เอกสารแนบท้ายการประกวดราคาจ้างด้วยวิธีการทางอิเล็กทรอนิกส์
บำรุงรักษาและซ่อมแซมแก้ไขระบบคอมพิวเตอร์แม่ข่าย อุปกรณ์ต่อพ่วง และอุปกรณ์เครือข่ายภายใน
พร้อมอุปกรณ์ด้านความมั่นคง ประจำปีงบประมาณ พ.ศ.2556
ตามประกาศสำนักงานสถิติแห่งชาติ
ลงวันที่ .....

---

1. **ความเป็นมาของโครงการ**

สำนักงานสถิติแห่งชาติเป็นหน่วยงานหลักในการผลิตข้อมูลสถิติของประเทศเพื่อ ให้บริการสารสนเทศสถิติต่อผู้ใช้ทั้งภาครัฐ เอกชน ประชาชนทั่วไปและจัดการระบบสถิติของประเทศ โดยมีเป้าประสงค์ที่ต้องการให้สังคมทุกภาคส่วนมีข้อมูลสถิติที่มีคุณภาพใช้ในการวางแผนและการตัดสินใจ สามารถนำไปพัฒนาประเทศให้เกิดความเจริญก้าวหน้า สร้างความเป็นอยู่ที่ดีต่อสังคม

ระบบคอมพิวเตอร์แม่ข่าย อุปกรณ์ต่อพ่วง และอุปกรณ์เครือข่าย อุปกรณ์ด้านความมั่นคง เป็นทรัพยากรพื้นฐานที่สนับสนุนให้การดำเนินงานที่กล่าวมาข้างต้นบรรลุวัตถุประสงค์ จึงต้องสามารถใช้งานให้บริการได้ตลอดเวลา

เพื่อเป็นการลดความเสี่ยงการหยุดให้บริการสารสนเทศสถิติต่อผู้ใช้บริการ สำนักงานสถิติแห่งชาติจึงจำเป็นต้องจัดหาผู้รับจ้างบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ต่อพ่วง อุปกรณ์ความมั่นคงปลอดภัย อุปกรณ์เครือข่าย และซอฟต์แวร์ที่ติดตั้งใช้งานในศูนย์คอมพิวเตอร์สำนักงานสถิติแห่งชาติ

2. **วัตถุประสงค์**

2.1. จัดหาผู้รับจ้างบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ต่อพ่วง อุปกรณ์ความมั่นคงปลอดภัย อุปกรณ์เครือข่าย และซอฟต์แวร์ในระบบของสำนักงานสถิติแห่งชาติ

2.2. ซ่อมแซมแก้ไขเครื่องคอมพิวเตอร์และอุปกรณ์หากเกิดการชำรุดเสียหาย เพื่อให้อุปกรณ์กลับมาใช้งานได้ดังเดิมด้วยความรวดเร็ว

2.3. เพื่อปรับปรุงระบบการบำรุงรักษาให้เป็นไปตามมาตรฐานและข้อกำหนดการดำเนินงานภายในของสำนักงานสถิติแห่งชาติ

3. **หลักเกณฑ์การพิจารณา**

สำนักงานสถิติแห่งชาติได้กำหนดเกณฑ์การพิจารณาเพื่อประเมินระดับความสามารถและความพร้อมของผู้รับจ้างในการจัดการระบบบำรุงรักษาในการดำเนินงานโครงการ โดยมีหลักเกณฑ์การพิจารณาให้คะแนนดังตารางนี้

ตารางการพิจารณาระดับความสามารถ

ประเด็น	การพิจารณา	คะแนน
1. การนำมาตรฐานสากลมาประยุกต์ใช้ในการบำรุงรักษา	จากเอกสารที่แสดงการนำมาตรฐาน ITIL มาประยุกต์ใช้ในกระบวนการบำรุงรักษาของสำนักงานสถิติแห่งชาติ	30
2. ความสามารถในการตอบสนองต่อปัญหาที่ได้รับแจ้ง	มีศูนย์รับแจ้งปัญหา พร้อมหมายเลขโทรศัพท์และขั้นตอนการรับแจ้งปัญหาเพื่อให้ผู้รับบริการได้รับการแก้ไขปัญหาและแนวทางในการแก้ปัญหาตามข้อ 5.8	20
3. ความสามารถในการควบคุมการเปลี่ยนแปลงในการซ่อมบำรุง	มีกระบวนการควบคุมการซ่อมบำรุงที่มีคุณภาพและไม่ส่งผลกระทบต่อการสูญเสียข้อมูลในระบบ	20
4. ความรู้ความสามารถของทีมงาน	ประเมินข้อเสนอของคณะทำงานและความรู้ความสามารถ ประสบการณ์การทำงาน	30
	รวม	100

ในการพิจารณาเพื่อประเมินระดับความสามารถในการจัดการระบบบำรุงรักษา สำนักงานสถิติแห่งชาติจะให้เวลาในการนำเสนอไม่เกิน 3 ชั่วโมง และเป็นไปตามวันและเวลาที่สำนักงานสถิติแห่งชาติกำหนด

เกณฑ์การตัดสินนั้นสำนักงานสถิติแห่งชาติจะคัดเลือกผู้เสนอราคาที่มีผลคะแนนรวม 80 คะแนน หรือมากกว่า ขึ้นไปเพื่อเข้าประกวดราคาด้วยวิธีการทางอิเล็กทรอนิกส์ต่อไป

4. คุณสมบัติของผู้เสนอราคา

4.1. เป็นนิติบุคคลที่จดทะเบียนในประเทศไทย ซึ่งมีวัตถุประสงค์ในการประกอบธุรกิจเกี่ยวกับ การขายหรือติดตั้งระบบคอมพิวเตอร์ หรือรับจ้างให้บริการบำรุงรักษาระบบคอมพิวเตอร์ มาแล้วไม่น้อยกว่า 1 ปี

4.2. ต้องมีผลงานการให้บริการการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วงเครื่องคอมพิวเตอร์แม่ข่าย วงเงิน 5 ล้านบาทขึ้นไปต่อหนึ่งสัญญา ให้หน่วยงานราชการหรือรัฐวิสาหกิจ หรือเอกชน อย่างน้อย 1 ราย โดยเป็นผลงานในระยะเวลาไม่เกิน 3 ปี นับถึงวันที่ยื่นซอง ซึ่งหนังสือรับรองผลงาน ออกโดยหัวหน้าหน่วยของเอกชน หรือหัวหน้าหน่วยของราชการ หรือผู้มีอำนาจปฏิบัติราชการแทนโดยถูกต้องตามกฎหมาย

/5. เอกสาร...

5. เอกสารประกอบการเสนอราคา

5.1. เอกสารรับรองผลงานฉบับจริง และสำเนาสัญญาหรือใบสั่งจ้างการให้บริการการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วง ซึ่งหนังสือรับรองผลงาน ออกโดยหัวหน้าหน่วยของเอกชน หรือหัวหน้าหน่วยของราชการ หรือผู้มีอำนาจปฏิบัติราชการแทนโดยถูกต้องตามกฎหมาย ที่ออกให้ไม่เกิน 6 เดือน

5.2. เอกสารรายชื่อและคุณสมบัติของเจ้าหน้าที่ในการให้บริการที่สำนักงานสถิติแห่งชาติอย่างน้อย 1 คน

5.3. เอกสารแสดงความสามารถและประสบการณ์ของทีมงานของผู้บำรุงรักษาโดยรวมเจ้าหน้าที่ที่ให้บริการที่สำนักงานสถิติแห่งชาติตามข้อ 5.2

5.4. เอกสารรายละเอียดข้อเสนอการให้บริการ ซ่อมแซมและแก้ไขปัญหา (Corrective Maintenance) และบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) ในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์

5.5. เอกสารที่แสดงการนำมาตรฐานสากลมาประยุกต์ใช้ในการบำรุงรักษา

5.6. เอกสารที่แสดงรายละเอียดศูนย์รับแจ้งปัญหา พร้อมหมายเลขโทรศัพท์และขั้นตอนการรับแจ้งปัญหาให้ผู้รับบริการ

5.7. เอกสารรายละเอียดกระบวนการควบคุมการเปลี่ยนแปลงในการซ่อมบำรุงระบบคอมพิวเตอร์

5.8. เอกสารแนวทางแก้ปัญหาในการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ต่อพ่วง อุปกรณ์ความมั่นคงปลอดภัย อุปกรณ์เครือข่าย และซอฟต์แวร์ ซึ่งเป็นเหตุเกิดจากเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์อื่นๆ ที่กำหนดไว้ในกลุ่มที่ผู้ผลิตประกาศเป็น EOSL (ในภาคผนวก ก.) และการจัดหาจากหลายโครงการหรือหลายสัญญาที่ผ่านมา อาจทำให้เกิดข้อตกลงที่สำนักงานสถิติแห่งชาติไม่อาจทราบได้จากการซื้อขายหรือจัดหา หากผู้เสนอราคามีข้อจำกัดในเรื่องนี้ ต้องเสนอแนวทางในการแก้ปัญหาให้คณะกรรมการประกวดราคาพิจารณา โดยต้องมีคุณสมบัติไม่ต่ำกว่าของเดิมที่ใช้งานอยู่

หากกรณีอุปกรณ์ที่อยู่ในสัญญาไม่สามารถแก้ไขให้ใช้งานได้ และผู้รับจ้างได้เสนออุปกรณ์ทดแทนในระหว่างสัญญาเพื่อให้ระบบงานของสำนักงานสถิติแห่งชาติทำงานต่อไปได้ เมื่อสิ้นสุดสัญญาผู้รับจ้างต้องส่งมอบอุปกรณ์ดังกล่าวให้กับสำนักงานสถิติแห่งชาติโดยไม่คิดค่าใช้จ่ายใดๆ เพิ่มเติม

5.9. เอกสารตัวอย่างแบบรายงานผลการบำรุงรักษาอุปกรณ์ และเอกสารรายงานสรุปผลการดำเนินงาน

6. ขอบเขตของงาน

6.1. ตรวจสอบความผิดปกติต้นรอบการบำรุงรักษา

6.1.1. ผู้รับจ้างต้องตรวจสอบความผิดปกติทางกายภาพของเครื่องและอุปกรณ์ภายนอกที่ปรากฏในภาคผนวก ก. ทุกรายการ จำนวน 1 ครั้ง ภายใน 30 วันทำการ หลังจากลงนามในสัญญา โดยการตรวจสอบต้องดำเนินการควบคู่กับเจ้าหน้าที่ของสำนักงานสถิติแห่งชาติที่ได้รับมอบหมายในการควบคุมการบำรุงรักษาระบบคอมพิวเตอร์

6.1.2. ผู้รับจ้างต้องตรวจสอบความผิดปกติการทำงานและการแจ้งเตือนด้วยสัญญาณทางไฟฟ้าที่ตัวอุปกรณ์ เช่น การกระพริบเตือนที่ผิดปกติ

6.1.3. ผู้รับจ้างต้องตรวจสอบความผิดปกติของจอภาพ KVM ต้องไม่มีการสั่นไหวที่แสดงออกชัดเจนและส่งผลต่อผู้ใช้งานจอภาพ

/6.1.4...

6.1.4. ผู้รับจ้างต้องตรวจสอบความผิดปกติของเสียงที่ปรากฏจากพัดลมบนตู้แร็ค ต้องไม่มีเสียงดังหรือเกิดการสั่นสะเทือนผิดปกติปรากฏ

6.1.5. หากผู้รับจ้างตรวจพบปัญหาให้ดำเนินการแก้ไขปัญหาที่ตรวจพบให้แล้วเสร็จอย่างไม่มีเงื่อนไขโดยเร็ว และให้รายงานผลให้สำนักงานสถิติแห่งชาติทราบ

6.1.6. ให้จัดทำรายงานผลการตรวจสอบเป็นลายลักษณ์อักษรส่งมอบให้สำนักงานสถิติแห่งชาติแล้วเสร็จภายใน 30 วันทำการ หลังการดำเนินการตรวจสอบความผิดปกติข้างต้นแล้ว

6.2. บำรุงรักษา เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ต่อพ่วง อุปกรณ์เครือข่าย และอุปกรณ์ความมั่นคงปลอดภัยฯ

6.2.1. บริการบำรุงรักษาเชิงป้องกันและบริการแก้ไขความเสียหายของอุปกรณ์ ตามรายการในภาคผนวก ก.

6.2.2. บำรุงรักษาเชิงป้องกันตามข้อกำหนดข้อ 6.7

6.2.3. ให้บริการแก้ไขความเสียหายตามข้อกำหนดข้อ 6.8

6.2.4. ผู้รับจ้างต้องซื้อหรือต่อ Support แบบ Onsite Service (5x8) ตลอดระยะเวลาสัญญา ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ต่อพ่วง อุปกรณ์เครือข่ายและอุปกรณ์ความมั่นคงปลอดภัยฯ จากตัวแทนจำหน่ายในประเทศไทย ตามรายการในภาคผนวก ก. โดยผู้รับจ้างเป็นผู้รับผิดชอบค่าใช้จ่าย

กรณีที่อุปกรณ์ใดไม่มีตัวแทนจำหน่ายในประเทศไทย ผู้รับจ้างสามารถดำเนินการซื้อหรือต่อ Support จากเจ้าของผลิตภัณฑ์ได้ โดยต้องมีหนังสือยืนยันการต่อ Support จากเจ้าของผลิตภัณฑ์แสดงต่อคณะกรรมการตรวจรับ

6.2.5. กรณีอุปกรณ์ความมั่นคงปลอดภัยฯ ผู้รับจ้างต้องรับผิดชอบค่าใช้จ่ายในการต่ออายุ License และ Update Signature หรือ Patch ให้เป็นปัจจุบัน จากตัวแทนจำหน่ายในประเทศไทย เพื่อให้อุปกรณ์ดังกล่าวใช้งานอย่างเต็มประสิทธิภาพตามลักษณะการใช้งานของแต่ละอุปกรณ์ตามรายการในภาคผนวก ก. ข้อ 5

กรณีที่อุปกรณ์ใดไม่มีตัวแทนจำหน่ายในประเทศไทย ผู้รับจ้างสามารถดำเนินการต่ออายุ License และ Update Signature หรือ Patch ให้เป็นปัจจุบัน จากเจ้าของผลิตภัณฑ์ได้ โดยต้องมีหนังสือยืนยันการต่ออายุ License และ Update Signature หรือ Patch จากเจ้าของผลิตภัณฑ์แสดงต่อคณะกรรมการตรวจรับ

6.2.6. ผู้รับจ้างต้องดำเนินการตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ ตามภาคผนวก ก. ที่ผู้ผลิตประกาศเป็น EOSL เพิ่มเติม และจัดทำเอกสารสรุปส่งมอบให้สำนักงานสถิติแห่งชาติ

6.3. บำรุงรักษาซอฟต์แวร์

6.3.1. ผู้รับจ้างต้องต่ออายุการใช้งานซอฟต์แวร์ และซื้อ Support จากตัวแทนจำหน่ายในประเทศไทย ตามรายการในภาคผนวก ก. ข้อ 8 โดยผู้รับจ้างเป็นผู้รับผิดชอบค่าใช้จ่าย

6.3.2. ผู้รับจ้างต้องดำเนินการปรับแก้ปัญหาของซอฟต์แวร์ที่ติดตั้งอยู่บนคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วง ตามภาคผนวก ก. ข้อ 8 ให้สามารถทำงานได้เป็นปกติ

/6.3.3 กรณี...

6.3.3. กรณีที่ซอฟต์แวร์ใดไม่มีตัวแทนจำหน่ายในประเทศไทย ผู้รับจ้างสามารถดำเนินการต่ออายุการใช้งานซอฟต์แวร์ และซื้อ Support จากเจ้าของผลิตภัณฑ์ได้ โดยต้องมีหนังสือยืนยันการต่ออายุ ซอฟต์แวร์ จากเจ้าของผลิตภัณฑ์แสดงต่อคณะกรรมการตรวจรับ โดยผู้รับจ้างเป็นผู้รับผิดชอบค่าใช้จ่าย

6.4. ข้อกำหนดทั่วไป

6.4.1. ในกรณีที่มีบุคคลภายนอกกล่าวอ้างหรือใช้สิทธิเรียกร้องใด ๆ ว่ามีการละเมิดลิขสิทธิ์ หรือสิทธิบัตรเกี่ยวกับอุปกรณ์ และหรือ ฮาร์ดแวร์ ซอฟต์แวร์ที่เสนอ ผู้รับจ้างต้องดำเนินการทั้งปวง เพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็วและผู้รับจ้างต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายต่าง ๆ ที่เกิดขึ้นทั้งหมด

6.4.2. **ในกรณีที่เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ต่อพ่วง อุปกรณ์เครือข่าย และอุปกรณ์ความมั่นคงปลอดภัยฯ ขาดการต่ออายุ License หรือ Signature หรือ Support ผู้รับจ้างต้องดำเนินการต่ออายุและรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด**

6.4.3. **กรณีการต้องต่ออายุ License และ Update Signature หรือ Patch ผู้รับจ้างต้องส่งเจ้าหน้าที่ผู้เชี่ยวชาญเฉพาะด้านมาดำเนินการที่สำนักงานสถิติแห่งชาติเท่านั้น และต้องได้รับความเห็นชอบจากสำนักงานสถิติแห่งชาติ**

6.4.4. ผู้รับจ้างต้องให้คำปรึกษาพร้อมทั้งแก้ไขปัญหาที่เกิดขึ้นกับระบบงานของสำนักงานสถิติแห่งชาติ ให้สามารถใช้งานได้เป็นปกติ ดังนี้

6.4.4.1. LDAP
6.4.4.2. DNS
6.4.4.3. Proxy
6.4.4.4. Operating System (Solaris , HP-UX , AIX , Linux , Windows Sever)
6.4.4.5. SUN One Web Server
6.4.4.6. Microsoft Active Directory
6.4.4.7. Microsoft Internet Information Service
6.4.4.8. Microsoft DHCP, Apache Tomcat
6.4.4.9. Qmail, Squirrel Mail
6.4.4.10. FTP Pro
6.4.4.11. Squid Proxy
6.4.4.12. Radius Server
6.4.4.13. Mongrel Web Server
6.4.4.14. Apache Web Server
6.4.4.15. IPV6

ทั้งนี้หากผู้รับจ้างไม่สามารถแก้ไขปัญหาได้ผู้รับจ้างจะต้องจัดหาผู้มีความรู้ความเชี่ยวชาญเพื่อดำเนินการแก้ไขปัญหาดังกล่าว

6.4.5 ผู้รับจ้าง...

6.4.5. ผู้รับจ้างต้องจัดหาผู้บริหารงานโครงการ (Project Manager) สำหรับควบคุม ติดตามการปฏิบัติงานให้เป็นไปตามแผนการดำเนินงานและติดต่อประสานงานกับเจ้าหน้าที่ของสำนักงานสถิติแห่งชาติ ตลอดอายุของสัญญา

6.4.6. ผู้รับจ้างต้องรายงานความก้าวหน้าผลการดำเนินงานในแต่ละงวดให้คณะกรรมการตรวจรับฯ ทราบ อย่างน้อย 15 วันก่อนการส่งมอบงานในแต่ละงวด

6.4.7. ผู้รับจ้างต้องปฏิบัติตามระเบียบและประกาศในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสถิติแห่งชาติ ที่ใช้ควบคุมในการปฏิบัติงาน (รายละเอียดดูได้จากภาคผนวก ง)

6.5. ข้อกำหนดการปกปิดข้อมูลสำคัญ

มีการลงนามของผู้รับจ้างที่จะไม่นำข้อมูลในเรื่องระบบคอมพิวเตอร์ของสำนักงานสถิติแห่งชาติไปเปิดเผยต่อผู้อื่นโดยเด็ดขาดไม่ว่าในกรณีใด ๆ และ ห้ามการคัดลอก หรือ แอบถ่ายข้อมูลที่สำคัญ และ ปฏิบัติตามประกาศด้านความมั่นคง ศูนย์คอมพิวเตอร์สำนักงานสถิติแห่งชาติ อย่างเคร่งครัด

6.6. ข้อกำหนดรายการอุปกรณ์บำรุงรักษาตามภาคผนวก ก.

6.6.1. เครื่องคอมพิวเตอร์แม่ข่าย

6.6.1.1. บำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายที่ผู้ผลิตไม่ประกาศเป็น EOSL จำนวน 58 ชุด ตามภาคผนวก ก. ข้อ 1.1

6.6.1.2. บำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายที่ผู้ผลิตประกาศเป็น EOSL จำนวน 17 ชุด ตามภาคผนวก ก. ข้อ 1.2

6.6.2. หน่วยเก็บข้อมูล

6.6.2.1. บำรุงรักษาอุปกรณ์ SAN Switch ที่ผู้ผลิตไม่ประกาศ EOSL จำนวน 2 ชุด พร้อมสายไฟเบอร์เชื่อมต่อ ตามภาคผนวก ก. ข้อ 2.1

6.6.2.2. บำรุงรักษาอุปกรณ์ SAN Switch ที่ผู้ผลิตประกาศ EOSL จำนวน 2 ชุด พร้อมสายไฟเบอร์เชื่อมต่อ ตามภาคผนวก ก. ข้อ 2.2

6.6.2.3. บำรุงรักษาอุปกรณ์ SAN ที่ผู้ผลิตไม่ประกาศ EOSL จำนวน 11 ชุด ตามภาคผนวก ก. ข้อ 2.3

6.6.2.4. บำรุงรักษาอุปกรณ์ SAN ที่ผู้ผลิตประกาศ EOSL จำนวน 2 ชุด ตามภาคผนวก ก. ข้อ 2.4

6.6.3. ระบบสำรองข้อมูลและกู้คืน

6.6.3.1. บำรุงรักษาอุปกรณ์เทปชนิด Library ที่ผู้ผลิตไม่ประกาศ EOSL จำนวน 1 ชุด ตามภาคผนวก ก. ข้อ 3.1

6.6.3.2. บำรุงรักษาอุปกรณ์เทปชนิดเดี่ยว จำนวน 3 ชุด ตามภาคผนวก ก. ข้อ 3.2

6.6.4. อุปกรณ์เครือข่าย

6.6.4.1. บำรุงรักษาอุปกรณ์ Core Switch จำนวน 1 ชุด ตามภาคผนวก ก. ข้อ 4.1

6.6.4.2. บำรุงรักษาอุปกรณ์ Workgroup Switch จำนวน 10 ชุด ตามภาคผนวก ก. ข้อ 4.2

/6.6.5. อุปกรณ์...

6.6.5.1. บำรุงรักษาอุปกรณ์ FW จำนวน 5 ชุด ตามภาคผนวก ก. ข้อ 5.1

6.6.5.2. บำรุงรักษาอุปกรณ์ IPS/IDS ที่ผู้ผลิตประกาศ EOSL และซอฟต์แวร์ Signature จำนวน 2 ชุด ตามภาคผนวก ก. ข้อ 5.2

6.6.5.3. บำรุงรักษาอุปกรณ์ Virus Gateway จำนวน 2 ชุด ตามภาคผนวก ก. ข้อ 5.3.

6.6.5.4. บำรุงรักษาอุปกรณ์ Proxy Server จำนวน 2 ชุด ตามภาคผนวก ก. ข้อ 5.4

6.6.5.5. บำรุงรักษาอุปกรณ์ Vulner จำนวน 3 ชุด ตามภาคผนวก ก. ข้อ 5.5

6.6.6. พัดลมระบายความร้อนบนตู้แร็ค

6.6.6.1. บำรุงรักษาพัดลมระบายความร้อนจำนวน 90 ชุด ตามภาคผนวก ก. ข้อ 6

6.6.7. อุปกรณ์ KVM

6.6.7.1. บำรุงรักษาอุปกรณ์ KVM จำนวน 13 ชุด ตามภาคผนวก ก. ข้อ 7

6.6.8. ซอฟต์แวร์

6.6.8.1. บำรุงรักษาซอฟต์แวร์ ตามภาคผนวก ก. ข้อ 8

6.7. ข้อกำหนดการให้บริการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance)

6.7.1. ผู้รับจ้างต้องทำการบำรุงรักษาตามข้อเสนอในข้อ 5.4 ที่เสนอ

6.7.2. ผู้รับจ้างต้องตรวจสอบสภาพและบำรุงรักษาตามรายการในภาคผนวก ก. ณ สถานที่ตั้ง จำนวน 2 ครั้ง โดยไม่ต้องทำการปิดระบบ โดยแต่ละครั้งห่างกันไม่น้อยกว่า 60 วัน ทั้งนี้ไม่รวมการตรวจสอบความผิดปกติต้นรอบการบำรุงรักษาตามข้อ 6.1 เพื่อให้ System Availability ของ Mission-Critical Servers เป็นไปตาม Service Level Agreement ดังนี้

6.7.2.1. เครื่องคอมพิวเตอร์แม่ข่าย ตามภาคผนวก ค. ข้อ 1.

6.7.2.2. San Switch ตามภาคผนวก ค. ข้อ 2.

6.7.2.3. Storage, Monitor Console & KVM 8 Port, Back Product ตามภาคผนวก ค. ข้อ 3.

6.7.2.4. อุปกรณ์ Tape Backup ตามภาคผนวก ค. ข้อ 4.

6.7.2.5. อุปกรณ์เครือข่าย ตามภาคผนวก ค. ข้อ 5.

6.7.2.6. อุปกรณ์ความมั่นคงปลอดภัย ตามภาคผนวก ค. ข้อ 6.

6.7.2.7. อุปกณ์ KVM ตามภาคผนวก ค. ข้อ 7.

6.7.3. ผู้รับจ้างต้องจดบันทึกผลของการตรวจสอบลงใน Service Report โดยมีรายละเอียดของรายงานการบำรุงรักษาเป็นไปตามที่สำนักงานสถิติแห่งชาติกำหนด และรายงานให้ผู้ดูแลระบบ (System Administrator) ของสำนักงานสถิติแห่งชาติรับทราบเป็นลายลักษณ์อักษร

6.7.4. ผู้รับจ้างต้องทำความสะอาดดังนี้

6.7.4.1. ทำความสะอาดตู้แร็คทั้งภายนอกและภายในตู้โดยการดูดฝุ่นและเช็ดด้วยน้ำยาทำความสะอาด กรณีทำความสะอาดภายในตู้ให้ทำความสะอาดในส่วนที่สามารถเข้าถึงได้และไม่เป็นอันตรายต่อทรัพย์สินและชีวิต

/6.7.4.2...

6.7.4.2. ทำความสะอาดภายนอกตัวเครื่องคอมพิวเตอร์และอุปกรณ์ ตามรายการภาคผนวก ก. ด้วยน้ำยาทำความสะอาด

6.7.5. ผู้รับจ้างต้องจัดทำเอกสารรายงานผลการบำรุงรักษารายอุปกรณ์ และเอกสารรายงานสรุปเสนอต่อสำนักงานสถิติแห่งชาติ หลังการให้การบำรุงรักษาเชิงป้องกันในแต่ละรอบ ก่อนส่งมอบงานตามสัญญา

6.7.6. ผู้รับจ้างต้องนำเสนอผลการบำรุงรักษาเชิงป้องกันในแต่ละรอบต่อคณะกรรมการตรวจรับพัสดุ ก่อนส่งมอบงานตามสัญญา

6.8. ข้อกำหนดการซ่อมแซมและแก้ไขปัญหา (Corrective Maintenance)

6.8.1. ผู้รับจ้างต้องทำการซ่อมแซมและแก้ไขตามข้อเสนอในข้อ 5.4 ที่เสนอ

6.8.2. เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่อยู่ในสายการผลิต มีข้อกำหนดดังนี้

6.8.2.1. ผู้รับจ้างต้องมีเจ้าหน้าที่ Stand by เพื่อสามารถรับการติดต่อจากสำนักงานสถิติแห่งชาติโดยทางโทรศัพท์ และทำการซ่อมแซมแก้ไขระบบให้ทำงานปกติได้ทันตามข้อกำหนดระดับการให้บริการ (Service Level Agreement) กับสำนักงานสถิติแห่งชาติ ตามข้อกำหนดข้อ 6.12

6.8.2.2. ผู้รับจ้างให้บริการซ่อมแซม Hardware แก้ไขปัญหาที่เกิดจาก OS และ System Software และลง Patch ให้กับ Server อุปกรณ์ต่อพ่วง อุปกรณ์ความมั่นคงปลอดภัย เพื่อแก้ไขปัญหา ณ สถานที่ตั้งของสำนักงานสถิติแห่งชาติ

6.8.2.3. ผู้รับจ้างต้องเปลี่ยนอุปกรณ์อะไหล่ทุกชิ้นที่เสียด้วยของใหม่จากผู้ผลิต

6.8.3. เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์<u>ที่ไม่อยู่ในสายการผลิต</u> มีข้อกำหนด ดังนี้

6.8.3.1. ผู้รับจ้างจะต้องมีเจ้าหน้าที่ Stand by เพื่อสามารถรับการติดต่อจากสำนักงานสถิติแห่งชาติโดยทางโทรศัพท์ และทำการซ่อมแซมแก้ไขระบบให้ทำงานปกติ

6.8.3.2. ผู้รับจ้างให้บริการซ่อมแซมเปลี่ยนอุปกรณ์อะไหล่ชิ้นที่เสียหายและทำให้ระบบสามารถใช้งานได้ตามปกติ

6.8.4. ผู้รับจ้างต้องจัดทำเอกสารรายงานผลการซ่อมแซมและแก้ไขปัญหา และจัดทำเอกสารรายงานสรุป เสนอต่อสำนักงานสถิติแห่งชาติ ทันทีที่ดำเนินการเสร็จสิ้น

6.9. ข้อกำหนดบำรุงรักษาตามกรอบงานระบบความมั่นคงปลอดภัยของสำนักงานสถิติแห่งชาติ (NSO-ISMF) **ซึ่งมีคุณสมบัติดังนี้**

6.9.1. ผู้รับจ้างต้องทำการตรวจสอบหาช่องโหว่ของระบบปฏิบัติการ และ Service ที่อยู่บนเครื่องคอมพิวเตอร์แม่ข่าย และระบบโปรแกรมประยุกต์ที่พัฒนาขึ้นใช้งาน โดยใช้อุปกรณ์ Vulner ของสำนักงานสถิติแห่งชาติ ซึ่งติดตั้งซอฟต์แวร์ McAfee Vulnerability Manager

6.9.2. ผู้รับจ้างต้องทำการปิดช่องโหว่ ที่ตรวจพบในข้อ 6.9.1 ในส่วนของระบบปฏิบัติการ และ Service โดยต้องได้รับอนุญาตจากสำนักงานสถิติแห่งชาติก่อนการดำเนินงาน

6.10. ข้อกำหนดบำรุงรักษาตามกรอบงานระบบสำรองและกู้คืนข้อมูล ของสำนักงานสถิติแห่งชาติ (NSO-BRMF) **ซึ่งมีคุณสมบัติดังนี้**

6.10.1. **ผู้รับจ้างต้องทำการเพิ่มหรือปรับปรุง** Scheduled Backup Job ระบบสำรองข้อมูลของสำนักงานสถิติแห่งชาติ ให้สำรองข้อมูลบนเครื่องที่สำนักงานสถิติแห่งชาติกำหนด ทั้งประเภท FileSystem หรือฐานข้อมูล หากสำนักงานสถิติแห่งชาติมีระบบใหม่เพิ่มขึ้น โดยใช้ License ที่สำนักงานสถิติแห่งชาติมีอยู่

6.10.2. **ผู้รับจ้างต้องทำการทดสอบการกู้คืนระบบตามข้อกำหนดดังต่อไปนี้**

6.10.2.1. ทดสอบกู้คืน FileSystem บนเครื่องที่มีระบบปฏิบัติการ Windows และ UNIX ประเภทละ 1 เครื่อง ตามที่สำนักงานสถิติแห่งชาติกำหนด

6.10.2.2. ทดสอบกู้คืนฐานข้อมูล Oracle และ MySQL ประเภทละ 1 เครื่อง ตามที่สำนักงานสถิติแห่งชาติกำหนด

6.10.2.3. ทดสอบกู้คืนระบบงาน จำนวน 1 ระบบ ตามที่สำนักงานสถิติแห่งชาติกำหนด

ทั้งนี้ผู้รับจ้างต้องเป็นผู้จัดเตรียมความพร้อมในส่วนของ Configuration บนเครื่องที่สำนักงานสถิติแห่งชาติจัดหาให้สำหรับการทดสอบ

6.11. ข้อกำหนดการบำรุงรักษาสถาปัตยกรรมระบบ

6.11.1. **ผู้รับจ้างต้องจัดเตรียมเจ้าหน้าที่ด้านระบบคอมพิวเตอร์และสถาปัตยกรรม จำนวนอย่างน้อย 1 คน ปฏิบัติหน้าที่ที่สำนักงานสถิติแห่งชาติ สัปดาห์ละ 1 วัน เพื่อสนับสนุนรองรับการปรับปรุงระบบ, การปิดเปิดระบบคอมพิวเตอร์ตามที่สำนักงานสถิติแห่งชาติต้องการ โดยมีคุณสมบัติดังนี้**

6.11.1.1. **วุฒิการศึกษาขั้นต่ำ ปริญญาตรีสาขาวิชาวิศวกรรมคอมพิวเตอร์ หรือ วิศวกรรมอิเล็กทรอนิกส์ หรือ วิศวกรรมไฟฟ้า หรือ วิทยาการคอมพิวเตอร์**

6.11.1.2. **มีประสบการณ์ในการทำงานด้านเทคโนโลยีสารสนเทศ ไม่น้อยกว่า 5 ปี**

6.11.1.3. **มีความรู้หรือประสบการณ์ และสามารถแก้ปัญหาการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายได้เป็นอย่างดี**

6.11.1.4. **มีความรู้ สามารถติดตั้งและใช้งานระบบปฏิบัติการ ดังนี้**

6.11.1.4.1. Windows Sever **ได้แก่** MS Windows NT Server **หรือ** MS Windows 2003 Server **หรือ** MS Windows 2008 Server

6.11.1.4.2. Unix Server **ได้แก่** SUN Solaris **หรือ** HP-UX **หรือ** AIX

6.11.1.4.3. **เคยผ่านการอบรมหลักสูตร** UNIX Administration **หรือ** Microsoft Windows 2003 Server **หรือ** Microsoft Windows 2008 Server

6.11.1.4.4. **สามารถให้คำปรึกษาแนะนำและแก้ปัญหาให้กับเจ้าหน้าที่ของสำนักงานสถิติแห่งชาติ ตามที่สำนักงานสถิติแห่งชาติร้องขอ**

6.11.2. **ผู้รับจ้างต้องจัดทำคู่มือการปฏิบัติงานของอุปกรณ์** Firewall **ตามรายการในภาคผนวก ก ข้อ 5.1 เพื่อให้เจ้าหน้าที่ของสำนักงานสถิติแห่งชาติสามารถนำไปใช้ปฏิบัติงานได้ด้วยตนเอง**

/6.11.3...

6.11.3. สำนักงานสถิติแห่งชาติขอสงวนสิทธิ์เปลี่ยนเจ้าหน้าที่ใหม่ หากเจ้าหน้าที่ไม่สามารถปฏิบัติงานตามที่สำนักงานสถิติแห่งชาติกำหนดหรือมอบหมาย

6.12. ข้อกำหนดระดับการให้บริการ (Service Level Agreement)

6.12.1. ผู้รับจ้างต้องมีการบริการทางโทรศัพท์ (On Call Service) ตลอด 8 ชั่วโมง (ทำการ) x 5 วัน (ทำการ) ตลอดระยะเวลาสัญญา โดยให้บริการต่อไปนี้ เป็นอย่างน้อย

6.12.1.1. ให้บริการตอบคำถามทางโทรศัพท์ในการแก้ไขปัญหาต่าง ๆ

6.12.1.2. ให้บริการแก้ไขปัญหา Onsite Service ของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์

6.12.1.3. สำหรับกรณีที่ปัญหาไม่สามารถแก้ไขได้โดยการแนะนำทางโทรศัพท์ ผู้รับจ้างต้องส่งเจ้าหน้าที่ที่เชี่ยวชาญไปยังจุดที่เกิดปัญหา โดย สำนักงานสถิติแห่งชาติไม่เสียค่าใช้จ่ายใดๆ ทั้งสิ้น

6.12.1.4. หากอุปกรณ์เกิดความเสียหายจนไม่สามารถทำงานได้ตามปกติ ผู้รับจ้างต้องทำการแก้ปัญหาดังนี้

6.12.1.4.1. ภายหลังรับแจ้งปัญหาต้องดำเนินการสอบถามปัญหาเบื้องต้นและสาเหตุ เช่น การเสียหายทางฮาร์ดแวร์ ต้องจัดส่งเจ้าหน้าที่มาแก้ไขที่สถานที่ (Onsite Service) ติดตั้ง ภายในเวลา 4 ชั่วโมง (ทำการ)หลังจากได้รับแจ้งด้วยวาจาหรือลายลักษณ์อักษรจากเจ้าหน้าที่ของสำนักงานสถิติแห่งชาติ

6.12.1.4.2. ดำเนินการแก้ไขให้สามารถใช้งานได้ภายในระยะเวลาที่กำหนดในภาคผนวก ข.

6.12.1.4.3. หากไม่สามารถดำเนินการแก้ไขให้อุปกรณ์ทำงานได้เป็นปกติผู้รับจ้างต้องทำการวิเคราะห์หาสาเหตุปัญหาที่แท้จริงและจัดทำเอกสารรายงานแนวทางการแก้ไขปัญหา เสนอต่อสำนักงานสถิติแห่งชาติ ภายใน 3 วันทำการ

6.12.2. สำนักงานสถิติแห่งชาติขอสงวนสิทธิ์ดำเนินการติดต่อกับผู้ผลิตหรือเจ้าของผลิตภัณฑ์เองในเรื่องของการให้บริการผลิตภัณฑ์ โดยสำนักงานสถิติแห่งชาติไม่เสียค่าใช้จ่ายใดๆ ในกรณีที่ผู้รับจ้างไม่สามารถแก้ไขปัญหาให้กับสำนักงานสถิติแห่งชาติได้ภายในเวลาที่กำหนด

6.13. ข้อกำหนดการแก้ปัญหาอื่น ๆ

ในกรณีที่ในทางปฏิบัติผู้รับจ้างไม่สามารถบำรุงรักษาอุปกรณ์ในรายการใดได้ให้ทำหนังสือแจ้งพร้อมสาเหตุและแนวทางในการแก้ปัญหาให้สำนักงานสถิติแห่งชาติรับทราบเป็นลายลักษณ์อักษร

6.14. ข้อกำหนดอื่นๆ

ภายหลังการเสนอราคาด้วยวิธีการทางอิเล็กทรอนิก ผู้เสนอราคาต้องจัดทำเอกสารแสดงราคาการบำรุงรักษาเป็นรายอุปกรณ์ตามรายการในภาคผนวก ก. ให้สำนักงานสถิติแห่งชาติ ภายใน 1 วัน

/6.15...

6.15. การรับประกันผลงาน

ผู้รับจ้างต้องดำเนินการซ่อมแซมอุปกรณ์ที่อยู่ในสัญญาบำรุงรักษาให้สามารถใช้งานได้ตามปกติ ตลอดช่วงระยะเวลาสัญญาบำรุงรักษาฯ ตามข้อกำหนดระดับการให้บริการ (Service Level Agreement) ตามข้อ 6.12 หากผู้รับจ้างไม่สามารถดำเนินการได้ สำนักงานสถิติแห่งชาติจะคิดค่าปรับตามระเบียบพัสดุ ทั้งนี้ให้เริ่มนับเวลาที่ครบกำหนดในภาคผนวก ข ยกเว้นกรณีของความเสียหายหรือขัดข้องที่เกิดขึ้นเนื่องจากอุปกรณ์อื่นใดที่อยู่นอกเหนือสัญญาที่สำนักงานสถิติแห่งชาตินำมาเชื่อมต่อกับอุปกรณ์ที่ผู้รับจ้างบำรุงรักษา

7. ระยะเวลาดำเนินงานและส่งมอบและการจ่ายเงิน

กำหนดระยะเวลาการดำเนินงานและส่งมอบงานถึงวันที่ 30 กันยายน พ.ศ. 2556 โดยแบ่งการเบิกจ่ายเงินเป็น 2 งวด ของวงเงินตามสัญญา ดังนี้

7.1. งวดที่ 1 เป็นจำนวนเงินในอัตราร้อยละ 60 ของค่าจ้าง เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงานภายใน90 วัน นับถัดจากวันลงนามในสัญญา ดังนี้

7.1.1. ตรวจสอบความผิดปกติต้นรอบการบำรุงรักษาพร้อมดำเนินการแก้ไขปัญหางานจากการตรวจสอบความผิดปกติต้นรอบการบำรุงรักษา และส่งมอบเอกสารรายงานการตรวจสอบความผิดปกติต้นรอบและการแก้ไขปัญหา

7.1.2. ปฏิบัติงานตามข้อกำหนดการให้บริการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) ครั้งที่ 1 และส่งมอบเอกสารรายงานการให้บริการบำรุงรักษาเชิงป้องกัน ครั้งที่ 1

7.1.3. ปฏิบัติงานตามข้อกำหนดการซ่อมแซมและแก้ไขปัญหา (Corrective Maintenance) และส่งมอบเอกสารรายงานการซ่อมแซมและแก้ไขปัญหา

7.1.4. ดำเนินการต่ออายุสัญญาลิขสิทธิ์ซอฟต์แวร์พร้อมส่งมอบเอกสารลิขสิทธิ์ซอฟต์แวร์ ตามข้อ 6.3.1 (รายละเอียดตามภาคผนวก ก. ข้อ 8)

7.1.5. ดำเนินการต่ออายุสัญญา License และ Update Signature หรือ Patch และต่อ Support ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ต่อพ่วง อุปกรณ์เครือข่าย และอุปกรณ์ความมั่นคงปลอดภัยฯ จากเจ้าของผลิตภัณฑ์หรือตัวแทนจำหน่าย ตามรายการในภาคผนวก ก. ข้อ 5

7.1.6. ส่งมอบเอกสารรายงานการตรวจสอบช่องโหว่ ตามข้อ 6.9.1

7.1.7. นำเสนอผลการดำเนินงานในงวดที่ 1 ให้สำนักงานสถิติแห่งชาติรับทราบ

7.2. งวดสุดท้าย เป็นจำนวนเงินในอัตราร้อยละ 40 ของค่าจ้าง เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงานภายใน 30 กันยายน 2556 ดังนี้

7.2.1. ปฏิบัติงานตามข้อกำหนดการให้บริการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) ครั้งที่ 2 และส่งมอบเอกสารรายงานการให้บริการบำรุงรักษาเชิงป้องกัน ครั้งที่ 2

7.2.2. ปฏิบัติงานตามข้อกำหนดการซ่อมแซมและแก้ไขปัญหา (Corrective Maintenance) และส่งมอบเอกสารรายงานการซ่อมแซมและแก้ไขปัญหา

7.2.3. ส่งมอบเอกสารยืนยันจากเจ้าของผลิตภัณฑ์ของเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วงเครื่องคอมพิวเตอร์แม่ข่าย ที่มีสาขาในประเทศไทยในการเป็นตัวแทนการให้บริการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วงเครื่องคอมพิวเตอร์แม่ข่าย ที่ประกาศเป็น EOSL เพิ่มเติม

7.2.4. ส่งมอบเอกสารการปิดช่องโหว่ ตามข้อ 6.9.2

7.2.5. ส่งมอบเอกสารข้อกำหนดการบำรุงรักษาตามกรอบงานระบบสำรองข้อมูลและกู้คืนข้อมูล NSO-BRMF ตามข้อ 6.10

7.2.6. ส่งมอบเอกสารการทดสอบการกู้คืนระบบ ตามข้อ 6.10

7.2.7. ส่งมอบเอกสารรายงานสรุปผลการปฏิบัติงานตามที่สำนักงานสถิติแห่งชาติมอบหมายในการปฏิบัติงาน

7.2.8. นำเสนอผลการดำเนินงานในงวดสุดท้าย ให้สำนักงานสถิติแห่งชาติรับทราบ

8. วงเงินในการจัดทำ

งบประมาณ 14,400,000 บาท (สิบสี่ล้านสี่แสนบาทถ้วน)

/ภาคผนวก ก...

ภาคผนวก ก. รายการบำรุงรักษา

1. เครื่องคอมพิวเตอร์แม่ข่าย

1.1. เครื่องคอมพิวเตอร์แม่ข่ายที่ผู้ผลิตไม่ประกาศ EOSL จำนวน 58 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แจ้งซ่อม
1	SUN	V210	FM40210010	NSO-0938-0091/47	26
2	SUN	V240	FN53250073	1105-02-12061000-0573-0938-0034/49	26
3	SUN	V240	FN53140224	1105-02-12061000-0549-0938-0021/49	5
4	SUN	V240	FN53140158	1105-02-12061000-0550-0938-0022/49	2
5	SUN	V240	FN53250064	1105-02-12061000-0552-0938-0024/49	5
6	SUN	V240	FN53140204	1105-02-12061000-0574-0938-0035/49	27
7	SUN	V240	FN53340296	1105-02-12061000-0551-0938-0023/49	15
8	SUN	V240	FN53130438	1105-02-12061000-0575-0938-0036/49	26
9	ATEC	Premier600	576-803-00009	1105-02-12061000-8682-0938-0432/51	3
10	Compaq	ML350 G3	T00UKT461D	NSO-0938-0437/47	12
11	Compaq	ML350	T00TKT461D	NSO-0938-0439/47	4
12	Compaq	ML350 G3	T00SKT461D	NSO-0938-0438/47	5
13	Dell	PowerEdge 2900	535RR1S	1105-02-12061000-6354-0938-0002/51	2
14	Dell	PowerEdge R410	JVCN426	1105-02-12061000-1198-0938-0310/54	22
15	IBM	System X3650	99P3120	อยู่ระหว่างการตรวจสอบครุภัณฑ์	27
16	IBM	System X3650	99GB074	1105-02-12061000-8917-0938-0119/52	3
17	IBM	system P5	O63E34A	1105-83-12061000-8751-0938-0436/51	12

เครื่องที่	Brand	Model	Serial	ครุภัณฑ์คอมพิวเตอร์	ปีที่ผลิต
18	IBM	system P5	O63E32A	1105-83-12061000-8865-0938-0437/51	12
19	IBM	X3850 M2	99C1425	1105-02-12061000-8744-0938-0434/51	24
20	IBM	X3650	99CM697	1105-02-12061000-8745-0938-0435/51	25
21	IBM	X236	99PM367	NSO-0938-0051/49	12
22	IBM	System P5	06A49EH	1105-02-12061000-8881-0938-0042/53	17
23	IBM	System x3850	99E0003	1105-02-12061000-8882-0938-0043/53	17
24	IBM	System P5	06A49FH	1105-02-12061000-8880-0938-0041/53	11
25	HP	DL380 G5	SGH808BKK9	1105-02-12061000-8757-0938-0439/51	15
26	HP	ML350 G5	CN773600FW	1105-83-12061000-8753-0938-0438/51	2
27	HP	DL380 G5	SGH848XNNW	1105-02-1206100-8915-0983-0118/52	3
28	HP	9000 rp4440	SGH474054T	1105-02-12061000-5074-0938-0150/51	10
29	HP	9000 rp4440	SGH474054R	1105-02-12061000-5073-0938-0149/51	10
30	HP	ML350 G4	TWT53000J1	1105-02-12061000-0577-0938-0038/49	6
31	HP	ML350 G4	TWT53000J0	1105-02-12061000-0564-0938-0029/49	5
32	HP	ML350 G4	TWT53000J2	1105-02-12061000-0565-0938-0030/49	27
33	HP	ML350 G4	TWT53000J9	1105-02-12061000-0581-0938-0055/49	6
34	HP	ML350 G4	TWT53000J7	1105-02-12061000-0553-0938-0025/49	9
35	HP	ML350 G4	TWT53000J4	1105-02-12061000-0570-0938-0032/49	4

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง
36	HP	ML350 G4	TWT53000J6	1105-02-12061000-0571-0938-0033/49	4
37	HP	ML350 G4	TWT53000J3	1105-02-12061000-0569-0938-0031/49	27
38	HP	ML350 G4	TWT53000J5	อยู่ระหว่างการตรวจสอบครุภัณฑ์	6
39	HP	9000 rp4440	SGH641LYH	NSO-0938-0007/50	8
40	HP	DL580 G3	SGH641X5AN	NSO-0938-0008/50	27
41	HP	DL380 G4	SGH641X5AR	NSO-0938-0017/50	22
42	HP	9000 rp4410	SGH4641LXL	NSO-0938-0010/50	22
43	HP	DL380G4	SGH641X5B5	1105-02-12061000-0938-0011/50	12
44	HP	9000 rp4440	SGH4641LXS	NSO-0938-0012/50	15
45	HP	DL580 G3	SGH641X5AP	NSO-0938-0013/50	24
46	HP	DL380 G4	SGH641X5AX	NSO-0938-0009/50	16
47	HP	DL380 G4	SGH641X5B6	NSO-0938-0015/50	5
48	HP	DL380 G4	SGH641X5B4	NSO-0938-0016/50	22
49	HP	DL380 G4	SGH641X5AT	NSO-0938-0014/50	22
50	HP	DL380 G4	SGH641X5B3	NSO-0938-0053/50	4
51	HP	DL380 G4	SGH641X5B8	NSO-0938-0055/50	4
52	HP	DL380 G4	SGH641X5B7	NSO-0938-0056/50	25
53	HP	DL380 G4	SGH641X5AV	NSO-0938-0057/50	4
54	HP	DL380 G4	SGH641X5AS	NSO-0938-0060/50	6
55	HP	DL380 G4	SGH641X5AW	NSO-0938-0061/50	5
56	HP	ML310 G4	CN67320C81	1105-02-12061000-7827-0938-0206/51	23
57	HP	DL580 G4	SGH742AP44	1105-02-12061000-7720-0938-0203/51	3
58	HP	DL580 G4	SGH742AP45	1105-02-12061000-7719-0938-0202/51	15

1.2. เครื่องคอมพิวเตอร์แม่ข่ายที่ผู้ผลิตประกาศ EOSL จำนวน 17 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง	กลุ่มที่
1	SUN	V250	FQ34930049	NSO-0938-0464/47	23	2
2	SUN	280R	332AD2E44	NSO-0938-0436/47	24	1

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	หน้าที่ใช้	กลุ่มที่
3	SUN	V480	0532AM013D	1105-02-12061000-0578-0938-0039/49	8	1
4	SUN	V480	0530AM00D0	1105-02-12061000-0538-0938-0020/49	8	1
5	SUN	V480	0532AM019E	1105-02-12061000-0579-0938-0040/49	5	1
6	SUN	280R	0442AD1498	1105-02-12061000-2601-0938-0139/48	16	2
7	SUN	280R	0345AD1D50	1105-02-12061000-2602-0938-0142/48	23	1
8	SUN	280R	0444AD1152	1105-02-12061000-2598-0938-0136/48	24	1
9	SUN	280R	0444AD1148	1105-02-12061000-2599-0938-0137/48	25	1
10	SUN	V480	322V0101	NSO-0938-0078/46	26	1
11	Dell	PowerEdge 1800	49T6J1S	1105-02-12061000-3482-0938-0054/49	16	2
12	Dell	PowerEege 2800	GTSFC1S	1105-02-12061000-2600-0938-0138/48	9	2
13	Dell	PowerEdge 2600	2TGF81S	NSO-0938-0077/46	27	2
14	DELL	PowerEdge 1800	H3N7H15	NSO-0938-0056/49	12	2
15	SUN	280R	334AD1F4B	NSO-0938-0435/47	25	2
16	SUN	480	247V0288	NSO-0938-0055/46	9	2
17	SUN	280R	04444AD1082	1105-02-12061000-2603-0938-0140/48	25	2

หมายเหตุ : กลุ่มที่ 1 = เครื่องคอมพิวเตอร์แม่ข่ายที่กำหนดให้แก้ไขใช้งานได้ภายใน 12 ชั่วโมง
กลุ่มที่ 2 = เครื่องคอมพิวเตอร์แม่ข่ายที่กำหนดให้แก้ไขใช้งานได้ภายใน 16 ชั่วโมง

2. หน่วยเก็บข้อมูล

2.1. อุปกรณ์ SAN Switch ที่ผู้ผลิตไม่ประกาศ EOSL จำนวน 2 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	หน้าที่ใช้
1.	HP	Storage Work 4/16	usb629x3z1	1105-02-12061000-3660-0957-0001/50	19

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง
2.	HP	Storage Work 4/16	usb629x3y2	1105-02-12061000-3660-0957-0001/50	19

2.2. อุปกรณ์ SAN Switch ที่ผู้ผลิตประกาศ EOSL จำนวน 2 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง
1.	Brocade	3850	0523660210	1105-02-12061000-0540-0964-0001/49	18
2.	Brocade	3850	0522660179	1105-02-12061000-0540-0964-0002/49	18

2.3. อุปกรณ์ SAN ที่ผู้ผลิตไม่ประกาศ EOSL จำนวน 11 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง
1	SUN	StorEdge 3500	1094MIL-0531086D7B	1105-02-12061000-0539-0957-0001/49	18
2	HP	Storage Work MSL6000	USX649Z050	1105-02-12061000-3368-0965-0001/50	19
3	HP	Storage Work	USX649Z050	1105-02-12061000-3660-0957-0001/50	19
4	HP	HSV-200-A (Controller)	UB629X3Y2	1105-02-12061000-3660-0957-0001/50	19
5	HP	HSV-200-A (Controller)	UB629X3Z1	1105-02-12061000-3660-0957-0001/50	19
6	HP	Storage Works (Disk Array)	SGM06403XN	1105-02-12061000-3660-0957-0001/50	19
7	HP	Storage Works (Disk Array)	SGM06403RP	1105-02-12061000-3660-0957-0001/50	19
8	HP	Storage Works (Disk Array)	SGM06403WN	1105-02-12061000-3660-0957-0001/50	19
9	HP	Storage Works (Disk Array)	SGM06403RS	1105-02-12061000-3660-0957-0001/50	19
10	SUN	StorageTek 6140-CU-2GB/4PT	0910DHG01L	อยู่ระหว่างการตรวจสอบครุภัณฑ์	18
11	Storage Flex	HA-3969	RA1406001N	รอหมายเลขครุภัณฑ์จากพัสดุ	10

2.4. อุปกรณ์ SAN ที่ผู้ผลิตประกาศ EOSL จำนวน 2 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง
1	SUN	StorEdge D1000	GS490206	อยู่ระหว่างการตรวจสอบครุภัณฑ์	16
2	SUN	StorEdge 3300	02390000D2	อยู่ระหว่างการตรวจสอบครุภัณฑ์	9

3. ระบบสำรองข้อมูลและกู้คืน

3.1. อุปกรณ์เทปชนิด Library ที่ผู้ผลิตไม่ประกาศ EOSL จำนวน 1 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง
1	HP	Storage Work MSL6000	USX649Z050	1105-02-12061000-3368-0965-0001/50	19

3.2. อุปกรณ์เทปชนิดเดี่ยว จำนวน 3 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง
1	HP	Storage Works Ultrium 960	HU107363HK	1105-02-12061000-5073-0938-0149/51	10
2	IBM	System Storage Ultrium LTO3	6882187	1105-02-12061000-8893-0965-0001/53	16
3	HP	Ultrium LTO4 Tandberg Data	MXB3H03030	อยู่ระหว่างการตรวจสอบครุภัณฑ์	12

4. รายการอุปกรณ์เครือข่าย

4.1. อุปกรณ์ Core Switch จำนวน 1 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง
1	Huawei 3COM	S7506R	210235A13xx069000005	NSO-0964-0001/50	3

4.2. อุปกรณ์ Workgroup Switch จำนวน 10 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง
1	Alcatel	OmniSwitch 6800-24	F25Q0259	1105-02-12061000-0561-0964-0005/49	1
2	Alcatel	OmniSwitch 6800-24	F25Q0073	1105-02-12061000-3418-0964-0009/49	1

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ติด
3	CISCO	Cytalyst 3560	FD01124Y4SK	1105-02-12061000-8166-6964-0059/51	1
4	Huawei	Quidway S5600	210235A126A064000062	NSO-0964-0003/50	1
5	Huawei	Quidway S5600	210235A1270057000031	NSO-0964-0002/50	1
6	Alcatel	OmniSwitch 6624	9020831032833386	อยู่ระหว่างการตรวจสอบครุภัณฑ์	1
7	Alcatel	OmniSwitch 6624	90208310338J0893	อยู่ระหว่างการตรวจสอบครุภัณฑ์	1
8	Alcatel	OmniSwitch 6624	9020831032833343	อยู่ระหว่างการตรวจสอบครุภัณฑ์	1
9	CISCO	Cytalyst Express 500G-12TC	FOC1250V07V	1105-02-12061000-8897-0964-0001/53	1
10	Radware	LinkProof 202	20916210	1105-02-12061000-9637-0976-0001/53	4

5. อุปกรณ์ความมั่นคงปลอดภัย

5.1. อุปกรณ์ Firewall จำนวน 5 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ติด
1	Check Ponit (FW-1)	UTM1-2070	0818800499	อยู่ระหว่างการตรวจสอบครุภัณฑ์	5
2	StoneGate StoneSoft (FW-2)	SG-3000	VM-050610-10-04	1105-02-12061000-0560-0938-0026/49	5
3	McAfee/FW	S3008	W044121332	รอหมายเลขครุภัณฑ์จากพัสดุ	5
4	Crossbeam (FW-4)	C30	G4080168	NSO-0938-0049/50	5
5	Checkpoint SSL VPN	Connectra 3070	0908B00434	1105-02-12061000-9638-0977-0001/53	6

5.2. อุปกรณ์ IPS/IDS ที่ผู้ผลิตประกาศ EOSL และซอฟต์แวร์ Signature จำนวน 2 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง
1	ISS	Appliance A604 series	AZCW3461027	1105-02-12061000-0563-0938-0028/49	5
2	ISS	Appliance G200 series	AZCW4410257	1105-02-12061000-0562-0938-0027/49	5

5.3. อุปกรณ์ Virus Gateway จำนวน 2 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง
1	Symantec	Web Gateway 8450	63PX5L1	อยู่ระหว่างการตรวจสอบครุภัณฑ์	5
2	IronPort	C160	0025643C1394-CJ7F0L1	1105-02-12061000-9639-0967-0001/53	6

5.4. อุปกรณ์ Proxy Server จำนวน 2 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง
1	Blue Coat	800 Series	2805000021	1105-02-12061000-0576-0938-0037/49	5
2	Blue Coat	SG900	2211244134	1105-02-12061000-12261-0960-0001/55	5

5.5. อุปกรณ์ Vulner จำนวน 3 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง
1	McAfee	MVM3100	W046122097	รอหมายเลขครุภัณฑ์จากพัสดุ	5
2	McAfee	MVM2100	W057121167	รอหมายเลขครุภัณฑ์จากพัสดุ	5
3	McAfee	MVM2100	W057121167	รอหมายเลขครุภัณฑ์จากพัสดุ	5

6. พัดลมระบายความร้อนบนตู้ Rack จำนวน 90 ชุด

7. อุปกรณ์ KVM จำนวน 13 ชุด

เครื่องที่	Brand	Model	Serial	หมายเลขครุภัณฑ์	แร็คที่ตั้ง
1	HP	TFT7600	MY2921F4HJ	NSO-0964-0005/50	R22
2	NOVAVIEW	Rextron KNV104	N03000EE00016	อยู่ระหว่างการตรวจสอบครุภัณฑ์	R23

[illegible]	Brand	Model	Serial	[illegible]	[illegible]
3	AVOCENT	AUTOVIEW 1415	270146902	อยู่ระหว่างการตรวจสอบครุภัณฑ์	R24
4	NTI	UNIMUX	713UNIMUX-USBV-8-220V-USA	1105-02-12061000-0584-0964-0006/49	R26
5	ATEN	CS1758	Z88AV027AFD0036	1105-02-12061000-8896-0938-0041/53	R27
6	ATEN	OSD	Z88AV027AFD0036	1105-02-12061000-8896-0938-0041/53	R17
7	NOVAVIEW	UNV108D	G51000FH00016	อยู่ระหว่างการตรวจสอบครุภัณฑ์	R16
8	NOVAVIEW	UNV108D	G51000FH00014	อยู่ระหว่างการตรวจสอบครุภัณฑ์	R15
9	NOVAVIEW	UNV108D	G51000FH00022	อยู่ระหว่างการตรวจสอบครุภัณฑ์	R8
10	D-LINK	DKVM-8E	BS0I285000730	1105-02-12061000-8686-0964-0060/51	R9
11	D-LINK	DKVM-8E	BS01134000311	อยู่ระหว่างการตรวจสอบครุภัณฑ์	R10
12	ATEN	CS-84A	A188U183BDH0453	อยู่ระหว่างการตรวจสอบครุภัณฑ์	R11
13	Avocent	MPU2032-101	0520020726	รอหมายเลขครุภัณฑ์จากพัสดุ	R1

8. ซอฟต์แวร์

8.1. ซอฟต์แวร์ควบคุมเนื้อหาที่ไม่เหมาะสม WebSense จำนวน 1 ชุด

รายละเอียด	จำนวน
Web filter	1,000

8.2. ซอฟต์แวร์การเก็บข้อมูลจราจร ArcSight จำนวน 1 ชุด

รายละเอียด	จำนวน
ARCSIGHT PREMIUM SUPPORT – Initial License Fee	1
SECURITY CONTENT SUBSCRIPTION	1
ARCSIGHT PREMIUM SUPPORT	1
SECURITY CONTENT SUBSCRIPTION	1

8.3. ซอฟต์แวร์ป้องกันไวรัส Symantec จำนวน 1 ชุด

รายละเอียด	จำนวน
SYMC PROTECTION SUITE ENTERPRISE EDITION 3.0 PER USER RENEWAL ESSENTIAL 12 MONTHS GOV BAND A	300
SYMC WEB GATEWAY URL FILTERING ADD ON 4.5 PER USER SUB LIC GOV BAND A ESSENTIAL 12 MONTHS	300

8.4. ซอฟต์แวร์ป้องกันไวรัส NOD32 จำนวน 1 ชุด

รายละเอียด	จำนวน
ESET NOD32 Antivirus Business Edition	1,000

8.5. ซอฟต์แวร์สำรองข้อมูล Veritas Netbackup จำนวน 1 ชุด

รายละเอียด	จำนวน
VRTS STORAGE FOUNDATION STANDARD 5.1 UNX PER SERVER TIER C RENEWAL ESSENTIAL 12 MONTHS GOV BAND S	1
SYMC NETBACKUP CLIENT APPLICATION AND DATABASE PACK 7.1 UNX 1 SERVER TIER 1 RENEWAL ESSENTIAL 12 MONTHS GOV BAND S	1
SYMC NETBACKUP CLIENT APPLICATION AND DATABASE PACK 7.1 UNX 1 SERVER TIER 1 RENEWAL ESSENTIAL 12 MONTHS GOV BAND S	2
SYMC NETBACKUP OPTION LIBRARY BASED TAPE DRIVE 7.1 XPLAT 1 DRIVE RENEWAL ESSENTIAL 12 MONTHS GOV BAND S	2
SYMC NETBACKUP OPTION SHARED STORAGE OPTION 7.1 XPLAT 1 DRIVE RENEWAL ESSENTIAL 12 MONTHS GOV BAND S	2
SYMC NETBACKUP ENTERPRISE CLIENT 7.1 UNX 1 SERVER TIER 1 RENEWAL ESSENTIAL 12 MONTHS GOV BAND S	3

8.6. ซอฟต์แวร์สำรองข้อมูล HP Data Protector จำนวน 1 ชุด

รายละเอียด	จำนวน
One drive for UNIX/NAS/SAN LTU (License-to-use)	2
Online Backup for Windows LTU	1
Online Backup for UNIX LTU	1
Advanced Backup to Disk for UNIX LTU	1
Open File Backup 10-Server LTU	2
Start Pack for Windows DVD LTU	1

8.7. ซอฟต์แวร์ AppManager จำนวน 300 License

8.8. ซอฟต์แวร์ OpManager จำนวน 250 License

/ภาคผนวก ข

ภาคผนวก ข. ค่าตัวถ่วง

ประเภทของอุปกรณ์	ค่าน้ำหนักความสำคัญ (ค่าตัวถ่วง)	จำนวนชั่วโมงทำการที่กำหนดให้แก้ไขใช้งานได้
1. เครื่องคอมพิวเตอร์แม่ข่าย		
1.1. เครื่องคอมพิวเตอร์แม่ข่ายที่ผู้ผลิตไม่ประกาศ EOSL	0.18	8 ช.ม.
1.2. เครื่องคอมพิวเตอร์แม่ข่ายที่ผู้ผลิตประกาศ EOSL กลุ่มที่ 1	0.18	16 ช.ม.
1.3. เครื่องคอมพิวเตอร์แม่ข่ายที่ผู้ผลิตประกาศ EOSL กลุ่มที่ 2	0.18	12 ช.ม.
2. หน่วยเก็บข้อมูล		
2.1. อุปกรณ์ SAN Switch ที่ผู้ผลิตไม่ประกาศ EOSL	0.24	4 ช.ม.
2.2. อุปกรณ์ SAN Switch ที่ผู้ผลิตประกาศ EOSL	0.24	8 ช.ม.
2.3. อุปกรณ์ SAN ที่ผู้ผลิตไม่ประกาศ EOSL	0.24	4 ช.ม.
2.4. อุปกรณ์ SAN ที่ผู้ผลิตประกาศ EOSL	0.24	8 ช.ม.
3. ระบบสำรองข้อมูลและกู้คืน		
3.1. อุปกรณ์เทปชนิด Library ที่ผู้ผลิตไม่ประกาศ EOSL	0.12	8 ช.ม.
3.2. อุปกรณ์เทปชนิดเดี่ยว	0.06	8 ช.ม.
4. รายการอุปกรณ์เครือข่าย		
4.1. อุปกรณ์ Core Switch	0.24	4 ช.ม.
4.2. อุปกรณ์ Workgroup Switch	0.24	4 ช.ม.
5. อุปกรณ์ความมั่นคงปลอดภัย		
5.1. อุปกรณ์ Firewall	0.24	4 ช.ม.
5.2. อุปกรณ์ IPS/IDS และซอฟต์แวร์ Signature	0.18	8 ช.ม.
5.3. อุปกรณ์ Virus Gateway	0.06	8 ช.ม.
5.4. อุปกรณ์ Proxy Server	0.24	8 ช.ม.
5.5. อุปกรณ์ Vulner	0.12	8 ช.ม.
6. พัดลมระบายความร้อนบนตู้ Rack	0.06	16 ช.ม.
7. อุปกรณ์ KVM	0.12	16 ช.ม.

/ภาคผนวก ค...

ภาคผนวก ค.

เครื่องคอมพิวเตอร์แม่ข่าย/SUN

ภาคผนวก ค.ข้อ 1.

Organization

Project Name : ..... Contract No. .....

Project Code : ..... Action : ..... Service ..... Time(s)

Service

Product : ..... Serial No. .....

1. Equipment Working & Cleaning		2. Checking OS & Analyze		
☐ Monitor	☐ Power System	☐ /etc/passwd	☐ /etc/shadow	☐ Solaris Version : .....
☐ Keyboard/mouse	☐ Magnetic Field	☐ Diagnostic Program	☐ prtdiag (for sun 4U)	☐ Kernal Patch Version : .....
☐ All Connector	☐ Network	☐ explorer	☐ messages files	☐ OBP Version : .....
☐ Removable Drive	☐ SCSI	☐ Hostid :		☐ IP Address : .....
☐ IDE (for U5&U10)	☐	☐ date :	☐	☐ Host Name : .....

3. Clecа File for Prevent File System Full		4. Blower	Result of System
☐ lastlog	☐ Messages files	☐ Internal & System Equipment	☐ Normal ☐ Fault
☐ sulog	☐ utmp, utmpx	☐ Post	.....
☐ vold.log,syslog	☐ wtmp, wtmpx	☐ External Device	.....
For no clearing any file		☐	.....
☐ Customer would like to keep all files		☐	.....

รายงานผลการตรวจสอบการใช้พื้นที่เก็บข้อมูลบนเครื่องคอมพิวเตอร์แม่ข่าย

เครื่องแม่ข่าย : ..... สถานที่ : .....

รายละเอียดของการใช้พื้นที่เก็บข้อมูล

	Mountpoint	size	Avail	% Usage
รายละเอียด				
คำแนะนำ				

(.....)

Service Representative Signature

Date .....

(.....)

Customer Signature

Date .....

เครื่องคอมพิวเตอร์แม่ข่าย/HP, IBM, DELL

Server PM Checklist

ภาคผนวก ง ฉบับ 1

1. Hardware Inspecifition

Server Name : ..... Room Version : ..... IP Address : .....

HW Model : ..... Memory : ..... CPU Speed : .....

Serial No. ..... Harddisk : ..... HDD Type : .....

Network Card :

2. Disk Redundant .....

☐ None Raid ☐ RAID 0 ☐ RAID 1 ☐ RAID 5 ☐ Other :

3. More often, the hard disk space becomes hogged and leaves an user to think what's the cause. So that disk space checking to help help you for analyze disk space usage.

Disk Capacity	C:	.....	D:	.....	E:	.....	more : .....
- Used space	C:	.....	D:	.....	E:	.....	more : .....
- Free space	C:	.....	D:	.....	E:	.....	more : .....

Total No. of Storage Disk : .....

4. Windows Checking and Performance

OS Version : .....

Lastest Service Pack : .....

Perfomance

CPU Usage : ..... PF Usage: ..... Commit Charge : .....

Physical Memory (K)

Total : ..... Proposed Action : .....

Available . ...

System Cache : ....

Check for the lastest Service Packs

☐ Empty the Recycle Bin. (Periodically Checking and emptying the Recycle Bin is a Good Habit)

☐ Clean out Windows Temprary Files. (Delete all * .tmp files that have been created prior to the current day)

☐ Clean out Windows Temprary Internet Files. (Clean out the c:\Windows\Temporary Internet Files Folder.)

☐ Delete * .chk files.

☐ Review Windows Event Log. (If the error is a Fatal Error message, write it down. Otherwise you can do a Print Screen.

5. AntiVirus Checking

AntiVirus Program : ..... Program Version : .....

Engine Version : .....

Download and Install Anti-Virus Updates (Definitions) Virus pattern file number : .....

☐ Yes ☐ No Virus pattern release date : .....

☐ Automatic update pattern file ☐ Real time scan options ☐ Set Schedule scanc .....

Perform a virus scan of entire drives

☐ Not Found ☐ Clean, Delete

6. Softwares nessesary of HP Server Proposed Action : .....

☐ Installed the HP Array Configuration Utility .....

☐ Installed the HP Integrate Management Log Viewer .....

(.....)

Customer Signature

Date .....

(.....)

Engineer Signature

Date .....

SAN Switch

Switch Name : ..... IP Address : ..... PM No. : .....

Firmware Version : ..... Location : ..... Date: .....

Model : .....

การตรวจสอบการทำงานของ SAN Switch	ระยะเวลาที่ใช้	ผลการตรวจสอบ (ปกติ/ไม่ปกติ)
1. ตรวจสอบสถานะของ LED ของ SAN Switch	.....	.....
2. ทำการตรวจสอบการเชื่อมต่อผ่านทาง Telnet	.....	.....
3. ทำการตรวจสอบและเก็บสถานะการทำงานของ Power	.....	.....
4. ทำการตรวจสอบและเก็บสถานะการทำงานของ FAN	.....	.....
5. ทำการตรวจสอบการเชื่อมต่อของอุปกรณ์ในแต่ละ Port บน SAN Switch	.....	.....
6. ทำการตรวจสอบและเก็บสถานะของ ISL (Inter Switch Link) ของ SAN Switch	.....	.....
7. ทำการตรวจสอบ Log ที่มีการบันทึกไว้ใน SAN Switch	.....	.....
8. ทำการเก็บผลการแสดงการทำงานทั้งหมดในส่วนของ SAN Switch โดยใช้คำสั่ง supportshow	.....	.....
9. ทำการเก็บ Configuration ของ SAN Switch	.....	.....
10. ทำการตรวจสอบการเชื่อมต่อผ่านทาง http	.....	.....
11. ใช้โปรแกรม SAN Health เพื่อรวบรวมข้อมูลเกี่ยวกับ SAN Switch ทั้งหมด	.....	.....

1. ตรวจสอบสถานะของ LED ของ SAN Switch

ตรวจสอบ LED ที่เกิดขึ้นบน Switch

	สถานะของ LED (ปกติ/ไม่ปกติ)	หมายเหตุ
System Status	.....	.....
Power Status	.....	.....
Port LED	.....	.....

2. ทำการตรวจสอบการเชื่อมต่อ

จากเครื่อง PC ทำการเชื่อมต่อ Switch

- ถ้าสามารถเชื่อมต่อและกรอก User/Password ได้ (สถานะปกติ)
- ถ้าไม่สามารถเชื่อมต่อและกรอก User/Password ได้ (ผิดปกติ)

สถานะของการเชื่อมต่อ (ปกติ/ไม่ปกติ)	หมายเหตุ
.....	.....

3. ทำการตรวจสอบและเก็บสถานะการทำงานของ Power

ทำการเรียกคำสั่งในการตรวจสอบ Power โดยใช้คำสั่ง psshow โดยปกติ จะต้องมีสถานะเป็น OK

สถานะของการทำงาน (ปกติ/ไม่ปกติ)	หมายเหตุ
.....	.....

4. ทำการตรวจสอบและเก็บสถานะการทำงานของ FAN

ทำการเรียกคำสั่งในการตรวจสอบสถานะการทำงานของ FAN โดยใช้คำสั่ง Fanshow จะต้องมีสถานะเป็น OK

สถานะของการทำงาน (ปกติ/ไม่ปกติ)	หมายเหตุ
.....	.....

5. ทำการตรวจสอบการเชื่อมต่อของอุปกรณ์ในแต่ละ Port บน SAN Switch

ทำการเรียกคำสั่งในการตรวจสอบสถานะการเชื่อมต่อของอุปกรณ์ต่างๆ ที่เชื่อมต่อกับ SAN Switch โดยจะต้องมีสถานะ online ของแต่ละ Port ที่เชื่อมต่ออยู่แล้ว

สถานะของการเชื่อมต่อ (ปกติ/ไม่ปกติ)	หมายเหตุ
.....	.....

6. ทำการตรวจสอบและเก็บสถานะของ ISL (Inter Switch Link) ของ SAN Switch

ทำการเรียกคำสั่งในการตรวจสอบสถานะการทำงานของ Inter Switch Link ที่เป็นการเชื่อมต่อกันระหว่าง SAN Switch กับ SAN Switch

สถานะของการเชื่อมต่อ (ปกติ/ไม่ปกติ)	หมายเหตุ
.....	.....

7. ทำการตรวจสอบ Log ที่มีการบันทึกไว้ใน SAN Switch ทำการเรียกคำสั่งในการแสดงผลของ log ที่มีบันทึกเก็บไว้ใน SAN Switch และทำการวิเคราะห์ log ที่เกิดขึ้นในช่วงระยะเวลาการทำ PM	ผลการวิเคราะห์ (ปกติ/ไม่ปกติ)	หมายเหตุ .....

8. ทำการเก็บผลการแสดงการทำงานทั้งหมดในส่วนของ SAN Switch	ได้ทำตามขั้นตอน (ทำ/ไม่ได้ทำ)	หมายเหตุ .....

9. ทำการเก็บ Configuration ของ SAN Switch ทำการเรียกคำสั่งในการเก็บค่า Configuration	ได้ทำตามขั้นตอน (ทำ/ไม่ได้ทำ)	หมายเหตุ .....

10. ใช้โปรแกรม SAN Health เพื่อรวบรวมข้อมูลเกี่ยวกับ SAN Switch ทั้งหมด ใช้โปรแกรม SAN Health ในการรวบรวมข้อมูล ซึ่งจะเป็นโปรแกรมที่ลงบน PC จากนั้นทำการเรียกโปรแกรม SAN Health	ได้ทำตามขั้นตอน (ทำ/ไม่ได้ทำ)	หมายเหตุ .....

หมายเหตุ (ถ้ามี)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

(.....)

Service Representative Signature

Date .....

(.....)

Customer Signature

Date .....

Storage

Product : .....

Band ..... Serial No..... World Wide Node Name : .....

Name : .....

Harddisk Bay 1:	.....	GB	State :	☐ Good	☐ Fail
Harddisk Bay 2:	.....	GB	State :	☐ Good	☐ Fail
Harddisk Bay 3:	.....	GB	State :	☐ Good	☐ Fail
Harddisk Bay 4:	.....	GB	State :	☐ Good	☐ Fail
Harddisk Bay 5:	.....	GB	State :	☐ Good	☐ Fail
Harddisk Bay 6:	.....	GB	State :	☐ Good	☐ Fail
Harddisk Bay 7:	.....	GB	State :	☐ Good	☐ Fail
Harddisk Bay 8:	.....	GB	State :	☐ Good	☐ Fail
Harddisk Bay 9:	.....	GB	State :	☐ Good	☐ Fail
Harddisk Bay 10:	.....	GB	State :	☐ Good	☐ Fail
Harddisk Bay 11:	.....	GB	State :	☐ Good	☐ Fail
Harddisk Bay 12:	.....	GB	State :	☐ Good	☐ Fail
Harddisk Bay 13:	.....	GB	State :	☐ Good	☐ Fail
Harddisk Bay 14:	.....	GB	State :	☐ Good	☐ Fail

(.....)

Customer Signature

Date .....

(.....)

Engineer Signature

Date .....

ภาคผนวก ค.ข้อ 3.

Monitor Console & KVM 8 Port

Product : ....

Band :	Model :	Serial No :....................	Rack No: :	
Monitor	Operational State :	....	Signal Cable	Operational State : ....
Keyboard	Operational State :	....	Power Supply	Operational State : ....
Band :	Model :	Serial No :....................	Rack No: :	
Monitor	Operational State :	....	Signal Cable	Operational State : ....
Keyboard	Operational State :	....	Power Supply	Operational State : ....
Band :	Model :	Serial No :....................	Rack No: :	
Monitor	Operational State :	....	Signal Cable	Operational State : ....
Keyboard	Operational State :	....	Power Supply	Operational State : ....
Band :	Model :	Serial No :....................	Rack No: :	
Monitor	Operational State :	....	Signal Cable	Operational State : ....
Keyboard	Operational State :	....	Power Supply	Operational State : ....

(...)
Customer Signature
Date ....

(...)
Engineer Signature
Date ....

Backup Product

- Product : ....

Band : .... Model : .... Serial No :.......................... Rack No: : ....

Power Supply	Operational State :	....
Load/Eject	Operational State :	....
Read/Write	Operational State :	....
Wire Connection	Operational State :	....

Band : .... Model : .... Serial No :.......................... Rack No: : ....

Power Supply	Operational State :	....
Load/Eject	Operational State :	....
Read/Write	Operational State :	....
Wire Connection	Operational State :	....

Band : .... Model : .... Serial No :.......................... Rack No: : ....

Power Supply	Operational State :	....
Load/Eject	Operational State :	....
Read/Write	Operational State :	....
Wire Connection	Operational State :	....

Band : .... Model : .... Serial No :.......................... Rack No: : ....

Power Supply	Operational State :	....
Load/Eject	Operational State :	....
Read/Write	Operational State :	....
Wire Connection	Operational State :	....

Band : .... Model : .... Serial No :.......................... Rack No: : ....

Power Supply	Operational State :	....
Load/Eject	Operational State :	....
Read/Write	Operational State :	....
Wire Connection	Operational State :	....

(..)	(..)
Customer Signature	**Engineer Signature**
Date	**Date** ....

เอกสารแนบ ก.ข้อ 4.

Tape Backup

* Product : ....

Band : .... Model : .... Serial No :.................... Rack No: : ....

Power Supply Operational State : ....

Load/Eject Operational State : ....

Read/Write Operational State : ....

Wire Connection Operational State : ....

Band : .... Model : .... Serial No :.................... Rack No: : ....

Power Supply Operational State : ....

Load/Eject Operational State : ....

Read/Write Operational State : ....

Wire Connection Operational State : ....

Band : .... Model : .... Serial No :.................... Rack No: : ....

Power Supply Operational State : ....

Load/Eject Operational State : ....

Read/Write Operational State : ....

Wire Connection Operational State : ....

Band : .... Model : .... Serial No :.................... Rack No: : ....

Power Supply Operational State : ....

Load/Eject Operational State : ....

Read/Write Operational State : ....

Wire Connection Operational State : ....

Band : .... Model : .... Serial No :.................... Rack No: : ....

Power Supply Operational State : ....

Load/Eject Operational State : ....

Read/Write Operational State : ....

Wire Connection Operational State : ....

(..) (..)

Customer Signature **Engineer Signature**

Date .... Date ....

อุปกรณ์เครือข่ายคอมพิวเตอร์ ภาคผนวก ก.ข้อ 5.

หน่วยงาน/องค์กร .....
ที่อยู่ .....
อาคาร/ห้อง .....
ตู้ Rack ที่ : .....

วันที่ PM : .....
Contract NO : .....
PM ครั้งที่ : .....

1. รายละเอียดอุปกรณ์

ยี่ห้อ/Part Number : ..... รายละเอียดอุปกรณ์ : .....
ชื่ออุปกรณ์ (ถ้ามี) ..... Serial Number : .....

2. สภาพแวดล้อมอุปกรณ์ ☐ อยู่ในตู้ Rack ☐ วางไว้ใช้งาน

อุณหภูมิ ในตู้ Rack ..... ☐ ดี ☐ ไม่ดี นอกตู้ Rack ..... ☐ ดี ☐ ไม่ดี
ความชื้นในตู้ Rack ..... ☐ ดี ☐ ไม่ดี ความชื้นนอกตู้ Rack ..... ☐ ดี ☐ ไม่ดี
พัดลมในตู้ ☐ มี ☐ ปกติ ☐ ไม่ปกติ ☐ ไม่มี
ความเป็นระเบียบเรียบร้อย ในตู้ Rack ☐ ดี ☐ ไม่ดี นอกตู้ Rack ☐ ดี ☐ ไม่ดี
ระบบไฟฟ้า ☐ มี UPS ☐ ไม่มี UPS ☐ มี ระบบ Ground ☐ ไม่มี ระบบ Ground
☐ ค่าความต่างศักย์ระหว่าง Line กับ Neutral ..... Volt ☐ ค่าความต่างศักย์ระหว่าง Neutral กับ Ground ..... Volt

สรุปการทำงานของอุปกรณ์
☐ ทำงานได้ตามปกติ ☐ ทำงานได้แต่มี Error หรือสิ่งผิดปกติ ..... ☐ ไม่สามารถทำงานได้
☐ ข้อเสนอแนะ/การดำเนินการ .....

3. Management/Configuration

การรองรับ Management ของอุปกรณ์ ☐ อุปกรณ์รองรับ ☐ อุปกรณ์รองรับ แต่ไม่ได้ใช้งาน (ข้ามไปข้อถัดไป)
☐ อุปกรณ์ไม่รองรับ (ข้ามไปข้อถัดไป)

ในกรณีที่อุปกรณ์รองรับการ Management

Device IP Address : ..... Subnet Mask : .....
Hardware Version : ..... Flash Size : .....
Firmware Version : ..... RAM Size : .....
☐ ได้บันทึกค่า Configuration ของอุปกรณ์ไว้แล้ว ชื่อไฟล์ .....

4. การดำเนินการทำความสะอาดอุปกรณ์

☐ ได้ทำความสะอาดอุปกรณ์แล้ว
☐ ไม่ได้ทำความสะอาดอุปกรณ์
เนื่องจาก .....

5. รายละเอียด/ข้อเสนอแนะเพิ่มเติม

.....
.....
.....

6. เกณฑ์มาตรฐานสภาพแวดล้อม

มาตรฐาน	ค่าที่เหมาะสม
อุณหภูมิภายในตู้ Rack	10-30 C
อุณหภูมิภายนอกตู้ Rack	10-30 C
ความชื้นภายในตู้ Rack	20-60 %RH
ความชื้นภายนอกตู้ Rack	20-80 %RH
ค่าความต่างศักย์ระหว่าง Line กับ Neutral	210-230 Volt
ค่าความต่างศักย์ระหว่าง Neutral กับ Ground	0-4 Volt

(.....)
เจ้าหน้าที่ผู้ให้บริการ PM
ID Code : .....
Date .....

(.....)
Customer Signature
Date .....

อุปกรณ์ความ[illegible] **ภาคผนวก ค.ข้อ 6.**

หน่วยงาน/องค์กร ....

ที่อยู่ ....

อาคาร/ห้อง ....

วันที่ PM : ....

Contact : ....

PM ครั้งที่ : ....

☐ 5 x 8 Contract Service ☐ Installation ☐ Others: ....

☐ 7 x 24 Contract Service ☐ Percall

Date of Service	....
Time In / Out	....
Travel Time	....

Equipment Details

Manufacturer	Description	Model No.	Serial No.
....	....	....	....
....	....	....	....
....	....	....	....
....	....	....	....
....	....	....	....

Action / Reported Condition

....

....

....

....

....

....

....

....

Parts Replaced / Parts Number

Part No.	Description	Date Code/HW/FW	QTY	Remarks
....	....	....	....	....
....	....	....	....	....
....	....	....	....	....
....	....	....	....	....
....	....	....	....	....

(......................................)

เจ้าหน้าที่ผู้ให้บริการ PM

Date ....

(......................................)

Customer Signature

Date ....

KVM

ภาคผนวก ก.ข้อ 7.

หน่วยงาน/องค์กร .....

ที่อยู่ .....

อาคาร/ห้อง .....

ตู้ Rack ที่ : .....

Model : ..... Serial No. ..... Name : .....

Part/Items	Condition/Test				Acceptance				Remarks
Power Source	Power On	☐	Power Off	☐	Yes	☐	No	☐	.....
Power Led Lights	Working	☐	Not Working	☐	Yes	☐	No	☐	.....
KVM Port 1	Working	☐	Not Working	☐	Yes	☐	No	☐	.....
KVM Port 2	Working	☐	Not Working	☐	Yes	☐	No	☐	.....
KVM Port 3	Working	☐	Not Working	☐	Yes	☐	No	☐	.....
KVM Port 4	Working	☐	Not Working	☐	Yes	☐	No	☐	.....
KVM Port 5	Working	☐	Not Working	☐	Yes	☐	No	☐	.....
KVM Port 6	Working	☐	Not Working	☐	Yes	☐	No	☐	.....
KVM Port 7	Working	☐	Not Working	☐	Yes	☐	No	☐	.....
KVM Port 8	Working	☐	Not Working	☐	Yes	☐	No	☐	.....

Local Console	Condition/Test				Acceptance				Remarks
Monitor	Working	☐	Not Working	☐	Yes	☐	No	☐	.....
Keyboard	Working	☐	Not Working	☐	Yes	☐	No	☐	.....
Mouse	Working	☐	Not Working	☐	Yes	☐	No	☐	.....

(.....)

Customer Signature

Date .....

(.....)

Engineer Signature

Date .....

ภาคผนวก ง.

ภาคผนวก ๕

ประกาศสำนักงานสถิติแห่งชาติ

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

พ.ศ. ๒๕๕๕

ด้วย สำนักงานสถิติแห่งชาติ มีบทบาทและอำนาจหน้าที่ตามพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐ ในฐานะเป็นหน่วยงานกลางของรัฐ เกี่ยวกับการดำเนินการด้านสถิติของประเทศ บริหารจัดการสถิติและสารสนเทศของชาติอย่างเป็นระบบเพื่อการพัฒนา และเสริมสร้างศักยภาพการแข่งขัน โดยการจัดทำสำมะโนหรือสำรวจด้วยตัวอย่าง การอำนวยการเพื่อให้ได้ฐานข้อมูลทางด้านเศรษฐกิจสังคม เทคโนโลยีสารสนเทศ และอื่นๆ ของประเทศ รวมทั้งการให้ความร่วมมือและประสานงานกับองค์กรระหว่างประเทศในงานเกี่ยวกับสถิติ

ปัจจุบัน สำนักงานสถิติแห่งชาติ นำระบบคอมพิวเตอร์เครือข่าย และวิธีการทางอิเล็กทรอนิกส์มาใช้ในกระบวนการบริหารจัดการระบบสถิติ กระบวนการผลิตข้อมูลสถิติ กระบวนการให้บริการข้อมูลสถิติและสารสนเทศ เพื่อให้เกิดประสิทธิภาพสูงสุดในการปฏิบัติงาน จึงอาศัยอำนาจตามความใน มาตรา ๕ และ มาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกอบประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. ๒๕๕๓ สำนักงานสถิติแห่งชาติจึงได้จัดทำประกาศฉบับนี้ขึ้น เพื่อเป็นแนวทางให้ทุกภาคส่วนขององค์กรนำไปปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความเชื่อถือต่อผู้ใช้ข้อมูลและสารสนเทศ โดยมีเนื้อหาสาระดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

๑) "สำนักงานสถิติแห่งชาติ" หมายความว่า หน่วยงานภายในสังกัด สำนักงานสถิติแห่งชาติ รวมถึงสำนักงานสถิติจังหวัด

๒) "กระบวนการสถิติ" หมายความว่า กระบวนการที่สร้างคุณค่า และกระบวนการสนับสนุน

๓) "กระบวนการที่สร้างคุณค่า" หมายความว่า กระบวนการผลิตข้อมูลสถิติ กระบวนการให้บริการข้อมูลสถิติ กระบวนการบริหารจัดการระบบสถิติ

๔) "กระบวนการสนับสนุน" หมายความว่า กระบวนการเทคโนโลยีและสารสนเทศ กระบวนการพัฒนาบุคลากร กระบวนการประชาสัมพันธ์ กระบวนการบริหารจัดการองค์ความรู้ด้านสถิติ กระบวนการบริหารทั่วไป กระบวนการประสานความร่วมมือด้านสถิติกับหน่วยงานภายในและต่างประเทศ

๕) "ผู้ใช้งาน" หมายความว่า เจ้าหน้าที่สำนักงานสถิติแห่งชาติ ผู้ติดต่อราชการ และผู้ใช้ภายนอก

๖) "เจ้าหน้าที่สำนักงานสถิติแห่งชาติ" หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว จ้างเหมารายวัน

๗) "ผู้ติดต่อราชการ" หมายความว่า ผู้รับบริการข้อมูล ผู้รับการฝึกอบรม ผู้เข้าร่วมประชุม และผู้สนับสนุนจากภายนอก

๘) "ผู้ใช้ภายนอก" หมายความว่า ผู้ใช้ทั่วไป และผู้ใช้สมาชิก ที่เข้าถึงผ่านระบบเครือข่ายอินเทอร์เน็ต

๙) "ผู้ใช้ทั่วไป" หมายความว่า บุคคลภายนอกที่ใช้ระบบสารสนเทศโดยไม่จำเป็นต้องลงทะเบียนสมาชิก

๑๐) "ผู้ใช้สมาชิก" หมายความว่า บุคคลภายนอกที่ผ่านการลงทะเบียนเพื่อใช้ระบบสารสนเทศที่เปิดให้บริการ

๑๑) "ผู้สนับสนุนจากภายนอก" หมายความว่า เจ้าหน้าที่จากหน่วยงานภายนอกที่เข้ามาสนับสนุนการดำเนินงาน

๑๒) "สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับทรัพย์สินสารสนเทศ

๑๓) "สินทรัพย์" หมายความว่า ทรัพย์สินสารสนเทศของสำนักงานสถิติแห่งชาติ ประกอบด้วย

(๑) ระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบความมั่นคงปลอดภัย และระบบงานคอมพิวเตอร์

(๒) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(๓) ซอฟต์แวร์ โปรแกรมประยุกต์ และระบบสารสนเทศ

(๔) ข้อมูลและสารสนเทศสถิติ ในรูปข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๑๔) "ระบบสารสนเทศ" หมายความว่า ระบบงานคอมพิวเตอร์ที่สนับสนุนในกระบวนงานของสำนักงานสถิติแห่งชาติ ประกอบด้วย

(๑) ระบบสารสนเทศเพื่อการบริหารจัดการองค์กร

(๒) ระบบสารสนเทศเพื่อการผลิตข้อมูล

(๓) ระบบสารสนเทศเพื่อการบริการข้อมูลและสารสนเทศสถิติ

(๔) ระบบสารสนเทศเพื่อการจัดการระบบสถิติ

๑๕) "สารสนเทศเพื่อการบริหารจัดการองค์กร" หมายความว่า โปรแกรมประยุกต์ที่ใช้สนับสนุนการบริหารจัดการองค์กร ผู้มีสิทธิเข้าถึงเฉพาะเจ้าหน้าที่สำนักงานสถิติแห่งชาติเท่านั้น

๑๖) "สารสนเทศเพื่อการผลิตข้อมูล" หมายความว่า โปรแกรมประยุกต์ที่ใช้สนับสนุนการดำเนินงานในกระบวนการจัดเก็บ ประมวลผล และวิเคราะห์ข้อมูล

๑๗) "สารสนเทศเพื่อการบริการข้อมูลและสารสนเทศสถิติ" หมายความว่า โปรแกรมประยุกต์ที่ใช้สนับสนุนการดำเนินงานในการให้บริการกับผู้ใช้ข้อมูลทั่วไป และผู้ใช้สมาชิก

๑๘) "สารสนเทศเพื่อการจัดการระบบสถิติ" หมายความว่า โปรแกรมประยุกต์ที่ใช้สนับสนุนการจัดการระบบสถิติของประเทศ

๑๙) "สารสนเทศสถิติ" หมายความว่า ข้อมูลที่ได้จากการประมวลผลหรือวิเคราะห์ด้วยระเบียบวิธีสถิติ

๒๐) "ข้อมูลสถิติ" หมายความว่า ข้อมูลที่ได้จากการดำเนินการเกี่ยวกับสถิติตามหลักวิชาการ ประกอบด้วย ข้อมูลดิบ ข้อมูลระดับย่อย ข้อมูลเฉพาะบุคคล

๒๑) "ข้อมูลดิบ" หมายความว่า ข้อมูลรายละเอียดจากแบบสอบถามของโครงการสำมะโน/สำรวจต่างๆ ของสำนักงานสถิติแห่งชาติที่ผ่านการตรวจสอบความถูกต้องและยังมิได้ประมวลผล

๒๒) "ข้อมูลระดับย่อย" หมายความว่า ข้อมูลรายบุคคลทั้งหมดที่ผ่านการตรวจสอบความถูกต้อง ความครบถ้วน และความแบบนัยของข้อมูลไว้เรียบร้อยแล้ว พร้อมที่จะนำไปใช้ในการประมวลผลเป็นสถิติต่อไป

๒๓) "ข้อมูลเฉพาะบุคคล" หมายความว่า ข้อมูลของบุคคล หรือนิติบุคคล ห้างหุ้นส่วนสามัญ ห้างหุ้นส่วนจำกัด ซึ่งเป็นเจ้าของข้อมูลที่ได้ให้ข้อมูลหรือกรอกแบบสอบถามให้แก่สำนักงานสถิติแห่งชาติ

๒๔) "ระบบคอมพิวเตอร์" หมายถึง เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่ต่อพ่วงรวมถึงซอฟต์แวร์ที่ใช้งาน

๒๕) "ระบบเครือข่าย" หมายถึง ระบบเครือข่ายระยะไกล ระบบเครือข่ายภายใน NGX ระบบเครือข่ายไร้สาย

๒๖) "ระบบเครือข่าย NGX" หมายถึง ระบบคอมพิวเตอร์เครือข่ายภายในแบบใช้สายและไร้สาย ของศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา อาคารรัฐประศาสนภักดี (อาคาร B) ซึ่งจัดการโดยบริษัท ทีโอที จำกัด (มหาชน)

๒๗) "ระบบเครือข่าย GIN" หมายถึง ระบบคอมพิวเตอร์เครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ

๒๘) "อุปกรณ์ด้านความมั่นคง" หมายความว่า อุปกรณ์ Firewall อุปกรณ์ IPS/IDS อุปกรณ์ Proxy อุปกรณ์ Web Gateway อุปกรณ์ E-Mail Gateway หรืออุปกรณ์อื่นที่สนับสนุนงานระบบความมั่นคงปลอดภัย

๒๙) "การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับผู้ติดต่อราชการ ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๓๐) "ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

๓๑) "การรักษาความลับ (Confidentiality)" หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์ จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

๓๒) "การรักษาความครบถ้วน (Integrity)" หมายความว่า การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งาน ประมวลผล โอน หรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

๓๓) "การรักษาสภาพพร้อมใช้งาน (Availability)" หมายความว่า การจัดทำให้ทรัพย์สินสารสนเทศสามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

๓๔) "เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายความว่า การเกิดเหตุการณ์ หรือสภาพของบริการที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๓๕) "สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๓๖) "ผู้ดูแลระบบ" หมายความว่า ผู้ดูแลระบบคอมพิวเตอร์ ผู้ดูแลระบบเครือข่าย ผู้ดูแลระบบความมั่นคงปลอดภัย ผู้ดูแลระบบโปรแกรมประยุกต์ ผู้ดูแลระบบฐานข้อมูล ผู้ดูแลระบบสารสนเทศ ผู้ดูแลระบบสำรองข้อมูล

๓๗) "ผู้ดูแลระบบคอมพิวเตอร์" หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบคอมพิวเตอร์แม่ข่าย

๓๘) "ผู้ดูแลระบบเครือข่าย" หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบคอมพิวเตอร์เครือข่าย

๓๙) "ผู้ดูแลระบบความมั่นคงปลอดภัย" หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ

๔๐) "ผู้ดูแลระบบโปรแกรมประยุกต์" หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการโปรแกรมประยุกต์

๔๑) "ผู้ดูแลระบบฐานข้อมูล" หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบฐานข้อมูล

๔๒) "ผู้ดูแลระบบสำรองข้อมูล" หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบสำรองข้อมูลและกู้คืน

๔๓) "ผู้ดูแลระบบสารสนเทศ" หมายความว่า เจ้าหน้าที่ผู้ได้รับมอบหมายในการจัดการระบบสารสนเทศ

๔๔) "วิธีการแบบปลอดภัย" หมายความว่า วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์

๔๕) "ธุรกรรมทางอิเล็กทรอนิกส์" หมายความว่า ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือบางส่วน

๔๖) "ธุรกรรม" หมายความว่า การกระทำใดๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์ หรือในการดำเนินงานของรัฐตามที่กำหนด

๔๗) "ข้อมูลอิเล็กทรอนิกส์" หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

๔๘) "การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์" หมายความว่า การส่งหรือรับข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์โดยใช้มาตรฐานที่กำหนดไว้ล่วงหน้า

ข้อ ๒ ให้มีหมวดของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จำนวน ๑๑ หมวด และให้มีการปรับปรุงให้สอดคล้องกับภารกิจและเป็นปัจจุบันอยู่เสมอในทุก ๒ ปี ดังนี้

หมวดที่ ๑ การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อให้ระบบความมั่นคงปลอดภัยด้านสารสนเทศ รองรับกับภารกิจและกระบวนงานของสำนักงานสถิติแห่งชาติ มีความน่าเชื่อถือ มีคุณสมบัติ การรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และ การรักษาสภาพพร้อมใช้งาน (Availability)

หมวดที่ ๒ โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อกำหนดความรับผิดชอบและข้อตกลงการดำเนินงานในกิจกรรมระบบความมั่นคงปลอดภัยด้านสารสนเทศ ของเจ้าหน้าที่สำนักงานสถิติแห่งชาติและผู้สนับสนุนจากภายนอก

หมวดที่ ๓ การบริหารจัดการทรัพย์สินสารสนเทศ

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อปกป้องให้ทรัพย์สินสารสนเทศมีสภาพความพร้อมในการใช้งาน ไม่เกิดความเสียหายเป็นอุปสรรคต่อการดำเนินงาน

หมวดที่ ๔ การสร้างความมั่นคงปลอดภัยด้านบุคลากร

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อเป็นการป้องกันความเสียหายที่เกิดจากบุคลากรภายในหรือจากภายนอกเป็นสำคัญ

หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาใช้ในการป้องกันทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์สินอื่นใดจากการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบงานคอมพิวเตอร์

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อการจัดการช่องทางสื่อสารและระบบคอมพิวเตอร์ให้มีความปลอดภัยรองรับกับการใช้งาน

หมวดที่ ๗ การควบคุมการเข้าถึงทรัพย์สินสารสนเทศ

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อควบคุมการเข้าถึงของผู้ใช้ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบความมั่นคงปลอดภัย โปรแกรมประยุกต์ ไฟล์ข้อมูล และระบบฐานข้อมูล

หมวดที่ ๘ การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อรับมือกับภัยธรรมชาติ ภัยบนระบบเครือข่าย และภัยอื่นๆ ที่อาจสร้างความเสียหายกับทรัพย์สินสารสนเทศ อย่างเป็นขั้นตอน

หมวดที่ ๙ การบริหารจัดการด้านการบริการเพื่อให้มีความต่อเนื่อง

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อเตรียมความพร้อม กู้คืนระบบคอมพิวเตอร์ การสำรองข้อมูล การกู้คืนข้อมูล หรือ กำหนดทางเลือกใช้ศูนย์คอมพิวเตอร์สำรอง ให้ระบบสารสนเทศกลับมาดำเนินการได้ในเวลาที่รวดเร็ว

หมวดที่ ๑๐ การจัดหา การพัฒนา และการบำรุงรักษา

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาควบคุมการจัดหา การติดตั้ง การพัฒนาโปรแกรมประยุกต์ และการบำรุงรักษาระบบเพื่อให้มีสภาพพร้อมใช้งานตลอดเวลา

หมวดที่ ๑๑ การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบายและข้อกำหนด

ให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาใช้ในการตรวจสอบและประเมินระบบความมั่นคงปลอดภัยด้านสารสนเทศ จากหน่วยตรวจสอบภายใน หรือหน่วยตรวจสอบภายนอก

ข้อ ๓ ให้มีแนวปฏิบัติในแต่ละหมวด พร้อมทั้งระเบียบการใช้งานที่เกี่ยวกับงานความมั่นคงปลอดภัยด้านสารสนเทศ และบทลงโทษที่เหมาะสมหากมีการละเมิดหรือฝ่าฝืนแนวปฏิบัติ ระเบียบการใช้งาน อย่างเป็นลายลักษณ์อักษร พร้อมกับประกาศให้เจ้าหน้าที่สำนักงานสถิติแห่งชาติรับทราบโดยทั่วกัน

ข้อ ๔ ส่งเสริมและสนับสนุนให้มีการนำแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ และระเบียบการใช้งานทรัพย์สินสารสนเทศ บังคับใช้ในองค์กรอย่างจริงจัง และ ให้มีคณะกรรมการด้านความมั่นคงและปลอดภัยด้านสารสนเทศ หรือ คณะกรรมการเทคโนโลยีสารสนเทศของหน่วยงาน เพื่อกำกับและติดตามงานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

ข้อ ๕ ส่งเสริมและสนับสนุนให้มีการกำกับดูแลระบบสารสนเทศที่ดี (IT Governance) การจัดการความเสี่ยงด้านไอที (IT Risk) และการปฏิบัติตามกฎหมาย (Compliance) ระเบียบ การควบคุมภายใน

ข้อ ๖ ส่งเสริมและสนับสนุนให้ทุกส่วนงานของสำนักงานสถิติแห่งชาติใช้วิธีการแบบปลอดภัยในกระบวนการสถิติทั้งในกระบวนการสร้างที่สร้างคุณค่า และกระบวนการสนับสนุน

ข้อ ๗ ส่งเสริมและสนับสนุนให้มีการนำเทคโนโลยีด้านความมั่นคงปลอดภัยที่จำเป็นมาติดตั้งใช้งาน เพื่อสร้างความเข้มแข็งให้เพียงพอต่อการป้องกันภัยร้ายบนระบบเครือข่ายทั้งสำนักงานสถิติแห่งชาติและสำนักงานสถิติจังหวัด

ข้อ ๘ ส่งเสริมและสนับสนุนให้มีการซ้อมแผนฉุกเฉินจากเหตุการณ์อันไม่พึงประสงค์ ประกอบด้วย เพลิงไหม้ น้ำท่วม และภัยคุกคามจากระบบเครือข่ายอินเทอร์เน็ตเป็นประจำ เพื่อเตรียมความพร้อมหากเกิดเหตุการณ์ฉุกเฉินและไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้

ข้อ ๙ ส่งเสริมและสนับสนุนให้กลุ่มตรวจสอบภายในสามารถตรวจสอบระบบความมั่นคงปลอดภัยด้านสารสนเทศในระดับเบื้องต้นที่เกี่ยวกับระเบียบการใช้งาน และใช้ผู้ตรวจสอบจากภายนอกในการตรวจสอบความครบถ้วนของระบบความมั่นคงปลอดภัย

ข้อ ๑๐ ส่งเสริมให้มีการเผยแพร่ความรู้ และ จัดการอบรมความรู้ความเข้าใจของเจ้าหน้าที่ ให้ตระหนักในภัยร้ายและการร่วมมือในการปกป้องภัยร้ายประเภทต่างๆ ที่อาจเกิดขึ้น

ข้อ ๑๑ ส่งเสริมให้บุคลากรที่ดูแลและจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศได้รับการอบรมและมีความรู้ความสามารถผ่านเกณฑ์มาตรฐานที่ยอมรับ

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๘ มิถุนายน ๒๕๕๕

(นายวิบูลย์ทัต สุทันธนกิตติ์)
ผู้อำนวยการสำนักงานสถิติแห่งชาติ

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๕

ด้วยข้อมูลและสารสนเทศสถิติของสำนักงานสถิติแห่งชาติ มีการจัดเก็บด้วยวิธีการทางอิเล็กทรอนิกส์ ถือเป็นทรัพย์สินสารสนเทศหลักขององค์กรที่ต้องมีวิธีการจัดการให้มีความปลอดภัย ถูกต้องและน่าเชื่อถือ และด้วยปัญหาภัยคุกคามด้านความมั่นคงปลอดภัยด้านสารสนเทศที่มีต่อระบบสารสนเทศขององค์กรมีแนวโน้มเพิ่มมากขึ้น มีหลายปัจจัยทั้งจากภายนอกและภายในซึ่งอาจสร้างความเสียหายต่อทรัพย์สินสารสนเทศและภาพพจน์ของสำนักงานสถิติแห่งชาติจนนำไปสู่การขาดความน่าเชื่อถือต่อผู้ใช้ข้อมูลและสารสนเทศสถิติ ประกอบกับมาตรา ๓๕ ในพระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐ ระบุไว้ว่าบรรดาข้อมูลเฉพาะบุคคลหรือเฉพาะรายที่ได้มา ต้องถือเป็นความลับโดยเคร่งครัด สำนักงานสถิติแห่งชาติจึงได้จัดทำแนวปฏิบัติให้สอดคล้องกับนโยบายเพื่อเป็นแนวทางในการกำหนดมาตรการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานให้มีประสิทธิภาพ

หมวดที่ ๑
การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

วัตถุประสงค์

เพื่อให้การจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศมีคุณสมบัติการรักษาความลับ (Confidentiality) ความครบถ้วน (Integrity) และการรักษาสภาพความพร้อมใช้งาน (Availability) การดำเนินการจึงต้องมีวงจรการบริหารแบบคุณภาพ (PDCA) กำกับการดำเนินงาน ประกอบด้วย การวางแผน (Plan) การปฏิบัติตามแผน (Do) การตรวจสอบ (Check) และ การปรับปรุงแก้ไข (Act)

แนวทางปฏิบัติ

๑. ให้มีการวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยในกระบวนการสถิติพร้อมระบุวิธีการแบบปลอดภัยในกระบวนการสถิติ ทั้งกระบวนการที่สร้างคุณค่า และกระบวนการสนับสนุน เพื่อใช้เป็นกรอบการดำเนินงานด้านความมั่นคงปลอดภัยด้านสารสนเทศ

๒. การจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศต้องไม่ส่งผลกระทบต่อผู้รับบริการ

๓. ให้กำหนดกิจกรรมการบริหารระบบความมั่นคงปลอดภัย (Information Security Management System) เพื่อใช้เป็นกระบวนการการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ ดังนี้

๓) กิจกรรมในการวางแผนมีข้อกำหนด ดังนี้

(๑) ให้จัดทำ ทบทวน ปรับปรุง นโยบาย แนวปฏิบัติตามข้อกำหนดในนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศ ๑๑ หมวด และสถาปัตยกรรมระบบความมั่นคงปลอดภัยอย่างสม่ำเสมอทุก ๒ ปี เพื่อให้สอดคล้องกับความต้องการของกระบวนการสถิติ สภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงและข้อบังคับของกฎหมาย

(๒) ให้วางแผนการปรับปรุงเทคโนโลยีด้านความมั่นคงปลอดภัยสารสนเทศ และกำหนดในแผนแม่บทเทคโนโลยีสารสนเทศสำนักงานสถิติแห่งชาติ

(๓) ให้วางแผนการประเมินผลด้วยตนเองอย่างสม่ำเสมอเพื่อติดตามความครบถ้วนการดำเนินงานในกระบวนการการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

๒) กิจกรรมการปฏิบัติตามแผนมีข้อกำหนด ดังนี้

(๑) ให้ประกาศให้ทุกภาคส่วนของสำนักงานสถิติแห่งชาติได้รับทราบถึง นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศ ๑๑ หมวด รวมทั้งระเบียบการใช้งานทรัพย์สินสารสนเทศ ให้ทราบทั่วกัน

(๒) ให้นำข้อกำหนดในแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศ ๑๑ หมวด มาดำเนินงาน โดยให้มีการเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้นเป็นประจำวัน และการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศ

(๓) ให้รายงานให้ผู้บริหารได้รับทราบเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศขึ้นในสำนักงานสถิติแห่งชาติ

(๔) ให้เผยแพร่ข้อมูล และให้ความรู้กับบุคลากรให้รู้ทันภัยร้ายและตระหนักในความมั่นคงปลอดภัยด้านสารสนเทศเป็นประจำอย่างสม่ำเสมอ

(๕) ให้ประสานความร่วมมือกับหน่วยงานภายนอกทั้งในและต่างประเทศเพื่อรู้เท่าทันในภัยคุกคามบนระบบเครือข่ายที่อาจเกิดขึ้น

๓) กิจกรรมการตรวจสอบมีข้อกำหนด ดังนี้

(๑) ให้ประเมินความเสี่ยงและจัดการกับความเสี่ยงที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศที่สำคัญเป็นประจำอย่างสม่ำเสมอ โดยมีขั้นตอน การระบุปัจจัยที่มีผลทำให้เกิดความเสี่ยง และการระบุความเสี่ยงที่มีโอกาสเกิดขึ้น (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการบริหารจัดการกับความเสี่ยง (Risk Management)

(๒) ให้ตรวจสอบช่องโหว่ (Vulnerability Scanning) ของทรัพย์สินสารสนเทศที่สำคัญเป็นประจำอย่างสม่ำเสมอ และให้ปิดช่องโหว่ (Hardening) ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย อุปกรณ์ด้านความมั่นคงปลอดภัย โปรแกรมประยุกต์ ที่ได้จากการตรวจพบ และแจ้งให้ผู้มีส่วนร่วมได้รับทราบเพื่อแก้ไขและเฝ้าระวัง

(๓) ให้ทดสอบแผนการจัดการเหตุการณ์ที่ไม่คาดฝันเป็นประจำอย่างสม่ำเสมอ

(๔) ให้ตรวจสอบพฤติกรรมการใช้งานของผู้ใช้เป็นประจำสม่ำเสมอและแจ้งเตือนให้รับทราบ และควบคุมการใช้งานที่สร้างความเสียหายต่อผู้ใช้ในการปฏิบัติราชการและการให้บริการต่อผู้รับบริการ

๔) การปรับปรุงแก้ไขมีข้อกำหนด ดังนี้

(๑) ให้มีการตรวจสอบและประเมินระบบความมั่นคงปลอดภัยด้านสารสนเทศเป็นประจำอย่างสม่ำเสมอและให้นำผลการตรวจสอบและการประเมินมาใช้ในกิจกรรมวางแผนเพื่อปรับปรุงระบบความมั่นคงปลอดภัยด้านสารสนเทศต่อไป

(๒) ให้ทบทวนและวิเคราะห์ช่องว่างการบริหารระบบความมั่นคงปลอดภัย (Gap Analysis)

หมวดที่ ๒
โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร

วัตถุประสงค์

เพื่อกำหนดผู้รับผิดชอบในการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศและการดำเนินงานในกิจกรรมที่เกี่ยวเนื่อง ซึ่งประกอบด้วยผู้รับผิดชอบหลักที่เป็นเจ้าหน้าที่ของสำนักงานสถิติแห่งชาติ และผู้สนับสนุนจากภายนอก

แนวทางปฏิบัติ

๑. ให้รองผู้อำนวยการสำนักงานสถิติแห่งชาติซึ่งเป็นผู้ที่ได้รับมอบหมายจากผู้อำนวยการสำนักงานสถิติแห่งชาติเป็นผู้ดูแลด้านความมั่นคงปลอดภัยด้านสารสนเทศ ในกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ให้คณะกรรมการด้านความมั่นคงปลอดภัยด้านสารสนเทศ หรือคณะกรรมการเทคโนโลยีสารสนเทศ ทำหน้าที่ในการทบทวน ปรับปรุง นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ

๓. ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทำหน้าที่ในการบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ และกำหนดสถาปัตยกรรมระบบความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับภารกิจของสำนักงานสถิติแห่งชาติ

๔. ให้สำนักงานสถิติจังหวัดทำหน้าที่ในการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสถิติจังหวัดให้สอดคล้องกับภารกิจของสำนักงานสถิติจังหวัดใน ๖ หมวด ประกอบด้วย

หมวดที่ ๓ การบริหารจัดการทรัพย์สินสารสนเทศ
หมวดที่ ๔ การสร้างความมั่นคงปลอดภัยด้านบุคลากร
หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบงานคอมพิวเตอร์
หมวดที่ ๗ การควบคุมการเข้าถึงทรัพย์สินสารสนเทศ
หมวดที่ ๘ การบริหารจัดการด้านการบริการเพื่อให้มีความต่อเนื่อง

๕. ให้กลุ่มนิติการทำหน้าที่ประสานงานการดำเนินงานทางทางคดีหากมีการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือพระราชบัญญัติอื่น

๖. ให้กลุ่มการเจ้าหน้าที่ทำหน้าที่ในการแจ้งรายชื่อบุคลากรของสำนักงานสถิติแห่งชาติที่ลาออกให้ศูนย์เทคโนโลยีและสารสนเทศรับทราบเป็นรายเดือน เพื่อใช้ในการยกเลิกสิทธิผู้ใช้งานออกจากระบบการใช้งาน

๗. ให้กลุ่มตรวจสอบภายในทำหน้าที่ในการบริหารและจัดการระบบการตรวจสอบหรือประเมินระบบความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสถิติแห่งชาติ

๘. ให้มีการจัดทำข้อตกลงการปกปิดข้อมูลและห้ามเปิดเผยข้อมูลที่เป็นความลับสำหรับผู้สนับสนุนจากภายนอกที่เข้ามาดำเนินงานติดตั้ง งานบำรุงรักษา และงานที่มีความเกี่ยวเนื่องกับระบบความมั่นคงปลอดภัยด้านสารสนเทศ

๙. ให้ผู้รับผิดชอบในระบบแลกเปลี่ยนข้อมูลจัดทำข้อตกลงการปกปิดข้อมูล การดูแลระบบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง สำหรับหน่วยงานภายนอกที่สำนักงานสถิติแห่งชาติได้นำไปติดตั้งตามกระทรวงต่างๆ

๑๐. ให้ผู้ดูแลระบบซึ่งประกอบด้วย ผู้ดูแลระบบสารสนเทศ ผู้ดูแลโปรแกรมประยุกต์ ผู้ดูแลระบบคอมพิวเตอร์ ผู้ดูแลระบบเครือข่าย และผู้ดูแลระบบสำรองข้อมูล ทำหน้าที่ในการบริหารจัดการระบบตามหน้าที่ที่ได้รับมอบหมายและปฏิบัติตามข้อกำหนดในแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในส่วนงานที่เกี่ยวเนื่อง

๑๑. ให้มีคณะกรรมการประสานงานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่ออำนวยการและประสานการดำเนินงานเมื่อเกิดภัยพิบัติในภาวะวิกฤต

๑๒. ให้มีคณะทำงานตอบสนองต่อภัยพิบัติด้านสารสนเทศ เพื่อจัดทำแผนสร้างความต่อเนื่องและสนับสนุนการกู้คืนระบบสารสนเทศให้กลับสู่ภาวะปกติ

๑๓. สำหรับในภารกิจที่ไม่ปรากฏผู้รับผิดชอบและหน้าที่ไว้เป็นการเฉพาะและมีเหตุต้องจัดการกับภารกิจนั้น ให้แต่งตั้งคณะทำงานเฉพาะขึ้นมาเพื่อดำเนินการแทน

๑๔. ให้ศูนย์/ สำนัก/ กลุ่มชี้นตรงผู้บริหาร/ สำนักงานสถิติจังหวัด นำแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศไปใช้ในการปฏิบัติงานประจำ

หมวดที่ ๓
การบริหารจัดการทรัพย์สินสารสนเทศ

วัตถุประสงค์

เพื่อจัดการทรัพย์สินสารสนเทศของสำนักงานสถิติแห่งชาติ ประกอบด้วย ระบบเครือข่าย คอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบความมั่นคงปลอดภัย ระบบงานคอมพิวเตอร์ เอกสาร ข้อมูลสารสนเทศ และทรัพย์สินอื่นๆ ให้มีความพร้อมต่อการใช้ในการปฏิบัติงานและการให้บริการ

แนวทางปฏิบัติ

๑. ให้จัดทำระเบียบการใช้งานทรัพย์สินสารสนเทศอย่างเป็นลายลักษณ์อักษรและประกาศให้ผู้ใช้งานได้รับทราบถึงวิธีการใช้งานที่ถูกต้อง ข้อห้าม และบทลงโทษหากมีการฝ่าฝืนหรือละเมิดการใช้งาน

๒. ให้จัดทำทะเบียนสินทรัพย์และปรับปรุงข้อมูลให้เป็นปัจจุบันอยู่เสมอทุกปี โดยต้องมีข้อมูลดังนี้

๑) หมายเลขครุภัณฑ์
๒) ประเภทครุภัณฑ์
๓) ผู้ครอบครองหรือผู้ดูแล
๔) สถานที่ใช้งาน
๕) ระดับความสำคัญ
๖) มูลค่าการจัดหา
๗) วิธีการเก็บรักษา
๘) การควบคุมการใช้งาน

๓. ให้จัดการสินทรัพย์ เครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล ระบบความมั่นคงปลอดภัย ระบบงานคอมพิวเตอร์ ตามข้อกำหนดดังต่อไปนี้

๑) ให้ทำข้อตกลงการใช้ทรัพย์สินสารสนเทศก่อนการใช้งานให้เป็นไปตามระเบียบการใช้งานทรัพย์สินสารสนเทศ

๒) ให้ทำระบบการยืม/คืน ทรัพย์สินสารสนเทศที่สำคัญในการปฏิบัติงานภายนอกเพื่อตรวจสอบและป้องกันความเสียหาย

๓) ให้มีการควบคุมการเคลื่อนย้ายสินทรัพย์ที่ต้องนำออกไปภายนอกและการนำทรัพย์สินจากภายนอกเข้ามาใช้งานภายในองค์กร

๔. ให้จัดการสินทรัพย์ ซอฟต์แวร์ โปรแกรมประยุกต์ ระบบสารสนเทศ ตามข้อกำหนดดังต่อไปนี้

๑) จำแนกหมวดหมู่ของระบบสารสนเทศออกเป็น สารสนเทศเพื่อการบริหารจัดการองค์กร สารสนเทศเพื่อการผลิตข้อมูล สารสนเทศเพื่อการบริการข้อมูลและสารสนเทศสถิติ และสารสนเทศเพื่อการจัดการระบบสถิติ

๒) จำแนกทะเบียนโปรแกรมประยุกต์ตามหมวดหมู่ของระบบสารสนเทศและมีข้อมูลดังต่อไปนี้

(๑) ผู้ใช้งาน
(๒) เจ้าของระบบ
(๓) ผู้ดูแลระบบ
(๔) ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล
(๕) ระดับชั้นการเข้าถึง
(๖) เวลาที่ได้เข้าถึง
(๗) ช่องทางการเข้าถึง

๓) จำแนกทะเบียนซอฟต์แวร์และมีข้อมูลดังต่อไปนี้

(๑) ผู้ใช้งาน
(๒) สถานที่เก็บ
(๓) การใช้งาน
(๔) การอ้างอิงสิทธิ์การใช้งาน

๕. ให้จัดการทรัพย์สิน ข้อมูลและสารสนเทศสถิติ ในรูปข้อมูลอิเล็กทรอนิกส์ ข้อมูลคอมพิวเตอร์ ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการจัดทำทะเบียนข้อมูลและเอกสารที่สำคัญที่ต้องมีชั้นความลับในการควบคุมและกำหนดใช้วิธีการจัดการและควบคุม ให้เป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

๒) ให้มีการจำแนกทะเบียนเอกสารที่สำคัญดังต่อไปนี้

(๑) เปิดเผยต่อสาธารณะ เฉพาะสมาชิก หรือเฉพาะกลุ่ม
(๒) ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล
(๓) ระดับชั้นการเข้าถึง
(๔) เวลาที่ได้เข้าถึง
(๕) ช่องทางการเข้าถึง

๓) ให้มีการจำแนกทะเบียนข้อมูลดังต่อไปนี้

(๑) ประเภทของข้อมูล แบ่งเป็น ข้อมูลดิบ ข้อมูลระดับย่อย และข้อมูลเฉพาะบุคคล

(๒) ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

(๓) ระดับชั้นการเข้าถึง

(๔) เวลาที่ได้เข้าถึง

(๕) ช่องทางการเข้าถึง

๖. ให้บันทึกความเสียหายจากการใช้งานทรัพย์สินสารสนเทศลงในแบบบันทึกโดยมีข้อมูลดังต่อไปนี้

๑) วัน/เวลา

๒) หมายเลขครุภัณฑ์

๓) ความเสียหายที่เกิดขึ้น

๔) สาเหตุ

๕) ผลกระทบ

๗. ให้มีการจัดการการเข้าถึงตามระดับชั้นความลับดังต่อไปนี้

๑) ให้มีการลงทะเบียนผู้ใช้งานเพื่อควบคุมสิทธิ มีการจำกัดข้อมูลที่สำคัญ และฟังก์ชั่นของระบบได้แก่ สิทธิที่สามารถแก้ไขข้อมูล สิทธิการลบข้อมูล สิทธิการอ่านข้อมูลทั้งหมด สิทธิการส่งออกข้อมูล และสิทธิการอ่านข้อมูลเฉพาะสคมก์ เป็นต้น

๒) ให้กำหนดรหัสผู้ใช้และรหัสผ่าน และมอบสิทธิการใช้ระบบงานตามลำดับชั้นของข้อมูล โดยมีการควบคุมด้วยเมนูเพื่อควบคุมการเข้าถึงข้อมูลและฟังก์ชั่นต่างๆ ของระบบงานที่สอดคล้องกับนโยบายการควบคุมการเข้าถึง

๓) กำหนดช่องทางการเข้าถึงข้อมูลที่มีชั้นความลับปานกลางในระบบอินทราเน็ตที่เป็นระบบปิดภายในตลอด ๒๔ ชั่วโมง สำหรับผู้ใช้งานภายใน

๔) กำหนดช่องทางการเข้าถึงข้อมูลที่มีชั้นความลับปานกลางในระบบเชื่อมโยงสื่อสารข้อมูลหน่วยงานภาครัฐตลอด ๒๔ ชั่วโมง สำหรับสำนักงานสถิติจังหวัด

๕) กำหนดช่องทางการเข้าถึงข้อมูลที่ไม่มีชั้นความลับผ่านระบบอินเตอร์เน็ตได้ตลอด ๒๔ ชั่วโมง สำหรับผู้ใช้ทั่วไปและผู้ใช้แบบสมาชิก

๖) ใช้ระบบการเข้ารหัสข้อมูลที่มีความสำคัญหรือมีชั้นความลับในระบบงานที่เป็นความลับ

หมวดที่ ๔
การสร้างความมั่นคงปลอดภัยด้านบุคลากร

วัตถุประสงค์

เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดจากบุคลากรเป็นสำคัญ โดยให้มีการแจ้งระเบียบการใช้งานทรัพย์สินสารสนเทศก่อนทำหน้าที่และการให้ความรู้และตระหนักถึงภัยร้ายเพื่อไม่ตกเป็นผู้กระทำความผิดสร้างความเสียหายให้เกิดกับองค์กรและผู้อื่นโดยขาดความระมัดระวัง รวมทั้งการยกเลิกสิทธิและเรียกคืนสินทรัพย์ที่ใช้งานในหน้าที่กลับคืนเมื่อพ้นหน้าที่ความรับผิดชอบ

แนวทางปฏิบัติ

๑. ให้มีการชี้แจงความรับผิดชอบ และการอบรมให้กับเจ้าหน้าที่ที่เข้าใหม่ของสำนักงานสถิติแห่งชาติ ให้สามารถใช้งานทรัพย์สินสารสนเทศได้อย่างปลอดภัย และรับทราบระเบียบการใช้งานทรัพย์สินสารสนเทศ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ให้มีการชี้แจงการรักษาความลับข้อมูลเฉพาะบุคคลหรือเฉพาะราย พระราชบัญญัติสถิติ พ.ศ. ๒๕๕๐ มิให้ถูกเปิดเผยไม่ว่าด้วยวิธีการใดก็ตามให้กับเจ้าหน้าที่ที่เข้าใหม่ได้รับทราบ

๓. ให้มีการอบรมให้กับเจ้าหน้าที่ประจำให้มีองค์ความรู้และความตระหนักในด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างต่อเนื่องเป็นประจำอย่างสม่ำเสมอ เพื่อมิให้ตกเป็นผู้กระทำความผิดตามกฎหมายหรือละเมิดระเบียบที่สำนักงานสถิติแห่งชาติประกาศใช้งาน

๔. ให้มีการทบทวนสิทธิของผู้ใช้ระบบสารสนเทศเป็นประจำทุกปีดังต่อไปนี้

๑) ยกเลิกสิทธิของผู้ใช้งานระบบสารสนเทศ หรือบริการพื้นฐาน เช่น การใช้งานจดหมายอิเล็กทรอนิกส์ การใช้งานอินเตอร์เน็ต ตามรายชื่อที่กลุ่มการเจ้าหน้าที่แจ้งเมื่อมีการลาออกหรือพ้นหน้าที่ความรับผิดชอบ

๒) เรียกคืนทรัพย์สินสารสนเทศ สำหรับบุคคลที่ไม่มีสิทธิการใช้งาน เช่น เครื่องคอมพิวเตอร์ บัตรประจำตัว เป็นต้น

หมวดที่ ๕
การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

วัตถุประสงค์

เพื่อควบคุมความปลอดภัยด้านกายภาพและสิ่งแวดล้อมซึ่งอาจเกิดความเสียหายต่อทรัพย์สินสารสนเทศที่สำคัญ ในบริเวณที่มีทรัพย์สินสารสนเทศติดตั้งใช้งานอยู่ เช่น ศูนย์คอมพิวเตอร์ ห้องฝึกอบรม โต๊ะทำงาน เพื่อป้องกันการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

แนวทางปฏิบัติ

๑. ให้ตรวจสอบและเฝ้าระวังศูนย์คอมพิวเตอร์ หรือ ห้องคอมพิวเตอร์ดังต่อไปนี้

๑) ให้จัดทำประกาศรักษาความมั่นคงปลอดภัยที่เป็นพื้นที่ควบคุมในการเข้าถึงและเฝ้าระวังศูนย์คอมพิวเตอร์

๒) ให้จัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ไว้ในศูนย์คอมพิวเตอร์หรือในพื้นที่ที่มีการป้องกันหรือควบคุมเพียงพอ และต้องกำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์แต่เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ เจ้าหน้าที่ดูแลระบบ ทั้งนี้ให้รวมถึงโครงสร้างพื้นฐานที่ใช้ในงานนั้นๆ ด้วย เช่น ระบบไฟฟ้า ระบบไฟฟ้าสำรอง ระบบปรับอากาศ ระบบระบายอากาศ ระบบเครือข่าย ระบบดับเพลิง เป็นต้น

๓) ให้มีระบบเก็บบันทึกการเข้าออกห้องคอมพิวเตอร์แม่ข่ายหรือพื้นที่เฝ้าระวังจากบุคคลภายนอก โดยในบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก

๔) ให้มีการตรวจสอบสภาพความสมบูรณ์ของระบบสายไฟฟ้าและอุปกรณ์ให้มีสภาพพร้อมใช้งานและไม่เป็นอันตรายต่อการเกิดเพลิงไหม้

๕) ให้ติดตั้งอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา

๖) ให้มีถังดับเพลิงเพื่อใช้สำหรับดับเพลิงในเบื้องต้น และต้องมีการตรวจสอบ อย่างสม่ำเสมอ

๒. ให้ตรวจสอบและเฝ้าระวังการใช้งานผู้เข้าร่วมประชุมจากภายนอกที่นำเครื่องคอมพิวเตอร์เชื่อมต่อกับระบบเครือข่ายภายในองค์กรทั้งในแบบใช้สายและไร้สาย ตามข้อกำหนดดังต่อไปนี้

๑) เครื่องคอมพิวเตอร์ที่ใช้ต้องมีโปรแกรมป้องกันไวรัสคอมพิวเตอร์และทันสมัย

๒) ไม่มีการติดตั้งโปรแกรมตรวจจับรหัสผ่านหรือโปรแกรมประสงค์ร้าย

๓. ให้ตรวจสอบและเฝ้าระวังเครื่องคอมพิวเตอร์ในห้องอบรม ตามข้อกำหนดดังต่อไปนี้

๑) เครื่องคอมพิวเตอร์ต้องมีโปรแกรมป้องกันไวรัสคอมพิวเตอร์และทันสมัย

๒) ให้บันทึกความเสียหายที่เกิดขึ้นจากการใช้งานของผู้อบรม

๓) ให้จัดทำประกาศการใช้เครื่องคอมพิวเตอร์หรือซอฟต์แวร์สำหรับบุคคลภายนอกที่เข้ารับการฝึกอบรมในหลักสูตรต่างๆ

๔. ให้ตรวจสอบและเฝ้าระวังเครื่องคอมพิวเตอร์ในห้องบริการข้อมูล ตามข้อกำหนดดังต่อไปนี้

๑) เครื่องคอมพิวเตอร์ต้องมีโปรแกรมป้องกันไวรัสคอมพิวเตอร์และทันสมัย

๒) ให้บันทึกความเสียหายที่เกิดขึ้นจากการใช้บริการของผู้ใช้

๓) ให้มีการควบคุมสื่อเก็บข้อมูลภายนอกที่นำมาเชื่อมต่อกับเครื่องคอมพิวเตอร์

๔) ให้จัดทำประกาศการใช้เครื่องคอมพิวเตอร์หรือซอฟต์แวร์สำหรับบุคคลภายนอกที่เข้าใช้บริการข้อมูลและสารสนเทศ

๕. ให้ตรวจสอบและเฝ้าระวังพื้นที่ต้องห้าม ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการควบคุมการเข้าถึงบุคคลภายนอกเข้าภายในด้วยระบบควบคุมและติดตั้งกล้องวงจรปิดในจุดที่สำคัญ

๒) ให้มีการตรวจสอบการทำงานของอุปกรณ์ในระบบกล้องวงจรปิดสามารถทำงานได้เป็นปกติ และสามารถบันทึกภาพได้ตลอดเวลา

หมวดที่ ๖
การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบงานคอมพิวเตอร์

วัตถุประสงค์

เพื่อเป็นการวางแผนและการจัดการระบบสื่อสารและระบบคอมพิวเตอร์แม่ข่าย ลูกข่าย ให้สามารถใช้งานได้ตลอดเวลาลดความเสี่ยงของความล้มเหลวของระบบ

แนวทางปฏิบัติ

๑. ให้มีการวิเคราะห์และวางแผนเพื่อรองรับปริมาณการใช้งาน ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการวางแผนและการจัดการระบบสื่อสารและระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วงให้สามารถรองรับปริมาณการใช้งาน การเก็บข้อมูล และการให้บริการของผู้ใช้

๒) ให้มีการวิเคราะห์สถาปัตยกรรมการเชื่อมต่อที่สอดคล้องกับโปรแกรมประยุกต์และผู้ใช้งานปลายทางเพื่อกำหนดเส้นทางการส่งผ่านข้อมูลที่มีประสิทธิภาพและปลอดภัย

๒. ให้มีขั้นตอนการปฏิบัติงานการจัดการระบบเครือข่ายและระบบคอมพิวเตอร์ ตามข้อกำหนดดังต่อไปนี้

๑) ให้ผู้รับผิดชอบในการจัดการระบบเครือข่ายและระบบคอมพิวเตอร์ ดำเนินการตามข้อกำหนดดังต่อไปนี้

(๑) ให้ผู้ดูแลระบบเครือข่ายและระบบคอมพิวเตอร์จัดทำคู่มือการจัดการระบบเครือข่าย

(๒) ให้ผู้ดูแลระบบเครือข่ายและระบบคอมพิวเตอร์ดำเนินการตรวจสอบระบบเครือข่ายเป็นประจำ

(๓) ให้ผู้ดูแลระบบเครือข่ายและระบบคอมพิวเตอร์ใช้มาตรฐานการบริหารงานไอที (ITIL) ในการปฏิบัติงานดูแลระบบงานคอมพิวเตอร์ประจำวัน

๒) ให้ผู้รับผิดชอบในการให้บริการช่องสื่อสาร กำหนดระดับคุณภาพของการให้บริการ ตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีข้อกำหนดเกณฑ์คุณภาพการให้บริการ (SLA) จากผู้ให้บริการ

(๒) ให้จัดทำข้อตกลงระหว่างผู้ให้บริการระบบสื่อสารข้อมูลให้มีการจัดการช่องสัญญาณด้วยวิธีการแบบปลอดภัย และ ให้มีการจัดทำรายงานปริมาณการใช้งานช่องสัญญาณเป็นรายเดือน

๓. ให้จัดการความปลอดภัยบนระบบเครือข่าย ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการควบคุมการเชื่อมต่ออุปกรณ์เข้ากับระบบเครือข่ายทั้งแบบใช้สายและไร้สาย

๒) ให้เก็บข้อมูลและรายละเอียดข้อกำหนดของการเชื่อมต่อและสำรองข้อมูลไว้ และมีแผนการกู้คืนหากระบบเครือข่ายไม่สามารถใช้งานได้

๓) ให้ตรวจสอบสแกนช่องโหว่ของระบบเครือข่าย เครื่องคอมพิวเตอร์ อุปกรณ์ความมั่นคงโปรแกรมประยุกต์ ระบบฐานข้อมูล เป็นประจำทุกปี และให้มีการปรับแก้ให้อยู่ในระดับที่ปลอดภัย

๔) ให้ติดตั้งอุปกรณ์ป้องกันการโจมตีจากระบบเครือข่าย ประกอบด้วย อุปกรณ์ป้องกันการโจมตีและตรวจจับผู้บุกรุกบนเครือข่าย (IPS/IDS) อุปกรณ์ควบคุมบริการบนเครือข่าย (Firewall) อุปกรณ์ควบคุมบริการ (Security Gateway) และระบบป้องกันไวรัสคอมพิวเตอร์ โดยคำนึงถึงความจำเป็นและความสามารถในการจัดการระบบ

๕) ให้จัดการอุปกรณ์ป้องกันการโจมตีและตรวจจับผู้บุกรุกบนเครือข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ให้ตรวจสอบฐานข้อมูลการตรวจจับเป็นประจำสม่ำเสมอ

(๒) ให้เฝ้าติดตามสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดจากการตรวจจับเป็นประจำทุกวัน

๖) ให้จัดการอุปกรณ์ควบคุมบริการบนเครือข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ตรวจสอบกฎของการควบคุม (Firewall Policy) เป็นไปตามการจัดการระบบที่ดี

(๒) ควบคุมบริการเฉพาะที่กำหนดเพื่อป้องกันการใช้บริการที่ไม่อนุญาตใช้งาน ที่เป็นอันตรายต่อระบบเครือข่าย

(๓) การปรับเปลี่ยนกฎของการควบคุมต้องไม่ทำให้ระบบความมั่นคงปลอดภัยขององค์กรลดลงหรือมีความเสี่ยงต่อการสูญเสียบริการ

๗) ให้จัดการอุปกรณ์ควบคุมบริการ (Security Gateway) ตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีระบบเฝ้าติดตามการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Gateway) เพื่อกำจัด Spam Mail และติดตามสถานการณ์โจมตีของระบบจดหมายอิเล็กทรอนิกส์

(๒) ให้มีระบบเฝ้าติดตามการใช้งานอินเทอร์เน็ต ตามข้อกำหนดดังต่อไปนี้

(๒.๑) ติดตั้งระบบเฝ้าติดตามการแพร่ระบาดไวรัสบนอินเทอร์เน็ต (Web Gateway) เพื่อติดตามสถานการณ์การภัยร้ายของไวรัสบนอินเทอร์เน็ต

(๒.๒) ติดตั้งระบบกรองเว็บที่เป็นอันตราย (URL Filtering) เพื่อควบคุมการเข้าถึงข้อมูลที่ไม่เหมาะสมและป้องกันการใช้โปรโตคอลที่สร้างความเสียหายต่อระบบเครือข่ายและ มีเนื้อหาไม่เหมาะสมและเป็นอันตรายต่อองค์กร

(๒.๓) ตรวจสอบและติดตามพฤติกรรมการใช้งานที่ละเมิดต่อระเบียบการใช้งานทรัพย์สินสารสนเทศของสำนักงานสถิติแห่งชาติ

๘) ให้จัดเก็บข้อมูลเพื่อการตรวจสอบระบบเครือข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ตั้งเวลาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ด้านความมั่นคงทุกเครื่อง โดยอิงกับเวลามาตรฐานกลางของโลก

(๒) จัดเก็บข้อมูลจราจรระบบเครือข่ายและโปรแกรมประยุกต์ที่ให้บริการ เพื่อการวิเคราะห์และตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยและเป็นไปตามกฎหมายที่กำหนด

๔. ให้มีการจัดการระบบงานคอมพิวเตอร์ ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการจัดการระบบคอมพิวเตอร์แม่ข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีการตรวจสอบสภาพของตัวเครื่องและอุปกรณ์เป็นประจำวัน

(๒) ให้มีการตรวจสอบสภาพของระบบสนับสนุนห้องศูนย์คอมพิวเตอร์เป็นประจำวัน

(๓) ให้มีการเฝ้าติดตามการให้บริการเป็นประจำวัน

(๔) ให้มีการตรวจสอบค้นหาช่องโหว่ของระบบปฏิบัติการเป็นประจำเพื่อให้เท่าทันในภัยร้ายที่เกิดขึ้นบนระบบเครือข่าย

(๕) ให้มีการจัดการโปรแกรมประยุกต์ที่ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่าย ตามข้อกำหนด ดังต่อไปนี้

(๕.๑) โปรแกรมประยุกต์บนเว็บที่ให้บริการบนระบบเครือข่ายอินเทอร์เน็ตต้องมีการตรวจสอบและให้เป็นไปตามมาตรฐาน OWASP หรือมาตรฐานสากลอื่นๆ

(๕.๒) โปรแกรมประยุกต์ที่ใช้งานบนเว็บต้องใช้พอร์ตมาตรฐาน HTTP (๘๐) และ HTTPS (๔๔๓) เท่านั้น

(๕.๓) ให้มีการควบคุมช่วงอายุการใช้งาน (Session) และ ช่วงเวลาในการเข้าถึงเพื่อป้องกันภัยร้ายจากโปรแกรม

๒) ให้มีการจัดการระบบคอมพิวเตอร์ลูกข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ให้จัดทำข้อกำหนดการติดตั้งโปรแกรมและข้อกำหนดการเชื่อมต่อ ที่ส่งผลเสียต่อระบบเครือข่ายขององค์กร

(๒) ให้มีการควบคุมโปรแกรมการติดตั้งของลูกข่ายเฉพาะที่ใช้ในการปฏิบัติงานและไม่ใช้เพื่อเป็นเครื่องให้บริการต่อผู้ใช้

๓) ให้มีการจัดการระบบป้องกันไวรัสเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) ตรวจสอบความทันสมัยของฐานข้อมูลไวรัสคอมพิวเตอร์เป็นประจำสม่ำเสมอ

(๒) ติดตามเครื่องคอมพิวเตอร์ที่ขาดการปรับปรุงฐานข้อมูลไวรัสคอมพิวเตอร์ให้ทันสมัย

(๓) ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัสคอมพิวเตอร์ให้มีการทำงานเป็นปกติ

(๔) รายงานการติดไวรัสคอมพิวเตอร์ของเครื่องคอมพิวเตอร์ลูกข่าย พร้อมทั้งรายละเอียดข้อมูลของไวรัสคอมพิวเตอร์ที่แพร่กระจายในองค์กร

หมวดที่ ๗
การควบคุมการเข้าถึงทรัพย์สินสารสนเทศ

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงทรัพย์สินสารสนเทศขององค์กรให้กับผู้มีสิทธิใช้งานให้เป็นไปตามหน้าที่ความรับผิดชอบ เพื่อป้องกันความเสียหายที่เกิดขึ้นจากการใช้งานโดยขาดการควบคุม จนอาจสร้างความเสียหายต่อระบบสารสนเทศขององค์กรหรือกระทบต่อการปฏิบัติงานประจำวัน

แนวทางปฏิบัติ

๑. ให้มีการควบคุมการเข้าถึงทรัพย์สินสารสนเทศของผู้ใช้เป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้มีแนวปฏิบัติในการควบคุมการเข้าถึงระบบคอมพิวเตอร์ การเข้าถึงระบบปฏิบัติการ การเข้าถึงระบบเครือข่าย การเข้าถึงคอมพิวเตอร์ลูกข่าย การเข้าถึงระบบสารสนเทศ การเข้าถึงโปรแกรมประยุกต์ การเข้าถึงระบบฐานข้อมูล การเข้าถึงไฟล์ข้อมูล และการเข้าถึงเอกสารและสื่อเก็บข้อมูล

๒) ให้มีการจัดทำทะเบียนควบคุมทรัพย์สินสารสนเทศที่สำคัญขององค์กร และมีการตรวจสอบสภาพและการมีอยู่ของทรัพย์สินสารสนเทศเหล่านั้นเป็นประจำทุกปี

๓) ให้มีการลงทะเบียนผู้ใช้งานภายในและผู้ใช้งานภายนอกแบบสมาชิกก่อนการใช้งานระบบสารสนเทศ

๒. ให้มีการจัดการสิทธิของผู้ใช้งานเป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการลงทะเบียนผู้ใช้งานเป็นไปตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีการลงทะเบียน โดยผู้ใช้งานต้องลงทะเบียนตามแบบที่ผู้จัดการระบบกำหนด และมีการลงนามรับทราบในเงื่อนไขพร้อมให้ผู้บังคับบัญชาลงนามรับรองการใช้งาน

(๒) ในแบบลงทะเบียนผู้ใช้งานต้องประกอบด้วยข้อมูลดังต่อไปนี้เป็นอย่างน้อย

(๒.๑) ชื่อ/นามสกุล
(๒.๒) หมายเลขบัตรประชาชนหรือบัตรทางราชการ
(๒.๓) สังกัด
(๒.๔) เบอร์ติดต่อ
(๒.๕) กลุ่มผู้ใช้ (ข้าราชการ สมาชิก ทั่วไป)
(๒.๖) บริการที่ขอใช้งาน
(๒.๗) วันหมดอายุ
(๒.๘) เงื่อนไขข้อกำหนดการใช้งาน
(๒.๙) ผู้รับรอง

(๓) ให้แจ้งรหัสผ่านผู้ใช้งานโดยวิธีการรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึกไม่สามารถมองเห็นได้

๒) ให้มีการจัดการทะเบียนผู้ใช้งานให้เป็นไปตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีทะเบียนคุมผู้ใช้งานเพื่อใช้ในการตรวจสอบการใช้งานในภายหลังต้องประกอบด้วยข้อมูลดังต่อไปนี้เป็นอย่างน้อย
(๑.๑) ชื่อ/นามสกุล
(๑.๒) หมายเลขบัตรประชาชนหรือบัตรทางราชการ
(๑.๓) สังกัด
(๑.๔) เบอร์ติดต่อ
(๑.๕) รหัสผู้ใช้
(๑.๖) รหัสผ่าน
(๑.๗) สิทธิการใช้งาน
(๑.๘) วันหมดอายุ

(๒) ให้จัดเก็บทะเบียนผู้ใช้งานอย่างปลอดภัยโดยมีการเข้ารหัสไฟล์และเป็นเอกสารที่เป็นความลับห้ามเปิดเผยต่อบุคคลภายนอกหรือบุคคลที่ไม่เกี่ยวข้อง

(๓) ให้ใช้วิธีการจัดการสิทธิการเข้าถึงเป็นไปตามข้อกำหนดดังต่อไปนี้
(๓.๑) ใช้การควบคุมแบบกลุ่ม (Group-Based) และหน้าที่ (Role-Based) สำหรับควบคุมการเข้าถึงระบบสารสนเทศ
(๓.๒) ใช้การควบคุมแบบรายบุคคล (Identity-Based) ควบคุมการเข้าถึงระบบเครือข่าย ระบบปฏิบัติการ และโปรแกรมประยุกต์
(๓.๓) ให้มีการมอบสิทธิการใช้งานให้กับผู้ใช้งานเป็นรายบุคคล เป็นความลับและป้องกันการปฏิเสธความรับผิดชอบของผู้ใช้งานได้

๓) ให้มีการทบทวนสิทธิการใช้งานผู้ใช้งานเป็นประจำทุกปีเป็นไปตามข้อกำหนดดังต่อไปนี้

(๑) ให้หน่วยงานการเจ้าหน้าที่ หรือผู้บังคับบัญชาแจ้งหากผู้ใช้งานลาออก
(๒) ทบทวนสิทธิประจำปีการเข้าถึงทรัพย์สินสารสนเทศของผู้ใช้งานใน ๙ หมวดข้างต้น
(๓) ให้ยกเลิกสิทธิการใช้งานออกจากระบบทะเบียนและในระบบหากพบเงื่อนไขของผู้ใช้งานดังนี้
(๓.๑) ไม่มีการใช้งานเกิน ๖ เดือน
(๓.๒) ไม่สามารถติดต่อยืนยันการใช้งานจากผู้ใช้งานโดยตรงนั้นได้ในระยะเวลา ๓ เดือน

๓. ให้มีการพิสูจน์ตัวตนผู้ใช้งานเป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้ใช้โปรแกรมสร้างรหัสผ่านที่เข้มแข็งโดยต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (มีการผสมผสานกันระหว่างตัวอักษร ตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

๒) ให้มีการพิสูจน์ตัวตนผู้ใช้งานด้วยรหัสผู้ใช้และรหัสผ่านเป็นอย่างน้อย และต้องเป็นแบบปลอดภัยโดยต้องเข้ารหัสข้อมูล

๓) ให้ใช้โปรโตคอลที่ปลอดภัยในกระบวนการพิสูจน์ตัวตนของผู้ใช้ในการใช้งาน

๔) ให้มีฐานข้อมูลกลาง (LDAP) ที่เก็บข้อมูลผู้ใช้และรหัสผ่านโดยมีการเข้ารหัสให้ปลอดภัย

๕) ให้จัดทำข้อตกลงเพื่อป้องกันการปฏิเสธความรับผิดชอบหากเกิดความเสียหายจากการใช้งาน

๔. ให้มีการควบคุมการป้องกันทรัพย์สินสารสนเทศในระหว่างที่ไม่ได้ใช้งานเป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้ตั้งค่าข้อกำหนดการปิดหน้าจอและล็อคหน้าจอด้วยรหัสผ่านเครื่องคอมพิวเตอร์ หากระบบไม่ได้รับการโต้ตอบจากผู้ใช้งานภายในเวลา ๑๕ นาที

๒) ให้ตั้งค่าข้อกำหนดการปิดการเชื่อมต่อเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย อุปกรณ์ความมั่นคงปลอดภัย หากผู้ใช้งานขาดการโต้ตอบจากระบบภายในเวลา ๑๕ นาที

๓) ให้ตั้งค่ายุติการใช้งานโปรแกรมประยุกต์ หากผู้ใช้ว่างเว้นการใช้ภายในเวลา ๑๕ นาที

๕. ให้มีการควบคุมการเข้าถึงระบบคอมพิวเตอร์ในศูนย์คอมพิวเตอร์ เป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการควบคุมการเข้าถึงศูนย์คอมพิวเตอร์ โดยจัดทำประกาศความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์

๒) ให้มีการควบคุมการเข้าถึงตัวเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย อุปกรณ์ความมั่นคงปลอดภัย ผ่านแบบบันทึกขอแก้ไขและต้องได้รับอนุมัติจากผู้ที่ได้รับมอบอำนาจ

๖. ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย เป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้จัดทำทะเบียนรายชื่อโปรแกรมที่ยินยอมให้ติดตั้งใช้งานบนเครื่องคอมพิวเตอร์ลูกข่าย และให้มีการตรวจสอบการละเมิดการใช้โปรแกรมนอกเหนือจากที่กำหนด

๒) ให้กำหนดเฉพาะเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบปฏิบัติการและให้ใช้โปรโตคอลที่มีการเข้ารหัสในการเข้าถึง

๓) ให้ทำทะเบียนคุมรายชื่อผู้ใช้ระบบปฏิบัติการและจำแนกสิทธิการใช้งานตามหน้าที่ของผู้ใช้งาน

๔) ให้มีการตรวจสอบและประเมินบัญชีผู้ใช้เครื่องคอมพิวเตอร์แม่ข่ายเป็นประจำทุกปี

๕) ให้มีการปรับปรุงช่องโหว่ของระบบปฏิบัติการให้มีความเข้มแข็งอย่างต่อเนื่อง

๖) ให้ผู้ดูแลระบบเครื่องคอมพิวเตอร์เก็บรักษารหัสผ่านไว้เป็นความลับและให้เปลี่ยนรหัสผ่านใหม่ในทุกๆ ๒ เดือนและเป็นรหัสผ่านที่มีความเข้มแข็ง

๗) ให้มีการควบคุมการติดตั้งโปรแกรมอรรถประโยชน์ลงบนเครื่องคอมพิวเตอร์แม่ข่ายที่อาจทำให้ระบบเกิดช่องโหว่ในการเข้าถึงตามกระบวนการบริหารจัดการเปลี่ยนแปลง และให้มี

ระบบการป้องกันโหลดไฟล์จากอินเทอร์เน็ตที่อาจทำความเสียหายต่อระบบความมั่นคงจากภายนอกด้วยโปรแกรมตรวจกรอง (Web Filtering)

๘) ให้มีการควบคุมระยะเวลาการใช้งานระบบปฏิบัติการเพื่อป้องกันการใช้งานจากผู้ประสงค์ร้าย

๙) ให้กำหนดสภาพแวดล้อมของระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) กำหนดเวลาของเครื่องให้เป็นมาตรฐานสากลเพื่อการตรวจสอบเหตุการณ์ด้านความมั่นคง

(๒) มีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์และตรวจสอบความทันสมัยของฐานข้อมูลไวรัสคอมพิวเตอร์

๗. ให้มีการควบคุมการเข้าถึงระบบเครือข่าย ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการควบคุมอุปกรณ์เครือข่าย ตามข้อกำหนดดังนี้

(๓) อุปกรณ์เครือข่ายต้องติดตั้งอยู่ในตู้และมีการลงทะเบียนหมายเลขไอพี (IP Address) ของอุปกรณ์

(๒) มีการควบคุมการเปิดปิดพอร์ตของเครือข่ายที่ไม่ได้ใช้งานเพื่อป้องกันการนำอุปกรณ์เครือข่ายจากภายนอกมาเชื่อมต่อเพื่อกระจายสัญญาณ

(๓) มีการกำหนดหมายเลขไอพีของเครือข่ายออกเป็นกลุ่ม (VLAN) แยกจากกันเพื่อควบคุมสิทธิการใช้งาน

(๔) ไม่อนุญาตทำการเข้าถึงจากระยะไกลผ่านระบบเครือข่ายสำหรับอุปกรณ์ที่สำคัญ

๒) ให้มีการควบคุมการเข้าถึงเครือข่ายแบบสายสัญญาณภายใน ตามข้อกำหนดดังนี้

(๓) ให้ลงทะเบียนเครื่องคอมพิวเตอร์ลูกข่าย และอุปกรณ์ทกพาในการใช้งานระบบเครือข่าย และตรวจสอบเครื่องคอมพิวเตอร์ลูกข่าย และอุปกรณ์ทกพาที่เข้าเชื่อมต่อระบบเครือข่ายเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัย

(๒) ให้ผู้ดูแลระบบเครือข่ายจัดทำทะเบียนพอร์ตการใช้งานและรายละเอียดของอุปกรณ์เครือข่ายและโครงสร้างการเชื่อมต่อของระบบเครือข่าย

(๓) ให้มีการติดตามตรวจสอบเครื่องคอมพิวเตอร์ลูกข่าย มีการตั้งค่าข้อกำหนดเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัย ปีละ ๑ ครั้ง

(๔) ให้มีการควบคุมการใช้งานในระดับพอร์ต (Port Security) เป็นอย่างน้อย

(๕) ให้จัดการระบบเครือข่ายออกเป็นโซนหรือ Segment ดังนี้

(๕.๓) ให้แบ่งแยกเครือข่ายภายในและเครือข่ายภายนอกออกจากกันด้วยอุปกรณ์ Firewall

(๕.๒) ให้แบ่งแยกเครือข่ายออกเป็น ๕ โซน ดังนี้

(๕.๒.๓) Internet Zone เป็นเครือข่ายการเข้าถึงสำหรับสารสนเทศบริการผู้ใช้ทางอินเทอร์เน็ต

(๕.๒.๒) Core Stat Zone เป็นเครือข่ายสำหรับสารสนเทศระบบประมวลผลข้อมูล และเข้าถึงเฉพาะผู้มีสิทธิเฉพาะเท่านั้น

(๕.๒.๓) GIN Zone เป็นเครือข่ายสำหรับระบบสารสนเทศสนับสนุนสำนักงานสถิติจังหวัด และเข้าถึงเฉพาะผู้มีสิทธิเฉพาะเท่านั้น

(๕.๒.๔) MIS Zone เป็นเครือข่ายสำหรับระบบสารสนเทศเพื่อการบริหารและจัดการในองค์กร และเข้าถึงเฉพาะผู้มีสิทธิเฉพาะเท่านั้น

(๕.๒.๕) Infra Zone เป็นเครือข่ายสำหรับการจัดการระบบไอที และเข้าถึงเฉพาะผู้มีสิทธิเฉพาะเท่านั้น

๓) การเข้าถึงเครือข่ายแบบไร้สาย ตามข้อกำหนด ดังนี้

(๑) ให้มีการลงทะเบียนเครื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์พกพาในการใช้งานระบบเครือข่ายไร้สาย และตรวจสอบเครื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์พกพาที่เข้าเชื่อมต่อระบบเครือข่ายเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัย

(๒) ให้มีระบบการพิสูจน์ตัวตนด้วยชื่อผู้ใช้และรหัสผ่านโดยวิธีที่ปลอดภัยของผู้ใช้งานเพื่อป้องกันการปฏิเสธความรับผิดชอบ

(๓) ให้มีการแบ่งกลุ่มผู้ใช้เครือข่ายไร้สายออกเป็นแบบเกสท์ (Guest) และบุคลากร (Employee)

๔) การเข้าถึงอุปกรณ์จากระบบเครือข่ายระยะไกล ตามข้อกำหนด ดังนี้

(๑) ให้ใช้ช่องทางเชื่อมต่อเสมือนและเข้ารหัส (VPN SSL) ในการเข้าถึงทรัพย์สินสารสนเทศภายในเมื่ออยู่ภายนอกสำนักงานสถิติแห่งชาติ

(๒) ให้กำหนดสิทธิการเข้าถึงระบบสารสนเทศตามความจำเป็นในหน้าที่และความรับผิดชอบในการทำงาน

(๓) ให้มีระบบการพิสูจน์ตัวตนด้วยชื่อผู้ใช้และรหัสผ่านโดยวิธีที่ปลอดภัยของผู้ใช้งานเพื่อป้องกันการปฏิเสธความรับผิดชอบ

๕) การเข้าถึงเครือข่ายอินเทอร์เน็ต ตามข้อกำหนดดังต่อไปนี้

(๑) ให้มีการลงทะเบียนการใช้บริการเครือข่ายอินเทอร์เน็ต และจดหมายอิเล็กทรอนิกส์ก่อนการใช้งาน และแนบคำแนะนำการใช้งานอย่างปลอดภัยให้ผู้ใช้งานได้รับทราบไปพร้อมกัน

(๒) ให้มีการพิสูจน์ตัวตนด้วยชื่อผู้ใช้และรหัสผ่านโดยวิธีที่ปลอดภัยของผู้ใช้งาน เพื่อป้องกันการปฏิเสธความรับผิดชอบ

(๓) ให้มีการจัดทำรายงานพฤติกรรมการใช้งานให้ผู้บริหารขององค์กรได้รับทราบอย่างสม่ำเสมอ

๖) ให้มีวิธีการแบบปลอดภัยในการแลกเปลี่ยนข้อมูลระหว่างเครือข่าย ตามข้อกำหนดดังต่อไปนี้

(๑) การโอนไฟล์ข้อมูลระหว่างเครื่องต้องใช้โปรโตคอลที่สามารถเข้ารหัสก่อนส่งผ่านข้อมูล

(๒) การแลกเปลี่ยนข้อมูลบริการแบบเว็บเซอร์วิส (Web Service) โปรโตคอลที่ใช้ในการส่งผ่านข้อมูลระหว่างระบบแบบอัตโนมัตินั้น ต้องมีการเข้ารหัสก่อนส่งผ่านข้อมูล เช่น XML Encryption

๘. ให้มีการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์ลูกข่าย ตามข้อกำหนดดังต่อไปนี้

๑) ให้ตั้งรหัสผู้ใช้และรหัสผ่านก่อนการเข้าใช้งานเครื่องคอมพิวเตอร์ลูกข่าย

๒) ให้ตั้งการควบคุมหน้าจอด้วยรหัสผู้ใช้และรหัสผ่านก่อนการเข้าใช้งานหลังจากมีการหยุดใช้งานไปแล้ว ๕ นาที

๓) ให้มีการควบคุมการแชร์ไฟล์ข้อมูลบนระบบเครือข่ายอย่างปลอดภัย

๔) ให้มีการควบคุมการตั้งค่าและการเปลี่ยนแปลงข้อกำหนดของเครื่องคอมพิวเตอร์ลูกข่าย

๕) ให้มีการควบคุมการติดตั้งโปรแกรมบนเครื่องคอมพิวเตอร์ลูกข่าย

๖) ให้มีการปิดช่องโหว่ระบบปฏิบัติการของเครื่องคอมพิวเตอร์เมื่อตรวจพบ

๙. ให้มีการควบคุมการเข้าถึงระบบสารสนเทศ ตามข้อกำหนดดังต่อไปนี้

๑) ให้จัดทำทะเบียนระบบสารสนเทศขององค์กร และปรับปรุงให้ทันสมัยเป็นประจำทุกปี

๒) ให้มีการควบคุมการเข้าถึงระบบสารสนเทศที่เป็นภารกิจหลักและมีผลต่อองค์กรโดยตรงที่ใช้งานภายใน ประกอบด้วย ระบบบันทึกข้อมูล ระบบประมวลผลข้อมูล เฉพาะผู้ที่รับผิดชอบเท่านั้น และให้มีการควบคุมทางกายภาพของระบบ และไม่อนุญาตใช้งานผ่านระบบเครือข่ายระยะไกล

๓) ให้ผู้จัดการระบบสารสนเทศกำหนดสิทธิของผู้ใช้งานโปรแกรมประยุกต์ตามบทบาทและหน้าที่ของผู้ใช้

๔) ให้ผู้จัดการระบบสารสนเทศตรวจสอบสิทธิของผู้ใช้งานในระบบงานเป็นประจำสม่ำเสมอ

๑๐. ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์ ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการลงทะเบียนโปรแกรมประยุกต์และตรวจสอบความครบถ้วนในแบบลงทะเบียนโปรแกรมประยุกต์

๒) ให้มีการควบคุมโปรแกรมประยุกต์ที่มีความสำคัญหรือมีความเสี่ยงสูงไว้ในองค์ประกอบที่มั่นคงปลอดภัย โดยแบ่งแยกด้วยอุปกรณ์ไฟร์วอล (Firewall) และจำกัดการเข้าถึงเฉพาะกลุ่มผู้ใช้ที่มีสิทธิเท่านั้น

๓) ให้มีการควบคุมระยะเวลาการเชื่อมต่อการใช้งานของโปรแกรมประยุกต์ที่มีความเสี่ยงและความสำคัญสูงโดยไม่ให้มีการเชื่อมต่อค้างเป็นเวลาเกิน ๔ ชม.

๔) ให้จำแนกโปรแกรมประยุกต์ที่ให้บริการผู้ใช้ภายนอก และโปรแกรมประยุกต์ที่ใช้งานภายในองค์กร

๕) ให้มีการเก็บรายละเอียดการเข้าใช้งานของผู้ใช้เพื่อใช้ในการตรวจสอบการใช้งานประจำปี

๑๑. ให้มีการควบคุมระบบฐานข้อมูล ตามข้อกำหนดดังต่อไปนี้

๑) ให้ผู้จัดการฐานข้อมูลกำหนดสิทธิและจัดทำทะเบียนผู้ใช้งานฐานข้อมูลและปรับปรุงให้ทันสมัย

๒) ให้ตรวจสอบช่องโหว่ของระบบฐานข้อมูลและดำเนินการปรับปรุงเป็นประจำสม่ำเสมอ

๓) ให้มีระบบการตรวจสอบการเข้าถึงระบบฐานข้อมูลที่มีความสำคัญต่อการปฏิบัติงาน เพื่อการอ้างอิงในภายหลัง โดยต้องมีรายละเอียดเกี่ยวกับรหัสผู้ใช้และวันเวลาที่เข้าถึง

๔) ห้ามใช้ชื่อผู้ใช้ที่สิทธิสูงสุด (DBA) ของระบบฐานข้อมูลใช้ในการเชื่อมต่อในโปรแกรมประยุกต์

๕) ให้มีการควบคุมไฟล์ที่กำหนดข้อมูลการเชื่อมต่อระบบฐานข้อมูลของโปรแกรมประยุกต์

๓๒. ให้มีการควบคุมไฟล์ข้อมูล ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการควบคุมการเข้าถึงไฟล์ข้อมูลที่ได้จากกระบวนงานที่มีสถานะเป็นไฟล์ข้อมูลดิบ ไฟล์ข้อมูลระดับย่อย และไฟล์ข้อมูลเฉพาะบุคคล เฉพาะผู้ที่ได้รับอนุญาตให้เข้าถึงเท่านั้น และให้มีการเข้ารหัสไฟล์ข้อมูลหากมีความจำเป็น รวมทั้งควบคุมการแก้ไขไฟล์ข้อมูลให้ดำเนินการตามข้อกำหนดที่ประกาศขึ้นใช้งาน

๒) ให้มีการควบคุมไฟล์ข้อมูลที่มีเนื้อหาและมีระดับชั้นความลับควบคุมให้ดำเนินการตามข้อกำหนดที่ประกาศขึ้นใช้งาน

๓๓. ให้มีการควบคุมการเข้าถึงเอกสารและสื่อเก็บข้อมูล ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการควบคุมเอกสารการปฏิบัติราชการ ดังนี้

(๑) เอกสารการปฏิบัติราชการของสำนักงานสถิติแห่งชาติ ให้ปฏิบัติตามระเบียบการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

(๒) เอกสารที่ปฏิบัติงานในการจัดการระบบไอซีที ประกอบด้วย เอกสารรหัสผ่าน เอกสารเชิงระบบที่มีหมายเลขไอพีปรากฏ เอกสารข้อกำหนดของระบบ ห้ามนำไปเปิดเผยต่อบุคคลภายนอก หรือวางบนโต๊ะทำงานโดยไม่มีการจัดเก็บให้ปลอดภัย และหากเป็นไฟล์ให้มีการเข้ารหัสป้องกัน

(๓) คู่มือหรือเอกสารที่ใช้ในการปฏิบัติงานและมีเนื้อหาสำคัญและหากถูกเปิดเผยอาจทำความเสียหายต่อระบบสารสนเทศได้ให้มีข้อกำกับการนำไปใช้อย่างชัดเจน

๒) ให้มีการควบคุมสื่อเก็บข้อมูลภายนอกที่สามารถนำมาเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์ที่มีไฟล์ข้อมูลเฉพาะบุคคล

๓๔. ให้มีการควบคุมระบบที่ไวต่อการรบกวน ตามข้อกำหนดดังต่อไปนี้

๑) ระบบที่มีความไวต่อการถูกรบกวนที่ต้องควบคุมประกอบด้วย

(๑) ระบบบันทึกข้อมูลผ่านเว็บ

(๒) ระบบบริการข้อมูลระดับย่อย

(๓) ระบบแลกเปลี่ยนข้อมูล

๒) การกำหนดบริเวณที่ต้องมีการรักษาความปลอดภัย

(๑) กำหนดและจำแนกพื้นที่ใช้งานสารสนเทศตามสิทธิการเข้าถึงโดยแยกพื้นที่ออกเป็นห้องที่สามารถควบคุมการเข้าออกได้ เช่น ห้องคอมพิวเตอร์ เป็นต้น

(๒) กำหนดให้มีผู้รับผิดชอบในการควบคุมบริเวณที่ต้องมีการรักษาความปลอดภัย

๓) การควบคุมการเข้าออกสถานที่และการเข้าออกห้องคอมพิวเตอร์

(๑) ให้มีระบบวงจรปิดเพื่อตรวจสอบหากเกิดปัญหา

(๒) ให้มีระบบตรวจสอบลายนิ้วมือการเข้าถึงห้องคอมพิวเตอร์

(๓) ให้จัดทำประกาศเพื่อควบคุมพื้นที่และข้อปฏิบัติการใช้ห้อง

(๔) ผู้ที่อยู่ในข่ายของการควบคุมประกอบด้วย ผู้ดูแลศูนย์คอมพิวเตอร์โดยตรง ผู้จัดการระบบ ผู้สนับสนุนจากภายนอก และบุคคลภายนอกที่ใช้พื้นที่

(๕) ให้มีการตรวจสอบการเข้าออกเป็นประจำทุกเดือน

๔) การกำหนดระดับการควบคุมเครื่องคอมพิวเตอร์แม่ข่าย

(๑) ควบคุมในระดับสูงสุด ประกอบด้วยเครื่องคอมพิวเตอร์แม่ข่ายให้บริการฐานข้อมูลและฐานข้อมูลทะเบียนกลาง (LDAP)

(๒) ควบคุมในระดับสูง ประกอบด้วยเครื่องคอมพิวเตอร์แม่ข่ายให้บริการโปรแกรมประยุกต์ และ Middle Ware

(๓) ควบคุมในระดับปานกลาง ประกอบด้วยเครื่องคอมพิวเตอร์แม่ข่ายให้บริการเว็บ

๕) การกำหนดระดับการควบคุมระบบคอมพิวเตอร์เครือข่าย

(๑) ควบคุมในระดับสูงสุด ประกอบด้วยระบบเครือข่ายแบบไร้สาย

(๒) ควบคุมในระดับสูง ประกอบด้วยระบบเครือข่ายภายในห้ามมีการเชื่อมต่อไปใช้ยังสถานที่อื่นที่ไม่ใช่พื้นที่ของหน่วยงาน

๖) การควบคุมการเข้าใช้งานระบบจากภายนอก

(๑) ควบคุมพอร์ตการเข้าถึงเฉพาะพอร์ตที่ใช้งานเท่านั้น

(๒) ควบคุมการเข้าถึงแบบ Remote Access เฉพาะเครื่องคอมพิวเตอร์ลูกข่ายที่ถูกกำหนดสิทธิการเข้าถึงเท่านั้น

๗) การพิสูจน์ตัวตนจากภายนอก

(๑) กำหนดรหัสผู้ใช้และรหัสผ่านเพื่อเข้าระบบงานและให้มีการพิสูจน์ตัวตนของผู้ใช้ข้อมูลในแต่ละระบบและแต่ละชั้นความลับ

(๒) กำหนดช่องทางการเข้าถึงเฉพาะวิธีการแบบปลอดภัยด้วยระบบ Virtual Private Network

หมวดที่ ๘
การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์

วัตถุประสงค์

เพื่อให้มีแผนการจัดการหากเกิดสถานการณ์อันไม่พึงประสงค์และไม่คาดคิดกับระบบสารสนเทศ เช่น ภัยจากการโจมตีบนระบบเครือข่ายอินเทอร์เน็ต หรือภัยจากเพลิงไหม้ ภัยจากธรรมชาติ หรือภัยอื่นๆ ให้ระงับได้อย่างรวดเร็ว เพื่อให้เกิดผลกระทบต่อระบบสารสนเทศของสำนักงานสถิติแห่งชาติให้น้อยที่สุด

แนวทางปฏิบัติ

๑. ให้มีการวิเคราะห์ กำหนด และทบทวนเหตุการณ์ที่เป็นภัยคุกคามต่อทรัพย์สินสารสนเทศที่สำคัญ ซึ่งนำไปสู่ความเสียหายต่อระบบสารสนเทศ จนส่งผลกระทบต่อการดำเนินงานตามภารกิจขององค์กร โดยให้จัดทำแผนการจัดการเหตุการณ์ภัยที่ไม่พึงประสงค์เป็นไปตามลำดับความสำคัญและความน่าจะเป็นที่จะเกิดขึ้น

๒. ในจัดทำแผนจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ โดยต้องมีองค์ประกอบตามข้อกำหนดดังต่อไปนี้

๑) มีแผนการป้องกัน

(๑) การวิเคราะห์การเกิดของสถานการณ์

(๒) การกำหนดผู้รับผิดชอบต่อสถานการณ์

(๓) การประเมินความเสียหายทรัพย์สินสารสนเทศ

(๔) การกำหนดเครื่องมือในการดำเนินการ

(๕) การให้ความรู้และการฝึกซ้อม

(๖) การเตรียมการรับมือเหตุการณ์

(๗) สถานที่ปฏิบัติงาน

๒) มีแผนการตรวจจับและเฝ้าระวัง

(๑) ให้มีกระบวนการตรวจจับและเฝ้าระวัง

(๒) กำหนดแบบฟอร์มที่ใช้จัดเก็บข้อมูล

(๓) จัดเก็บข้อมูลเหตุการณ์ที่เกิดขึ้นลงในแบบฟอร์ม

(๔) มีแผนการป้องกัน

๓) มีแผนการเผชิญเหตุ

(๑) เครื่องมือในการปฏิบัติงาน

(๒) การติดต่อสื่อสาร

(๓) ขั้นตอนการปฏิบัติตามระดับความรุนแรงของเหตุการณ์

๔) มีแผนการสอบสวนและเก็บหลักฐาน

(๑) การดำเนินคดีตามกฎหมาย

(๒) การเก็บหลักฐานเพื่อการสอบสวน

๕) มีแผนการกู้คืนเพื่อกลับสู่สภาพเดิม

(๑) เครื่องมือการกู้คืนระบบ

(๒) ผู้รับผิดชอบในการกู้คืน

๓. ให้มีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะผิดปกติผ่านระบบเครือข่าย และรายงานจุดอ่อน ช่องโหว่ที่ตรวจพบโดยเร่งด่วน โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ

๑) ความพยายามในการบุกรุกผ่านระบบเครือข่าย

๒) การใช้งานในลักษณะผิดปกติ

๓) การใช้งานที่มีการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๔. ให้มีการซ้อมแผนและฝึกอบรมเผชิญเหตุสำหรับแผนป้องกันไฟไหม้เป็นประจำทุกปีหรือในความถี่ที่เหมาะสม และนำมาปรับปรุงการดำเนินงานอย่างต่อเนื่อง

หมวดที่ ๙
การบริหารจัดการด้านการบริการเพื่อให้มีความต่อเนื่อง

วัตถุประสงค์

เพื่อเป็นการเตรียมความพร้อมหากทรัพย์สินสารสนเทศขององค์กรได้รับความเสียหายจากสถานการณ์อันไม่พึงประสงค์จนทำให้ระบบสารสนเทศและข้อมูลเสียหายหรือหยุดงานไม่สามารถให้บริการได้ จึงต้องมีความพร้อมในการทำให้ระบบกลับมาใช้งานได้เช่นเดิม

แนวทางปฏิบัติ

๑. ให้จัดทำแผนสร้างความต่อเนื่องของการดำเนินงาน (Business Continuity Plan) โดยต้องมีองค์ประกอบตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการวิเคราะห์ผลกระทบของระบบสารสนเทศต่อภารกิจขององค์กร (Business Impact Analysis)

๒) ให้มีการระบุถึงเหตุการณ์ที่ต้องนำแผนฉุกเฉินมาใช้งาน

๓) ให้มีการกำหนดสถานการณ์ หรือลำดับความรุนแรงของปัญหา

๔) ให้มีการวิเคราะห์ทางเลือกใช้ศูนย์สำรองข้อมูล และสถานที่สำหรับใช้เป็นศูนย์สำรอง

๕) ให้มีการกำหนดหน้าที่ที่รับผิดชอบและผู้มีอำนาจในการตัดสินใจ รวมทั้งกำหนดช่องทางการติดต่อเมื่อมีเหตุการณ์เกิดขึ้น

๖) ให้กำหนดวิธีปฏิบัติโดยละเอียดเมื่อมีเหตุการณ์เกิดขึ้น

๗) ให้กำหนดวิธีปฏิบัติเพื่อโยกย้ายกิจกรรมไปยังสถานที่ชั่วคราว

๘) ให้กำหนดวิธีปฏิบัติภายหลังจากการโยกย้ายเพื่อกลับมาดำเนินการตามปกติ

๙) ให้มีการให้ความรู้และสร้างความตระหนักแก่บุคลากรที่เกี่ยวข้องกับแผนฉุกเฉิน

๑๐) ให้มีการทดสอบและปรับปรุงแผนต่อเนื่องปีละ ๑ ครั้ง เพื่อให้เป็นปัจจุบันอยู่เสมอ และเก็บแผนฉุกเฉินไว้นอกสถานที่

๒. ให้มีระบบสำรองเป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้กำหนดวิธีปฏิบัติ หรือขั้นตอนในการสำรองข้อมูลให้ชัดเจน เช่น ข้อมูลที่จะสำรอง ความถี่ในการสำรองข้อมูล สื่อที่ใช้ สถานที่เก็บ วิธีการเก็บรักษา และการนำมาใช้งาน

๒) ให้จัดทำนโยบาย ขั้นตอน หรือวิธีปฏิบัติในการสำรองข้อมูลโดยต้องมีองค์ประกอบตามข้อกำหนดดังต่อไปนี้

(๑) ข้อมูลที่ต้องสำรอง

(๒) ความถี่ในการสำรอง

(๓) ประเภทสื่อบันทึก (Media)

(๔) จำนวนที่ต้องสำรอง (Copy)

(๕) ขั้นตอนและวิธีการสำรองโดยละเอียด

(๖) สถานที่และวิธีการเก็บรักษาสื่อสำรองให้ปลอดภัย

(๗) การเฝ้าติดตามตรวจสอบผลการสำรองข้อมูล

๓) ให้มีการบันทึกการปฏิบัติงาน (Log Book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าว พร้อมทั้งรายงานอย่างสม่ำเสมอ

(๑) ให้มีการติดฉลากที่มีรายละเอียดเกี่ยวกับข้อมูลในสื่อบันทึกไว้บนสื่อบันทึกข้อมูลสำรองไว้ให้ชัดเจน เพื่อให้สามารถค้นหาข้อมูลได้โดยเร็วและเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

(๒) ให้จัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่จัดเก็บดังกล่าวต้องให้มีระบบควบคุมการเข้าออก และระบบป้องกันความเสียหายของข้อมูลด้วย

(๓) ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ควรคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย อาทิ การเก็บอุปกรณ์และซอฟต์แวร์ ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกไว้

๓. ให้มีระบบทดสอบการกู้คืนข้อมูล เป็นไปตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการจัดเตรียมเครื่องคอมพิวเตอร์แม่ข่ายเพื่อใช้ในการทดสอบการกู้คืนข้อมูลที่สำคัญ

๒) ให้ทดสอบการกู้คืนข้อมูลที่สำรองอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าข้อมูลรวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้ ตลอดจนขั้นตอนและวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน

หมวดที่ ๑๐
การจัดหา การพัฒนา และการบำรุงรักษา

วัตถุประสงค์

เพื่อให้ระบบสารสนเทศที่พัฒนาขึ้นมาใหม่รวมทั้งที่มีอยู่มีความปลอดภัยเพียงพอสำหรับการใช้งานจริงป้องกันการสูญเสียการใช้งานตลอดเวลา จากการเปลี่ยนแปลงแก้ไขซอฟต์แวร์และโปรแกรมประยุกต์ ด้วยมาตรการและวิธีการควบคุม เริ่มจากการจัดหา การพัฒนาโปรแกรมประยุกต์ การติดตั้งระบบ การควบคุมการเปลี่ยนแปลง และการบำรุงรักษา

แนวทางปฏิบัติ

๑. ให้มีการควบคุมการติดตั้งระบบคอมพิวเตอร์และระบบสารสนเทศ ตามข้อกำหนดดังต่อไปนี้
   ๑) ให้มีการลงทะเบียนระบบสารสนเทศและโปรแกรมประยุกต์
   ๒) ให้มีการตรวจสอบช่องโหว่ของโปรแกรมประยุกต์หลังการติดตั้งใช้งานเพื่อป้องกันผลกระทบกับบริการที่เปิดใช้

๒. ให้มีข้อกำหนดด้านความมั่นคงปลอดภัยด้านสารสนเทศอยู่ในการจัดทำข้อกำหนดคุณสมบัติของการพัฒนาโปรแกรมประยุกต์ เป็นไปตามข้อกำหนดดังต่อไปนี้
   ๑) ให้ใช้วิธีการปลอดภัยในการพัฒนาชุดคำสั่งตามมาตรฐาน OWASP หรือมาตรฐาน CWE TOP ๒๕ ที่มีกระบวนการควบคุมการนำเข้าข้อมูล การแสดงผล การควบคุมการประมวลผล เป็นอย่างน้อย
   ๒) ให้ใช้วิธีการทางวิศวกรรมซอฟต์แวร์ในการพัฒนาโปรแกรม เช่น มาตรฐาน ISO/IEC ๒๔๗๑๐

๓. ให้มีข้อกำหนดการเปลี่ยนแปลงแก้ไขระบบสารสนเทศของผู้ให้บริการเป็นไปตามข้อกำหนดดังต่อไปนี้
   ๑) ให้มีการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศ ที่ใช้งานตามแบบคำขอให้แก้ไข ต้องมาจากผู้ที่มีสิทธิและต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ ต้องมีการเก็บรายละเอียดของคำขอไว้ตรวจสอบ
   ๒) ให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ต้องมีการควบคุมหรือตรวจสอบผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้
   ๓) ให้ผู้ให้บริการใช้เครื่องคอมพิวเตอร์ลูกข่ายเฉพาะที่อนุญาตเท่านั้นเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายเพื่อแก้ไขซอฟต์แวร์

๔. ให้มีการควบคุมงานบริการจากผู้ให้บริการภายนอก ตามข้อกำหนดดังต่อไปนี้

๑) ให้กำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการที่มีคุณภาพ มีขั้นตอนการปฏิบัติงานที่ดี

๒) ให้มีระบุความคาดหวังของการให้บริการ (SLA) สำหรับผู้ให้บริการ

๓) ให้ทำข้อตกลงการรักษาความลับของข้อมูลและขอบเขตงาน และเงื่อนไขในการให้บริการอย่างชัดเจน

๔) ให้มีเกณฑ์ในการตรวจรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือทรัพยากรสารสนเทศอื่นๆ รวมทั้งต้องทดสอบก่อนที่จะตรวจรับระบบนั้นด้วย

๕) ให้ผู้ให้บริการจัดทำรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางการแก้ไข

๕. ให้มีการบำรุงรักษาระบบและเฝ้าติดตามคุณภาพการใช้งาน ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการบำรุงรักษาระบบสนับสนุนห้องศูนย์คอมพิวเตอร์ ประกอบด้วย ระบบสำรองไฟฟ้า ระบบดับเพลิง ระบบตรวจจับควันไฟ ระบบปรับอากาศ ระบบตรวจจับการรั่วซึมของน้ำ ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง อุปกรณ์เครือข่าย และระบบความมั่นคงปลอดภัย อย่างต่อเนื่องเป็นประจำทุกปี

๒) ให้ผู้ดูแลระบบทำการปรับปรุงคู่มือการจัดการระบบ คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องให้มีความถูกต้องและทันสมัยตลอดเวลา

๓) ให้เฝ้าติดตามการใช้งานของทรัพยากรในระบบและติดตามคุณภาพการให้บริการเป็นรายระบบ และหากพบให้ปรับปรุงให้มีค่าเป็นไปตามที่กำหนดไว้

๖. ให้มีมาตรการเข้ารหัสมาใช้ในการรับ/ส่งข้อมูล ตามข้อกำหนดดังต่อไปนี้

๑) การตรวจสอบสิทธิของผู้ใช้งานในหน้าเว็บ

๒) โปรแกรมประยุกต์และบริการบนเครือข่ายอินเทอร์เน็ตที่ต้องการความปลอดภัย

๓) การโอนไฟล์ข้อมูลระหว่างเครื่องที่มีข้อมูลที่ต้องปกปิด

๗. ให้มีมาตรการควบคุมไฟล์ข้อมูลที่ถูกเปลี่ยนแปลง ตามข้อกำหนดดังต่อไปนี้

๑) ให้มีการจัดการและควบคุมสิทธิการเข้าถึงและแก้ไขไฟล์ข้อมูล

๒) ให้มีการวิเคราะห์ไฟล์ที่เปลี่ยนแปลงมีผลกระทบต่อการบริการอื่นหรือไม่

๓) ให้มีการสำรองไฟล์ข้อมูลที่จะถูกเปลี่ยนแปลงในทุกครั้งก่อนดำเนินการเปลี่ยนแปลงเพื่อใช้ในการกู้คืนในภายหลัง

๘. ให้มีการตรวจสอบช่องโหว่ (Vulnerability) ของระบบสารสนเทศเป็นประจำ ตามข้อกำหนดดังต่อไปนี้

๑) การตรวจสอบช่องโหว่ของระบบเครือข่าย ช่องโหว่ของระบบคอมพิวเตอร์แม่ข่าย และช่องโหว่ของโปรแกรมประยุกต์

๒) ให้มีการปรับแก้เพื่อปิดช่องโหว่ที่ตรวจพบและเป็นภัยที่อันตรายต่อระบบโดยเร็ว

หมวดที่ ๑๑
การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบายและข้อกำหนด

วัตถุประสงค์

เพื่อเป็นการตรวจสอบการนำนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งการใช้งานทรัพย์สินสารสนเทศของผู้ใช้งานเป็นไปตามระเบียบที่กำหนด โดยใช้กระบวนการตรวจสอบด้วย

ตนเองสำหรับผู้ปฏิบัติ การตรวจสอบจากหน่วยตรวจสอบภายในสำหรับผู้ใช้งาน และการตรวจสอบจากหน่วยตรวจสอบภายนอกในการจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

แนวทางปฏิบัติ

๑. ให้ผู้รับผิดชอบงานด้านความมั่นคงปลอดภัยด้านสารสนเทศ ประเมินตนเองเพื่อนำมาสู่การปรับปรุงกระบวนงานให้มีความสมบูรณ์สูงสุดเป็นประจำทุกปี ตามข้อกำหนดดังนี้

๑) ประเมินตนเองด้วยแบบประเมินตนเองเพื่อวิเคราะห์ช่องว่าง (Gap)

๒) ประเมินตนเองด้วยการทดสอบการเจาะระบบ (Penetration Testing)

๒. ให้ผู้รับผิดชอบงานด้านความมั่นคงปลอดภัยด้านสารสนเทศทำการประเมินตนเอง

๓. ให้หน่วยตรวจสอบภายในของสำนักงานสถิติแห่งชาติ ตรวจประเมินผู้ใช้งานมีการปฏิบัติตามระเบียบการใช้งานทรัพย์สินสารสนเทศและการนำแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศมาใช้ในการปฏิบัติงานเป็นประจำสม่ำเสมอในทุกๆ ๒ ปี

๔. ให้หน่วยตรวจสอบภายนอกตรวจประเมินระบบความมั่นคงปลอดภัยที่มีความซับซ้อนต้องใช้ความรู้ความเชี่ยวชาญเฉพาะเป็นประจำสม่ำเสมอในทุกๆ ๒ ปี

๕. ให้มีการตรวจสอบโดยหน่วยตรวจสอบภายในและหน่วยตรวจสอบภายนอกอย่างต่อเนื่องและให้นำผลการประเมินของหน่วยตรวจสอบมาใช้ในการวางแผนการปรับปรุงระบบความมั่นคงปลอดภัยด้านสารสนเทศในปีถัดไป

ประกาศสำนักงานสถิติแห่งชาติ
เรื่อง การรักษาความมั่นคงปลอดภัยศูนย์คอมพิวเตอร์

เพื่อให้ระบบสารสนเทศของสำนักงานสถิติแห่งชาติเป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถบริการได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการปฏิบัติงานที่ไม่ถูกต้อง ซึ่งอาจก่อให้เกิดความเสียหายแก่ระบบคอมพิวเตอร์และระบบสารสนเทศ

สำนักงานสถิติแห่งชาติ จึงได้จัดทำประกาศ การรักษาความมั่นคงปลอดภัยศูนย์คอมพิวเตอร์ เพื่อใช้เป็นแนวทางการปฏิบัติงานและควบคุมการเข้าถึงทรัพยากรที่สำคัญภายในศูนย์คอมพิวเตอร์สำนักงานสถิติแห่งชาติ ดังนี้

ข้อปฏิบัติของเจ้าหน้าที่สำนักงานสถิติแห่งชาติ

๑. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้กำกับระบบงานศูนย์คอมพิวเตอร์ มีอำนาจหน้าที่ ดังต่อไปนี้

๑.๑. การกำหนดสิทธิและขณสิกสิทธิ การเข้า - ออก ห้องคอมพิวเตอร์ของเจ้าหน้าที่ปฏิบัติงาน

๑.๒. อนุญาตให้บุคคลที่ไม่มีสิทธิในการเข้าศูนย์คอมพิวเตอร์แต่มีความจำเป็นต้องเข้าไปปฏิบัติงานภายในห้องคอมพิวเตอร์

๑.๓. อนุญาตให้มีการนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์อื่นเข้าหรือออกศูนย์คอมพิวเตอร์เพื่อการซ่อมบำรุง โดยบริษัทต้องบันทึกข้อมูลลงในแบบรับ/ส่งเครื่องคอมพิวเตอร์และอุปกรณ์

๒. ผู้กำกับระบบงานศูนย์คอมพิวเตอร์ หมายถึง ผู้ที่ได้รับมอบหมายอย่างเป็นทางการจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารในการควบคุมและกำกับศูนย์คอมพิวเตอร์ให้มีความมั่นคงปลอดภัย

๓. ให้ข้าราชการที่ได้รับมอบหมายปฏิบัติงานในศูนย์คอมพิวเตอร์ประจำวัน มีหน้าที่ติดตามดูแลการปฏิบัติงานของเจ้าหน้าที่บริษัทที่เข้ามาปฏิบัติงานให้ปฏิบัติตามประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยศูนย์คอมพิวเตอร์

๔. ห้องคอมพิวเตอร์ที่อยู่ภายใต้การการกำกับและควบคุมให้เป็นไปตามประกาศฉบับนี้ประกอบด้วย ห้องระบบสนับสนุนห้องคอมพิวเตอร์แม่ข่าย ห้องคอมพิวเตอร์เครือข่าย ห้องฝึกอบรม และห้องเกม

ข้อปฏิบัติของเจ้าหน้าที่บริษัทภายนอก

๑. เจ้าหน้าที่บริษัทที่เข้ามาปฏิบัติงานต้องทำการลงทะเบียนผู้มาติดต่อในแบบลงทะเบียนผู้มาติดต่อ ซึ่งประกอบด้วย วัน/เวลา ชื่อ สังกัด เหตุผลที่มาติดต่อ และชื่อผู้ติดต่อ ทุกครั้งที่มาทำงาน

๒. เจ้าหน้าที่บริษัทหรือผู้มาติดต่อต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

๒.๑. ห้ามทำการคัดลอกข้อมูลในระบบออกไปภายนอก

๒.๒. ห้ามนำวัตถุระเบิด เชื้อเพลิง วัสดุติดเพลิงง่าย อาวุธ สารเคมี แร่แม่เหล็ก หรือสิ่งอื่นใดอันอาจก่อให้เกิดความเสียหายนี้ต่อชีวิตและทรัพย์สินเข้าภายในบริเวณศูนย์คอมพิวเตอร์

๒.๓. ห้ามสูบบุหรี่ หรือกระทำการใดๆ อันอาจก่อให้เกิดควัน เพลิงหรือความเสียหายต่อชีวิตและทรัพย์สินภายในบริเวณศูนย์คอมพิวเตอร์

๒.๔. ห้ามนำอาหาร เครื่องดื่ม ของขบเคี้ยวทุกชนิดเข้าภายในศูนย์คอมพิวเตอร์

๒.๕. ห้ามเปิดประตูทางเข้าค้างไว้ในทุกกรณี

๒.๖. ห้ามใส่รองเท้าที่ไม่ได้จัดเตรียมไว้เข้าภายในห้องคอมพิวเตอร์

๒.๗. ให้คืนบัตร เข้า-ออก พร้อมลงรายมือชื่อในแบบลงทะเบียนผู้มาติดต่อ

๓. เจ้าหน้าที่บริษัทจะต้องได้รับอนุญาตจากเจ้าหน้าที่ของสำนักงานสถิติแห่งชาติ ก่อนการดำเนินงานดังต่อไปนี้

๓.๑ การปฏิบัติงานที่เกี่ยวกับระบบฐานข้อมูล หรือ ข้อมูล

๓.๒ การปฏิบัติงานที่มีผลต่อการหยุดบริการของเครื่องคอมพิวเตอร์และอุปกรณ์

๓.๓ การปฏิบัติงานที่มีผลต่อการหยุดบริการของระบบเครือข่ายอินเตอร์เน็ต

๓.๔ การปฏิบัติงานที่มีผลต่อระบบความมั่นคงปลอดภัยสารสนเทศขององค์กร

๓.๕ การปฏิบัติงานที่มีผลต่อการรั่วไหลของข้อมูล

ข้อปฏิบัติในภาวะฉุกเฉิน

๑. ในกรณีเกิดเหตุฉุกเฉินเพลิงไหม้ขึ้นภายในศูนย์คอมพิวเตอร์ให้ปฏิบัติตามแผนผังแสดงขั้นตอนการดับเพลิงห้องศูนย์คอมพิวเตอร์ ที่ปรากฏหน้าห้อง

ข้อปฏิบัติในการเก็บข้อมูลตรวจสอบ

๑. ให้มีการเก็บแบบลงทะเบียนผู้มาติดต่อเพื่อการตรวจสอบอย่างน้อย ๕๐ วัน

๒. ให้มีการบันทึกภาพเคลื่อนไหวผ่านกล้องวงจรปิด ที่มีการติดตั้งใช้งานในศูนย์คอมพิวเตอร์โดยข้อมูลที่บันทึกไว้จะต้องสามารถตรวจสอบย้อนหลังได้อย่างน้อย ๓๐ วัน

จึงประกาศมาเพื่อทราบและถือปฏิบัติอย่างเคร่งครัด

ประกาศ ณ วันที่ ๑๐ กันยายน พ.ศ. ๒๕๕๑

(นางจิราวรรณ บุณเพิ่ม)
ผู้อำนวยการสำนักงานสถิติแห่งชาติ