็บรักษาได้

๕.๑.๒ หมวด: คู่มือและข้อแนะนำ

๕.๑.๒.๑ ข้อกำหนด: มีเอกสารคู่มือที่ระบุข้อมูลต่าง ๆ ที่จำเป็นสำหรับการใช้งานระบบ ประกอบไปด้วยรายละเอียดต่าง ๆ ดังต่อไปนี้

- แนะนำระบบ
- ความต้องการของระบบ
- สภาพแวดล้อมการทำงานที่เหมาะสม
- ความสามารถ ข้อจำกัดต่าง ๆ ของระบบ
- รูปแบบและวิธีการเชื่อมต่อกับระบบเครือข่าย อุปกรณ์ หรือคอมพิวเตอร์เครื่องอื่น ๆ

- การเตรียมการก่อนติดตั้ง
- วิธีการติดตั้ง
- การเริ่มต้นใช้งานอย่างย่อ
- การใช้งาน การปรับตั้งค่าต่าง ๆ
- การกำหนด หรือเปลี่ยนรหัสผ่าน
- วิธีการเรียกดูข้อมูล รวมทั้งวิธีการนำข้อมูลออกในกรณีที่เจ้าหน้าที่ร้องขอ
- การตรวจสอบและแก้ไขปัญหาเบื้องต้น
- ข้อมูลรายละเอียดที่เกี่ยวข้องกับการแฮช

๕.๑.๒.๒ **ข้อกำหนด:** เอกสารคู่มือและข้อแนะนำการใช้งานเป็นภาษาไทย

- เอกสารคู่มือและข้อแนะนำต่าง ๆ ต้องจัดทำเป็นภาษาไทยเพื่อทำให้เกิดการสื่อความหมายที่ตรงกัน หากมีส่วนที่เป็นภาษาอื่นต้องไม่ทำให้เกิดความเสี่ยงในการใช้งานตามปกติ

๕.๑.๓ หมวด: การแสดงเครื่องหมายและฉลาก

๕.๑.๓.๑ **ข้อกำหนด:** การแสดงเครื่องหมายหรือข้อความบนเปลือกหุ้มด้านนอกของบรรจุภัณฑ์ และบนเปลือกหุ้มของบริภัณฑ์หรือระบบ ประกอบไปด้วยข้อมูลอย่างน้อย

- ชื่อแบบรุ่น และชื่อผู้จัดทำ
- ประเภทของข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บได้
- คุณสมบัติพื้นฐานที่มีให้ หรือคุณลักษณะพื้นฐานที่ต้องการด้านการประมวลผลของระบบ ได้แก่ แบบรุ่นของหน่วยประมวลผล ขนาดของหน่วยความจำ
- ความสามารถในการจัดเก็บข้อมูล หรือขนาดความจุของฮาร์ดดิสก์หรือสื่ออื่น ๆ ที่ต้องการ

๕.๑.๓.๒ **ข้อกำหนด:** เครื่องหมายหรือข้อความ บนเปลือกหุ้มด้านนอกของบรรจุภัณฑ์ และบนเปลือกหุ้มของบริภัณฑ์ ต้องมีความคงทนต่อการใช้งานตามปกติ และอ่านเข้าใจได้ง่าย

- เครื่องหมายดังกล่าวมีความคงทนต่อน้ำ ความชื้น น้ำมันหรือคราบไขมัน ทำการทดสอบได้โดยการใช้ผ้าชุบน้ำอุ่น ๆ เป็นเวลา ๑๕ นาที และใช้ผ้าชุบน้ำมันปิโตรเลียมอุ่น ๆ เป็นเวลา ๑๕ นาที เครื่องหมายและข้อความต่าง ๆ ต้องยังสามารถแสดงได้ชัดเจน ไม่หลุดลอกหรือพังงอ
- หากวัสดุที่ใช้ทำฉลาก เป็นคนละชิ้นกับบรรจุภัณฑ์หรือเปลือกหุ้มบริภัณฑ์ ควรยึดติดกับบรรจุภัณฑ์หรือเปลือกหุ้มบริภัณฑ์ ด้วยอุปกรณ์หรือวิธีการที่แข็งแรง ไม่หลุดหรือลอกได้ง่าย

๕.๑.๓.๓ **ข้อกำหนด:** ระบบต้องแสดงข้อมูลต่อไปนี้ในเอกสารข้อแนะนำการติดตั้งระบบ

- ประเภทของข้อมูลจราจรที่จัดเก็บได้ รวมถึงรายละเอียดที่เกี่ยวข้องกัน อาทิ ชื่อและรุ่นของซอฟต์แวร์ประยุกต์ ชื่อและรุ่นของอุปกรณ์หรือบริการหรือระบบต้นทางใด ๆ ที่เป็นแหล่งกำเนิดข้อมูลจราจรทางคอมพิวเตอร์
- คุณสมบัติพื้นฐานที่มีให้ หรือคุณลักษณะพื้นฐานที่ต้องการ ด้านการประมวลผลของระบบ ได้แก่ แบบรุ่นของหน่วยประมวลผล ขนาดหน่วยความจำ

- ความสามารถในการจัดเก็บข้อมูลที่มีให้ หรือวิธีการคำนวณความสามารถในการจัดเก็บ
- จำนวนผู้ใช้งานสูงสุด และจำนวนเหตุการณ์สูงสุดต่อหน่วยเวลา ที่รองรับได้
- ความสามารถสูงสุด ที่สามารถขยาย หรือเพิ่มเติมได้ (ถ้ามี)

การตรวจสอบคือตรวจดูว่ามีข้อมูลแสดงครบถ้วนหรือไม่ เช่นตัวอย่างต่อไปนี้

ระบบ ก. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ในประเภทต่อไปนี้ได้ และจัดเก็บได้จาก อุปกรณ์และซอฟต์แวร์ ดังต่อไปนี้

ประเภท ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย

๑. พรอคซีเซิร์ฟเวอร์ squid และ พรอคซีเซิร์ฟเวอร์ bluecode
๒. อุปกรณ์ที่รองรับการจัดเก็บข้อมูลโดยมาตรฐาน syslog

ประเภท ง. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ

๑. เว็บเซิร์ฟเวอร์ Apache
๒. เว็บเซิร์ฟเวอร์ Microsoft IIS
๓. อุปกรณ์ที่รองรับการจัดเก็บข้อมูลโดยมาตรฐาน syslog

คุณสมบัติทางฮาร์ดแวร์ของระบบ

หน่วยประมวลผล: ซีพียูสแควร์ 2.4 GHz

หน่วยความจำ: 2 GB

ฮาร์ดดิสก์ไดรว: 500 GB

ความสามารถของระบบ

รองรับจำนวนเครื่องเซิร์ฟเวอร์ได้ไม่เกิน ๕ เครื่อง

รองรับอัตราการส่งข้อมูลได้สูงสุด ๑ ๐๐๐ เหตุการณ์ต่อวินาที

รองรับปริมาณข้อมูลจราจรทางคอมพิวเตอร์ได้เฉลี่ยวันละ 5.5 GB (เพื่อให้สามารถเก็บได้ถึง ๙๐ วัน)

สามารถขยายความจุฮาร์ดดิสก์เพื่อให้เก็บข้อมูลจราจรทางคอมพิวเตอร์เพิ่มขึ้นได้อีก ๑ ตัว ความจุสูงสุด 2 TB

๕.๑.๔ หมวด: ข้อกำหนดของระบบ

๕.๑.๔.๑ **ข้อกำหนด:** ระบบต้องสามารถเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามประเภทและความสามารถที่ระบุไว้ และต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ได้ต่อเนื่องเป็นเวลาไม่น้อยกว่า ๙๐ วัน เนื่องจากไม่มีวิธีการที่จะบอกได้ว่าระบบจะเก็บข้อมูลได้ครบ ๙๐ วันได้โดยตรง จำเป็นต้องตรวจสอบด้วยวิธีโดยอ้อมดังนี้

- ระบบต้องมีเอกสารที่บ่งบอกถึงความสามารถในการจัดเก็บ ข้อจำกัดต่าง ๆ สถานการณ์หรือสภาวะแวดล้อมต่าง ๆ เพื่อให้สามารถเลือกใช้ได้ตรงตามความต้องการ
- การตรวจสอบว่าระบบนั้นเหมาะสมกับการใช้ในองค์กรหรือไม่ ควรทำการประเมินองค์การตามข้อ ๓.๑.๓ การวิเคราะห์ปริมาณข้อมูลจราจรทางคอมพิวเตอร์ที่ต้องทำการจัดเก็บเบื้องต้น โดยอาจจะประเมินเผื่อถึงการใช้งานในอนาคตซึ่งอาจจะมีการใช้งานมากขึ้น จากนั้นนำผลที่ได้มาเปรียบเทียบกับคุณสมบัติของระบบ
- กรณีที่คาดว่าจะมีการขยายขนาดการใช้งานเครือข่ายในอนาคตซึ่งไม่อาจประมาณขนาดล่วงหน้าได้ อาจจะพิจารณา**ระบบ**ที่สามารถขยายความสามารถได้ เช่น การเพิ่มดิสก์สำหรับจัดเก็บข้อมูล

๕.๑.๔.๒ **ข้อกำหนด: ระบบต้องสามารถปรับตั้งนาฬิกาภายใน ให้ตรงกับเวลาอ้างอิงมาตรฐานระดับชาติ ได้โดยอัตโนมัติ**

- โดยปกติเมื่อระบบเชื่อมต่อเข้ากับเครือข่ายแล้ว ระบบจะตั้งเวลาจากเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลา (time server) ผ่านเครือข่ายอินเทอร์เน็ตโดยอัตโนมัติ การตรวจสอบในเบื้องต้นคือให้ดูเวลาที่อาจจะแสดงบนหน้าจอของระบบ เปรียบเทียบกับคอมพิวเตอร์เครื่องอื่นที่มีการตั้งเวลาจากเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลา ผ่านเครือข่ายอินเทอร์เน็ตเช่นกันว่าถูกต้องตรงกันหรือไม่ ซึ่งเป็นการตรวจสอบอย่างคร่าว ๆ
- ตรวจสอบว่าระบบมีการตั้งเวลาอัตโนมัติจากเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลามาตรฐานระดับชาติหรือไม่ ซึ่งอาจจะตรวจสอบได้โดยดูว่า ระบบสามารถแสดงหรือตั้งค่าเกี่ยวกับเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลามาตรฐานได้หรือไม่ หรือมีระบุไว้ในเอกสารคู่มือหรือไม่ว่ามีการตั้งค่าเวลาจากเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลามาตรฐาน หรืออาจจะทราบจากการสอบถามทางเทคนิคจากผู้จัดทำระบบ

รายการเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลามาตรฐานระดับชาติ ได้แก่

- (๑) สถาบันมาตรวิทยาแห่งชาติ ได้แก่ time1.nimt.or.th (203.185.69.60)
time2.nimt.or.th (203.185.69.59) time3.nimt.or.th (203.185.69.56)
- (๒) กรมอุทกศาสตร์ กองทัพเรือ ได้แก่ time.navy.mi.th (113.53.247.3)
- (๓) ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ได้แก่
clock.nectec.or.th (203.185.57.115)

อนุญาตให้ปรับเทียบเวลากับเครื่องแม่ข่ายภายในองค์กรที่ให้บริการปรับเทียบเวลา ที่เทียบเท่าเวลามาตรฐานระดับชาติ โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

๕.๑.๔.๓ **ข้อกำหนด: ระบบต้องมีการกำหนดการป้องกันการเข้าถึงระบบโดยผู้ไม่ได้รับอนุญาต ทั้งทางกายภาพและทางอิเล็กทรอนิกส์อย่างเหมาะสม**

- โดยปกติระบบควรจะมีการตรวจสอบยืนยันตัวบุคคลที่เข้าใช้งานระบบด้วยวิธีล็อกอินด้วยชื่อผู้ใช้และรหัสผ่าน หรืออาจจะเป็นวิธีอื่นที่คล้ายกันหรือดีกว่า
- ถ้าล็อกอินจากระยะไกล ระบบควรจัดให้อยู่ในสถานะการเชื่อมต่อที่มีความปลอดภัย เช่น HTTPS, SSH, SSL
- การติดตั้งเครื่องไว้ในห้องที่ปิดกันมิดชิด มีระบบรักษาความปลอดภัยแน่นอนหนา
- อาจจะใช้วิธีการอื่นๆ ต่อไปนี้ เพื่อช่วยเสริมให้มีความปลอดภัยมากขึ้น ได้แก่
 - การจำกัดรูปแบบและวิธีการเข้าถึง
 - การจำกัดจำนวนผู้ใช้
 - การจำกัดเวลาการใช้
 - การกำหนดช่วงเวลาที่ย่อนุญาต
 - จำกัดสิทธิ์ที่สำคัญบางอย่างถ้าเข้าถึงจากระยะไกล

– การปิดฝาเครื่อง

- ๕.๑.๔.๔ **ข้อกำหนด:** ระบบต้องสามารถควบคุมและป้องกันการเปลี่ยนแปลงการตั้งค่าต่าง ๆ ของระบบโดยผู้ใช้ได้ สำหรับการตั้งค่าที่อนุญาตให้เปลี่ยนแปลงได้ ต้องสามารถควบคุมและป้องกันการเปลี่ยนแปลงการตั้งค่า โดยผู้ที่ไม่เกี่ยวข้องได้
- ผู้ใช้ทั่วไปที่เข้าใช้ระบบ จะต้องไม่สามารถเข้าถึงส่วนบริหารจัดการระบบได้
 - เมื่อพยายามเข้าสู่ส่วนบริหารจัดการระบบโดยตรง เช่น ทรานซูอาร์แอล (universal resource locator, URL) โดยตรงที่จะเข้าไปได้ ระบบต้องมีการตรวจสอบสิทธิ์ก่อนว่ามีสิทธิ์หรือไม่ ถ้าไม่มีต้องไม่อนุญาตให้เข้าถึงได้
 - ถ้าเป็นการเข้าถึงผ่านเว็บ ต้องมีระบบจัดการช่วงเวลาสื่อสาร (session management) ที่ปลอดภัย
- ๕.๑.๔.๕ **ข้อกำหนด:** ระบบต้องสามารถระบุและจำแนกตัวบุคคล และบันทึกประวัติการเข้าถึงและใช้งานระบบได้ รวมถึงต้องสามารถป้องกันการแก้ไข เปลี่ยนแปลง การปลอมแปลงข้อมูลที่เกี่ยวข้องเพื่อการเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาตได้ เทคนิคและวิธีที่ใช้ในการระบุตัวบุคคลและป้องกันการเปลี่ยนแปลง ควรเป็นเทคนิคที่ถูกตรวจสอบยืนยันความใช้ได้แล้ว
- ตรวจสอบว่าระบบมีการจำแนกตัวบุคคลหรือไม่ คือมีบัญชีผู้ใช้ของแต่ละคนแยกจากกัน และมีการระบุตัวบุคคลได้โดยวิธีการต่าง ๆ เช่นรหัสผ่าน
 - ตรวจสอบว่ามีบันทึกประวัติการเข้าถึงและใช้งานระบบได้
- ๕.๑.๔.๖ **ข้อกำหนด:** ระบบควรมีการตรวจสอบความใช้ได้ของข้อมูลอื่น ที่ไม่ใช่ข้อมูลจราจรทางคอมพิวเตอร์ ที่รับเข้าสู่ระบบ (input validation)
- ทดสอบการป้อนข้อมูลที่ทำให้เกิดข้อผิดพลาดหรือช่องโหว่ถ้าไม่ได้มีการตรวจสอบการรับข้อมูล เช่น กรอกข้อความว่า 'anything' OR 'x'='x ลงไปในช่องชื่อผู้ใช้ แล้วลองกดปุ่มล็อกอินและลองสลับไปใส่ในช่องรหัสผ่าน แล้วกดล็อกอินตามลำดับ ถ้าระบบไม่มีการตรวจสอบข้อมูลที่รับเข้าสู่ระบบ ระบบอาจจะยอมให้เข้าใช้ระบบได้โดยไม่ต้องใช้ชื่อผู้ใช้ และรหัสผ่านหรือแสดงให้เห็นว่าเกิดปัญหาที่ระบบไม่ได้เตรียมการรองรับไว้
 - ทดสอบการรับไฟล์เข้าสู่ระบบด้วยไฟล์ที่อาจทำให้เกิดข้อผิดพลาดหรือช่องโหว่กับระบบได้ เช่น เอกซ์คิวทไฟล์ (executed file) พิเอสคิปสคริป (php script) ระบบควรมีการตรวจสอบไฟล์และไม่ควรยอมรับ (หรือปฏิเสธการรับ) ไฟล์ที่อาจทำให้เกิดข้อผิดพลาดหรือช่องโหว่กับระบบได้ ในกรณีที่ระบบไม่มีการตรวจสอบการรับไฟล์เข้าสู่ระบบและยอมรับไฟล์ที่อาจทำให้เกิดข้อผิดพลาดหรือช่องโหว่กับระบบ การเปิดใช้งานไฟล์ (หรือสั่งให้ทำงาน) ต้องไม่ทำให้ระบบเกิดข้อผิดพลาดหรือช่องโหว่ได้
- ๕.๑.๔.๗ **ข้อกำหนด:** ระบบควรจัดให้มีคำอธิบายเพื่อให้ความช่วยเหลือ ในการแก้ไขปัญหาและข้อบกพร่องต่าง ๆ ที่มักเกิดขึ้น อย่างเหมาะสมและเพียงพอ
- มีส่วนที่อำนวยความสะดวกในการใช้งาน เพื่อให้การทำงานเป็นไปอย่างถูกต้อง เช่น มีระบบให้ความช่วยเหลือในหน้าต่างหลักของโปรแกรม มีการจัดทำตัวช่วยตั้งค่าแบบ wizard ในส่วนการตั้งค่าที่ซับซ้อน

๕.๑.๕ หมวด: การรับและเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

๕.๑.๕.๑ **ข้อกำหนด: ระบบต้องสามารถรับข้อมูลจราจรทางคอมพิวเตอร์จากอุปกรณ์ บริการหรือระบบ**
ต้นทาง ตามที่ระบุได้ อย่างครบถ้วน ถูกต้อง และหากเป็นไปได้ระบบควรมีระบบตรวจสอบและ
ปฏิเสธข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลอื่นที่ส่งมาจากระบบต้นทาง ที่ไม่ถูกต้องหรือผิด
ปกติ

- ในกรณีที่ระบบสามารถรับข้อมูลจราจรทางคอมพิวเตอร์จากอุปกรณ์ บริการหรือระบบ
ต้นทางอื่นได้ ระบบต้องมีการระบุความสามารถในการรับข้อมูลสูงสุด เช่น สามารถรับข้อมูล
จราจรได้สูงสุด ๑๕๐๐ เหตุการณ์ต่อวินาที และในสภาวะดังกล่าว ข้อมูลจราจรต้องได้รับครบ
ถ้วน ไม่ตกหล่น

การทดสอบสามารถทำได้โดยใช้โปรแกรม loggen ซึ่งมาพร้อมกับชุดซอฟต์แวร์ syslog-ng
เพื่อสร้างข้อมูลจราจรทางคอมพิวเตอร์จำลองขึ้นในอัตราต่าง ๆ และตรวจสอบจำนวนข้อมูล
ที่ได้รับ เทียบกับจำนวนข้อมูลที่สร้างขึ้นจริง

- การจะรับข้อมูลจากอุปกรณ์ บริการหรือระบบต้นทางต่าง ๆ จะต้องมีการกำหนดให้ลง
ทะเบียนอุปกรณ์ บริการหรือระบบต้นทางนั้น ๆ ก่อน
- หากมีการส่งข้อมูลจากอุปกรณ์ บริการหรือระบบต้นทางที่ไม่ได้ลงทะเบียน ระบบจะต้อง
ปฏิเสธไม่รับข้อมูล หรือแยกเก็บต่างหากเพื่อความสะดวกในการตรวจสอบภายหลัง

๕.๑.๕.๒ **ข้อกำหนด: ข้อมูลจราจรทางคอมพิวเตอร์ ที่รับเข้ามาในระบบต้อง**

- เก็บในสื่อที่สามารถรักษาคุณภาพของข้อมูลได้อย่างเหมาะสมและป้องกันการสูญหาย เสีย
หาย ถูกกลบ ทำลาย แก้ไข ดัดแปลง ทั้งโดยเจตนาและไม่เจตนา
- เข้าถึงได้เฉพาะผู้ดูแลข้อมูล และไม่สามารถเข้าถึงได้โดยผู้ไม่เกี่ยวข้องหรือผู้ไม่ได้รับอนุญาต
- ถูกเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าที่ได้ระบุไว้ และต้องไม่น้อยกว่า ๙๐ วัน

การตรวจสอบ

- สื่อที่บันทึกข้อมูลจราจรทางคอมพิวเตอร์ ควรมีการจัดทำให้มีความปลอดภัยอย่างหนึ่งอย่าง
ใดหรือหลายอย่างรวมกันต่อไปนี้
 - ใช้ดีสก์ระบบ RAID ที่มีความปลอดภัย เช่น RAID-1 หรือ RAID-5
 - มีระบบสำรองข้อมูล โดยมีกระบวนการเก็บสำเนาที่ปลอดภัย เช่น เก็บในตู้ที่ปิดล็อกได้
 - ใช้คุณสมบัติการตรวจสอบฮาร์ดดิสก์อัตโนมัติในตัวดิสก์ (S.M.A.R.T.) โดยคอยเข้าไป
อ่านค่าในตัวดิสก์อย่างสม่ำเสมอ หากพบความผิดปกติ ต้องรีบแจ้งเตือนผ่านระบบทันที
 - อยู่ในพื้นที่ที่มีความปลอดภัยจากบุคคลที่ไม่เกี่ยวข้อง จากอันตรายต่าง ๆ เช่น ความ
ร้อน แสงแดด ความชื้น น้ำ ฝุ่น
- ระบบ สื่อที่เก็บข้อมูลจราจรหลัก สื่อที่เก็บข้อมูลจราจรที่เป็นสำเนา ต้องไม่ถูกเข้าถึงได้โดยผู้
ไม่เกี่ยวข้องโดยเด็ดขาด
- การเข้าถึงข้อมูลจากระยะไกลต้องเข้าถึงได้จากผู้ดูแลข้อมูลเท่านั้น โดยใช้วิธีการพิสูจน์ตัวตน
ที่ปลอดภัย

- ข้อมูลจราจรที่จัดเก็บต้องจัดเก็บได้อย่างน้อยตามที่ระบุไว้ในคุณสมบัติของระบบ และไม่น้อยกว่า ๙๐ วัน โดยใช้วิธีประเมินวิธีใดวิธีหนึ่ง หรือหลายวิธีดังต่อไปนี้
 - ผู้ผลิตมีเอกสารแนะนำวิธีการคำนวณหรือประเมินขนาดของสื่อที่เชื่อว่าควรใช้ขนาดเท่าใดเพื่อให้เก็บข้อมูลจราจรได้อย่างน้อย ๙๐ วัน
 - ดูจากปริมาณข้อมูลจราจรที่เก็บในแต่ละวันว่าเป็นเท่าใด และคาดการณ์ว่าในอนาคตจะมีปริมาณเพิ่มขึ้นเท่าไร แล้วใช้ประเมินขนาดสื่อที่ต้องใช้เก็บว่ามีเพียงพอหรือไม่
 - ระบบรองรับการเพิ่มขยายความจุของสื่อที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ได้
 - ระบบสามารถลบข้อมูลจราจรทางคอมพิวเตอร์ที่เกิน ๙๐ วันได้โดยอัตโนมัติ

๕.๑.๕.๓ **ข้อกำหนด:** ระบบต้องสามารถป้องกันการแก้ไข เปลี่ยนแปลง ลบ ทำลายข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลการใช้งานระบบ และข้อมูลคอมพิวเตอร์อื่น ๆ ที่เกี่ยวข้อง โดยผู้ดูแลข้อมูล และผู้อื่นที่ไม่เกี่ยวข้องได้ ทั้งโดยเจตนาและไม่เจตนา

การตรวจสอบ

- ผู้ดูแลข้อมูลไม่สามารถแก้ไข ลบ หรือเพิ่มข้อมูลจราจรได้
- ระบบถูกติดตั้งในตำแหน่งที่ปลอดภัยในเน็ตเวิร์ค เช่น อยู่ในโซนเดียวกันกับเซิร์ฟเวอร์หรืออุปกรณ์ที่เป็นแหล่งกำเนิดข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งไม่เกี่ยวข้องกับโซนของผู้ใช้ทั่วไป และบุคคลอื่น ๆ

๕.๑.๕.๔ **ข้อกำหนด:** ระบบต้องสามารถตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้ได้ รวมถึงการจัดให้มีการเฝ้าระวังบูรณาการของข้อมูลอย่างเหมาะสม

- ระบบสามารถตรวจสอบความถูกต้องของข้อมูลที่จัดเก็บได้ เพื่อให้มั่นใจว่าข้อมูลที่เก็บยังคงถูกต้อง และใช้เป็นหลักฐานได้ อาจจะกำหนดให้ตรวจสอบอัตโนมัติตามช่วงเวลาก็ได้
- การตรวจสอบความถูกต้องควรใช้วิธีการทำแฮช ที่ได้รับความน่าเชื่อถือ เช่น MD5 SHA-1 SHA-256 หรือสูงกว่า

๕.๒ การตรวจสอบความปลอดภัยของการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

๕.๒.๑ การตรวจสอบความถูกต้องของข้อมูลจราจรทางคอมพิวเตอร์

๕.๒.๑.๑ การตรวจสอบความถูกต้องของข้อมูลด้วย MD5

ก) บนระบบปฏิบัติการลินุกซ์ ให้ใช้คำสั่ง md5sum ตัวอย่าง เช่น

- md5sum log-2017-02-11.tar.gz
5c2b79ab0c574af22aedfe6cd9180817 log-2017-02-11.tar.gz
- จะได้ค่าไจเรสต์คือ 5c2b79ab0c574af22aedfe6cd9180817 เพื่อนำไปเปรียบเทียบกับถูกต้องตรงกันหรือไม่

ข) บนระบบปฏิบัติการวินโดวส์ ให้ติดตั้งซอฟต์แวร์ที่สามารถหาค่า MD5 จากแฟ้มต่าง ๆ ได้ เช่น โปรแกรมคำสั่งแบบคอมมานด์ไลน์ชื่อ md5sum.exe จากเว็บไซต์ <http://www.pc->

tools.net/win32/md5sums/

- ตัวอย่างการตรวจสอบด้วย md5sum.exe ซึ่งต้องเปิด Command Prompt ขึ้นมาก่อน แล้วสั่ง
C:\Downloads> md5sum log-2017-02-11.tar.gz
5c2b79ab0c574af22aedfe6cd9180817 log-2017-02-11.tar.gz
- จากนั้นก็นำค่าไจเรสต์ที่ได้ไปเปรียบเทียบกับถูกต้องตรงกันหรือไม่

ภาคผนวก ก. การตรวจสอบความถูกต้องสมบูรณ์ของข้อมูล

ก.๑ วิธีแฮช (hash)

การตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูลโดยวิธีแฮช หมายถึง กรรมวิธีตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูล โดยอาศัยหลักการของการเข้ารหัสลับ (cryptography) ที่ใช้ฟังก์ชันแฮช (hash function) ที่ถูกออกแบบมาโดยเฉพาะสำหรับใช้ในด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศ เช่น MD5, SHA-1, SHA-256 หรือสูงกว่า ซึ่งคุณสมบัติของฟังก์ชันแฮชเหล่านี้คือ เมื่อนำข้อมูลนำเข้า (input data) มาคำนวณค่ากับฟังก์ชันแฮช จะได้ผลลัพธ์เป็นค่าเฉพาะตัวค่าหนึ่งหรือที่เรียกว่าค่าแฮช ซึ่งเป็นค่าที่แตกต่างในทุกๆข้อมูลนำเข้า และค่าเฉพาะตัวนี้ได้รับการรับรองการจัดการข้อมูลที่จะไม่มีโอกาสซ้ำกันได้ในระดับการใช้งาน ที่ได้รับการยอมรับเป็นสากล จากคุณสมบัติดังกล่าว ฟังก์ชันแฮช จึงถูกนำมาใช้ในการตรวจสอบความถูกต้องของข้อมูล โดยการคำนวณค่าแฮช แล้วนำค่ามาเก็บไว้ก่อน ที่จะนำข้อมูลไปใช้งานและเมื่อต้องการการตรวจสอบความถูกต้องให้นำข้อมูลนั้น กลับมาคำนวณค่าแฮช อีกครั้ง ถ้าพบว่าค่าแฮช มีค่าเดิมจะถือว่าข้อมูลมีความถูกต้องและสมบูรณ์ แต่หากค่าแฮช มีค่าเปลี่ยนไปไม่เหมือนเดิม แสดงว่าเกิดการเปลี่ยนแปลงของข้อมูลเกิดขึ้น

บรรณานุกรม

๑. หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศและคณะอนุกรรมการด้านความมั่นคง ภายใต้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ในคณะอนุกรรมการธุรกรรมทางอิเล็กทรอนิกส์, “มาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕) ประจำปี ๒๕๕๐”, ISBN: 978-974-229-584-4, พิมพ์ครั้งที่ ๑, ธันวาคม ๒๕๕๐
๒. ISO/IEC 27002, Information technology – Security Technique – Code of practice for information security management
๓. Chaikorn Apiwathanokul, “Computer Time Synchronization Scheme”, http://www.etcommission.go.th/documents/standard/time_sync_server_v1_0.pdf, 3 October 2007
๔. ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย ภายใต้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, “แนวทางการจัดเก็บข้อมูลล็อกสำหรับองค์กรเพื่อให้สอดคล้องตาม พ.ร.บ. ว่า

ด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”,

http://www.thaicert.org/paper/auditing/LogImplementationandAuditingGuideline_r2.pdf,
๒๓ สิงหาคม ๒๕๕๐

๕. อสมารณ์ ฉัตรตติกรณ์ และ ขวลิท ทินกรสุตบุตร, “การเทียบเวลาด้วย Network Time Protocol ให้สอดคล้องกับ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”
<http://www.thaicert.org/paper/basic/NTPandLAW.php>, ๒๗ กุมภาพันธ์ ๒๕๕๑
๖. อสมารณ์ ฉัตรตติกรณ์ และ ขวลิท ทินกรสุตบุตร, “คู่มือการใช้บริการ Time Server [ฉบับปรับปรุง]”,
<http://www.thaicert.org/paper/basic/manualTimeServer.php>, ๒๗ กุมภาพันธ์ ๒๕๕๑
๗. W3C, "Extended Log File Format", <http://www.w3.org/pub/WWW/TR/WD-logfile-960221.html>, 19 May 2009
๘. IETF Working Groups, "RFC1738 - Uniform Resource Locators (URL)",
<http://www.ietf.org/rfc/rfc1738.txt>, December 1994
๙. IETF Working Groups, "RFC1321 - The MD5 Message-Digest Algorithm",
<http://www.ietf.org/rfc/rfc1321.txt>, April 1992
๑๐. IETF Working Groups, "US Secure Hash Algorithm 1 (SHA1)",
<http://www.ietf.org/rfc/rfc3164.txt>, September 2001
๑๑. IETF Working Groups, "The BSD syslog Protocol", <http://www.ietf.org/rfc/rfc3174.txt>,
August 2001
๑๒. Federal Information Processing Standards (FIPS), "FIPS-180-1 SECURE HASH STANDARD",
<http://www.itl.nist.gov/fipspubs/fip180-1.htm>, 1995 April 17
๑๓. Wikipedia, "Cryptographic hash function",
http://en.wikipedia.org/wiki/Cryptographic_hash_function, 19 May 2009
๑๔. Karen Kent and Murugiah Souppaya, NIST, Special Publication ๘๐๐-๙๒, “Guide to
Computer Security Log Management”, September 2006
๑๕. Roger Meyer, “Auditing a Corporate Log Server” GAIC Gold Certification, GIAC Systems and
Network Auditor (GSNA), SANS Institute 2006 Reading Room, 17 September 2006

คณะทำงาน

ที่ปรึกษา

นายศรีณย์ สัมฤทธิ์เดชขจร

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

คณะทำงาน ด้านเทคนิค

นายปิยวัฒน์ เลื่อนสุคันธ์

ผู้ทรงคุณวุฒิ

นายกำธร ไกรรักษ์

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นายกริช นาสิงห์ขันธ์

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นายธีรเจต พันพาไพร

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นายสุรพงษ์ แซ่เจียม

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นายสมเดช แสงสุรศักดิ์

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นางสาวปัญญดา ฤกษ์มังกร

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ