**คำสั่งองค์การสุรา กรมสรรพสามิต**

**ที่ 113 /2551**

**เรื่อง นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ**

**องค์การสุรา กรมสรรพสามิต**

---

เพื่อให้การดำเนินงานด้านระบบเทคโนโลยีสารสนเทศขององค์การสุราฯให้เป็นไปด้วยความมั่นคงปลอดภัยต่อเนื่องรวมถึงการเสริมสร้าง พัฒนาการบริหารจัดการป้องกันความเสียหาย หรือความสูญหายของระบบเทคโนโลยีสารสนเทศตลอดจนการรักษาข้อมูลระบบเทคโนโลยีสารสนเทศ และสนับสนุนการดำเนินกิจการขององค์กรได้อย่างมีประสิทธิภาพ ดังนี้

**<u>หมวด 1 เจ้าหน้าที่ผู้ดูแลระบบองค์การสุราฯ</u>**

**1. นโยบายการรักษาความปลอดภัยของพื้นที่ (Physical Area Security )**

1.1 แบ่งเขตของพื้นที่เพื่อกำหนดความปลอดภัยของพื้นที่ดังต่อไปนี้

- พื้นที่ติดตั้ง PC Terminal
- พื้นที่สำหรับระบบเครือข่ายข้อมูลคอมพิวเตอร์
- พื้นที่ติดตั้งระบบและจัดเก็บข้อมูล (Data Center Area)

1.2 ต้องจัดให้มีกฎระเบียบปฏิบัติควบคุมการเข้าและการออก พื้นที่ติดตั้งระบบและจัดเก็บข้อมูล

1.3 การเข้าและออกพื้นที่ปฏิบัติงาน พนักงาน องค์การสุราฯ ต้องแสดงสิทธิเข้าถึงพื้นที่ปฏิบัติงาน มีการบันทึก Log การเข้าปฏิบัติงาน สำหรับการตรวจสอบ สำหรับผู้ปฏิบัติงานชั่วคราว (Temporary Worker) ที่ไม่ใช่พนักงานองค์การสุราฯ ให้ปฏิบัติตามมาตรการรักษาความปลอดภัยของระบบ

**2. นโยบายการรักษาความปลอดภัยของระบบเครือข่าย (Network Security)**

2.1 ระบบเครือข่ายภายใน (Local Area Network)

อุปกรณ์ที่ทำหน้าที่เชื่อมโยงกับระบบเครือข่ายโดยติดตั้งใช้งานภายใน Local Area หรือเพื่อการทำงานภายในองค์การสุรา กรมสรรพสามิต ได้แก่ Router, Switching HUB กำหนดข้อปฏิบัติในการ ใช้งานดังนี้

2.1.1 อุปกรณ์ Router, Switching HUB และอุปกรณ์อื่น ๆ ที่ทำหน้าที่เป็นการขยายการ เชื่อมโยงเครือข่ายต้องปิด Service Port ที่ไม่จำเป็น และในการส่งข้อมูลการทำงานของอุปกรณ์เครือข่ายจะต้องไม่ใช้ค่า Default Community, Default Username และ Default Password เป็นต้น

2.1.2 การเชื่อมโยงเครือข่ายเพื่อใช้ระบบงานต่าง ๆ จะสามารถกระทำได้เมื่อได้รับอนุญาตจากคณะทำงานด้าน IT Security หรือผู้ดูแลเครือข่ายโดยความเห็นชอบของผู้อำนวยการองค์การสุราฯ การเชื่อมโยงเครือข่ายเองโดยพลการหากทำให้เกิดความเสียหายกับระบบเครือข่ายจะได้รับการพิจารณาโทษ

2.1.3 ต้องจัดให้มีแผนและดำเนินการบำรุงรักษาระบบเครือข่ายเพื่อให้อยู่ในสภาพที่พร้อมใช้งาน

2.1.4 ต้องจัดให้มีระบบจ่ายไฟฟ้าสำรองหรือ UPS เพื่อให้ระบบสามารถทำงานได้ต่อเนื่อง

2.1.5 IP address ภายในของระบบงานเครือข่ายภายในขององค์กร จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของห้องคอมพิวเตอร์แม่ข่ายได้โดยง่าย

2.1.6 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

2.2 ระบบ Remote Access

อุปกรณ์ Remote Access Server (RAS) ที่ติดตั้งใช้งานใน Remote Area หรือเพื่อการทำงานกับหน่วยงานภายนอก ได้แก่ Remote Access Server (RAS) กำหนดข้อปฏิบัติในการใช้งาน ดังนี้

2.2.1 อุปกรณ์ RAS จะต้องทำ Harden และบันทึกการทำ Configuration Set up ของอุปกรณ์ RAS ทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง

2.2.2 เมื่อทำการทดสอบการใช้งานอุปกรณ์ RAS แล้ว User/Password ที่ใช้งานทดสอบเมื่อเสร็จงานแล้วให้ทำการลบทิ้งทันที

2.2.3 อุปกรณ์ RAS ที่สามารถ Management ทาง Remote Terminal ได้จะต้องไม่มีค่า Default Community, Default Username และ Default Password

**3. นโยบายการรักษาความปลอดภัยของ Host (Host Security)**

3.1 การรักษาความปลอดภัยของ Server

3.1.1 ผู้ดูแลระบบต้องไม่ใช้ Default Username/Default Password

3.1.2 ต้อง Harden และบันทึกการConfiguration Set up ของอุปกรณ์ Server ทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง

3.1.3 กำหนดการใช้งาน Service Port ให้เปิด Service Port ที่จำเป็นเท่านั้น ส่วนที่ไม่ใช้งานให้ปิดทั้งหมดและต้องมีบันทึกการติดตั้ง Service Patch ทุกครั้ง

3.1.4 ต้องไม่เปิดเผย OS Version, Service Port และ Service Patch Version ให้บุคคลที่ไม่เกี่ยวข้องทราบ

3.1.5 การ Login ใช้งานที่ Console นั้นเมื่อจบการทำงานแล้วต้อง Log off User นั้นโดยทันที

3.1.6 ผู้ดูแลระบบจะต้องทำการสำรองข้อมูลและระบบปฏิบัติการอย่างน้อยทุกเดือน และทดสอบการสำรอง ข้อมูลอย่างน้อยปีละ 1 ครั้ง โดยสอดคล้องกับระดับความสำคัญของระบบ

3.2 การรักษาความปลอดภัยของ PC Terminal

3.2.1 เครื่อง PC Terminal ต้องตั้งชื่อเครื่องทุกเครื่องที่ติดต่อกับเครือข่าย

3.2.2 กำหนดการใช้งาน Protocol บน เครื่อง PC Terminal ต้องใช้ติดตั้ง Protocol เฉพาะที่ทำงานร่วมกับ Server เท่านั้น

3.2.3 การเชื่อมโยง PC Terminal กับเครือข่ายจะต้องอยู่ภายใต้มาตรฐานการเชื่อมโยงเครือข่ายที่ใช้งานร่วมกัน

3.2.4 การใช้งาน Remote Terminal Console เมื่อไม่ใช้งานแล้วจะต้อง Log off ทุกครั้ง

3.3 การรักษาความปลอดภัย Software

3.3.1 พนักงานต้องใช้คอมพิวเตอร์ซอฟต์แวร์ตามมาตรฐานที่องค์การสุราฯ กำหนด กรณีที่นำซอฟต์แวร์นอกเหนือจากมาตรฐานมาใช้ พนักงานต้องรับผิดชอบในผลเสียที่เกิดขึ้นกับองค์การสุราฯ

3.3.2 พนักงานไม่มีสิทธิ์ในการติดตั้งหรือรื้อถอนซอฟต์แวร์ที่องค์การสุราฯ ติดตั้งให้เป็นอันขาดหากกระทำโดยพลการและเกิดความเสียหายกับองค์การสุราฯต้องได้รับโทษ

**<u>หมวด 2 พนักงานเจ้าหน้าที่องค์การสุราฯ</u>**

**4. นโยบายการรักษาความปลอดภัยของข้อมูล**

4.1 การเข้าถึงข้อมูลต้องได้รับการอนุญาตจากเจ้าของข้อมูลเท่านั้น

4.2 ข้อมูลที่เป็นความลับต้องรักษาระดับความลับของข้อมูล ตรวจสอบระบบรักษาความลับของข้อมูลที่มีความสำคัญต่อการบริหารและการดำเนินการขององค์กร

4.3 ห้ามทำการสำเนา พิมพ์ข้อมูลที่เป็นความลับ ไม่ว่ากรณีใด เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูลหรือผู้อำนวยการองค์การสุรา เท่านั้น

ข้อมูลที่เป็นความลับ หมายความว่า ข้อมูลที่เกี่ยวข้องกับการดำเนินงานขององค์การสุราฯ

4.4 ต้องจัดให้มีแผนการสำรองข้อมูลเมื่อระบบถูกบุกรุกและแก้ไขข้อมูล

4.5 องค์การสุราฯ มีสิทธิที่จะตรวจสอบข้อมูล โปรแกรม หรือ เอกสารอิเล็กทรอนิกส์อื่น ๆ ที่พนักงานหรือผู้ปฏิบัติงานนำมาจัดเก็บไว้ในระบบเทคโนโลยีสารสนเทศขององค์การสุราฯ เพื่อให้สอดคล้องกับกฎหมาย ศีลธรรม และระเบียบปฏิบัติขององค์การสุราฯ หรือเพื่อการดำเนินการทางวินัยและกฎหมาย

**5. นโยบายการใช้รหัสผ่าน (Password)**

5.1 พนักงานต้องใช้ Password ที่เป็นของตนเองในการแสดงตนเข้าใช้งานหรือปฏิบัติงานในระบบข้อมูลตามสิทธิที่ได้รับเท่านั้น

5.2 พนักงานที่ได้รับ Password ในครั้งแรก ต้องเปลี่ยน Password ใหม่ให้เป็นความลับเฉพาะตัว และต้องทำการเปลี่ยน Password ใหม่ทันที หาก Password ถูกเปิดเผย

5.3 พนักงานต้องเปลี่ยน Password ทุก ๆ 90 วัน หรือตามระยะเวลาที่กำหนด และในการเปลี่ยน Password ใหม่ในแต่ละครั้งจะต้องไม่นำ Password ที่หมดอายุแล้วมาใช้ซ้ำอีก

5.4 พนักงานต้องทำการ Log out ออกจากระบบคอมพิวเตอร์ทันทีเมื่อเลิกใช้งาน หรือเมื่อไม่อยู่ที่หน้าจอคอมพิวเตอร์นานเกิน 10 นาที ให้ Screen Saver ควบคุมหน้าจอคอมพิวเตอร์ด้วย Password

5.5 หากพนักงานพบเหตุที่ก่อให้เกิดความสงสัยว่าถูกผู้อื่นนำ Password ไปใช้ให้แจ้งคณะทำงานด้าน IT Security

**6. นโยบายการใช้อินเตอร์เน็ต**

6.1 พนักงานต้องไม่ใช้อินเตอร์เน็ตในเครือข่ายขององค์การสุราฯ เพื่อหาประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเพื่อการเข้าสู่ Web Site ที่ไม่เหมาะสม เช่น Web Site ที่ขัดต่อศีลธรรมอันดี Web Site ที่มีเนื้อหาต่อต้านชาติ ศาสนา พระมหากษัตริย์ หรือ Web Site ที่เป็นภัยต่อสังคม รวมถึงลามกอนาจาร เป็นต้น

6.2 พนักงานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับองค์การสุราฯ

6.3 พนักงานมีหน้าที่ต้องรายงานต่อคณะทำงานด้าน IT Security ทันที หากพบเห็นการใช้อินเตอร์เน็ตในเครือข่ายขององค์การสุราฯ ไปในทางที่ไม่เหมาะสม หรือพบเห็นการบุกรุกหรือการละเมิดสิทธิขององค์การสุราฯ เช่น เล่นเกมส์ หรือส่งข้อมูลลูกค้าองค์การสุราฯให้บุคคลภายนอก

6.4 การเชื่อมต่อเครื่องคอมพิวเตอร์เพื่อเข้าใช้งานอินเตอร์เน็ต ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์การสุราฯ จัดสรรไว้เท่านั้น (ซึ่งจะผ่าน Proxy, Firewall, IDS เป็นต้น) ห้ามพนักงานทำการเชื่อมต่อเข้าสู่เครือข่ายอินเตอร์เน็ตโดยตรงโดยผ่านช่องทางอื่น เช่น Dial up Modem เว้นแต่ว่าจะได้รับอนุญาตเป็นกรณีพิเศษ

6.5 ให้ใช้เฉพาะเครื่อง PC Terminal ที่กำหนดให้ใช้อินเตอร์เน็ตเท่านั้น ห้ามใช้เครื่องที่เข้าสู่ระบบงานองค์การสุราฯเข้าอินเตอร์เน็ตเป็นอันขาด

6.6 การเข้าสู่ระบบงานเครือข่ายภายในองค์กร โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ ล๊อกอิน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

**7. นโยบายการรับ – ส่งจดหมายอิเล็กทรอนิกส์ (E-Mail)**

7.1 พนักงานควรระมัดระวังในการใช้ E-Mail เพื่อไม่ให้เกิดความเสียหายองค์การสุราฯ หรือละเมิดสิทธิ หรือสร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาผลประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาประโยชน์ในเชิงธุรกิจจากการใช้ E-Mail ในระบบขององค์การสุราฯ

7.2 พนักงานต้องรับผิดชอบในข้อความ รูปภาพ เสียง หรือแฟ้มข้อมูลที่ส่งออกจากเครื่องคอมพิวเตอร์ของพนักงานนั้นทั้งหมด

7.4 ก่อนที่จะ Download ไฟล์จาก E-Mail ต้องทำการ Scan Virus ก่อนทุกครั้ง

**8. นโยบายการป้องกันไวรัสคอมพิวเตอร์**

8.1 ห้ามพนักงานนำคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ หรือข้อมูลที่ไม่มั่นใจว่าติดไวรัสคอมพิวเตอร์ มาติดตั้งหรือใช้งานในองค์การสุราฯ เว้น แต่คอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์นั้นได้ผ่านการตรวจสอบจากองค์การสุราฯแล้วเท่านั้น

8.2 พนักงานควรทำการสำรองข้อมูลสำคัญที่อยู่บนเครื่องคอมพิวเตอร์ส่วนบุคคลไว้ เช่น CD-RW หรือ Flash Drive เพื่อลดปัญหาการกู้คืนสภาพข้อมูลที่ถูกทำลายโดยไวรัสคอมพิวเตอร์

8.3 ห้ามพนักงานปรับแต่ง หรือยกเลิกการทำงานของคอมพิวเตอร์ซอฟต์แวร์ ป้องกันไวรัสที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ตามที่องค์การสุราฯจัดหาให้

8.4 พนักงานควรมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้ โดยตรวจสอบว่ามีการ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอย่างสม่ำเสมอ และแจ้งให้ผู้ดูแลระบบทราบหากไม่สามารถ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

8.5 พนักงานควรแจ้งให้ผู้ดูแลระบบทราบ เมื่อพบว่าคอมพิวเตอร์หรือซอฟท์แวร์ที่ใช้มีพฤติกรรมผิดไปจากปกติ หรือเมื่อมีสงสัยว่ามีการติดไวรัสคอมพิวเตอร์

**9. นโยบายการปฏิบัติตามข้อกำหนด (Compliance)**

9.1 องค์การสุราฯ ต้องเก็บ Log file การจราจรคอมพิวเตอร์ไม่ต่ำกว่า 90 วัน

9.2 ห้ามตัดต่อภาพ ปรับเปลี่ยน แก้ไขข้อมูล บางส่วน หรือทั้งหมด ก่อนได้รับอนุญาตจากเจ้าของข้อมูลหรือกระทำกับข้อมูลอันเป็นการสร้างความเสียหายแก่ผู้อื่นโดยเด็ดขาด

ทั้งนี้ตั้งแต่วันที่ 17 กันยายน 2551 เป็นต้นไป

สั่ง ณ วันที่ 17 กันยายน 2551

(นายอิทธิเทพ วิเศษสมิต)
ผู้อำนวยการองค์การสุรา