สมอ./ศอ.พว./FDNS(2)

มีนาคม 2560

ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน

มาตรฐานฉบับสมบูรณ์จะมีประกาศในราชกิจจานุเบกษา

ร่าง

มาตรฐานผลิตภัณฑ์อุตสาหกรรม

# ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ – เล่ม 2 แนวทางในการจัดทำและตรวจสอบ

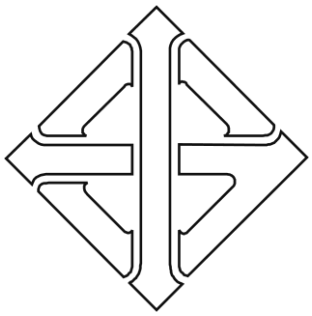
# COMPUTER LOG SYSTEM – PART 2 : IMPLEMENTATION AND EVALUTATION GUIDE

สำหรับเสนอคณะกรรมการวิชาการมาตรฐานระบบเก็บรักษาข้อมูลจราจรคอมพิวเตอร์

สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม

กระทรวงอุตสาหกรรม ถนนพระรามที่ 6 กรุงเทพฯ 10400

โทรศัพท์ 0 2202-33XX



**มาตรฐานผลิตภัณฑ์อุตสาหกรรม**

THAI INDUSTRIAL STANDARD

**มอก.XXXX – 25XX**

# ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ – เล่ม 2 แนวทางในการจัดทำและตรวจสอบ

COMPUTER LOG SYSTEMS –

PART 2 : IMPLEMENTATION AND EVALUTATION GUIDE

**สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม**

**กระทรวงอุตสาหกรรม**

ICS

ISBN

# มาตรฐานผลิตภัณฑ์อุตสาหกรรม
# ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ –
# เล่ม 2 แนวทางในการจัดทำและตรวจสอบ

มอก.XXXX – 25XX

**สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม**
**กระทรวงอุตสาหกรรม ถนนพระรามที่ 6 กรุงเทพฯ 10400**
**โทรศัพท์ 0 2202 3300**

**ประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม ตอนพิเศษ**
**วันที่ พุทธศักราช 25xx**

## คณะกรรมการวิชาการมาตรฐาน
## ระบบเก็บรักษาข้อมูลจราจรคอมพิวเตอร์

**ประธาน**

| | |
|---|---|
| นางสาวพลอยรวี เกริกพันธ์กุล | สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ<br>กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม |

**รองประธาน**

| | |
|---|---|
| - | สำนักงานคณะกรรมการคุ้มครองผู้บริโภค |

**กรรมการ**

| | |
|---|---|
| ร.ต.อ. วิทวัส สิงห์โตแก้ว | กองบังคับการสนับสนุนทางเทคโนโลยี<br>สำนักงานตำรวจแห่งชาติ |
| นายพงศธร วรรณสุคนธ์ | กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยี<br>กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม |
| นายณัฐ สกลชัย | สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม |
| นายวิรัตน์ พึ่งสาระ | สำนักงานส่งเสริมเศรษฐกิจดิจิทัล |
| นายสมญา พัฒนวรพันธุ์ | ผู้ทรงคุณวุฒิ |
| นายสว่างพงศ์ หมวดเพชร | สมาคมสมาพันธ์ซอฟต์แวร์โอเพนซอร์ส |
| - | สมาคมสมาพันธ์เทคโนโลยสารสนเทศแห่งประเทศไทย |
| นายขจร สินอภิรมย์สราญ | ผู้ทรงคุณวุฒิ |
| นายบรรจง หะรังสี | ผู้ทรงคุณวุฒิ |
| นายกมล เอื้อชินกุล | ผู้ทรงคุณวุฒิ |
| - | สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) |
| นายโกเมน พิบูลย์โรจน์ | บริษัท ที-เน็ต จำกัด |
| นายเจษฎา ทองก้านเหลือง | |
| นายนนทวัตต์ สาระมาน | สมาคมอุตสาหกรรมซอฟต์แวร์ไทย |
| นายกมลชัย นามวงศ์ | บริษัท ทีโอที จำกัด (มหาชน) |
| นายวิศรุต วรรธนะปราการ | |
| นายเถลิงศักดิ์ เวียงวิเศษ | |

**กรรมการและเลขานุการ**

| | |
|---|---|
| นายถิรเจต พันพาไพร | ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ |
| นายสมเดช แสงสุรศักดิ์ | |

# คณะทำงาน

## ที่ปรึกษา

| | |
|---|---|
| นายศรัณย์ สัมฤทธิ์เดชขจร | ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ |

## คณะทำงาน ด้านเทคนิค

| | |
|---|---|
| นายถิรเจต พันพาไพร | ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ |
| นายสุรพงษ์ แซ่เจียม | ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ |
| นายสมเดช แสงสุรศักดิ์ | ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ |
| ปัญญดา ฤกษ์มังกร | ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ |
| นายกำธร ไกรรักษ์ | ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ |
| นายปิยวัฒน์ เลื่อนสุคันธ์ | ผู้ทรงคุณวุฒิ |

ตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 กำหนดให้ ผู้ให้บริการเชื่อมต่อเข้ากับระบบอินเทอร์เน็ตประเภทต่าง ๆ ต้องมีหน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ที่เกิดขึ้นจากการให้บริการนั้น ๆ อย่างครบถ้วน ถูกต้อง และเป็นไปตามที่กฎหมายกำหนด ดังนั้น เพื่อให้มีข้อแนะนำในการจัดทำและตรวจประเมินระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์สำหรับใช้อ้างอิง จึงได้กำหนดมาตรฐานผลิตภัณฑ์อุตสาหกรรมระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ – เล่ม 2 แนวทางในการจัดทำและตรวจสอบขึ้น

มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้ จัดทำขึ้นตามความร่วมมือด้านการกำหนดมาตรฐานระหว่าง สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม กับ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ซึ่งตั้งอยู่ เลขที่ 112 อุทยานวิทยาศาสตร์ประเทศไทย ถนนพหลโยธิน ตำบลคลองหนึ่ง อำเภอคลองหลวง จังหวัดปทุมธานี 12120 โทรศัพท์ 02 564 6900 โทรสาร 02 564 6901..3 E-mail: info@nectec.or.th www.nectec.or.th และใช้ข้อมูลจากผู้ทำ ผู้ใช้ และจากเอกสารต่อไปนี้เป็นแนวทาง


ศอ. ๔๐๐๓.๒-๒๕๖๐ ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ เล่ม 2 แนวทางในการจัดทำและตรวจสอบ

ประกาศราชกิจจานุเบกษา, “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550”, วันที่ 18 มิถุนายน 2550

ประกาศราชกิจจานุเบกษา, “ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550”, วันที่ 23 สิงหาคม 2550

ประกาศราชกิจจานุเบกษา, “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560”, วันที่ 24 มกราคม 2560

หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศและคณะอนุกรรมการด้านความมั่นคงภายใต้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ในคณะอนุกรรมการธุรกรรมทางอิเล็กทรอนิกส์, “มาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550”, ISBN: 978-974-229-584-4, พิมพ์ครั้งที่ 1, ธันวาคม 2550

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

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

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย ภายใต้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, “แนวทางการจัดเก็บข้อมูลล็อกสำหรับองค์กรเพื่อให้สอดคล้องตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550”, http://www.thaicert.org/paper/auditing/LogImplementationandAuditingGuideline_r2.pdf , 23 สิงหาคม 2550

อสมาภรณ์ ฉัตรัตติกรณ์ และ ชวลิต ทินกรสูติบุตร, “การเทียบเวลาด้วย Network Time Protocol ให้สอดคล้องกับ

พ.ร.บ. 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

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

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

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

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

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

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

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

Karen Kent and Murugiah Souppaya, NIST, Special Publication 800-92, “Guide to Computer Security Log Management”, September 2006

Roger Meyer, “Auditing a Corporate Log Server” GAIC Gold Certification, GIAC Systems and Network Auditor (GSNA), SANS Institute 2006 Reading Room, 17 September 2006

มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้ เป็นหนึ่งในอนุกรมมาตรฐานเกี่ยวกับระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ คือ

มาตรฐานผลิตภัณฑ์อุตสาหกรรมระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ – เล่ม 1 ข้อกำหนด

มาตรฐานผลิตภัณฑ์อุตสาหกรรมระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ – เล่ม 2 แนวทางในการจัดทำและตรวจสอบ

คณะกรรมการมาตรฐานผลิตภัณฑ์อุตสาหกรรมได้พิจารณามาตรฐานนี้แล้ว เห็นสมควรเสนอรัฐมนตรีประกาศตามมาตรา 15 แห่งพระราชบัญญัติมาตรฐานผลิตภัณฑ์อุตสาหกรรม พ.ศ. 2511

**สารบัญ**

## สารบัญรูป

หน้า

ไม่พบรายการสารบัญภาพ

## สารบัญตาราง

หน้า

ไม่พบรายการสารบัญภาพ

**ประกาศกระทรวงอุตสาหกรรม**

**ฉบับที่ (พ.ศ. 2554)**

ออกตามความในพระราชบัญญัติมาตรฐานผลิตภัณฑ์อุตสาหกรรม

พ.ศ. 2511

เรื่อง กำหนดมาตรฐานผลิตภัณฑ์อุตสาหกรรม

ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ – เล่ม 2 แนวทางในการจัดทำและตรวจสอบ

---

อาศัยอำนาจตามความในมาตรา 15 แห่งพระราชบัญญัติมาตรฐานผลิตภัณฑ์อุตสาหกรรม พ.ศ. 2511 รัฐมนตรีว่าการกระทรวงอุตสาหกรรมออกประกาศกำหนดมาตรฐานผลิตภัณฑ์อุตสาหกรรม ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ – เล่ม 2 แนวทางในการจัดทำและตรวจสอบ มาตรฐานเลขที่ มอก. XXXX-25XX ไว้ ดังมีรายละเอียดต่อท้ายประกาศนี้

ประกาศ ณ วันที่ พ.ศ. 2560

รัฐมนตรีว่าการกระทรวงอุตสาหกรรม

# มาตรฐานผลิตภัณฑ์อุตสาหกรรม

# ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ –

# เล่ม 2 แนวทางในการจัดทำและตรวจสอบ

## 1. ขอบข่าย

1.1 มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้ เสนอข้อมูล หลักการ วิธีการ แนวคิด และตัวอย่าง เพื่อเป็นแนวทางในการจัดทำและตรวจสอบ ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ให้สอดคล้องและเป็นไปตาม “มาตรฐานผลิตภัณฑ์อุตสาหกรรม ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ เล่ม 1 ข้อกำหนด”

มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้ใช้ได้กับทั้งระบบ ซึ่งอาจหมายถึงหลายหน่วยต่อเชื่อมกันหรือหน่วยเดี่ยว และรวมถึงซอฟต์แวร์ประยุกต์ที่ออกแบบมาโดยประสงค์ให้ติดตั้งในระบบคอมพิวเตอร์ เพื่อให้ระบบคอมพิวเตอร์นั้นทำหน้าที่เป็นระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

1.2 มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้ไม่ครอบคลุมถึง

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

1.2 มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้ ไม่ครอบคลุมถึง

การทำงานของ โปรแกรม ซอฟต์แวร์ประยุกต์ อุปกรณ์เครือข่าย เครื่องและระบบคอมพิวเตอร์ อื่นซึ่งทำหน้าที่ให้บริการใดๆ ในระบบคอมพิวเตอร์ที่ต่อเชื่อมถึงกัน และมีหน้าที่ต้องส่งข้อมูลจราจรทางคอมพิวเตอร์ที่กำหนด ให้ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

**หมายเหตุ** ผู้ประกอบกิจการโทรคมนาคม และผู้ประกอบกิจการกระจายภาพและเสียง ที่ให้บริการอื่นๆ นอกเหนือจากการให้บริการโครงข่ายโทรคมนาคม และการกระจายภาพและเสียง ถูกพิจารณาว่าอยู่ในขอบข่ายของมาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้

## 2. บทนิยาม

ความหมายของคำที่ใช้ในมาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้ ให้เป็นไปดังต่อไปนี้

2.1 **ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์** ซึ่งต่อไปในมาตรฐานนี้จะเรียกว่า “**ระบบ**” หมายถึง คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่ทำหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ทั้งนี้หมายรวมถึงซอฟต์แวร์ที่จะติดตั้งในระบบคอมพิวเตอร์เพื่อให้ทำหน้าที่ดังกล่าวข้างต้น

2.2 **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์คอมพิวเตอร์ ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

2.3 **ข้อมูลจราจรทางคอมพิวเตอร์** หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรือข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

2.4 **ผู้ให้บริการ** หมายถึง ผู้ซึ่งมีเจตนา

2.4.1 ให้บริการแก่ บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือเพื่อประโยชน์ของบุคคลอื่น

2.4.2 ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

2.5 **ผู้ดูแลระบบ** หมายถึง บุคคล หรือกลุ่มบุคคล ที่มีหน้าที่ ดูแลรักษา ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ แต่จะไม่มีสิทธิ์ในการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ และอาจรวมถึงข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นๆ ที่เกี่ยวข้อง

2.6 **ผู้ดูแลข้อมูล** หมายถึง ผู้ที่ได้รับมอบสิทธิ์จากองค์กร/หน่วยงานในการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ และอาจรวมถึงข้อมูลคอมพิวเตอร์ และข้อมูลอื่นๆ ที่เกี่ยวข้อง สิทธิ์ในการเข้าถึงข้อมูลจะต้อง ไม่รวมถึงสิทธิ์ในการแก้ไข เปลี่ยนแปลง ลบ หรือ ทำลายข้อมูล

2.7 **ผู้ใช้** หมายถึง ผู้ดูแลระบบ หรือผู้ดูแลข้อมูล

2.8 **การยืนยันตัวบุคคล** หมายถึง ขั้นตอนการชี้บ่ง เพื่อยืนยันความถูกต้องของหลักฐานที่ใช้ระบุ (Identity) แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง สามารถแบ่งออกได้เป็น 2 ขั้นตอน คือ การระบุตัวตน และการพิสูจน์ตัวตน

2.9 **การระบุตัวตน** (identification) หมายถึง ขั้นตอนหรือวิธี ที่ผู้ใช้แสดงเป็นหลักฐานชี้บ่งตนเอง เช่น ชื่อผู้ใช้ (username) เป็นต้น

2.10 **การพิสูจน์ตัวตน** (authentication) หมายถึง ขั้นหรือวิธี การตรวจสอบหลักฐานแวดล้อมเพื่อยืนยันว่าเป็นบุคคลที่กล่าวอ้างจริง

2.11 **การล็อกอิน** หมายถึง การเข้าใช้งานระบบคอมพิวเตอร์ โดยต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

2.12 **ข้อมูลการล็อกอิน** หมายถึง ข้อมูลที่ใช้ในการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบคอมพิวเตอร์

2.13 **บูรณภาพของข้อมูล** (integrity) หมายถึง ความถูกต้อง เที่ยงตรง และความสมบูรณ์ของข้อมูล

2.14 **มาตรฐานเล่มที่ 1** หมายถึง มาตรฐานผลิตภัณฑ์อุตสาหกรรม ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ เล่ม 1 ข้อกำหนด

## 3. การประเมินข้อมูลพื้นฐาน

3.1 การประเมินองค์กรเพื่อวางแผนในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

การประเมินองค์กรเพื่อวางแผนในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ มีวัตถุประสงค์ ดังนี้

ก) เพื่อให้องค์กรได้รับรู้ถึงประเภทของผู้ให้บริการตามความหมายในพระราชบัญญัติ (พ.ร.บ.) ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 พร้อมทั้งจำแนกประเภทย่อยของผู้ให้บริการได้

ข) เพื่อให้องค์กรสามารถวิเคราะห์และจัดทำบัญชีรายชื่อของเครื่องให้บริการหรือระบบให้บริการที่จำเป็นต้องเก็บข้อมูลจราจรคอมพิวเตอร์

ค) เพื่อให้องค์กรสามารถเก็บข้อมูลจราจรคอมพิวเตอร์ได้ถูกต้องตามที่กฎหมายกำหนด

โดยขั้นตอนการประเมินอาจแบ่งได้เป็น 3 ขั้นตอนคือ

ก) การประเมินองค์กรเพื่อกำหนดประเภทของผู้ให้บริการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

ข) การวิเคราะห์และกำหนดระบบให้บริการหรือเครื่องให้บริการ ที่จำเป็นต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์

ค) การวิเคราะห์ปริมาณข้อมูลจราจรที่ต้องทำการจัดเก็บเบื้องต้น

3.1.1 การประเมินองค์กรเพื่อกำหนดประเภทของผู้ให้บริการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

จากประกาศ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษา ข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 ได้กำหนดประเภทของผู้ให้บริการซึ่งมีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์แบ่งได้ ดังนี้

(1) ผู้ให้บริการ 5(1) เป็น ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น จำแนกได้ 4 ประเภท ดังนี้

ก) ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (telecommunication and broadcast carrier)

ข) ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (access service provider)

ค) ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่างๆ (host service provider)

ง) ผู้ให้บริการร้านอินเทอร์เน็ต

(2) ผู้ให้บริการ 5(2) เป็น ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม (1) (content service provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอปพลิเคชันต่างๆ (application service provider)

ซึ่งผู้ให้บริการทั้ง 2 ประเภทนั้นมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์แตกต่างกัน ดังนั้นเพื่อให้องค์กรสามารถกำหนดประเภทของผู้ให้บริการขององค์กรได้ จำเป็นต้องพิจารณาประเภทของผู้ให้บริการดังต่อไปนี้

(1) พิจารณาว่าองค์กรจัดอยู่ในประเภทของผู้ให้บริการใด

| ที่ | ประเด็น | หลักการพิจารณา | ประเภทผู้ให้บริการ |
|---|---|---|---|
| 1 | พิจารณาวัตถุประสงค์การให้บริการอินเทอร์เน็ตขององค์กร | ให้บริการอินเทอร์เน็ตแก่บุคคลทั่วไปหรือบุคคลากรในองค์กร | ผู้ให้บริการ 5(1) |
| | | ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์แก่บุคคลอื่น | ผู้ให้บริการ 5(2) |

ตัวอย่าง ผู้ให้บริการ 5(1) เช่น

- ISP ต่างๆ ซึ่งเป็นผู้ให้บริการอินเทอร์เน็ตแก่บุคคลทั่วไป
- ผู้ให้บริการเครื่องข่ายมือถือที่มีการให้บริการอินเทอร์เน็ต
- หน่วยงานราชการหรือองค์กรต่างๆ ที่ให้บริการอินเทอร์เน็ต

ตัวอย่าง ผู้ให้บริการ 5(2) เช่น

- ผู้ให้บริการ web hosting
- ผู้ให้บริการ application hosting

(2) พิจารณาว่าองค์กรจัดอยู่ในประเภทผู้ให้บริการย่อยใด (เฉพาะในกรณีองค์กรจัดอยู่ในประเภทผู้ให้บริการ 5(1))

| ที่ | ประเด็น | หลักการพิจารณา | ประเภทผู้ให้บริการ |
|---|---|---|---|
| 1 | พิจารณาประเภท การให้บริการ | เป็นผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง | ผู้ให้บริการ 5(1) ก |
| | | เป็นผู้ให้บริการการเข้าถึงระบบเครือ ข่ายคอมพิวเตอร์ | ผู้ให้บริการ 5(1) ข |
| | | เป็นผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการ | ผู้ให้บริการ 5(1) ค |

| ที่ | ประเด็น | หลักการพิจารณา | ประเภทผู้ให้บริการ |
|---|---|---|---|
| | | โปรแกรมประยุกต์ต่าง ๆ | |
| | | เป็นผู้ให้บริการร้านอินเทอร์เน็ต | ผู้ให้บริการ 5(1) ง |

3.1.2 การวิเคราะห์และกำหนดระบบให้บริการหรือเครื่องให้บริการ ที่จำเป็นต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์

เพื่อให้สามารถระบุเครื่องให้บริการที่จำเป็นต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการควรจัดทำบัญชีรายชื่อของระบบให้บริการหรือเครื่องให้บริการที่จำเป็นต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยอาศัยขั้นตอนต่อไปนี้

3.1.2.1 วิเคราะห์ระบบให้บริการหรือเครื่องให้บริการขององค์กร

เมื่อองค์กรได้ทราบถึงประเภทของผู้ให้บริการขององค์กร พร้อมกับได้จำแนกประเภทย่อย ของผู้ให้บริการแล้ว จำเป็นต้องมีการวิเคราะห์ ระบบให้บริการหรือเครื่องให้บริการ ที่มีอยู่ทั้งหมดในองค์กร เพื่อให้องค์กรสามารถระบุระบบให้บริการหรือเครื่องให้บริการ ที่เกี่ยวข้องและจำเป็นต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยการวิเคราะห์ อาศัยหลักการพิจารณา ดังต่อไปนี้

(1) พิจารณาขอบเขตการให้บริการ

| ที่ | หลักการพิจารณา | การเก็บข้อมูลจราจรคอมพิวเตอร์ |
|---|---|---|
| 1 | ให้บริการเฉพาะภายในองค์กร เข้าถึงได้เฉพาะภายในองค์กร | พิจารณาตามความเหมาะสมและความจำเป็น |
| 2 | ให้บริการเฉพาะภายในองค์กร แต่บุคคลภายนอกสามารถเข้าถึงได้จากอินเทอร์เน็ต | ต้องเก็บข้อมูลจราจรคอมพิวเตอร์ |
| 3 | ให้บริการภายในองค์กร แต่มีการติดต่อสื่อสารกับบุคคลภายนอก | ต้องเก็บข้อมูลจราจรคอมพิวเตอร์ |
| 4 | ให้บริการสาธารณะ | ต้องเก็บข้อมูลจราจรคอมพิวเตอร์ |

(2) พิจารณาข้อมูลจราจรคอมพิวเตอร์ที่ผู้ให้บริการแต่ละประเภทต้องทำการจัดเก็บ

(2.1) ผู้ให้บริการประเภท 5(1) ข และ ค

ก) ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย

| หลักการพิจารณา | การดำเนินการ |
|---|---|
| 1. ต้องมีการเก็บข้อมูลจราจร | ตรวจสอบช่องทางการเชื่อมต่ออินเทอร์เน็ต ว่าองค์กรมี |

| หลักการพิจารณา | การดำเนินการ |
|---|---|
| คอมพิวเตอร์ ทุกช่องทางที่มีการเชื่อมต่อสู่อินเทอร์เน็ต | ช่องทางการเข้าสู่อินเทอร์เน็ตทางใดบ้างและในแต่ละช่องทางมีการเก็บข้อมูลจราจรคอมพิวเตอร์หรือไม่ |
| 2. รายละเอียดของข้อมูลที่ทำการจัดเก็บต้องมีครบถ้วนตามข้อกำหนด | ตรวจสอบรายละเอียดของข้อมูลจราจรคอมพิวเตอร์ที่ทำการจัดเก็บไว้ว่ามีข้อมูลถูกต้องตามข้อกำหนดหรือไม่ |
| 3. ข้อมูลจราจรคอมพิวเตอร์ที่จัดเก็บต้องสามารถระบุตัวตนของผู้ใช้งานได้ | ตรวจสอบรายละเอียดของข้อมูลที่ทำการจัดเก็บไว้ว่าเพียงพอสำหรับการระบุตัวตนของผู้ใช้งานหรือไม่<br><br>ตัวอย่าง เช่น<br><br>- ในองค์กรที่มีการใช้งานระบบ NAT (Network Address Translation) จะทำให้หมายเลข IP Address ของผู้ใช้งานอินเทอร์เน็ตเป็นหมายเลขเดียวกัน องค์กรจำเป็นต้องจัดให้มีมาตรการในการควบคุมผู้ใช้งานเพื่อให้สามารถระบุตัวตนผู้ใช้งานได้ เช่น การจัดทำระบบลงทะเบียนผู้ใช้งาน<br>- ในองค์กรที่มีการใช้งาน proxy server องค์กรจำเป็นต้องจัดให้มีมาตรการในการควบคุมผู้ใช้งานเพื่อให้สามารถระบุตัวตนผู้ใช้งานได้ เช่น การใช้กลไกการพิสูจน์ตัวตนก่อนเข้าใช้งานอินเทอร์เน็ต |

**หมายเหตุ** การเข้าถึงระบบเครือข่าย หมายรวมถึง การเข้าถึงระยะไกล (remote control access) และ การเชื่อมโยงผ่านเครือข่ายส่วนตัวเสมือน (virtual private network)

ข) ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail server)

| หลักการพิจารณา | การดำเนินการ |
|---|---|
| 1. ผู้ให้บริการอีเมลแก่องค์กร | ถ้ามีการให้บริการโดยผู้ให้บริการภายนอก ผู้ให้บริการภายนอกต้องทำการเก็บข้อมูลจราจรคอมพิวเตอร์ให้กับองค์กร |
| 2. รายละเอียดของข้อมูลที่ทำการจัดเก็บต้องมีครบถ้วนตามข้อกำหนด | ตรวจสอบรายละเอียดของข้อมูลจราจร คอมพิวเตอร์ที่ทำการจัดเก็บไว้ว่ามีข้อมูลถูกต้องตามข้อกำหนดหรือไม่ |

| หลักการพิจารณา | การดำเนินการ |
|---|---|
| 3. ต้องมีการเก็บข้อมูลจราจรคอมพิวเตอร์ที่ บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ ผ่านโปรแกรมจัดการจากเครื่องสมาชิก เช่น POP3 หรือ IMAP4 | ตรวจสอบว่าเครื่องให้บริการจดหมาย อิเล็กทรอนิกส์ ให้บริการอะไรบ้างเพื่อให้สมาชิก เข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ องค์กรต้องเก็บข้อมูลจราจรคอมพิวเตอร์ของโปรแกรมดังกล่าวด้วย เช่น บริการ POP3 บริการ IMAP4 และบริการอื่นๆ |

ค) ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล

| หลักการพิจารณา | การดำเนินการ |
|---|---|
| 1. รายละเอียดของข้อมูลที่ทำการจัดเก็บต้องมีครบถ้วนตามข้อกำหนด | ตรวจสอบรายละเอียดของข้อมูลจราจร คอมพิวเตอร์ที่ทำการจัดเก็บไว้ว่ามีข้อมูลถูกต้องตามข้อกำหนดหรือไม่ |

ง) ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ

| หลักการพิจารณา | การดำเนินการ |
|---|---|
| 1. รายละเอียดของข้อมูลที่ทำการจัดเก็บต้องมีครบถ้วนตามข้อกำหนด | ตรวจสอบรายละเอียดของข้อมูลจราจร คอมพิวเตอร์ที่ทำการจัดเก็บไว้ว่ามีข้อมูลถูกต้องตามข้อกำหนดหรือไม่ |

จ) ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)

| หลักการพิจารณา | การดำเนินการ |
|---|---|
| 1. รายละเอียดของข้อมูลที่ทำการจัดเก็บต้องมีครบถ้วนตามข้อกำหนด | ตรวจสอบรายละเอียดของข้อมูลจราจร คอมพิวเตอร์ที่ทำการจัดเก็บไว้ว่ามีข้อมูลถูกต้องตามข้อกำหนดหรือไม่ |

ฉ) ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ Instance Messaging (IM)

| หลักการพิจารณา | การดำเนินการ |
|---|---|
| 1. รายละเอียดของข้อมูลที่ทำการจัดเก็บต้องมีครบถ้วนตามข้อกำหนด | ตรวจสอบรายละเอียดของข้อมูลจราจร คอมพิวเตอร์ที่ทำการจัดเก็บไว้ว่ามีข้อมูลถูกต้องตามข้อกำหนดหรือไม่ |
| 2. พิจารณาการให้บริการขององค์กรที่มีอยู่ ว่าเป็นการให้บริการในขอบข่าย | ถ้าการให้บริการอยู่ในขอบข่าย ให้พิจารณาพอร์ตการสื่อสาร และทำการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ที่ |

| หลักการพิจารณา | การดำเนินการ |
|---|---|
| การโต้ตอบกันบนเครือข่ายอินเทอร์เน็ตหรือไม่ | พอร์ตของบริการดังกล่าว |

3.1.2.2 กำหนดและจัดทำบัญชีรายชื่อของระบบให้บริการ หรือและ เครื่องให้บริการ ที่จำเป็นต้องเก็บ ข้อมูลจราจรทางคอมพิวเตอร์

เมื่อองค์กรสามารถวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ที่ผู้ให้บริการแต่ละประเภทต้องทำการจัดเก็บได้แล้ว จึงควรจัดบัญชีรายชื่อของเครื่องให้บริการที่จำเป็นต้องเก็บข้อมูลจราจรคอมพิวเตอร์ เพื่อสะดวกใช้เป็นข้อมูลในการบริการจัดการของผู้ดูแลข้อมูลจราจรคอมพิวเตอร์

3.1.3 การวิเคราะห์ปริมาณข้อมูลจราจรคอมพิวเตอร์ที่ต้องทำการจัดเก็บเบื้องต้น

การวิเคราะห์ปริมาณข้อมูลจราจรที่ต้องการจัดเก็บ เป็นขั้นตอนส่วนหนึ่งที่องค์กรต้องทำการวิเคราะห์ข้อมูลเบื้องต้นเพื่อที่จะสามารถเลือกระบบเก็บข้อมูลจราจรคอมพิวเตอร์ได้อย่างเหมาะสม และสามารถเก็บข้อมูลได้อย่างเพียงพอตามที่กฎหมายกำหนด การวิเคราะห์ปริมาณข้อมูล จราจรคอมพิวเตอร์เพื่อหาขนาดหน่วยบันทึกข้อมูลที่ต้องการ อาจใช้การประมาณการขนาด ข้อมูลในแต่ละวัน เพื่อประมาณการข้อมูลที่พอเพียงสำหรับการใช้เก็บข้อมูลตาม กฎหมายได้ (โดยปกติกฎหมายกำหนดให้เก็บข้อมูล 90 วัน หากมีเหตุสามารถสั่งให้เก็บเพิ่มเป็น 2 ปี หรือ 730 วันได้) ซึ่งการคำนวณเบื้องต้นสามารถทำได้หลายวิธี ผลลัพธ์ของการคำนวณ อาจใช้ไม่ได้ ในกรณีที่สภาพแวดล้อมการทำงานที่ต่างกัน หรือมีเงื่อนไข อื่นๆเข้ามาเกี่ยวข้อง โดยในมาตรฐานฉบับนี้นำเสนอเพียงแนวคิดเบื้องต้น เพื่อให้สามารถประเมินค่าเบื้องต้นได้เท่านั้น ดังวิธีคำนวณ ที่จะอธิบายดังต่อไปนี้

(1) การคำนวณโดยประมาณการจากความเร็วในการเชื่อมต่ออินเทอร์เน็ตขององค์กร

(2) การคำนวณโดยผลรวมของค่าเฉลี่ยจากข้อมูลจราจรเดิม

**หมายเหตุ** การคำนวณแต่ละวิธีอาจจะเหมาะสมกับองค์กรในแต่ละแบบ แตกต่างกันออกไป ขึ้นอยู่กับ สภาพแวดล้อมการทำงาน และเงื่อนไขอื่นๆ ดังนั้นผู้ดูแลระบบขององค์กรจึงควร พิจารณาเลือกวิธีคำนวณให้เหมาะสม

3.1.3.1 การคำนวณแบบประมาณการจากความเร็วในการเชื่อมต่ออินเทอร์เน็ตขององค์กร

การคำนวณแบบนี้เป็นการประมาณการ (Estimation) เหมาะสำหรับองค์กรที่มีขนาดเล็ก มีความเร็วในการเชื่อมต่ออินเทอร์เน็ตไม่สูง ใช้เพื่อประมาณการหาค่าหน่วยบันทึกข้อมูล จราจรทางคอมพิวเตอร์ โดยใช้หลักการประมาณค่าขนาดของข้อมูลจราจรเป็น ร้อยละของ จำนวนปริมาณข้อมูลสูงสุดที่สามารถใช้งานได้ (Data Transfer/Sec) โดยแสดงข้อมูลสรุป การคำนวณตามตาราง

| ความเร็วของการเชื่อมต่ออินเทอร์เน็ต ( Mbps) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| ปริมาณข้อมูลใน 1 วินาที (KB) | 122.07 | 244.14 | 366.21 | 488.28 | 610.35 | 732.42 | 854.49 | 976.56 |

| ความเร็วของการเชื่อมต่ออินเทอร์เน็ต ( Mbps) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| ปริมาณข้อมูลใน 1 นาที (MB) | 7.15 | 14.31 | 21.46 | 28.61 | 35.76 | 42.92 | 50.07 | 57.22 |
| ปริมาณข้อมูลใน 1 ชั่วโมง (MB) | 429.15 | 858.31 | 1287.46 | 1716.61 | 2145.77 | 2574.92 | 3004.07 | 3433.23 |
| ปริมาณข้อมูลใน 1 วัน (GB) | 10.06 | 20.12 | 30.17 | 40.23 | 50.29 | 60.35 | 70.41 | 80.47 |
| ปริมาณข้อมูลใน 1 เดือน (30 วัน) (GB) | 301.75 | 603.50 | 905.25 | 1206.99 | 1508.74 | 1810.49 | 2112.24 | 2413.99 |
| ปริมาณข้อมูลใน 3 เดือน (90 วัน) (GB) | 905.25 | 1810.49 | 2715.74 | 3620.98 | 4526.23 | 5431.47 | 6336.72 | 7241.96 |
| ปริมาณข้อมูลใน 1 ปี (365 วัน) (GB) | 3671.9 | 7343.8 | 11012.1 | 14684.0 | 18355.9 | 22027.8 | 25699.7 | 29371.6 |
| ปริมาณข้อมูลใน 2 ปี (730 วัน) (GB) | 7343.8 | 14687.6 | 22024.1 | 29367.9 | 36711.7 | 44055.5 | 51399.3 | 58743.1 |
| ประมาณการข้อมูลจราจรคิดเป็น % จากปริมาณข้อมูล 3 เดือน (90 วัน) | | | | | | | | |
| ข้อมูลจราจร 1% (GB) | 9.05 | 18.10 | 27.16 | 36.21 | 45.26 | 54.31 | 63.37 | 72.42 |
| ข้อมูลจราจร 5% (GB) | 45.26 | 90.52 | 135.79 | 181.05 | 226.31 | 271.57 | 316.84 | 362.10 |
| ข้อมูลจราจร 10% (GB) | 90.52 | 181.05 | 271.57 | 362.10 | 452.62 | 543.15 | 633.67 | 724.20 |
| ประมาณการข้อมูลจราจรคิดเป็น % จากปริมาณข้อมูล 1 ปี เดือน (365 วัน) | | | | | | | | |
| ข้อมูลจราจร 1% (GB) | 36.7 | 73.4 | 110.1 | 146.8 | 183.6 | 220.3 | 257.0 | 293.7 |
| ข้อมูลจราจร 5% (GB) | 183.6 | 367.2 | 550.6 | 734.2 | 917.8 | 1101.4 | 1285.0 | 1468.6 |
| ข้อมูลจราจร 10% (GB) | 367.2 | 734.4 | 1101.2 | 1468.4 | 1835.6 | 2202.8 | 2570.0 | 2937.2 |
| ประมาณการข้อมูลจราจรคิดเป็น % จากปริมาณข้อมูล 2 ปี (730 วัน) | | | | | | | | |
| ข้อมูลจราจร 1% (GB) | 73.4 | 146.9 | 220.2 | 293.7 | 367.1 | 440.6 | 514.0 | 587.4 |
| ข้อมูลจราจร 5% (GB) | 367.2 | 734.4 | 1101.2 | 1468.4 | 1835.6 | 2202.8 | 2570.0 | 2937.2 |
| ข้อมูลจราจร 10% (GB) | 734.4 | 1468.8 | 2202.4 | 2936.8 | 3671.2 | 4405.6 | 5139.9 | 5874.3 |

**หมายเหตุ** ค่าปริมาณการใช้ข้อมูลสูงสุดเป็นค่าที่เกิดจากคำนวณโดย ประมาณการจากสมมติฐานว่า การส่งผ่านข้อมูลมีประสิทธิภาพสูงสุด (utilization 100%) ไม่คิดค่า overhead และค่าการสูญเสียต่างๆ

จากข้อมูลในตารางจะเห็นได้ว่าในองค์กรที่มีขนาดเล็กจำนวนผู้ใช้งานน้อย ความเร็วในการเชื่อมต่ออินเทอร์เน็ตไม่สูง ปริมาณพื้นที่การเก็บข้อมูลจะมีขนาดเล็กเมื่อเทียบกับราคาอุปกรณ์เก็บข้อมูลในปัจจุบัน (ความเร็วอินเทอร์เน็ต 6 Mbps หากคิดข้อมูลจราจร 5% และเก็บข้อมูล 90 วัน ใช้พื้นที่เก็บข้อมูล 271.57 GB)

3.1.3.2 การคำนวณโดยผลรวมของค่าเฉลี่ยจากข้อมูลจราจรเดิม

การคำนวณแบบนี้เป็นแบบที่ละเอียดมากกว่าแบบแรก เหมาะสำหรับองค์กรที่มีความซับซ้อนมากขึ้น และแบบนี้องค์กรต้องมีการจัดทำบัญชีรายชื่อ ระบบให้บริการหรือเครื่องให้บริการที่จำเป็นต้องมีการเก็บข้อมูลจราจรคอมพิวเตอร์ไว้แล้ว โดยการคำนวณสามารถทำได้ดังนี้

(1) คำนวณหาค่าของปริมาณข้อมูลจราจรคอมพิวเตอร์ในแต่ละบริการ ซึ่งโดยปกติ แล้วบริการโดยทั่วไปจะมีการเก็บข้อมูลจราจรไว้ที่เครื่องให้บริการนั้นๆ และทำซ้ำใน ทุกรายการในบัญชีรายชื่อ

(2) ในกรณีที่มีการเก็บข้อมูลจราจรคอมพิวเตอร์ในแต่ละบริการไว้มากกว่า 1 วัน เช่น 1 สัปดาห์ ให้คำนวณเป็นค่าเฉลี่ยแทน

(3) คำนวณผลรวมของปริมาณข้อมูลทั้งหมดในทุกบริการในช่วงเวลา 1 วัน คูณด้วยจำนวน วันที่ต้องการทราบขนาดของหน่วยบันทึกข้อมูล (90 วัน)

(4) ในกรณีที่ไม่สามารถคำนวณหรือตรวจสอบจากข้อมูลจราจรได้ในทุกบริการ ให้คำนวณ โดยใช้ปริมาณข้อมูลจราจรคอมพิวเตอร์จากเครื่องให้บริการที่มีปริมาณมากที่สุดแทน

(5) ในกรณีที่ต้องการข้อมูลโดยหยาบที่สุดให้ใช้วิธีตรวจสอบค่าของปริมาณข้อมูลจราจรคอมพิวเตอร์จากเครื่องให้บริการที่คาดว่าจะมีการใช้งานมากที่สุดเป็นตัวตั้งแล้วคูณด้วยจำนวนเครื่องให้บริการแทน แล้วคูณด้วยจำนวนวันที่ต้องการทราบขนาดของหน่วยบันทึกข้อมูลแทน

สรุป

ขนาดของพื้นที่เก็บข้อมูลจราจร = ผลรวมของปริมาณข้อมูลทั้งหมดในทุกบริการในช่วงเวลา 1 วัน x จำนวนวันที่ต้องการทราบ

หรือ

ขนาดของพื้นที่เก็บข้อมูลจราจร = ปริมาณข้อมูลของเครื่องให้บริการที่มีการใช้งานมากที่สุด x จำนวนเครื่องให้บริการ x จำนวนวันที่ต้องการทราบ

3.2 หลักการเก็บข้อมูลของระบบเก็บข้อมูลจราจรคอมพิวเตอร์

ประเภทของระบบเก็บข้อมูลจราจรทางคอมพิวเตอร์ หากแบ่งตามหลักการจัดเก็บข้อมูลจากระบบให้บริการหรือเครื่องให้บริการ อาจแบ่งได้เป็น 5 ประเภท

(1) แบบที่ใช้หลักการดักจับข้อมูลจากเครือข่าย

(2) แบบที่ทำหน้าเป็นเกตเวย์หลักของระบบ

(3) แบบที่ใช้โปรแกรมติดตั้งที่ตัวเครื่องให้บริการ เพื่อเก็บข้อมูล

(4) แบบที่รองรับการส่งข้อมูลจากเกณฑ์วิธีการสื่อสาร syslog (syslog protocol)

(5) แบบผสม

3.2.1 แบบที่ 1 อุปกรณ์ที่ใช้หลักการดักจับข้อมูลจากเครือข่ายเพื่อจัดเก็บเป็นข้อมูลจราจรทางคอมพิวเตอร์

แบบนี้ใช้ลักษณะการทำเก็บข้อมูลโดยการดักฟังข้อมูลจราจร แล้วทำการกรองเฉพาะข้อมูลที่ตรงตามกฎที่ได้มีการกำหนดค่าไว้

**ข้อดี**

- สามารถติดตั้งได้ทุกสภาวะแวดล้อมการทำงาน ติดตั้งง่าย โดยไม่มีผลต่อประสิทธิภาพของระบบเครือข่าย
- การติดตั้งสามารถทำได้ หลายแบบเช่น การทำพอร์ตมิเรอร์ (mirror porting) การใช้อุปกรณ์ฮับเน็ตเวิร์ก (hub network) เป็นตัวขั้นกลาง หรือ การแท็ปที่สายโดยตรง

**ข้อเสีย**

- เนื่องจากวิธีการเก็บข้อมูลด้วยวิธีนี้มีความเสี่ยงในการคัดกรองข้อมูลที่มีความอ่อนไหวทางด้านความเป็นส่วนตัวของผู้ใช้งาน ดังนั้นการพิจารณาเลือกใช้งาน จำเป็นต้องมีการพิจารณา การออกแบบระบบในส่วนของการเก็บข้อมูล และการคัดกรองข้อมูลโดยละเอียด
- การทำหนังสือแจ้งหรือข้อตกลงเพื่อให้พนักงานในองค์กรรับทราบ ว่ามีการบันทึกข้อมูล และให้ทำหนังสือยอมรับ
- ข้อมูลที่อนุญาตให้เก็บได้ต้องเป็นข้อมูลตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และไม่ขัดต่อข้อกำหนดภายใน พ.ร.บ. ว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

3.2.2 แบบที่ 2 อุปกรณ์ที่ทำหน้าที่เป็นเกตเวย์ของเครือข่าย (network gateway)

อุปกรณ์แบบนี้ ใช้การเก็บข้อมูลโดยทำตัวเป็นเกตเวย์ของระบบ ข้อมูลจราจรจะถูกส่งผ่านอุปกรณ์ แบบนี้ก่อนถึงจะส่งผ่านไปที่เกตเวย์เดิมอีกครั้ง หรือบางระบบสามารถใช้ทดแทนอุปกรณ์เกตเวย์เดิมได้ และบางครั้งยังมีความสามารถอื่นๆ เพิ่มเติมลงไปได้ด้วย เช่น การทำพิสูจน์ตัวตน การกรองเว็บไซต์ไม่เหมาะสม การเก็บข้อมูลการใช้งานเครือข่าย

**ข้อดี**

- สามารถประยุกต์ประโยชน์ด้านอื่นได้นอกจากเก็บข้อมูลจราจรทางคอมพิวเตอร์ (ขึ้นอยู่กับความสามารถของแต่ละระบบ)

**ข้อเสีย**

- ในการติดตั้งมีการกระทบกับระบบเครือข่ายเดิม ทั้งในด้านโครงสร้างและในด้านประสิทธิภาพ
- การออกแบบการเก็บข้อมูลโดยไม่เก็บข้อมูลที่กระทบต่อข้อมูลส่วนบุคคล หรือ เทคนิคเฉพาะทางของผู้ผลิต

3.2.3 แบบที่ 3 แบบที่ใช้โปรแกรมติดตั้งที่ตัวเครื่องให้บริการ

แบบนี้จะมีการทำงานโดย ต้องติดตั้งโปรแกรมที่เครื่องให้บริการหรือระบบที่ต้องการเก็บข้อมูล โดยโปรแกรมจะทำหน้าที่ส่งข้อมูลจราจรคอมพิวเตอร์มาให้กับ ระบบเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ ได้เอง บางระบบเป็นระบบขนาดใหญ่สามารถรองรับจำนวนไคลเอนต์ (client) ได้มากและสามารถนำข้อมูลที่ได้ต่างๆ มาวิเคราะห์เพื่อประโยชน์อื่นๆ ได้

**ข้อดี**

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

**ข้อเสีย**

- ราคาค่อนข้างสูงเนื่องจากเป็นระบบที่ต้องการพัฒนาส่วนประกอบต่างๆ
- ต้องเข้าไปยุ่งเกี่ยวกับระบบหรือโปรแกรมให้บริการ

3.2.4 แบบที่ 4 รองรับการส่งข้อมูลจากเครื่องให้บริการโดยตรง (syslog protocol)

ระบบแบบนี้เป็นระบบที่แพร่หลายมากที่สุด รองรับการทำงานที่หลากหลาย มีทั้งระบบที่เป็นโอเพ่นซอร์ส (open source) สามารถนำไปปฏิบัติ (implement) เองได้ จนไปถึงระดับวิสาหกิจ (enterprise) ทำงานด้วยมาตรฐาน syslog โดยส่วนมาก โปรแกรมหรือเครื่องให้บริการต่าง ๆ มักรองรับการส่งข้อมูลจราจรคอมพิวเตอร์ด้วย มาตรฐานนี้

**ข้อดี**

- สามารถเก็บข้อมูลจราจรได้ทันทีจากระบบให้บริการหรือเครื่องให้บริการที่รองรับการเก็บข้อมูลแบบ syslog protocol
- ราคาไม่สูงเนื่องจากตัวแกนหลักเป็นโอเพ่นซอร์ส
- สามารถนำข้อมูลไปวิเคราะห์เพื่อประโยชน์ด้านอื่นได้

**ข้อเสีย**

- โดยมาตรฐานของ syslog เองไม่รองรับการเข้ารหัสข้อมูล แต่ผู้ใช้งานสามารถเลือกอุปกรณ์ที่ระบุรองรับการใช้งานร่วมกับ SSL หรือเลือกใช้งานโพรโตคอลที่เทียบเท่ากับ syslog-ng เช่น rsyslog ที่สามารถรองรับการส่งข้อมูลแบบเข้ารหัส SSL ได้ทันที

3.2.5 แบบผสม

แบบผสมเป็นแบบที่มีมากที่สุดในท้องตลาดเนื่องจากปัจจุบันการเก็บข้อมูลจราจรคอมพิวเตอร์ด้วยวิธีแบบใดแบบหนึ่งมักไม่ ครอบคลุมโปรแกรมให้บริการหรือเครื่องให้บริการทั้งหมด จึงจำเป็นต้องใช้เทคนิคและวิธีการ หลายแบบเพื่อให้ครอบคลุม

ข้อดีและข้อเสียของระบบก็จะขึ้นอยู่กับชนิดหรือวิธีที่เลือกใช้ในแต่ละแบบที่ผู้ผลิตเลือก

**ข้อดี**

- รวมความสามารถของระบบแบบต่าง ๆ ไว้ด้วยกัน

**ข้อเสีย**

- มีความซับซ้อนในการใช้เนื่องจากมีกรรมวิธีในการเก็บข้อมูลหลายแบบ
- ผู้ใช้งานต้องเป็นผู้เลือกวิธีให้เหมาะสม

## 4. แนวทางการจัดทำ

4.1 แนวทางการปฏิบัติตามคุณลักษณะและข้อกำหนดต่าง ๆ ตามมาตรฐานเล่มที่ 1

มาตรฐานเล่มที่ 1 กำหนดคุณลักษณะและข้อกำหนด เพื่อให้ระบบทำงานได้อย่างถูกต้องปลอดภัยและเป็นไปตามกฎหมาย โดยคุณสมบัติหรือข้อกำหนดต่าง ๆ อ้างอิงหลักการของมาตรฐาน ISO/IEC 27001 ซึ่งเป็นมาตรฐานของระบบการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ที่ได้มีการประยุกต์ เพื่อให้มีความเหมาะสมกับ ระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ความเข้มงวดของข้อกำหนดในแต่ละข้อขึ้นอยู่กับความสามารถของระบบ ขนาด และสภาพแวดล้อมการทำงานของระบบที่ต่างกัน มาตรการต่าง ๆ อาจจำเป็นต้องมีการเพิ่มความเข้มงวด หรือไม่จำเป็นต้องใช้

คุณลักษณะและข้อกำหนดตามมาตรฐานเล่มที่ 1 ไม่ได้กำหนดรายละเอียดทางด้านเทคนิคในเชิงลึก เพื่อให้ผู้จัดทำระบบสามารถเลือกใช้มาตรการที่เหมาะสมกับระบบที่พัฒนาขึ้น และเพื่อให้สะดวกต่อการจัดทำระบบหรือการปฏิบัติตาม ข้อกำหนดของมาตรฐานนี้ เป็นการสรุปข้อกำหนดของมาตรฐานเล่มที่ 1 เป็น หมวดหมู่ โดยอ้างอิงตามมาตรฐาน ISO/IEC 27001 พร้อมยกตัวอย่างแนวทางการปฏิบัติประกอบเพื่อความเข้าใจมากยิ่งขึ้น ดังรายละเอียดดังต่อไปนี้

**หมวด** : **คุณลักษณะทั่วไป**

**(1) ข้อกำหนด:** การแบ่งกลุ่มผู้ใช้งาน เช่น ผู้ดูแลข้อมูล ผู้ดูแลระบบ ผู้ใช้งานทั่วไป และการจัดการสิทธิ์

**วัตถุประสงค์:** เพื่อให้สามารถกำหนดกลุ่มผู้ใช้งาน ซึ่งมีหน้าที่ที่แตกต่างกันออกไป ระบบจำเป็นต้องมีการแบ่งแยกกลุ่มของผู้ใช้งานตามสิทธิ์ที่ได้รับ เช่น

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

**แนวทางการปฏิบัติ**

- การจัดทำระบบลงทะเบียนผู้ใช้งานเพื่อแยกกลุ่มผู้ใช้งาน และระบุตัวตนผู้ใช้งานว่าเป็นบุคคลใด
- การป้องกันการลงทะเบียนผู้ใช้งานที่ซ้ำซ้อนกัน
- การป้องกันการถือครองสิทธิ์ของผู้ใช้งานมากกว่า 1 กลุ่มผู้ใช้งาน
- การจำกัดจำนวนผู้ดูแลข้อมูลและผู้ดูแลระบบให้มีน้อยที่สุด

(2) **ข้อกำหนด:** การจัดการและควบคุมสิทธิ์ ของกลุ่มผู้ใช้งานและผู้ใช้งานในกลุ่มต่างๆ

**วัตถุประสงค์:** เพื่อให้สามารถควบคุมและจัดการสิทธิ์ ของกลุ่มผู้ใช้งานและผู้ใช้งานในกลุ่มต่างๆ ระบบจำเป็นต้องมีการควบคุมสิทธิ์ของกลุ่มของผู้ใช้งานตามสิทธิ์ ที่ได้รับ

**แนวทางการปฏิบัติ**

- การเลือกใช้งานระบบพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย
- การจัดการชั้นความลับของข้อมูล
- การเข้ารหัสข้อมูลที่มีชั้นความลับ เพื่อป้องกันการเข้าถึง

**หมวด : คู่มือและข้อแนะนำ**

(3) **ข้อกำหนด:** การระบุข้อมูลต่างๆ ที่จำเป็นสำหรับการใช้งานระบบ

**วัตถุประสงค์:** เพื่อให้ผู้ใช้งาน ผู้ดูแลระบบ และระบบสามารถทำงานได้อย่างถูกต้อง ผู้ผลิตจำเป็นต้อง สร้างเอกสาร คู่มือ หรือ เอกสารการแนะนำวิธีติดตั้ง การใช้งาน การเตรียมการต่างๆ เบื้องต้น ทั้งนี้รวมถึง การแก้ไขปัญหาเบื้องต้น ที่เกิดจากการใช้งานด้วย

**ตัวอย่างการดำเนินการ**

- เอกสารแนะนำระบบ ความต้องการของระบบ สภาพแวดล้อมการทำงาน ความสามารถ ข้อจำกัดต่างๆ ของระบบ
- เอกสารคู่มือ การเริ่มการใช้งานอย่างย่อ (quick start) การเตรียมการเบื้องต้น วิธีติดตั้ง การแก้ไขปัญหาเบื้องต้น
- เอกสารคู่มือ แนะนำการเตรียมการ การเลือกและกำหนดพื้นที่ติดตั้ง วิธีติดตั้งซึ่งรวมถึงรูปแบบและวิธีการเชื่อมต่อกับคอมพิวเตอร์เครื่องอื่น การใช้งาน การปรับตั้งค่าต่างๆ การตรวจสอบและการแก้ไขปัญหา และข้อมูลอื่นที่จำเป็นโดยละเอียด

(4) **ข้อกำหนด:** เอกสารคู่มือและข้อแนะนำการใช้งาน ต้องจัดทำเป็นภาษาไทย สำหรับคู่มือหรือข้อแนะนำเพิ่มเติมอื่น ที่ใช้ประกอบเพื่อเป็นข้อมูล อนุญาตให้ใช้ภาษาอื่นได้หากไม่เป็น การเพิ่มความเสี่ยงในการใช้งานปกติ

**วัตถุประสงค์:** เพื่อการสื่อความหมายที่ตรงกัน และสามารถครอบคลุมผู้ใช้งานได้ทุกกลุ่มผู้ใช้งาน

**ตัวอย่างการดำเนินการ**

- จัดทำเอกสารต่าง ๆ เป็นภาษาไทย

**หมวด : การแสดงเครื่องหมายและฉลาก**

**(5) ข้อกำหนด:** การแสดงเครื่องหมายหรือข้อความบนเปลือกหุ้มด้านนอกของบรรจุภัณฑ์ และบนเปลือกหุ้มของบริภัณฑ์หรือระบบ ในลักษณะที่สามารถเห็นได้ง่ายและชัดเจน ประกอบข้อมูลอย่างน้อยดังนี้

- ชื่อแบบรุ่น และชื่อผู้ทำ
- ประเภทของข้อมูลจราจรทางคอมพิวเตอร์ ที่สามารถเก็บได้
- คุณลักษณะพื้นฐานที่มีให้ หรือคุณลักษณะพื้นฐานที่ต้องการ ด้านการประมวลผลของระบบ ได้แก่ แบบรุ่นของหน่วยประมวลผล ขนาดของหน่วยความจำ
- ความสามารถในการจัดเก็บข้อมูล หรือขนาดความจุของฮาร์ดดิสก์หรือสื่ออื่นๆ ที่ต้องการ

**วัตถุประสงค์:** เพื่อประโยชน์ในการเลือกใช้งาน ความมั่นใจในการตัดสินใจเลือกระบบที่เหมาะสมของผู้ใช้งาน และการแสดงคุณสมบัติ ความสามารถ ขีดความสามารถในการขยายต่อเพิ่ม ของบริภัณฑ์หรือระบบ

**ตัวอย่างการดำเนินการ**

- การจัดทำสลากระบุข้อมูลที่จำเป็นเช่น

รายละเอียดคุณลักษณะเฉพาะ (detail specification)

ชื่อผลิตภัณฑ์ (product name): SimpleLoG

ชื่อรุ่น (model): S001

ประเภทข้อมูลจราจรคอมพิวเตอร์ที่จัดเก็บได้ (log category): พรบ 5(1) ข และ ค

ข้อมูลจราจรคอมพิวเตอร์ที่รองรับ (log support): Syslog , Apache , IIS , MS Windows Event log, Etc...

รายละเอียดฮาร์ดแวร์ (hardware detail)

หน่วยประมวลผล (CPU):

หน่วยความจำ (RAM):

ฮาร์ดดิสก์ไดรว (HDD):

**(6) ข้อกำหนด:** เครื่องหมายหรือข้อความ บนเปลือกหุ้มด้านนอกของบรรจุภัณฑ์ และบนเปลือกหุ้ม ของบริภัณฑ์ ต้องมีความคงทนต่อการใช้งานตามปกติ และอ่านเข้าใจได้ง่าย

**วัตถุประสงค์:** เพื่อความสะดวกและคงทนต่อการใช้งานของเครื่องหมายและข้อความ

**ตัวอย่างการดำเนินการ**

- จัดทำเครื่องหมายหรือข้อความด้วยวัสดุที่คงทน เช่น เป็นโลหะ

- วัสดุควรยึดติดกับอุปกรณ์ ด้วยอุปกรณ์ที่แข็งแรงไม่หลุดหรือลอกได้ง่าย
- เลือกใช้การพิมพ์ข้อความที่มีความชัดเจนไม่สามารถลบหรือเลือนได้เมื่อโดนน้ำ (กันน้ำได้)

**(7) ข้อกำหนด:** ระบบต้องแสดงข้อมูลต่อไปนี้ในเอกสารข้อแนะนำการติดตั้งระบบ

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

**คำอธิบาย/วัตถุประสงค์:** เพื่อให้ผู้ใช้งานสามารถเลือกระบบที่เหมาะสมกับองค์กรหรือหน่วยงาน ผู้ผลิตจำเป็นต้องระบุข้อมูลความสามารถของเครื่อง ตามรายละเอียดที่ข้อกำหนดบังคับ

- ประเภทของข้อมูลจราจรที่จัดสามารถจัดเก็บได้ รวมถึงรายละเอียดที่เกี่ยวข้องกัน อาทิ ชื่อและรุ่นของซอฟต์แวร์ประยุกต์ ชื่อและรุ่นของอุปกรณ์หรือบริการหรือระบบต้นทางใดๆ ที่เป็นแหล่งกำเนิดข้อมูลจราจรทางคอมพิวเตอร์
- ข้อกำหนดนี้ใช้เพื่ออ้างอิงความสามารถในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ตามประเภทของผู้ให้บริการและประเภทของข้อมูลที่ทำการจัดเก็บ
- คุณลักษณะพื้นฐานที่มีให้ หรือคุณลักษณะพื้นฐานที่ต้องการ ด้านการประมวลผลของระบบ ได้แก่ แบบรุ่นของหน่วยประมวลผล ขนาดของหน่วยความจำ
- ความสามารถในการจัดเก็บข้อมูลที่มีให้ หรือวิธีการคำนวณความสามารถในการจัดเก็บ
- จำนวนผู้ใช้งานสูงสุด และจำนวนเหตุการณ์สูงสุดต่อหน่วยเวลา ที่สามารถรองรับได้
- ความสามารถสูงสุด ที่สามารถขยาย หรือเพิ่มเติมได้ (ถ้ามี)

ข้อกำหนดนี้ใช้เพื่ออ้างอิงความสามารถของระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ความสามารถของฮาร์ดแวร์ ความสามารถในการขยายขีดความสามารถ และความสามารถอื่นๆ ที่ผู้ผลิตต้องการแสดงให้ผู้ใช้งานทราบ

**ตัวอย่างการดำเนินการ**

ตัวอย่างของข้อความระบุรายละเอียด ประเภท ของข้อมูลจราจรที่จัดสามารถจัดเก็บได้ รวมถึงรายละเอียดที่เกี่ยวข้องกัน

ระบบ ก. สามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ในประเภทต่อไปนี้ได้ และสามารถจัดเก็บได้จาก อุปกรณ์และซอฟต์แวร์ 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

**หมวด : ข้อกำหนดของระบบ**

**(8) ข้อกำหนด:** ระบบต้องสามารถเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามประเภทและความสามารถ ที่ระบุไว้ และต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ได้ต่อเนื่องเป็นเวลาไม่น้อยกว่า 90 วัน

**คำอธิบาย/วัตถุประสงค์:** การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ ไว้ได้ต่อเนื่องเป็นเวลา 90 วัน ถือเป็นข้อบังคับในทางกฎหมาย ทั้งนี้การตรวจสอบไม่สามารถทำได้โดยตรง ขึ้นอยู่กับจำนวนของเครื่องต้นทางที่เป็นแหล่งกำเนิดข้อมูลจราจรทางคอมพิวเตอร์ อย่างไรก็ตาม ข้อกำหนดนี้ไม่สามารถละทิ้งได้ การตรวจสอบจึงอาจทำได้โดยอ้อมดังรายละเอียดบางส่วนตามตัวอย่าง

**ตัวอย่างการดำเนินการ**

- ระบบต้องมีความสามารถในการขยายหน่วยความจำสำหรับบันทึกข้อมูลจราจร เพื่อให้สามารถรองรับการเก็บข้อมูลจราจรได้ 90 วันในสภาวะแวดล้อมใช้งานที่แตกต่างกัน
- ผู้ผลิตทำการประเมินการทำงานเบื้องต้นในสภาวะต่างๆ ของระบบ และกำหนดค่าสภาวะแวดล้อมต่างๆ เป็นตัวอย่างเพื่อให้ผู้ใช้งานได้เลือกใช้

**(9) ข้อกำหนด:** ระบบต้องสามารถปรับตั้งนาฬิกาภายใน ให้ตรงกับเวลาอ้างอิงมาตรฐานระดับชาติ ได้โดยอัตโนมัติ และมีการกำหนดความถี่ในการปรับตั้งค่าอัตโนมัติ โดยพิจารณาจากข้อมูลแวดล้อมที่เกี่ยวข้อง อาทิ ความเสถียรของระบบ

**คำอธิบาย/วัตถุประสงค์:** เพื่อให้ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ มีเวลาที่ตรงกับมาตรฐานสากลและสามารถใช้อ้างอิงในการวิเคราะห์เหตุการณ์ต่างได้ถูกต้อง

**หมายเหตุ** รายชื่อหน่วยงานและเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลาอ้างอิงมาตรฐานระดับชาติ ได้แก่

1. สถาบันมาตรวิทยาแห่งชาติ ได้แก่ time1.nimt.or.th (203.185.69.60) time2.nimt.or.th (203.185.69.59) และ time3.nimt.or.th (203.185.69.56)
2. กรมอุทกศาสตร์ กองทัพเรือ ได้แก่ time.navy.mi.th (118.175.67.83)
3. ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) ได้แก่

| |
|---|
| clock1.thaicert.org (203.185.129.186) และ clock2.thaicert.org (203.185.129.187) |

**ตัวอย่างการดำเนินการ**

- ระบบใช้โพรโทคอล NTP ในการปรับตั้งค่ากับเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลาอ้างอิงมาตรฐานระดับชาติ

**(10) ข้อกำหนด:** ระบบต้องมีการกำหนดการป้องกันการเข้าถึงระบบโดยผู้ไม่ได้รับอนุญาต ทั้งทางกายภาพและทางอิเล็กทรอนิกส์อย่างเหมาะสม ทั้งนี้อาจหมายรวมถึงข้อแนะนำต่างๆ ที่เกี่ยวข้อง โดยอย่างน้อยวิธีใดวิธีหนึ่ง หรือรวมกันต่อไปนี้

- การใช้รหัสผ่านหรือการยืนยันตัวบุคคลหรือวิธีการอื่นที่คล้ายกัน
- การจำกัดรูปแบบและวิธีการเข้าถึง
- การจำกัดจำนวนผู้ใช้
- การจำกัดเวลาการใช้
- การกำหนดช่วงเวลาที่อนุญาต
- การกำหนดใช้นโยบายและเทคนิคด้านความมั่นคงปลอดภัยอื่น

หากระบบอนุญาตให้เข้าถึงระยะไกลได้ โดยผ่านระบบคอมพิวเตอร์ที่ต่อเชื่อมถึงกันโดยโครงข่ายภายในองค์กรหรือโครงข่ายสาธารณะ 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 มีระบบรักษาความปลอดภัยแน่นหนา
- การปิดกั้นฝาเครื่อง (ในกรณีที่ทำได้)

- การกำหนดเวลาใช้งานสำหรับผู้ใช้งานทั่วไป
- การใช้งานโพรโตคอลสื่อสารที่มีการเข้ารหัสในการเข้าถึงระบบจากระยะไกลเช่น HTTPS, SSH
- การสงวนสิทธิ์ในการบริการจัดการบางสิทธิ์ที่ไม่สามารถทำได้ถ้ามีการเข้าถึงจากระยะไกล (local login only)

**(11) ข้อกำหนด:** ระบบต้องสามารถควบคุมและป้องกันการเปลี่ยนแปลงการตั้งค่าต่างๆ ของระบบโดยผู้ใช้ได้ สำหรับการตั้งค่าที่อนุญาตให้เปลี่ยนแปลงได้ ต้องสามารถควบคุมและป้องกัน การเปลี่ยนแปลงการตั้งค่า โดยผู้ใช้ที่ไม่เกี่ยวข้องได้

การเปลี่ยนแปลงการตั้งค่าใดๆ ของระบบ และบัญชีผู้ใช้ ต้องไม่ทำให้คุณสมบัติตามข้อกำหนด ที่ต้องการของมาตรฐานฉบับนี้ ด้อยลง หรือเสียสภาพ หรือเกิดความผิดพร่องขึ้น

**คำอธิบาย/วัตถุประสงค์:** ข้อนี้หมายถึง ระบบต้องมีมาตรการการควบคุมสิทธิ์ในการเข้าถึงการเปลี่ยนแปลงการตั้งค่าต่างๆของระบบโดยผู้ใช้ที่ไม่รับอนุญาต หรือไม่ได้รับสิทธิ์นั้นๆ เช่น ผู้ใช้งานทั่วไปต้องไม่สามารถเข้าถึงส่วนบริหารจัดการระบบได้ แต่บางระบบไม่ได้มีการป้องกัน ไว้ทำให้ผู้ใช้งานสามารถเข้าถึงระบบบริหารจัดการได้ ยกตัวอย่างให้เห็นภาพได้ง่าย เช่น ในกรณีที่เป็นเว็บแอปพลิเคชัน ถ้าไม่มีการบริหารจัดการ session ที่เข้มแข็งพอ อาจทำให้ผู้ใช้บริการสาธารณะ หรือผู้ใช้งานที่ไม่มีสิทธิ์สามารถเข้าถึงหน้าระบบบริหารจัดการ ได้โดยไม่ต้องพิสูจน์ตัวตน

**ตัวอย่างการดำเนินการ**

- ระบบจำเป็นต้องมีการออกแบบให้มีการตรวจสอบสิทธิ์ก่อนกระทำการใดๆ เพื่อป้องกันปัญหาดังกล่าว
- การบริการจัดการ session สำหรับเว็บแอปพลิเคชันที่ปลอดภัย

**(12) ข้อกำหนด:** ระบบต้องสามารถระบุและจำแนกตัวบุคคล และบันทึกประวัติการเข้าถึง และใช้งานระบบได้ รวมถึงต้องสามารถป้องกันการแก้ไข เปลี่ยนแปลง การปลอมแปลงข้อมูล ที่เกี่ยวข้องเพื่อการเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาตได้ เทคนิคและวิธีที่ใช้ ในการระบุตัวบุคคลและป้องกันการเปลี่ยนแปลง ควรเป็นเทคนิคที่ถูกตรวจสอบยืนยันความใช้ได้แล้ว

**คำอธิบาย/วัตถุประสงค์:**

- เพื่อให้สามารถตรวจสอบย้อนหลังหรือตรวจสอบพฤติกรรมของผู้ใช้งานและผู้ดูแลระบบได้ ระบบจำเป็นต้องมีการจำแนกตัวบุคคลและบันทึกประวัติการเข้าถึงและใช้งานระบบไว้

**ตัวอย่างการดำเนินการ**

- จัดให้มีการจำแนกตัวบุคคล และบันทึกประวัติการเข้าถึงและใช้งานระบบ

**(13) ข้อกำหนด:** ระบบควรมีการตรวจสอบความใช้ได้ของข้อมูลอื่น ที่ไม่ใช่ข้อมูลจราจรทางคอมพิวเตอร์ที่รับเข้าสู่ระบบ (input validation)

**คำอธิบาย/วัตถุประสงค์:**

- การโจมตีระบบโดยการส่งข้อมูลอื่นที่ไม่ใช้ข้อมูลจราจรหรือข้อมูลที่ถูกต้องของระบบมีผลทำให้ระบบสูญเสียความปลอดภัยและอาจทำให้ระบบทำงานผิดพลาดได้

**ตัวอย่างการดำเนินการ**

- จัดระบบให้มีการตรวจสอบข้อมูลนำเข้า (input validation) โดยเฉพาะอย่างยิ่งในระบบที่มีช่องทางการเข้าใช้งานผ่านระบบเว็บแอปพลิเคชัน

**(14) ข้อกำหนด:** ระบบควรจัดให้มีคำอธิบายเพื่อให้ความช่วยเหลือ (help) ในการแก้ไขปัญหา และข้อบกพร่องต่าง ๆ ที่มักเกิดขึ้น อย่างเหมาะสมและเพียงพอ

**คำอธิบาย/วัตถุประสงค์:**

- การแสดงข้อมูลช่วยเหลือ ช่วยลดปัญหาที่จะเกิดในการใช้งานระบบและช่วยอำนวยความสะดวกแก่ผู้ใช้งาน ลดการเกิดข้อผิดพลาดในการทำงาน

**ตัวอย่างการดำเนินการ**

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

**(15) ข้อกำหนด:** ระบบต้องสามารถรับข้อมูลจราจรทางคอมพิวเตอร์ จากอุปกรณ์ บริการหรือ ระบบต้นทาง ตามที่ระบุได้ อย่างครบถ้วน ถูกต้อง และหากเป็นไปได้ระบบควรมีระบบตรวจสอบ และปฏิเสธข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลอื่นที่ส่งมาจากระบบต้นทาง ที่ไม่ถูกต้องหรือผิดปกติ

**คำอธิบาย/วัตถุประสงค์:**

- การตรวจสอบข้อมูลที่ได้รับจากอุปกรณ์ต้นทาง นั้นมีผลโดยตรงต่อความถูกต้องของข้อมูลจราจรทางคอมพิวเตอร์ หากไม่มีมาตรการการตรวจสอบ ไม่อาจทำให้ทราบได้ว่าข้อมูลที่ถูกส่งจากต้นทางมีความถูกต้องสมบูรณ์หรือไม่
- การตรวจสอบและปฏิเสธแหล่งต้นทางที่ส่งข้อมูลจราจรคอมพิวเตอร์ เป็นสิ่งที่จำเป็นมาก เนื่องจากหากไม่มีการตรวจแหล่งต้นทางอาจเกิดการปลอมแปลงข้อมูลจราจรทางคอมพิวเตอร์ได้

**ตัวอย่างการดำเนินการ**

- การตรวจสอบความถูกต้องของข้อมูลต้นทางและปลายทางโดยใช้ฟังก์ชั่นแฮช
- การกำหนดช่วงเวลาการตรวจสอบความถูกต้องที่แน่นอน เช่น รายชั่วโมงหรือรายวัน
- การควบคุมแหล่งต้นจราจรทางคอมพิวเตอร์ทางโดยใช้ ไฟร์วอลล์ (firewall)
- การแยกช่องทางสื่อสารสำหรับส่งข้อมูลจราจรคอมพิวเตอร์โดยเฉพาะ (management network หรือ logging network)

**(16) ข้อกำหนด:** ข้อมูลจราจรทางคอมพิวเตอร์ ที่รับเข้ามาในระบบต้อง

- เก็บในสื่อ (media) ที่สามารถรักษาบูรณภาพของข้อมูลได้อย่างเหมาะสมและป้องกันการสูญหาย เสียหาย ถูกลบ ทำลาย แก้ไข ดัดแปลง ทั้งโดยเจตนาและไม่เจตนา
- เข้าถึงได้เฉพาะผู้ดูแลข้อมูล และไม่สามารถเข้าถึงได้โดยผู้ไม่เกี่ยวข้องหรือผู้ไม่ได้รับอนุญาต
- ถูกเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าที่ได้ระบุไว้ และต้องไม่น้อยกว่า 90 วัน

**คำอธิบาย/วัตถุประสงค์:**

- การรักษาบูรณภาพของข้อมูลเป็นเครื่องหมายที่บ่งบอกถึงความถูกต้องและความน่าเชื่อถือของข้อมูล ดังนั้นการเลือกสื่อที่ใช้บันทึกจำเป็นต้องมีการรักษาบูรณภาพของข้อมูลให้เหมาะสม
- เช่นเดียวกันกับการรักษาบูรณภาพของข้อมูล การอนุญาตให้เข้าถึงข้อมูลโดยไม่มีการป้องการหรือมาตรการตรวจสอบที่เหมาะสม อาจเป็นเหตุให้สูญเสียความถูกต้องและความน่าเชื่อถือของข้อมูล ทั้งที่เกิดโดยเจตนาและไม่เจตนา
- ระยะเวลาในการเก็บข้อมูลเป็นปัจจัยหนึ่งที่สำคัญ เพื่อให้เกิดประสิทธิภาพในการตรวจสอบกิจกรรมที่เกิดขึ้นจำเป็นต้องมีข้อมูลจราจรคอมพิวเตอร์มากพอในช่วงเวลาหนึ่ง อย่างน้อยไม่ควรต่ำกว่า 90 วันเพื่อให้เป็นไปตามที่กฎหมายกำหนด

**ตัวอย่างการดำเนินการ**

- การจัดทำระบบป้องกันการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ เช่น การพิสูจน์ตัวตนก่อนเข้าถึงข้อมูล การจัดชั้นความลับของข้อมูล การเข้ารหัสข้อมูลที่มีความลับ
- การจัดเลือกใช้สื่อ ที่สามารถรักษาบูรณภาพของข้อมูลได้สูง เช่น การเลือกใช้ฮาร์ดดิสก์แบบเรด (raid) การสำรองข้อมูลลงบนแผ่นซีดีหรือดีวีดีแบบบันทึกได้
- มาตรการการตรวจสอบความถูกต้องของข้อมูลโดยวิธีแฮช
- มาตรการการสำรองข้อมูลโดยสม่ำเสมอ
- มาตรการป้องกันทางกายภาพของตัวเครื่องหรือสภาพแวดล้อมที่ติดตั้งระบบ

**(17) ข้อกำหนด:** ระบบต้องสามารถป้องกันการแก้ไข เปลี่ยนแปลง ลบ ทำลายข้อมูลจราจร ทางคอมพิวเตอร์ ข้อมูลการใช้งานระบบ และข้อมูลคอมพิวเตอร์อื่นๆ ที่เกี่ยวข้อง โดยผู้ดูแลข้อมูล และผู้อื่นที่ไม่เกี่ยวข้องได้ ทั้งโดยเจตนาและไม่เจตนา

**คำอธิบาย/วัตถุประสงค์:**

- ข้อกำหนดเหล่านี้เป็นสิ่งที่ป้องกันการสูญเสียความถูกต้องและความน่าเชื่อถือของข้อมูลและตัวระบบเช่น กรรมวิธีการทำลายข้อมูลส่วนเกิดหรือข้อมูลที่ไม่มีความจำเป็น หากไม่มีกรรมวิธีที่ถูกต้องข้อมูลเหล่านี้จะสามารถกู้คืนกลับมาได้ ส่งผลให้มีผลต่อความลับของข้อมูลโดยตรง

**ตัวอย่างการดำเนินการ**

- การใช้มาตรการป้องกันแบบเดียวกับข้อมูลจราจรทางคอมพิวเตอร์ ในข้อมูลที่เกี่ยวข้องกับระบบอื่นๆ
- กำหนดกรรมวิธีหรือมาตรการทำลายข้อมูลที่ปลอดภัย สำหรับข้อมูลที่ไม่ได้ใช้งานหรือข้อมูลที่เกินความจำเป็น

**(18) ข้อกำหนด:** ระบบต้องสามารถตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้ได้ รวมถึงควรจัดให้มีการเฝ้าระวังบูรณภาพของข้อมูลอย่างเหมาะสม

**คำอธิบาย/วัตถุประสงค์:**

- การรักษาบูรณภาพของข้อมูลเป็นเครื่องหมายที่บ่งบอกถึงความถูกต้องและความน่าเชื่อถือของข้อมูล ดังนั้นระบบจำเป็นต้องมีกรรมวิธีรักษาบูรณภาพของข้อมูลและสามารถตรวจสอบได้เองโดยผู้ใช้งานระบบ

**ตัวอย่างการดำเนินการ**

- การจัดทำระบบตรวจสอบบูรณภาพของข้อมูลโดยใช้วิธีแฮช โดยอาจมีการทำแบบอัตโนมัติ ตามช่วงเวลาหรือ สามารถเลือกทำได้เองจากผู้ใช้งาน

## 5. แนวทางการตรวจสอบ

5.1 การตรวจสอบคุณลักษณะและข้อกำหนดตามมาตรฐานเล่มที่ 1

5.1.1 หมวด: คุณลักษณะทั่วไป

5.1.1.1 ข้อกำหนด: การแบ่งกลุ่มผู้ใช้งาน เช่น ผู้ดูแลข้อมูล ผู้ดูแลระบบ ผู้ใช้งานทั่วไป และการจัดการสิทธิ์

- มีผู้ดูแลระบบ หรือสามารถลงทะเบียนผู้ใช้ให้มีสิทธิเป็นผู้ดูแลระบบ ซึ่งสามารถติดตั้ง ตั้งค่า และตรวจสอบการทำงานของระบบได้
- มีผู้ดูแลข้อมูล หรือสามารถลงทะเบียนผู้ใช้ให้มีสิทธิเป็นผู้ดูแลข้อมูล ซึ่งสามารถเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ได้ ได้แก่ สามารถแสดงข้อมูลจราจรคอมพิวเตอร์เมื่อมีเหตุจำเป็นได้ สามารถตรวจดูความถูกต้องของข้อมูลได้
- ระบบต้องไม่อนุญาตให้กำหนดให้ผู้ใช้มีสิทธิเป็นทั้งผู้ดูแลระบบ และผู้ดูแลข้อมูลพร้อมกัน
- เมื่อลงทะเบียนผู้ใช้ด้วยชื่อบัญชีที่มีอยู่แล้ว ระบบต้องไม่อนุญาตให้กระทำได้
- ระบบควรมีมาตรการในการจำกัดจำนวนผู้ดูแลข้อมูลและผู้ดูแลระบบให้มีน้อยที่สุด

5.1.1.2 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

5.1.2 หมวด: คู่มือและข้อแนะนำ

5.1.2.1 ข้อกำหนด: มีเอกสารคู่มือที่ระบุข้อมูลต่างๆ ที่จำเป็นสำหรับการใช้งานระบบ ประกอบไปด้วยรายละเอียดต่างๆ ดังต่อไปนี้

- แนะนำระบบ
- ความต้องการของระบบ
- สภาพแวดล้อมการทำงานที่เหมาะสม
- ความสามารถ ข้อจำกัดต่างๆ ของระบบ
- รูปแบบและวิธีการเชื่อมต่อกับระบบเครือข่าย อุปกรณ์ หรือคอมพิวเตอร์เครื่องอื่นๆ
- การเตรียมการก่อนติดตั้ง
- วิธีการติดตั้ง
- การเริ่มต้นใช้งานอย่างย่อ
- การใช้งาน การปรับตั้งค่าต่าง ๆ
- การกำหนด หรือเปลี่ยนรหัสผ่าน
- วิธีการเรียกดูข้อมูล รวมทั้งวิธีการนำข้อมูลออกในกรณีที่เจ้าหน้าที่ร้องขอ
- การตรวจสอบและแก้ไขปัญหาเบื้องต้น

5.1.2.2 ข้อกำหนด: เอกสารคู่มือและข้อแนะนำการใช้งานเป็นภาษาไทย

- เอกสารคู่มือและข้อแนะนำต่างๆ ต้องจัดทำเป็นภาษาไทยเพื่อทำให้เกิดการสื่อความหมายที่ตรงกัน หากมีส่วนที่เป็นภาษาอื่นต้องไม่ทำให้เกิดความเสี่ยงในการใช้งานตามปกติ

5.1.3 หมวด: การแสดงเครื่องหมายและฉลาก

5.1.3.1 ข้อกำหนด: การแสดงเครื่องหมายหรือข้อความบนเปลือกหุ้มด้านนอกของบรรจุภัณฑ์ และบนเปลือกหุ้มของบริภัณฑ์หรือระบบ ประกอบไปด้วยข้อมูลอย่างน้อย

- ชื่อแบบรุ่น และชื่อผู้จัดทำ
- ประเภทของข้อมูลจราจรทางคอมพิวเตอร์ที่เก็บได้

- คุณลักษณะพื้นฐานที่มีให้ หรือคุณลักษณะพื้นฐานที่ต้องการด้านการประมวลผลของระบบ ได้แก่ แบบรุ่นของหน่วยประมวลผล ขนาดของหน่วยความจำ
- ความสามารถในการจัดเก็บข้อมูล หรือขนาดความจุของฮาร์ดดิสก์หรือสื่ออื่นๆ ที่ต้องการ

5.1.3.2 ข้อกำหนด: เครื่องหมายหรือข้อความ บนเปลือกหุ้มด้านนอกของบรรจุภัณฑ์ และบนเปลือกหุ้มของบริภัณฑ์ ต้องมีความคงทนต่อการใช้งานตามปกติ และอ่านเข้าใจได้ง่าย

- เครื่องหมายดังกล่าวมีความคงทนต่อน้ำ ความชื้น น้ำมันหรือคราบไขมัน สามารถทดสอบได้โดยการใช้ผ้าชุบน้ำถูเบาๆ เป็นเวลา 15 นาที และใช้ผ้าชุบน้ำมันปิโตรเลียมถูเบาๆ เป็นเวลา 15 นาที เครื่องหมายและข้อความต่างๆ ต้องยังสามารถแสดงได้ชัดเจน ไม่หลุดลอก หรือพับงอ
- หากวัสดุที่ใช้ทำฉลาก เป็นคนละชิ้นกับบรรจุภัณฑ์หรือเปลือกหุ้มบริภัณฑ์ ควรยึดติดกับบรรจุภัณฑ์หรือเปลือกหุ้มบริภัณฑ์ ด้วยอุปกรณ์หรือวิธีการที่แข็งแรง ไม่หลุดหรือลอกได้ง่าย

5.1.3.3 ข้อกำหนด: ระบบต้องแสดงข้อมูลต่อไปนี้ในเอกสารข้อแนะนำการติดตั้งระบบ

- ประเภทของข้อมูลจราจรที่สามารถจัดเก็บได้ รวมถึงรายละเอียดที่เกี่ยวข้องกัน อาทิ ชื่อและรุ่นของซอฟต์แวร์ประยุกต์ ชื่อและรุ่นของอุปกรณ์หรือบริการหรือระบบต้นทางใดๆ ที่เป็นแหล่งกำเนิดข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น
- คุณลักษณะพื้นฐานที่มีให้ หรือคุณลักษณะพื้นฐานที่ต้องการ ด้านการประมวลผลของระบบ ได้แก่ แบบรุ่นของหน่วยประมวลผล ขนาดหน่วยความจำ
- ความสามารถในการจัดเก็บข้อมูลที่มีให้ หรือวิธีการคำนวณความสามารถในการจัดเก็บ
- จำนวนผู้ใช้งานสูงสุด และจำนวนเหตุการณ์สูงสุดต่อหน่วยเวลา ที่สามารถรองรับได้
- ความสามารถสูงสุด ที่สามารถขยาย หรือเพิ่มเติมได้ (ถ้ามี)

การตรวจสอบคือตรวจดูว่ามีข้อมูลแสดงครบถ้วนหรือไม่ เช่นตัวอย่างต่อไปนี้

ระบบ ก. สามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ในประเภทต่อไปนี้ได้ และสามารถจัดเก็บได้จากอุปกรณ์และซอฟต์แวร์ 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

**คุณสมบัติทางฮาร์ดแวร์ของระบบ**

CPU: XXX 2.0 GHz

RAM: 2 GB

HDD: 500 GB

**ความสามารถของระบบ**

รองรับจำนวนเครื่องเซิร์ฟเวอร์ได้ไม่เกิน 5 เครื่อง

รองรับอัตราการส่งข้อมูลได้สูงสุด 1,000 เหตุการณ์ต่อวินาที

รองรับปริมาณข้อมูลจราจรทางคอมพิวเตอร์ได้เฉลี่ยวันละ 5.5 GB (เพื่อให้สามารถเก็บได้ถึง 90 วัน)

สามารถขยายความจุฮาร์ดดิสก์เพื่อให้เก็บข้อมูลจราจรทางคอมพิวเตอร์เพิ่มขึ้นได้อีก 1 ตัว ความจุสูงสุด 2,000 GB

5.1.4 หมวด: ข้อกำหนดของระบบ

5.1.4.1 ข้อกำหนด: ระบบต้องสามารถเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามประเภทและความสามารถที่ระบุไว้ และต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ได้ต่อเนื่องเป็นเวลาไม่น้อยกว่า 90 วัน

เนื่องจากไม่มีวิธีการที่จะบอกได้ว่าระบบจะเก็บข้อมูลได้ครบ 90 วันได้โดยตรง จำเป็นต้องตรวจสอบด้วยวิธีโดยอ้อมดังนี้

- ระบบต้องมีเอกสารที่บ่งบอกถึงความสามารถในการจัดเก็บ ข้อจำกัดต่างๆ สถานการณ์หรือสภาวะแวดล้อมต่างๆ เพื่อให้สามารถเลือกใช้ได้ตรงตามความต้องการ

- การตรวจสอบว่าระบบนั้นเหมาะสมกับการใช้ในองค์กรหรือไม่ ควรทำการประเมินองค์กรตามข้อ 3.1.3 การวิเคราะห์ปริมาณข้อมูลจราจรคอมพิวเตอร์ที่ต้องทำการจัดเก็บเบื้องต้น โดยอาจจะประเมินเผื่อถึงการใช้งานในอนาคตซึ่งอาจจะมีการใช้งานมากขึ้น จากนั้นนำผลที่ได้มาเปรียบเทียบกับคุณสมบัติของระบบ
- กรณีที่คาดว่าจะมีการขยายขนาดการใช้งานเครือข่ายในอนาคตซึ่งไม่อาจประมาณขนาดล่วงหน้าได้ อาจจะพิจารณาระบบที่สามารถขยายความสามารถได้ เช่นการเพิ่มดิสก์สำหรับจัดเก็บข้อมูล

5.1.4.2 ข้อกำหนด: ระบบต้องสามารถปรับตั้งนาฬิกาภายใน ให้ตรงกับเวลาอ้างอิงมาตรฐานระดับชาติ ได้โดยอัตโนมัติ

- โดยปกติเมื่อระบบเชื่อมต่อเข้ากับเครือข่ายแล้ว ระบบจะตั้งเวลาจาก time server ผ่านเครือข่ายอินเทอร์เน็ตโดยอัตโนมัติ การตรวจสอบในเบื้องต้นคือให้ดูเวลาที่อาจจะแสดงบนหน้าจอของระบบ เปรียบเทียบกับคอมพิวเตอร์เครื่องอื่นที่มีการตั้งเวลาจาก time server ผ่านเครือข่ายอินเทอร์เน็ตเช่นกันว่าถูกต้องตรงกันหรือไม่ ซึ่งเป็นการตรวจสอบอย่างคร่าวๆ
- ตรวจสอบว่าระบบมีการตั้งเวลาอัตโนมัติจากเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลามาตรฐานระดับชาติหรือไม่ ซึ่งอาจจะตรวจสอบได้โดยดูว่าระบบสามารถแสดงหรือตั้งค่าเกี่ยวกับเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลามาตรฐานได้หรือไม่ หรือมีระบุไว้ในเอกสารคู่มือหรือไม่ว่ามีการตั้งค่าเวลาจากเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลามาตรฐาน หรืออาจจะทราบจากการสอบถามทางเทคนิคจากผู้อิมพลีเมนต์ระบบ หรือผู้จัดทำระบบ

รายการเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลามาตรฐานระดับชาติ ได้แก่

(1) สถาบันมาตรวิทยาแห่งชาติ ได้แก่ time1.nimt.or.th (203.185.69.60) time2.nimt.or.th (203.185.69.59) และ time3.nimt.or.th (203.185.69.56)

(2) กรมอุทกศาสตร์ กองทัพเรือ ได้แก่ time.navy.mi.th (118.175.67.83)

(3) ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) ได้แก่ clock1.thaicert.org (203.185.129.186) และ clock2.thaicert.org (203.185.129.187)

อนุญาตให้ปรับเทียบเวลากับเครื่องแม่ข่ายภายในที่ให้บริการปรับเทียบเวลา ที่เทียบเท่าเวลามาตรฐานระดับชาติ โดยผิดพลาดไม่เกิน 10 มิลลิวินาที

5.1.4.3 ข้อกำหนด: ระบบต้องมีการกำหนดการป้องกันการเข้าถึงระบบโดยผู้ไม่ได้รับอนุญาต ทั้งทางกายภาพและทางอิเล็กทรอนิกส์อย่างเหมาะสม

- โดยปกติระบบควรจะมีการตรวจสอบยืนยันตัวบุคคลที่เข้าใช้งานระบบด้วยวิธีล็อกอินด้วยชื่อผู้ใช้และรหัสผ่าน หรืออาจจะเป็นวิธีอื่นที่คล้ายกันหรือดีกว่า
- ถ้าล็อกอินจากระยะไกล ระบบควรจัดให้อยู่ในสถานะการเชื่อมต่อที่มีความปลอดภัย เช่น HTTPS, SSH, SSL

- การติดตั้งเครื่องไว้ในห้องที่ปิดกั้นมิดชิด มีระบบรักษาความปลอดภัยแน่นหนา
- อาจจะใช้วิธีการอื่นๆ ต่อไปนี้ เพื่อช่วยเสริมให้มีความปลอดภัยมากขึ้น ได้แก่
    - การจำกัดรูปแบบและวิธีการเข้าถึง
    - การจำกัดจำนวนผู้ใช้
    - การจำกัดเวลาการใช้
    - การกำหนดช่วงเวลาที่อนุญาต
    - จำกัดสิทธิ์ที่สำคัญบางอย่างถ้าเข้าถึงจากระยะไกล
    - การปิดฝาเครื่อง

5.1.4.4 ข้อกำหนด: ระบบต้องสามารถควบคุมและป้องกันการเปลี่ยนแปลงการตั้งค่าต่างๆ ของระบบโดยผู้ใช้ได้ สำหรับการตั้งค่าที่อนุญาตให้เปลี่ยนแปลงได้ ต้องสามารถควบคุมและป้องกันการเปลี่ยนแปลงการตั้งค่า โดยผู้ใช้ที่ไม่เกี่ยวข้องได้

- ผู้ใช้ทั่วไปที่เข้าใช้ระบบ จะต้องไม่สามารถเข้าถึงส่วนบริหารจัดการระบบได้
- เมื่อพยายามเข้าสู่ส่วนบริหารจัดการระบบโดยตรง เช่นทราบ URL โดยตรงที่จะเข้าไปได้ ระบบจะต้องมีการตรวจสอบสิทธิก่อนว่ามีสิทธิหรือไม่ ถ้าไม่มีต้องไม่อนุญาตให้เข้าถึงได้
- ถ้าเป็นการเข้าถึงผ่านเว็บ ต้องมีระบบ session ที่ปลอดภัย

5.1.4.4 ข้อกำหนด: ระบบต้องสามารถระบุและจำแนกตัวบุคคล และบันทึกประวัติการเข้าถึงและใช้งานระบบได้ รวมถึงต้องสามารถป้องกันการแก้ไข เปลี่ยนแปลง การปลอมแปลงข้อมูลที่เกี่ยวข้องเพื่อการเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาตได้ เทคนิคและวิธีที่ใช้ในการระบุตัวบุคคลและป้องกันการเปลี่ยนแปลง ควรเป็นเทคนิคที่ถูกตรวจสอบยืนยันความใช้ได้แล้ว

- ตรวจดูว่าระบบมีการจำแนกตัวบุคคลหรือไม่ คือมีบัญชีผู้ใช้ของแต่ละคนแยกจากกัน และมีการระบุตัวบุคคลได้โดยวิธีการต่างๆ เช่นรหัสผ่าน
- ตรวจดูว่ามีบันทึกประวัติการเข้าถึงและใช้งานระบบได้

5.1.4.5 ข้อกำหนด: ระบบควรมีการตรวจสอบความใช้ได้ของข้อมูลอื่น ที่ไม่ใช่ข้อมูลจราจรทางคอมพิวเตอร์ที่รับเข้าสู่ระบบ (input validation)

- ทดสอบการป้อนข้อมูลที่สามารถทำให้เกิดข้อผิดพลาดหรือช่องโหว่ถ้าไม่ได้มีการตรวจสอบการรับข้อมูล เช่น กรอกข้อความว่า anything' OR 'x'='x ลงไปในช่องชื่อผู้ใช้ แล้วลองกดปุ่มล็อกอิน และลองสลับไปใส่ในช่องรหัสผ่าน แล้วกดล็อกอินตามลำดับ ถ้าระบบไม่มีการตรวจสอบข้อมูลที่รับเข้าสู่ระบบ ระบบอาจจะยอมให้เข้าใช้ระบบได้โดยไม่ต้องใช้ชื่อผู้ใช้ และรหัสผ่าน หรือแสดงให้เห็นว่าเกิดปัญหาที่ระบบไม่ได้เตรียมการรองรับไว้

- ระบบที่ยอมให้รับไฟล์เข้าสู่ระบบได้ ระบบควรมีการตรวจสอบหรือจำกัดชนิดไฟล์ก่อนจัดเก็บลงบนระบบ โดยให้ทดสอบการรับไฟล์ด้วยไฟล์ที่อาจทำให้เกิดข้อผิดพลาดหรือช่องโหว่ได้ เช่น ไฟล์สกุล php ไฟล์สกุล cgi ไฟล์สกุล jsp ไฟล์กระทำการ (executable file) อื่น ๆ หากระบบที่ไม่มีการตรวจสอบหรือจำกัดชนิดไฟล์ฯ ระบบควรมีการปิดกั้นไม่ให้ไฟล์ดังกล่าวทำงานได้ เพื่อลดความเสี่ยงที่ระบบอาจทำงานผิดพลาดหรือล้มเหลว

5.1.4.6 ข้อกำหนด: ระบบควรจัดให้มีคำอธิบายเพื่อให้ความช่วยเหลือ ในการแก้ไขปัญหาและข้อบกพร่องต่าง ๆ ที่มักเกิดขึ้น อย่างเหมาะสมและเพียงพอ

- มีส่วนที่อำนวยความสะดวกในการใช้งาน เพื่อให้การทำงานเป็นไปอย่างถูกต้อง เช่น มีระบบให้ความช่วยเหลือในหน้าต่างหลักของโปรแกรม มีการจัดทำตัวช่วยตั้งค่าแบบ wizard ในส่วนการตั้งค่าที่ซับซ้อน

5.1.5 หมวด: การรับและเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

5.1.5.1 ข้อกำหนด: ระบบต้องสามารถรับข้อมูลจราจรทางคอมพิวเตอร์ จากอุปกรณ์ บริการหรือระบบต้นทาง ตามที่ระบุได้ อย่างครบถ้วน ถูกต้อง และหากเป็นไปได้ระบบควรมีระบบตรวจสอบและปฏิเสธข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลอื่นที่ส่งมาจากระบบต้นทาง ที่ไม่ถูกต้องหรือผิดปกติ

- ในกรณีที่ระบบสามารถรับข้อมูลจราจรทางคอมพิวเตอร์จากอุปกรณ์ บริการหรือระบบต้นทางอื่นได้ ระบบต้องมีการระบุความสามารถในการรับข้อมูลสูงสุด เช่น สามารถรับข้อมูลจราจรได้สูงสุด 1500 เหตุการณ์ต่อวินาที และในสภาวะดังกล่าว ข้อมูลจราจรต้องได้รับครบถ้วน ไม่ตกหล่น

  การทดสอบสามารถทำได้โดยใช้โปรแกรม loggen ซึ่งมาพร้อมกับชุดซอฟต์แวร์ syslog-ng เพื่อสร้างข้อมูลจราจรทางคอมพิวเตอร์จำลองขึ้นในอัตราต่างๆ และตรวจสอบจำนวนข้อมูลที่ได้รับเทียบกับจำนวนข้อมูลที่สร้างขึ้นจริง

- การจะรับข้อมูลจากอุปกรณ์ บริการหรือระบบต้นทางต่างๆ จะต้องมีการกำหนดให้ลงทะเบียนอุปกรณ์ บริการหรือระบบต้นทางนั้นๆ ก่อน

- หากมีการส่งข้อมูลจากอุปกรณ์ บริการหรือระบบต้นทางที่ไม่ได้ลงทะเบียน ระบบจะต้องปฏิเสธไม่รับข้อมูล หรือแยกเก็บต่างหากเพื่อความสะดวกในการตรวจสอบภายหลัง

5.1.5.2 ข้อกำหนด: ข้อมูลจราจรทางคอมพิวเตอร์ ที่รับเข้ามาในระบบต้อง

- เก็บในสื่อที่สามารถรักษาบูรณภาพของข้อมูลได้อย่างเหมาะสมและป้องกันการสูญหาย เสียหาย ถูกลบ ทำลาย แก้ไข ดัดแปลง ทั้งโดยเจตนาและไม่เจตนา

- เข้าถึงได้เฉพาะผู้ดูแลข้อมูล และไม่สามารถเข้าถึงได้โดยผู้ไม่เกี่ยวข้องหรือผู้ไม่ได้รับอนุญาต

- ถูกเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าที่ได้ระบุไว้ และต้องไม่น้อยกว่า 90 วัน

การตรวจสอบ

- สื่อที่บันทึกข้อมูลจราจรทางคอมพิวเตอร์ ควรมีการจัดทำให้มีความปลอดภัยอย่างหนึ่งอย่างใดหรือหลายอย่างรวมกันต่อไปนี้
    - ใช้ดิสก์ระบบ RAID ที่มีความปลอดภัย เช่น RAID-1 หรือ RAID-5
    - มีระบบสำรองข้อมูล โดยมีกระบวนการเก็บสำเนาที่ปลอดภัย เช่น เก็บในตู้ที่ปิดล็อกได้
    - ใช้คุณสมบัติการตรวจสอบฮาร์ดดิสก์อัตโนมัติในตัวดิสก์ (SMART) โดยคอยเข้าไปอ่านค่าในตัวดิสก์อย่างสม่ำเสมอ หากพบความผิดปกติ ต้องรีบแจ้งเตือนผ่านระบบทันที
    - อยู่ในพื้นที่ที่มีความปลอดภัยจากบุคคลที่ไม่เกี่ยวข้อง จากอันตรายต่างๆ เช่น ความร้อน แสงแดด ความชื้น น้ำ ฝุ่น
- ระบบ สื่อที่เก็บข้อมูลจราจรหลัก สื่อที่เก็บข้อมูลจราจรที่เป็นสำเนา ต้องไม่สามารถเข้าถึงได้โดยผู้ที่ไม่เกี่ยวข้องโดยเด็ดขาด
- การเข้าถึงข้อมูลจากระยะไกลต้องเข้าถึงได้จากผู้ดูแลข้อมูลเท่านั้น โดยใช้วิธีการพิสูจน์ตัวตนที่ปลอดภัย
- ข้อมูลจราจรที่จัดเก็บต้องสามารถจัดเก็บได้อย่างน้อยตามที่ระบุไว้ในคุณสมบัติของระบบ และไม่น้อยกว่า 90 วัน โดยใช้วิธีประเมินวิธีใดวิธีหนึ่ง หรือหลายวิธีดังต่อไปนี้
    - ผู้ผลิตมีเอกสารแนะนำวิธีการคำนวณหรือประเมินขนาดของสื่อที่ใช้ว่าควรใช้ขนาดเท่าใดเพื่อให้เก็บข้อมูลจราจรได้อย่างน้อย 90 วัน
    - ดูจากปริมาณข้อมูลจราจรที่เก็บในแต่ละวันว่าเป็นเท่าใด และคาดการณ์ว่าในอนาคตจะมีปริมาณเพิ่มขึ้นเท่าไหร่ แล้วใช้ประเมินขนาดสื่อที่ต้องใช้เก็บว่ามีเพียงพอหรือไม่
    - ระบบสามารถเพิ่มขยายความจุของสื่อที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ได้
    - ระบบสามารถลบข้อมูลจราจรทางคอมพิวเตอร์ที่เกิน 90 วันได้โดยอัตโนมัติ

5.1.5.3 ข้อกำหนด: ระบบต้องสามารถป้องกันการแก้ไข เปลี่ยนแปลง ลบ ทำลายข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลการใช้งานระบบ และข้อมูลคอมพิวเตอร์อื่นๆ ที่เกี่ยวข้อง โดยผู้ดูแลข้อมูล และผู้อื่นที่ไม่เกี่ยวข้องได้ ทั้งโดยเจตนาและไม่เจตนา

การตรวจสอบ

- ผู้ดูแลข้อมูลไม่สามารถแก้ไข ลบ หรือเพิ่มข้อมูลจราจรได้
- ระบบถูกติดตั้งในตำแหน่งที่ปลอดภัยในเน็ตเวิร์ค เช่นอยู่ในโซนเดียวกันกับเซิร์ฟเวอร์หรืออุปกรณ์ที่เป็นแหล่งกำเนิดข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งไม่เกี่ยวข้องกับโซนของผู้ใช้ทั่วไปและบุคคลอื่น ๆ

5.1.5.4 ข้อกำหนด**:** ระบบต้องสามารถตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้ได้ รวมถึงควรจัดให้มีการเฝ้าระวังบูรณภาพของข้อมูลอย่างเหมาะสม

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

5.2 การตรวจสอบความปลอดภัยของการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

5.2.1 การตรวจสอบความถูกต้องของข้อมูลจราจรคอมพิวเตอร์

5.2.1.1 การตรวจสอบความถูกต้องของข้อมูลด้วย MD5

ก) บนระบบปฏิบัติการลินุกซ์ ให้ใช้คำสั่ง md5sum ตัวอย่าง เช่น

- md5sum log-2011-02-11.tar.gz
  5c2b79ab0c594af22aedfe6cd9180817 log-2011-02-11.tar.gz
  จะได้ค่าไดเจสต์คือ 5c2b79ab0c594af22aedfe6cd9180817 เพื่อนำไปเปรียบเทียบว่าถูกต้องตรงกันหรือไม่

ข) บนระบบปฏิบัติการวินโดวส์ ให้ติดตั้งซอฟต์แวร์ที่สามารถหาค่า MD5 จากแฟ้มต่างๆ ได้ เช่น โปรแกรมคำสั่งแบบคอมมานด์ไลน์ชื่อ md5sum.exe จากเว็บไซต์ http://www.pc-tools.net/win32/md5sums/

- ตัวอย่างการตรวจสอบด้วย md5sum.exe ซึ่งต้องเปิด Command Prompt ขึ้นมาก่อน แล้วสั่ง
  C:\Dowloads> md5sum log-2011-02-11.tar.gz
  5c2b79ab0c594af22aedfe6cd9180817 log-2011-02-11.tar.gz
  จากนั้นก็นำค่าไดเจสต์ที่ได้ไปเปรียบเทียบว่าถูกต้องตรงกันหรือไม่

## ภาคผนวก ก.

(ข้อแนะนำ)
การตรวจสอบความถูกต้องครบถ้วนของข้อมูล
(ข้อ 4.1 (15))

ก.1 วิธีแฮช (hash)

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

---