Thai

Not only PROTECTION, but LEGALIZE your business NOW!

SRAN Log Module

Centralization Log Management System

มั่นใจว่าเก็บข้อมูลจราจรคอมพิวเตอร์ได้ถูกต้องตามกฎหมายประเทศไทย

เพราะเราผ่านตามข้อกำหนดมาตรฐาน มศอ. NTS 4003.1-2552 มาตรฐานระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log files) จากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC)

SRAN

SRAN Log Module (LM)

เป็นระบบรับข้อมูลจราจรคอมพิวเตอร์แบบรวมศูนย์ (Centralized Logs Management) คือ อุปกรณ์ในการจัดเก็บ Log files จากอุปกรณ์อื่นๆ ที่อยู่ภายในเครือข่าย สามารถจัดเก็บ log files ที่เกิดจากการส่งจากอุปกรณ์เครือข่าย ได้แก่ Router , Firewall , NIPS /IDS , Load Balancer เครื่องแม่ข่ายที่สำคัญในองค์กร ได้แก่ AD Server , Proxy Server , Web Server และ Data Base Server เป็นต้น

โดยมีโมเดลทั้งหมด เหมาะสมกับองค์กร ทั้งขนาดเล็ก ขนาดกลาง และขนาดใหญ่

โดยมีทั้งหมด 4 รุ่น คือรุ่น

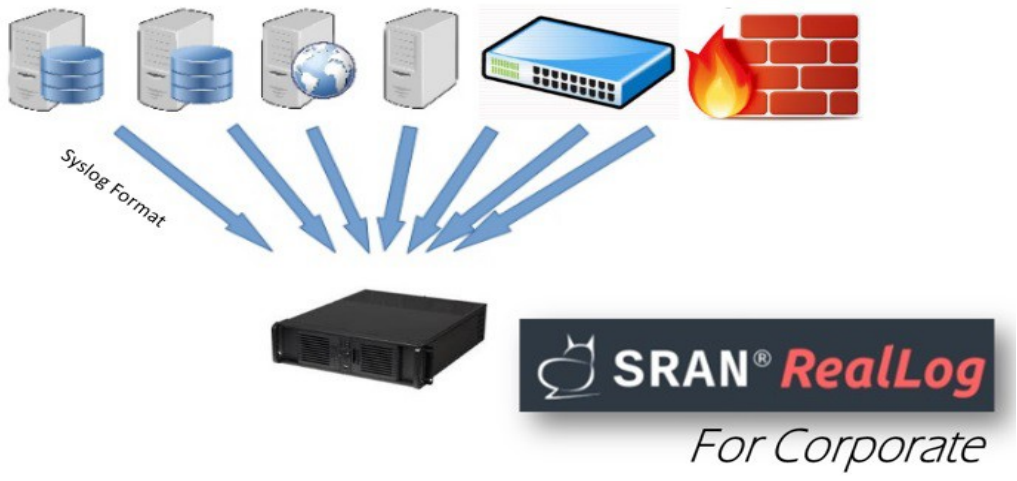
LM50 หน่วยงานขนาดเล็ก LM200 และ LM450 หน่วยงานขนาดกลาง LM850 สำหรับหน่วยงานขนาดใหญ่

ด้วยประสบการณ์ SRAN ที่พัฒนาสินค้าและผลิตภัณฑ์การจัดเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์มาอย่างยาวนาน ได้มีการปรับปรุงพัฒนาซอฟต์แวร์ Log Module เพื่อจัดเก็บบันทึกข้อมูลตามกฎหมายประเทศไทย

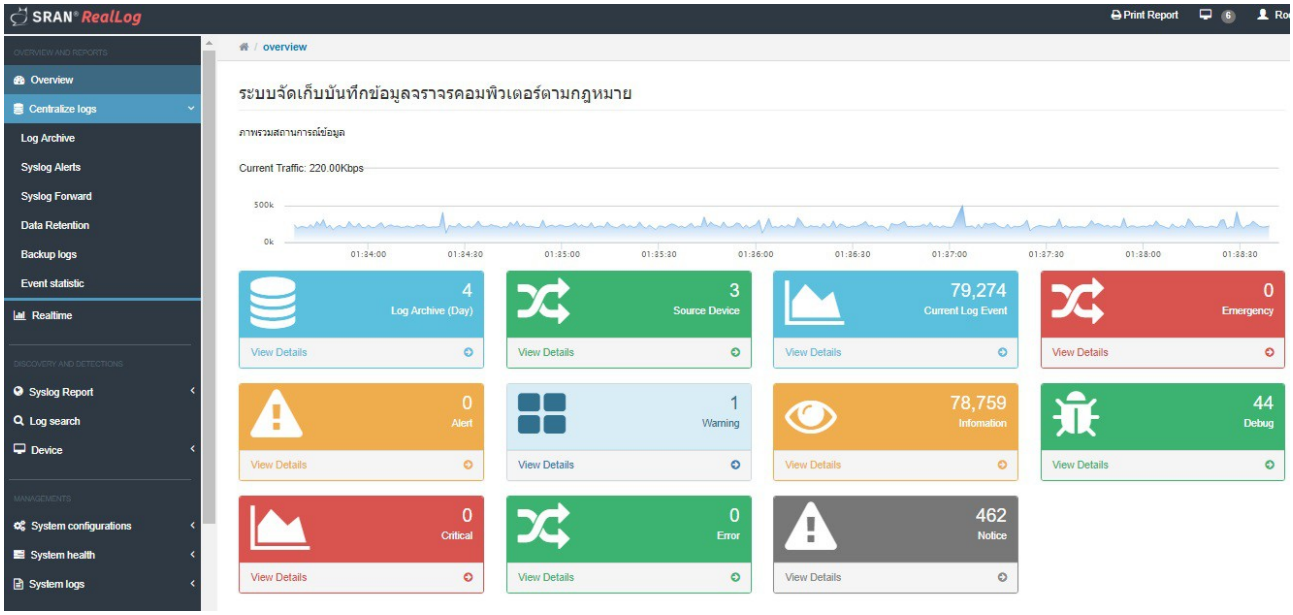
Code Name = “RealLog”

With Software SRAN Log Module

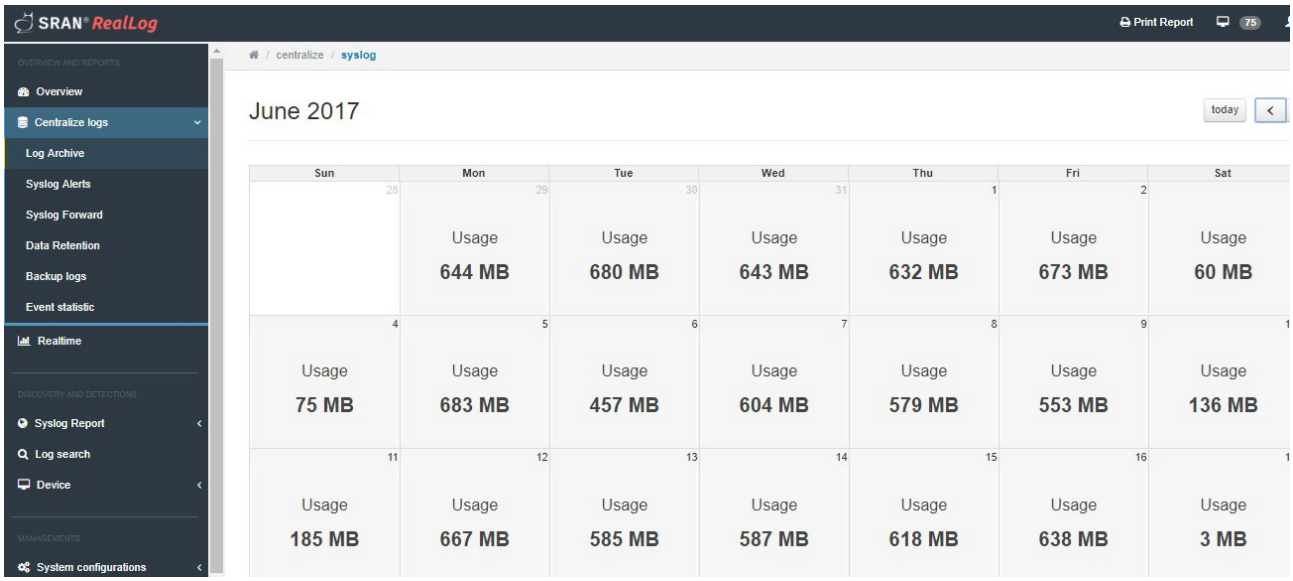
การออกแบบระบบรับค่าข้อมูลจราจรคอมพิวเตอร์จากส่วนกลาง (Centralized Logs Management)



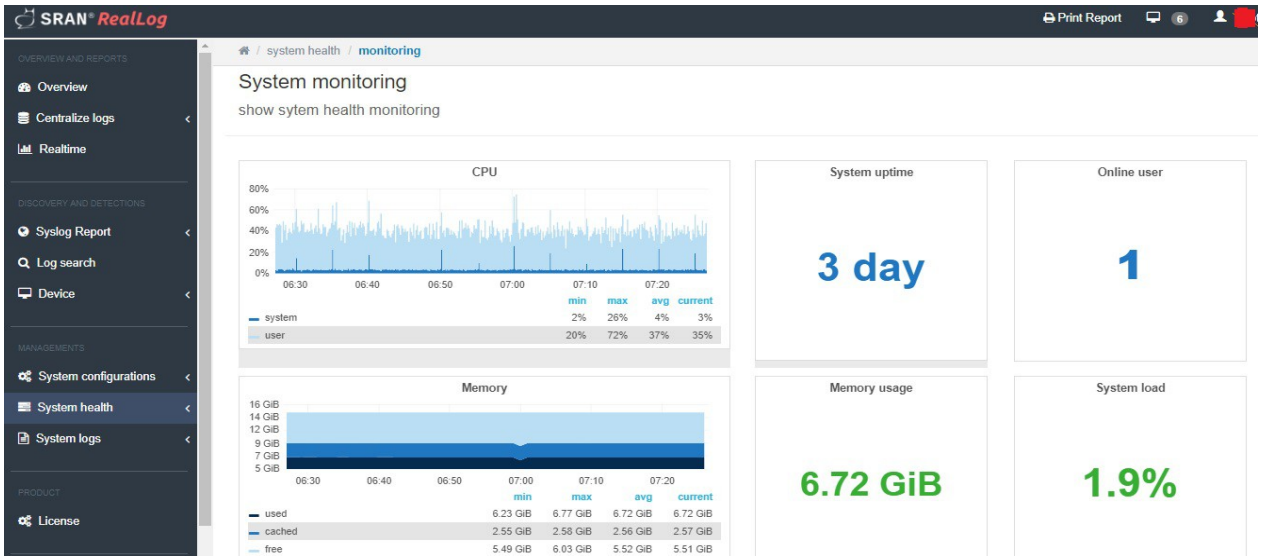
ตัวอย่างหน้าจอในการเก็บบันทึกข้อมูล



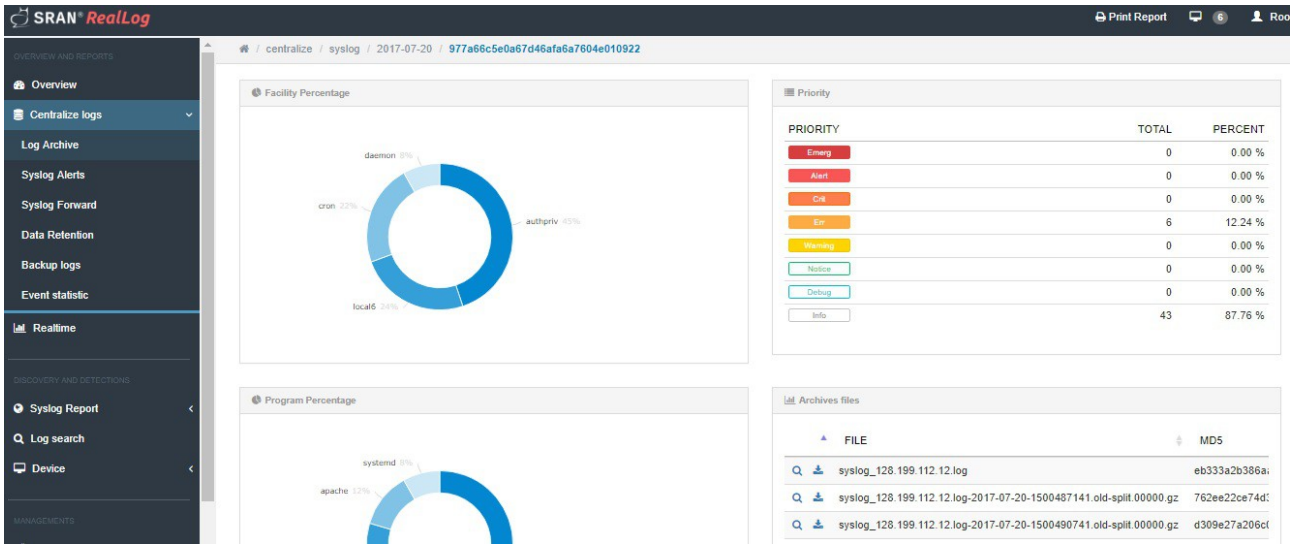
ภาพที่ 1 การแสดงผลรายงานภาพรวมการสถานการณ์การเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์ตามกฎหมาย โดยจัดทำรายงานตาม RFC5424 และ RFC 3164



ภาพที่ 2 การบันทึกจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log Archive) โดยเทคโนโลยีการบีบอัดข้อมูลและเข้ารหัสผ่านเพื่อยืนยันความถูกต้องของข้อมูล RAW Log



ภาพที่ 3 การแสดงผลภาพรวมของระบบแสดงผ่าน Web GUI ที่มีการตั้งค่าความมั่นคงปลอดภัยผ่านช่องทาง HTTPS



ภาพที่ 4 รายงานผลตามอุปกรณ์ (Devices) ที่ส่งค่า Log files เข้ามาเก็บ รองรับอุปกรณ์ที่เป็น Network Devices ได้แก่ Firewall , Switch , NIDS/IPS , Proxy และเครื่องแม่ข่าย (Server) ได้แก่ Web Server , Data Base Server และ Application Server

ตารางเปรียบเทียบสินค้า SRAN RealLog with Software Log Module for Corporate

คุณสมบัติ	LM 50	LM200	LM450	LM850
1. การรองรับค่าอุปกรณ์สามารถเก็บรวบรวมเหตุการณ์ (logs or Events) จากอุปกรณ์อื่น ในกรณีที่รับค่าจาก syslog	3 อุปกรณ์	5 อุปกรณ์	10 อุปกรณ์	15 อุปกรณ์
2. ขนาดพื้นที่ความจุข้อมูลจราจรคอมพิวเตอร์จากตัวเครื่องเอง	1 T สามารถรองรับการเชื่อมต่อ NAS ได้ (No Support Raid)	2 T สามารถรองรับการเชื่อมต่อ NAS ได้ (No Raid support)	4 T สามารถรองรับการเชื่อมต่อ NAS ได้ (Support Raid 5,10)	8T สามารถรองรับการเชื่อมต่อ NAS ได้ (Support Raid 5,10)
3. ขนาดเครื่อง	Desktop mini Server	Server 1 U	Server 1 U	Server 2 U
4. การเก็บรวมบรวมข้อมูล (Collect and Index Log Data) 4.1 สามารถรองรับค่า Log files จากอุปกรณ์ระบบเครือข่าย เครื่องแม่ข่าย และแอพลิเคชั่นผ่าน syslog protocol 4.2 สามารถทำตัวเป็น Log Archive เก็บ Log ย้อนหลังได้ไม่น้อยกว่า 90 วัน ตามกฎหมายกำหนด 4.3 มีหน้าแสดงผลผ่านเว็บเพจและสามารถควบคุมผ่านอินเทอร์เน็ตได้ (Web GUI) ผ่านการควบคุมช่องทางที่ปลอดภัยและมีการเข้ารหัส 4.4 ทำรายงานผล (Report) จากค่า syslog ได้ใน	Yes	Yes	Yes	Yes

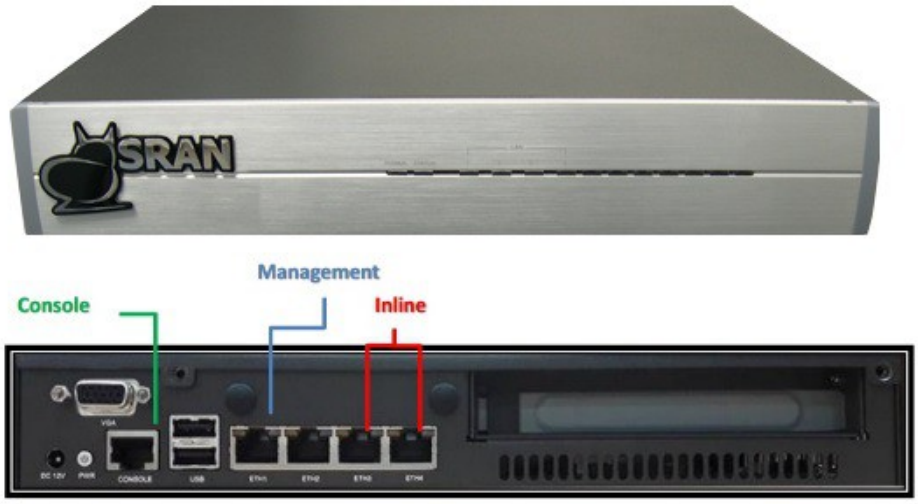
ตัวอุปกรณ์เอง 4.5 รองรับมาตรฐาน มศอ. การเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์ ตามกฎหมายประเทศไทย				
5. การรับและเข้าไปเรียกเก็บค่า Log จากอุปกรณ์อื่น สามารถทำได้ดังนี้ 5.1 การรับค่าจาก syslog , rsyslog , log forward แบบ agent less โดยอุปกรณ์ทำการส่งค่า Log files มาที่เครื่องส่วนกลางได้ 5.2 การรับค่าจากอุปกรณ์ Sensor โดยการติดตั้ง Sensor ตามจุดสำคัญของระบบเครือข่าย อันได้แก่ Extranal zone , Internal zone และ DMZ zone เป็นต้น 5.3 Log Crawler สามารถเข้าเก็บค่า Log files เพื่อนำมาเก็บบันทึกข้อมูลได้ผ่าน sFTP/FTP , SNMP , SNMP trap เป็นต้น	Yes	Yes	Yes	Yes
6. การเก็บบันทึกข้อมูลเหตุการณ์ (Data Archive) 6.1 มีการจัดเก็บเหตุการณ์ที่เกิดขึ้น โดยสามารถสืบค้นหาได้ และสามารถเปิดดูเหตุการณ์ต่างๆ ย้อนหลัง ตามวันเดือนปีที่กำหนดได้ โดยข้อมูลที่จัดเก็บมีการบีบอัดข้อมูล (Data Compression) และจัดทำ Data Hashing โดยวิธีการ SHA-1, MD5 เพื่อยืนยันความถูกต้องของข้อมูล 6.2 สามารถเก็บบันทึกข้อมูลได้มากกว่า 90 วัน 6.3 มีการยืนยันความถูกต้องของเนื้อไฟล์ Log เพื่อใช้ในชั้นศาล พร้อมทั้งมีระบบรักษาความปลอดภัยไม่ให้มีการนำ Log files ไปเรียกเปิด	Yes	Yes	Yes	Yes

ใช้กับที่อื่นได้โดยไม่ได้รับสิทธิ และการเข้ารหัสเฉพาะ (PGP) จากบริษัทหรือหน่วยงานที่ทำการใช้งานได้ 6.4 มีขั้นตอนการบีบอัดขนาดไฟล์เพื่อประหยัดพื้นที่ในการจัดเก็บข้อมูล (Compression files) 6.5 สามารถตั้งค่าเวลา Backup archive log data แยกไปยังอุปกรณ์ NAS Server ผ่าน NFS protocol ได้				
7. การค้นหา (Search) 7.1 สามารถทำการสืบหาข้อมูลย้อนหลังได้ โดยสามารถกำหนดช่วงเวลาที่จะทำการค้นหาได้ รวมถึงข้อความที่ต้องการจะทำการค้นได้ เพื่อให้การค้นหาเป็นไปอย่างได้สะดวก โดย SRAN Log Manager ใช้เทคนิค Full-text search โดยสามารถเขียน Regular Expression เพื่อเพิ่มเงื่อนไขในการค้นหาได้ 7.2 กำหนดการค้นหา สามารถค้นหาแบบ Full-text search โดยสามารถระบุเงื่อนไขในการค้นหาได้ เช่น AND , OR , Wildcard และกำหนดช่วงเวลาในการค้นหาได้ในระดับ วันที่ เวลา นาที และวินาทีที่กำหนดได้	Yes	Yes	Yes	Yes
8. การแจ้งเตือน (Alert) 8.1 สามารถทำการแจ้งเตือนไปยังผู้ดูแลระบบเมื่อเกิดเหตุการณ์ตาม Rules Filter ที่กำหนด เพื่อให้ผู้ดูแลระบบสามารถรับรู้ถึงเหตุการณ์ที่เกิดขึ้นได้อย่างทันท่วงที	Yes	Yes	Yes	Yes

8.2 สามารถแจ้งเตือนผ่าน E-mail ผู้ดูแลระบบ เมื่ออุปกรณ์ไม่ได้มีการส่งค่า Log files มาเก็บเข้า SRAN Log Manager ตามระยะเวลากำหนด 8.3 สามารถแจ้งเตือนผ่าน E-mail ผู้ดูแลระบบ เมื่อมีการใช้งานที่ทำให้พื้นที่ในการจัดเก็บข้อมูลใกล้เต็ม (Storage)				
9. การออกรายงาน (Reports) 9.1 สามารถกำหนดรูปแบบรายงาน และสามารถกำหนดให้ส่งรายงานตามช่วงเวลาที่กำหนดได้ 9.2 สามารถออกรายงานจากการค้นหาข้อมูล โดยออกเป็นค่า CSV และ PDF ได้ 9.3 รายงานสถานะการใช้งาน ปริมาณการรับค่า , ค่าสถานะการทำงานของระบบ	Yes	Yes	Yes	Yes
10. การบริหารจัดการระบบ (management) 10.1 มีระบบบริหารสิทธิการเข้าถึงข้อมูลโดยแยกระหว่าง System admin และ Data owner ผู้ที่มีสิทธิเข้าถึงข้อมูล Log files 10.2 มีการบริหารจัดการในการรับ-ส่งข้อมูลจากอุปกรณ์อื่น เพื่อรับค่า Log จากอุปกรณ์ได้อย่างเหมาะสม 10.3 มีการจัดการเรื่อง Time Server เพื่อให้ค่าการเก็บ Log file ตรงตามเวลามาตรฐาน และมีความสามารถแสดงค่าสถานะ Current Stratum 10.4 รองรับการเชื่อมต่อแบบ Cluster และการ	Yes	Yes	Yes	Yes

ทำงานร่วมกันเพื่อรักษาความเสถียรฐภาพ High Availability 10.5 สามารถรองรับ Log IPv4 และ IPv6 ได้				
11. ใบรับรองการทดสอบคุณภาพ (Certification) เป็นอุปกรณ์ Appliance หรือ Virtual Appliance ที่สามารถเก็บรวบรวมเหตุการณ์ (Logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น Appliances และ Non-Appliances แบบรวมศูนย์ หรือ Centralized Logs Management ให้สามารถแสดงผลอยู่ภายใต้รูปแบบ (Format) เดียวกันได้ตามพ.ร.บ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 ที่เข้ารับการทดสอบและผ่านตามข้อกำหนด NECTEC Standard NTS 4003.1-2552 มาตรฐานระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ จากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC)	Yes	Yes	Yes	Yes

มาตรฐานที่ได้รับจากฮาร์ดแวร์อุปกรณ์ SRAN และขั้นตอนในผลิตภัณฑ์ (Certification)



1. มาตรฐาน มศอ. 4003.1-2552 ระบบเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ตามกฎหมายเล่ม 1 ข้อกำหนดใช้ได้ถึง 8 เมษายน 2562

2. มาตรฐาน ศอ. 2001.2-2553 วิธีการประเมินสมรรถนะ สำหรับ บริภัณฑ์คอมพิวเตอร์และส่วนประกอบเชิงหน้าที่ เล่ม 2 ความร้อนใช้ได้ถึง 8 เมษายน 2562

3. มาตรฐาน ศอ. 2006.2.1-2555 วิธีการประเมินสมรรถนะ สำหรับบริภัณฑ์คอมพิวเตอร์และส่วนประกอบเชิงหน้าที่ เล่ม 2 ส่วนที่ 1 การใช้พลังงานในภาวะใช้กำลังไฟฟ้าต่ำ ใช้ได้ถึง 8 เมษายน 2562

4. มาตรฐาน ศอ. 2006.3-2556 วิธีการประเมินสมรรถนะ สำหรับบริภัณฑ์คอมพิวเตอร์ และส่วนประกอบเชิงหน้าที่ เล่ม 3 การคำนวณและประมวลผลข้อมูล ใช้ได้ถึง 8 เมษายน 2562

5. มาตรฐาน มอก. 1956-2548 บริภัณฑ์เทคโนโลยีสารสนเทศ เฉพาะด้านความปลอดภัยข้อกำหนดทั่วไป ใช้ได้ถึง 8 เมษายน 2562

6. มาตรฐาน มอก. 1956-2553 บริภัณฑ์เทคโนโลยีสารสนเทศ ขีดจำกัดสัญญาณรบกวนวิทยุ ใช้ได้ถึง 8 เมษายน 2562

7. มาตรฐาน มอก. 1448-2544 ความเข้ากันได้ทางแม่เหล็กไฟฟ้า เล่ม 3-2 : ขีดจำกัดสำหรับสิ่งที่ส่งออกมาซึ่งเป็นกระแสฮาร์โมนิก (กระแสไฟฟ้าเข้า 16 แอมแปร์ต่อเฟส) ใช้ได้ถึง 8 เมษายน 262

8. มาตรฐาน ISO 9001:2008 จาก SGS (Thailand) ให้กับการผลิตภัณฑ์ SRAN ในการให้บริการด้านความมั่นคงปลอดภัยข้อมูลสารนเทศภายใต้ผลิตภัณฑ์ ใช้ได้ถึง 14 กันยายน 2561

บริษัท โกลบอลเทคโนโลยี อินทิเกรเทด จำกัด
48/6 ซอยแจ้งวัฒนะ 14
ทุ่งสองห้อง หลักสี่ กรุงเทพฯ 10210
โทรศัพท์ : +66 2 982 5454
โทรสาร : +66 2 982 4004
อีเมล์ : info@gbtech.co.th

www.gbtech.co.th

Tunable

บริษัททูนาเบิล โปรเจค จำกัด

99/24 หมู่ 5 ตำบลบางพลับ อำเภอปากเกร็ด นนทบุรี 11120

Contact us info at tunable.co

Tel : 66851163311