บทที่ 5

เพิ่มประสิทธิภาพการบันทึกข้อมูลและประวัติผู้ใช้งาน

เพิ่มประสิทธิภาพการบันทึกข้อมูลและประวัติผู้ใช้งาน (ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550) ภายในระบบสารสนเทศสำนักบริหารบำรุงทาง ที่ปรึกษาจะดำเนินการ ดังต่อไปนี้

* 1. ศึกษาสถาปัตยกรรมของระบบสารสนเทศสำนักบริหารบำรุงทาง
  2. วิเคราะห์ และสรุป แนวทางการบันทึกข้อมูลและประวัติผู้ใช้งาน
  3. จัดสรรอุปกรณ์สนับสนุนการปฏิบัติงานและดำเนินการติดตั้งพร้อมทดสอบการใช้งาน
  4. **ศึกษาสถาปัตยกรรมของระบบสารสนเทศสำนักบริหารบำรุงทาง**

พร้อมทั้งตรวจสอบอุปกรณ์คอมพิวเตอร์ อุปกรณ์สนับสนุนการปฏิบัติงาน และอุปกรณ์เครือข่าย ภายในสำนักบริหารบำรุงทางการเก็บรักษาข้อมูลการใช้งานระบบคอมพิวเตอร์ผู้ให้บริการต้องใช้วิธีการที่มั่นคง และปลอดภัย คือ

* สื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้
* มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูล ที่เก็บรักษาไว้ เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archivin หรือทำ Data Hashing เป็นต้น เว้นแต่ ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของ หรือผู้บริหารองค์กร กำหนดให้ สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมาย เป็นต้น รวมทั้งเจ้าหน้าที่ตามพระราชบัญญัตินี้
* สามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ คือ ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือบริการ 1222 หรือ Wi-Fi Hostpot
* สามารถระบุรายละเอียดเวลาของผู้ใช้บริการเป็นรายบุคคลได้

จากการวิเคราะห์การใช้งานระบบคอมพิวเตอร์ของสำนักบริหารบำรุงทาง ได้ข้อสรุปเบื้องต้น ดังนี้

* รูปแบบโครงสร้างการเก็บข้อมูลตาม พ.ร.บ.คอมพิวเตอร์ในรูปแบบข้อมูลดิบ (Raw Data) ควรมีระบบ Report รายงานข้อมูล การวิเคราะห์และค้นหาปัญหาของระบบเครือข่ายควบคู่กับระบบ Log ให้ผู้ดูแลระบบ (Network Administrators) สามารถเห็นภาพรวมระบบปัจจุบัน แนวโน้มปัญหาเพื่อกำหนดแผนการดูแลหรือพัฒนาระบบเครือข่ายให้เหมาะสมกับปริมาณการใช้งานที่แท้จริงได้
* รูปแบบโครงสร้างข้อมูลใน Log file ครบถ้วนตามมาตรฐาน พ.ร.บ.คอมพิวเตอร์
* รูปแบบไฟล์ข้อมูลมีลักษณะเป็น Backup File ซึ่งจะทำการสำรองข้อมูลเป็นรายสัปดาห์   
  เพื่อป้องกันข้อมูลสูญหาย
* อุปกรณ์สนับสนุนการปฏิบัติงานเป็นไปตามมาตรฐาน พ.ร.บ.คอมพิวเตอร์
  1. **วิเคราะห์ และสรุป แนวทางการบันทึกข้อมูลและประวัติผู้ใช้งาน**

เพื่อรองรับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ให้แก่ระบบสารสนเทศสำนักบริหารบำรุงทาง บันทึกกิจกรรมของผู้ใช้ที่ระบุหรือทั้งหมด (Activity Log) และจัดทำโมดูล (Module) รายงานประวัติการใช้งานผู้ใช้งานระบบสารสนเทศสำนักบริหารบำรุงทางในรูปแบบที่เข้าใจได้โดยง่าย

* 1. **จัดสรรอุปกรณ์สนับสนุนการปฏิบัติงานและดำเนินการติดตั้งพร้อมทดสอบการใช้งาน**

เพื่อให้โครงการปรับปรุงข้อมูลในระบบฐานข้อมูลกลางและระบบอื่นที่เกี่ยวข้อง บรรลุวัตถุประสงค์และเกิดประสิทธิภาพสูงสุด คณะที่ปรึกษาจะจัดหาคอมพิวเตอร์และอุปกรณ์สนับสนุนให้เพียงพอสำหรับ  
ใช้งานในโครงการฯ และส่งมอบให้กับกรมทางหลวง โดยอย่างน้อยต้องประกอบด้วย

* + 1. เครื่องคอมพิวเตอร์แม่ข่าย แบบที่ 1 ซึ่งต้องมีคุณลักษณะพื้นฐานไม่ด้อยกว่า ดังต่อไปนี้
* มีหน่วยประมวลผลกลาง (CPU) แบบ 4 แกนหลัก (4 core) สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกา 2.4 GHz จำนวน 1 หน่วย
* CPU รองรับการประมวลผลแบบ 64 bit มีหน่วยความจำแบบ Cache Memory 10 MB และมีความเร็วบัส 1,366 MHz
* มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR3 มีขนาด 16 GB
* สนับสนุนการทำงาน RAID 0, 1, 5
* มีหน่วยจัดเก็บข้อมูล (Hard Disk) ชนิด SATA มีความเร็วรอบ 7,200 รอบต่อนาที และ  
  มีขนาดความจุ 1000 GB จำนวน 2 หน่วย
* มี DVD-ROM จำนวน 1 หน่วย
* มีช่องเชื่อมต่อระบบเครือข่าย แบบ 10/100/1,000 Mbps จำนวน 2 ช่อง
* มีจอภาพแบบ LCD ขนาด 18.5 นิ้ว จำนวน 1 หน่วย
* มี Power Supply แบบ Redundant Hot Swap จำนวน 2 หน่วย
* ติดตั้งซอฟต์แวร์ระบบปฏิบัติการพร้อมใช้งานที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย
  + 1. เครื่องคอมพิวเตอร์แม่ข่าย แบบที่ 2 ซึ่งต้องมีคุณลักษณะพื้นฐานไม่ด้อยกว่า ดังต่อไปนี้
* มีหน่วยประมวลผลกลาง (CPU) แบบ 4 แกนหลัก (4 core) สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกา 3.3 GHz จำนวน 2 หน่วย
* CPU รองรับการประมวลผลแบบ 64 bit มีหน่วยความจำแบบ Cache Memory 10 MB และมีความเร็วบัสไม่น้อยกว่า 1,600 MHz
* มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR3 ขนาด 32 GB
* สนับสนุนการทำงาน RAID 0, 1, 5
* มีหน่วยจัดเก็บข้อมูล (Hard Disk) ชนิด SAS ที่มีความเร็วรอบ 10,000 รอบต่อนาที และมีความจุ 600 GB จำนวน 4 หน่วย
* มี DVD-ROM จำนวน 1 หน่วย
* มีช่องเชื่อมต่อระบบเครือข่าย แบบ 10/100/1,000 Mbps จำนวน 2 ช่อง
* มีจอภาพแบบ LCD ขนาด 18.5 นิ้ว จำนวน 1 หน่วย
* มี Power Supply แบบ Redundant Hot Swap จำนวน 2 หน่วย
* ติดตั้งซอฟต์แวร์ระบบปฏิบัติการพร้อมใช้งานที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

5.3.3 อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย แบบที่ 2 มีคุณสมบัติดังต่อไปนี้

* เป็นอุปกรณ์ Appliance หรืออุปกรณ์คอมพิวเตอร์ที่สามารถเก็บรวบรวมเหตุการณ์   
   (logsor Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น   
   Firewall, Network Devices ต่างๆ, ระบบปฏิบัติการ, ระบบ appliances, ระบบเครือข่าย   
   และระบบฐานข้อมูล เป็นต้น ได้อย่างน้อย 5 อุปกรณ์ต่อระบบ โดยสามารถแสดงผลอยู่  
   ภายใต้รูปแบบเดียวกันได้
* มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน MD5   
   หรือ SHA-1 หรือดีกว่า
* สามารถเก็บ LogFile ในรูปแบบ Syslog ของอุปกรณ์ เช่น Router, Switch, Firewall,   
   VPN, Server เป็นต้น
* สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ   
   Secure Shell (SSH) ได้
* สามารถจัดเก็บ logfile ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับ  
   คอมพิวเตอร์ พ.ศ.2550 โดยได้รับรองมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ   
   log file ที่ได้
* มาตรฐานสากล เช่น มาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ.   
   4003.1-2552) เป็นต้น
* สามารถทำการสำรองข้อมูล (Data Backup) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น   
   Tape หรือ DVD หรือ External Storage เป็นต้น ได้
* สามารถจัดเก็บข้อมูลเหตุการณ์ต่อวินาที (Event sper Seconds) ได้ไม่น้อยกว่า 1,000 eps