ประกาศกรมสุขภาพจิต
เรื่อง รายชื่อผู้ผ่านการประเมินบุคคลเพื่อเลื่อนขึ้นแต่งตั้งให้ดำรงตำแหน่งประเภทวิชาการ ระดับชำนาญการ

ตามหนังสือสำนักงาน ก.พ. ที่ นร ๑๐๐๖/ว ๑๔ ลงวันที่ ๑๑ สิงหาคม ๒๕๖๔ ได้กำหนดหลักเกณฑ์และวิธีการประเมินบุคคลเพื่อเลื่อนขึ้นแต่งตั้งให้ดำรงตำแหน่งในตำแหน่งระดับควบ และมีผู้ครองตำแหน่งนั้นอยู่ โดยให้ผู้มีอำนาจสั่งบรรจุตามมาตรา ๕๗ หรือผู้ที่ได้รับมอบหมายเป็นผู้ประเมินบุคคลตามหลักเกณฑ์และวิธีการที่ อ.ก.พ. กรมสุขภาพจิต กำหนด นั้น

กรมสุขภาพจิต ได้คัดเลือกข้าราชการผู้ผ่านการประเมินบุคคลที่จะเข้ารับการประเมินผลงานเพื่อแต่งตั้งให้ดำรงตำแหน่งในระดับที่สูงขึ้น (ตำแหน่งระดับควบ) จำนวน ๒ ราย ดังรายละเอียดแนบท้ายประกาศนี้ โดยผู้ผ่านการประเมินบุคคลเพื่อเลื่อนขึ้นแต่งตั้งให้ดำรงตำแหน่งในระดับที่สูงขึ้น จะต้องจัดส่งผลงานประเมินตามจำนวนและเงื่อนไขที่คณะกรรมการประเมินผลงานกำหนด ภายใน ๖ เดือน นับแต่วันที่ประกาศรายชื่อผู้ผ่านการประเมินบุคคล หากพ้นระยะเวลาดังกล่าวแล้วผู้ผ่านการประเมินบุคคลยังไม่ส่งผลงาน จะต้องขอรับประเมินบุคคลใหม่ เว้นแต่กรณีผู้ผ่านการประเมินบุคคลจะเกษียณอายุราชการในปีงบประมาณใด ให้ส่งผลงานเข้ารับการประเมินล่วงหน้าไม่น้อยกว่า ๖ เดือน ในปีงบประมาณนั้น

ทั้งนี้ หากมีผู้ใดจะทักท้วงให้ทักท้วงได้ ภายใน ๓๐ วัน นับตั้งแต่วันประกาศรายชื่อผู้ผ่านการประเมินบุคคล การทักท้วงหากตรวจสอบแล้วมีหลักฐานว่า ข้อทักท้วงเป็นการกลั่นแกล้งหรือไม่สุจริต ให้ดำเนินการสอบสวนผู้ทักท้วง เพื่อหาข้อเท็จจริงและดำเนินการตามที่เห็นสมควรต่อไป

ประกาศ ณ วันที่ ๖ ตุลาคม พ.ศ. ๒๕๖๖

(นายจุมภฏ พรมสีดา)
รองอธิบดีกรมสุขภาพจิต
ปฏิบัติราชการแทนอธิบดีกรมสุขภาพจิต

บัญชีรายละเอียดแนบท้ายประกาศกรมสุขภาพจิต ลงวันที่ ๒ ตุลาคม ๒๕๖๖
เรื่อง รายชื่อผู้ผ่านการประเมินบุคคลเพื่อเลื่อนขึ้นแต่งตั้งให้ดำรงตำแหน่งประเภทวิชาการ ระดับชำนาญการ
ครั้งที่ ๑๐๐ /๒๕๖๖

ลำดับที่	ผู้ผ่านการประเมินบุคคล/หน่วยงาน	ตำแหน่งที่เข้ารับการประเมินผลงาน/หน่วยงาน	ชื่อผลงานที่เสนอขอประเมิน	ชื่อข้อเสนอแนวคิดเพื่อพัฒนางาน
๑.	นางสาวนาถชนก นิ่มจรรยา นักจิตวิทยาคลินิกปฏิบัติการ ตำแหน่งเลขที่ ๓๙๓๕ กลุ่มงานจิตวิทยา กลุ่มภารกิจบริการจิตเวชและสุขภาพจิต สถาบันกัลยาณ์ราชนครินทร์ กรมสุขภาพจิต	นักจิตวิทยาคลินิกชำนาญการ (ด้านจิตวิทยา) ตำแหน่งเลขที่ ๓๙๓๕ กลุ่มงานจิตวิทยา กลุ่มภารกิจบริการจิตเวชและสุขภาพจิต สถาบันกัลยาณ์ราชนครินทร์ กรมสุขภาพจิต	ผู้ป่วยนิติจิตเวชคดีลักทรัพย์ที่ถูกวินิจฉัยเป็นโรคชอบหยิบฉวย : กรณีศึกษา	การศึกษาคู่มือการประเมินความเสี่ยงความรุนแรงทางเพศ (Manual for the sexual violence risk - 20 : SVR - 20)
๒.	นายรุงโรจน์ เหมือนแปลก นักวิชาการคอมพิวเตอร์ปฏิบัติการ ตำแหน่งเลขที่ ๓๙๓๘ กลุ่มงานยุทธศาสตร์และแผนงานโครงการ กลุ่มภารกิจพัฒนาสู่ความเป็นเลิศ สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา กรมสุขภาพจิต	นักวิชาการคอมพิวเตอร์ชำนาญการ ตำแหน่งเลขที่ ๓๙๓๘ กลุ่มงานยุทธศาสตร์และแผนงานโครงการ กลุ่มภารกิจพัฒนาสู่ความเป็นเลิศ สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา กรมสุขภาพจิต	การบริหารจัดการศูนย์ข้อมูลสารสนเทศและระบบเครือข่าย สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา	การออกแบบและพัฒนาระบบเครือข่ายไร้สาย (Somdet-Wifi)

ส่วนที่ 3 แบบการเสนอผลงาน

(ผลงานที่เป็นผลการปฏิบัติงานหรือผลสำเร็จของงาน/ผลงานที่ผ่านมาไม่เกิน5หน้ากระดาษA4)

ชื่อผู้สมัครเข้ารับการประเมินบุคคล นายรุ่งโรจน์ เหมือนแปลก

◆ **ตำแหน่งที่ขอเข้ารับการประเมินบุคคล** นักวิชาการคอมพิวเตอร์ **ระดับ** ชำนาญการ
ตำแหน่งเลขที่ 3938 **กลุ่มงาน** ยุทธศาสตร์และแผนงานโครงการ
กลุ่มภารกิจ ภารกิจพัฒนาสู่ความเป็นเลิศ **หน่วยงาน** สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา
กรมสุขภาพจิต

---

1) **ชื่อผลงานเรื่อง** การบริหารจัดการศูนย์ข้อมูลสารสนเทศและระบบเครือข่าย สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา
2) **ระยะเวลาที่ดำเนินการ** กรกฎาคม - กันยายน 2565
3) **ความรู้ ความชำนาญงาน หรือความเชี่ยวชาญและประสบการณ์ที่ใช้ในการปฏิบัติงาน**

กลุ่มงานคอมพิวเตอร์ สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา มีภารกิจในการดูแล ควบคุม และบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ได้แก่ เครื่องระบบเครือข่าย (Network), คอมพิวเตอร์แม่ข่าย (Server), คอมพิวเตอร์ลูกข่าย (Computer) และอุปกรณ์สนับสนุนในห้องศูนย์ข้อมูลสารสนเทศ ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

การบริหารจัดการศูนย์ข้อมูลสารสนเทศและระบบเครือข่ายสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา จึงได้มีการนำกรอบความรู้ทางวิชาการหรือแนวความคิดมาประยุกต์ใช้ในการดำเนินงาน ประกอบด้วย

1. การควบคุมการเข้าออกศูนย์ข้อมูลสารสนเทศและการป้องกันความเสียหาย (Physical Security)
2. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)
3. การสำรองข้อมูลระบบคอมพิวเตอร์ (Backup Plan)
4. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)
5. ระบบเครือข่าย

3.1 การควบคุมการเข้าออกศูนย์ข้อมูลสารสนเทศและการป้องกันความเสียหาย (Physical Security)

วัตถุประสงค์

การควบคุมการเข้าออกศูนย์ข้อมูลสารสนเทศ มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มี อำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (Access risk) แก้ไขเปลี่ยนแปลง (Integrity risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (Availability risk) ส่วนการป้องกันความเสียหายมีวัตถุประสงค์ เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ (Availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้าออกศูนย์ข้อมูลสารสนเทศ และระบบป้องกันความเสียหายต่าง ๆ

แนวทางปฏิบัติ

1. การควบคุมศูนย์ข้อมูลสารสนเทศ

1.1 ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในศูนย์ข้อมูลสารสนเทศหรือพื้นที่หวงห้าม และมีการกำหนดสิทธิการเข้าออกห้อง ศูนย์ข้อมูลสารสนเทศให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ดูแลระบบ (System Administrator) เป็นต้น

1.2 ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออกศูนย์ข้อมูลสารสนเทศ

1.2 ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออกศูนย์ข้อมูลสารสนเทศ ในบางครั้ง ก็ต้องมีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีเจ้าหน้าที่ศูนย์ข้อมูลสารสนเทศ ควบคุมดูแล การทำงานตลอดเวลา เป็นต้น

1.3 ต้องมีระบบเก็บบันทึกการเข้าออกศูนย์ข้อมูลสารสนเทศ โดยบันทึกดังกล่าวต้องมีรายละเอียด เกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึก ดังกล่าวอย่างสม่ำเสมอ

1.4 ควรจัดศูนย์ข้อมูลสารสนเทศให้เป็นสัดส่วน เช่น แบ่งเป็นส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) เป็นต้น เพื่อสะดวก ในการปฏิบัติงานและยังทำให้ การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น นอกจากนี้ ควรแยกส่วน ที่ต้องมีการเข้าถึงโดยเจ้าหน้าที่หลายฝ่าย ออกจากศูนย์ข้อมูลสารสนเทศ เช่น ส่วนที่ใช้เก็บรายงาน ที่กลุ่มงานคอมพิวเตอร์ได้จัดพิมพ์ ให้หน่วยงานต่างๆ เป็นต้น

2. การป้องกันความเสียหาย

2.1 ระบบป้องกันอัคคีภัย

- ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือ ระงับเหตุไฟไหม้ได้ทันเวลา
- ศูนย์ข้อมูลสารสนเทศหลักต้องมีระบบดับเพลิงแบบอัตโนมัติ สำหรับศูนย์ข้อมูลสารสนเทศสำรอง อย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

2.2 ระบบป้องกันไฟฟ้าขัดข้อง

- มีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟ
- มีระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์ที่สำคัญ เพื่อให้การดำเนินงานมีความต่อเนื่อง

2.3 ระบบควบคุมอุณหภูมิและความชื้น

- มีการควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศ และตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์ เนื่องจาก ระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือ ความชื้นที่ไม่เหมาะสม

3.2 การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)

วัตถุประสงค์

การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์ มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (Access risk) หรือแก้ไขเปลี่ยนแปลง (Integrity risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง ส่วนการป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส รวมทั้ง Malicious code ต่างๆ มิให้เข้าถึง (Access risk) หรือสร้างความ เสียหาย (Availability risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย

แนวทางปฏิบัติ

1. การบริหารจัดการข้อมูล

1.1 มีการกำหนดชั้นความลับของข้อมูล ขั้นตอนปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทชั้นความลับ และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

1.2 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL การใช้ VPN เป็นต้น

1.3 ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output) ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (Distributed database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ ข้อมูลมีความถูกต้องครบถ้วนตรงกัน

1.4 มีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ เช่น ส่งซ่อม หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

2. การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege)

2.1 มีการกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ (Application system) สิทธิการใช้งานอินเตอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นในการปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

2.2 ในกรณีมีความจำเป็นต้องใช้ User ที่มีสิทธิพิเศษ ต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ในการพิจารณาว่าการควบคุม User ที่มีสิทธิพิเศษมีความรัดกุมเพียงพอหรือไม่นั้น หน่วยงานจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม

- มีการควบคุมการใช้งาน User ที่มีสิทธิพิเศษอย่างเข้มงวด เช่น กำหนดให้มีการ ควบคุมการใช้งาน user ดังกล่าวในลักษณะ dual control โดยให้เจ้าหน้าที่ 2 ราย ถือรหัสผ่านคนละครึ่ง หรือเก็บซอง password ไว้ในตู้เซฟ เป็นต้น และจำกัดการ ใช้งานเฉพาะกรณีจำเป็นเท่านั้น
- มีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการ ใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ก็ควรเปลี่ยน รหัสผ่านทุก 3 เดือน เป็นต้น

2.3 ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้ งานโดยบุคคลอื่นที่มิได้มีสิทธิและหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจาก ระบบงาน (Log out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น

2.4 ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การออกรายงาน Report เป็นต้น จะต้องเป็นการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิ ดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว แลเจ้าของข้อมูลต้องมีหลักฐานการให้สิทธิดังกล่าว และต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลา ดังกล่าว

2.5 ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่นเพื่อให้มีสิทธิใช้งานระบบคอมพิวเตอร์ในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติและต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้งบันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

3. การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

3.1 ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี user account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการ

กำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น สำนักงานจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม

- ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่ แนะนำให้มีความยาวขั้นต่ำ 8 ตัวอักษร
- ควรใช้ตัวอักษรทั้งพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลข และมีเครื่องหมายผสมกัน
- สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ 6 เดือน ส่วนผู้ใช้งานที่มีสิทธิพิเศษ เช่น ผู้บริหารระบบ (System Administrator) และผู้ใช้งาน ที่ติดมากับระบบ (Default User) เป็นต้น ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 3 เดือน
- ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย
- ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abc1234” “qwerty” “123456” เป็นต้น
- ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น
- ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม
- ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไป ไม่ควรเกิน 5 ครั้ง
- ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

3.2 ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันทีต้องมีระบบการเข้ารหัส (encryption) ไฟล์ที่เก็บ รหัสผ่านเพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง

3.3 ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิใช้งานระบบแล้ว เช่น บัญชีรายชื่อของเจ้าหน้าที่ หรือพนักงานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น Disable Password เป็นต้น ลบออกจากระบบ หรือ เปลี่ยน Password เป็นต้น

4. การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)

4.1 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติจะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานโดยทันที

4.2 ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติม

4.3 ต้องดำเนินการติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) เช่น ระบบปฏิบัติการ DBMS และ Web Server เป็นต้น อย่างสม่ำเสมอ

4.4 ควรทดสอบ System Software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา

4.5 ควรมีแนวทางปฏิบัติในการใช้งาน Software Utility เช่น Personal Firewall Password Cracker เป็นต้น และตรวจสอบการใช้งาน Software Utility อย่างสม่ำเสมอ

4.6 ควรกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของโปรแกรมระบบอย่างชัดเจน

5. การบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network)

5.1 ต้องแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่ายภายใน ส่วนเครือข่ายภายนอก ส่วน DMZ เป็นต้น

5.2 ต้องมีระบบป้องกันการบุกรุก เช่น Firewall เป็นต้น ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก

5.3 ต้องมีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่ายโดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ

- ความพยายามในการบุกรุกผ่านระบบเครือข่าย
- การใช้งานในลักษณะที่ผิดปกติ
- การใช้งาน และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจ หน้าที่เกี่ยวข้อง

5.4 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

5.5 ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบ เครือข่าย เช่น ตรวจสอบไวรัส ตรวจสอบการกำหนดค่า Parameter ต่างๆ เกี่ยวกับการรักษาความปลอดภัย เป็นต้น และต้องตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (Physicaldisconnect) และจุดเชื่อมต่อ (Disable Port) ที่ไม่มีความจำเป็นต้องเชื่อมต่อกับระบบ เครือข่าย ออกจากระบบเครือข่ายโดยสิ้นเชิง

5.6 ควรกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่าย และอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า Parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

5.7 การใช้เครื่องมือต่างๆ (Tools) เพื่อตรวจเช็คระบบเครือข่าย ควรได้รับการอนุมัติจากผู้มีอำนาจ หน้าที่ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

6. การป้องกันไวรัส และ Malicious Code

6.1 ต้องมีมาตรการป้องกันไวรัสที่มีประสิทธิภาพและปรับปรุงให้เป็นปัจจุบันอยู่เสมอสำหรับ เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น ติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น

6.2 กลุ่มงานคอมพิวเตอร์ควรจัดทำคู่มือในการป้องกันไวรัสให้แก่ผู้ใช้งานเพื่อใช้เป็นแนวทางปฏิบัติ รวมทั้งแจ้งและให้ความรู้แก่ผู้ใช้งานเกี่ยวกับไวรัสชนิดใหม่ๆ อย่างสม่ำเสมอ

6.3 ควรควบคุมมิให้ผู้ใช้งานระงับการใช้งาน (Disable) ระบบป้องกันไวรัสที่ได้ติดตั้งไว้ และ ควรแจ้งบุคคลที่เกี่ยวข้องทันทีในกรณีที่พบว่ามีไวรัส

7. บันทึกเพื่อการตรวจสอบ (Audit Logs)

7.1 ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกัน การบุกรุก เช่น บันทึกการเข้าออกระบบ (Login-Logout Logs) บันทึกการพยายามเข้าสู่ระบบ (Login Attempts) บันทึกการใช้ Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน

7.2 ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

7.3 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึก ต่างๆ ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

3.3 การสำรองข้อมูลระบบคอมพิวเตอร์ (Backup Plan)

วัตถุประสงค์

การสำรองข้อมูลระบบคอมพิวเตอร์ มีวัตถุประสงค์เพื่อให้มีข้อมูลระบบคอมพิวเตอร์ สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (Availability risk) โดยมีเนื้อหา ครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา

แนวทางปฏิบัติ

การสำรองข้อมูลระบบคอมพิวเตอร์

1. การสำรอง

1.1 ต้องสำรองข้อมูลสำคัญ รวมถึงโปรแกรมระบบปฏิบัติการ (Operating system) โปรแกรมระบบงานคอมพิวเตอร์ (Application System) และชุดคำสั่งที่ใช้ทำงาน ให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

1.2 ควรมีขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงาน โดยอย่างน้อยควรมีรายละเอียด ดังนี้

- ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
- ประเภทสื่อบันทึก (Media)
- จำนวนที่ต้องสำรอง (Copy)
- ขั้นตอนและวิธีการสำรองโดยละเอียด
- สถานที่และวิธีการเก็บรักษาสื่อบันทึก

1.3 ควรมีการบันทึกการปฏิบัติงาน (Log Book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

2. การทดสอบ

2.1 ต้องทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูลรวมทั้ง โปรแกรมระบบต่างๆ ที่ได้สำรองไว้มีความถูกต้องครบถ้วนและใช้งานได้

2.2 ควรมีขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน

3. การเก็บรักษา

3.1 ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบ ป้องกันความเสียหายตามที่กล่าวในข้อ Physical Security ด้วย

3.2 ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานานต้องคำนึงถึงวิธีการนำข้อมูล กลับมาใช้งานในอนาคตด้วย เช่น ถ้าจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการ เก็บอุปกรณ์และซอฟท์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น

3.3 ควรติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถ ค้นหาได้โดยเร็วและเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

3.4 การขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจหน้าที่ และ ควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมี รายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และเวลา

3.5 ควรมีขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึง ข้อมูลสำคัญต่างๆ ในฮาร์ดดิสก์ที่ยังค้างอยู่ใน Recycle bin

3.4 การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

วัตถุประสงค์

การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นอาจก่อให้เกิดความเสี่ยงต่อหน่วยงานในรูปแบบที่แตกต่างไปจากการดำเนินงานปกติของหน่วยงานเอง เช่น ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล (Access risk) ความเสี่ยงเกี่ยวกับความถูกต้องครบถ้วนของข้อมูลและการประมวลผลของ ระบบงาน (Integrity Risk) ที่อาจเพิ่มขึ้นจากการดำเนินงานของผู้ให้บริการ เป็นต้น ดังนั้น การควบคุมการใช้ บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นจึงมีวัตถุประสงค์เพื่อให้หน่วยงานใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการ

แนวทางปฏิบัติ

1. การคัดเลือกผู้ให้บริการ

1.1 ควรมีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ

1.2 ควรมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data Confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) อย่างชัดเจน

2. การควบคุมผู้ให้บริการ

2.1 ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้อง เข้าถึงส่วนที่ใช้งานจริง (Production Environment) ก็ต้องมีการควบคุมหรือตรวจสอบการ ให้บริการของผู้ให้บริการอย่างเข้มงวดเพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ เช่น ให้เจ้าหน้าที่บริษัทควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่หน่วยงาน (Onsite Service) และให้เจ้าหน้าที่หน่วยงานตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียด ในกรณีที่เป็นการให้บริการในลักษณะ Remote Access และปิดการเข้าถึงเครือข่ายทันทีที่การให้บริการเสร็จสิ้น เป็นต้น

2.2 ควรดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

2.3 ควรกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไข

2.4 ควรมีขั้นตอนในการตรวจรับงานของผู้ให้บริการ

3.5 ระบบเครือข่าย

ระบบเครือข่ายคอมพิวเตอร์หรือระบบเน็ตเวิร์กคือกลุ่มของคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่ถูกนำมาเชื่อมต่อกันเพื่อให้ผู้ใช้ในเครือข่ายสามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและใช้อุปกรณ์ต่างๆ ในเครือข่ายร่วมกันได้ เครือข่ายนั้นมีหลายขนาด ตั้งแต่ขนาดเล็กที่เชื่อมต่อกันด้วยคอมพิวเตอร์เพียงสองสามเครื่อง เพื่อใช้งานในบ้านหรือในบริษัทเล็กๆ ไปจนถึงเครือข่ายขนาดใหญ่ที่เชื่อมต่อกันทั่วโลก ส่วน Home Network หรือเครือข่ายภายในบ้าน ซึ่งเป็นระบบ LAN (Local Area Network) เป็นระบบเครือข่ายคอมพิวเตอร์ขนาดเล็กๆ หมายถึงการนำ

เครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกันในบ้าน สิ่งที่เกิดตามมาก็คือประโยชน์ในการใช้คอมพิวเตอร์ด้านต่างๆ ดังนี้

1. การใช้ทรัพยากรร่วมกัน หมายถึง การใช้อุปกรณ์ต่างๆ เช่น เครื่องพิมพ์ร่วมกัน กล่าวคือ มีเครื่องพิมพ์เพียงเครื่องเดียว ทุกคนในเครือข่ายสามารถใช้เครื่องพิมพ์นี้ได้ทำให้สะดวกและประหยัดค่าใช้จ่าย เพราะไม่ต้องลงทุนซื้อเครื่องพิมพ์หลายเครื่อง

2. การแชร์ไฟล์เมื่อคอมพิวเตอร์ถูกติดตั้งเป็นระบบเน็ตเวิร์กแล้ว การใช้ไฟล์ข้อมูลร่วมกันหรือการแลกเปลี่ยนไฟล์ทำได้อย่างสะดวกรวดเร็วไม่ต้องอุปกรณ์เก็บข้อมูลใดๆ ทั้งสิ้นในการโอนย้ายข้อมูลตัดปัญหาเรื่องความจุของสื่อบันทึกไปได้เลยยกเว้นอุปกรณ์ในการจัดเก็บข้อมูลหลักอย่างฮาร์ดดิสก์หากพื้นที่เต็มก็คงต้องหามาเพิ่ม

3. การติดต่อสื่อสาร โดยคอมพิวเตอร์ที่เชื่อมต่อเป็นระบบเน็ตเวิร์ก สามารถติดต่อพูดคุยกับเครื่องคอมพิวเตอร์อื่น โดยอาศัยโปรแกรมสื่อสารที่มีความสามารถใช้เป็นเครื่องคอมพิวเตอร์ได้เช่นเดียวกัน หรือการใช้อีเมล์ภายในก่อให้เครือข่าย Home Network หรือ Home Office จะเกิดประโยชน์นี้อีกมากมาย

4. การใช้อินเทอร์เน็ตร่วมกัน คอมพิวเตอร์ทุกเครื่องที่เชื่อมต่อในระบบเน็ตเวิร์ก สามารถใช้งานอินเทอร์เน็ตได้ทุกเครื่อง โดยมีโมเด็มตัวเดียวไม่ว่าจะเป็นแบบอนาล็อกหรือแบบดิจิตอลอย่าง ADSL ยอดฮิตในปัจจุบัน ระบบเครือข่ายคอมพิวเตอร์ได้กลายเป็นส่วนหนึ่งขององค์กร สถาบันการศึกษาและบ้านไปแล้วการใช้ทรัพยากรร่วมกันได้ทั้งไฟล์เครื่องพิมพ์ต้องใช้ระบบเครือข่ายเป็นพื้นฐาน ระบบเครือข่ายจะหมายถึงการนำคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไปมาเชื่อมต่อกันเพื่อจะทำการแชร์ข้อมูล และทรัพยากรร่วมกันเช่นไฟล์ข้อมูลและเครื่องพิมพ์

1. ประเภทของระบบเครือข่ายตามขนาด

ระบบเครือข่ายสามารถแบ่งตามขนาดได้เป็น 3 ประเภท ดังนี้

1.1 LAN (Local Area Network)

ซึ่งแปลได้ว่า "ระบบเครือข่ายขนาดเล็ก" ที่ต้องประกอบด้วย Server และ Client โดยจะต้องมีคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไป ซึ่งจะทำหน้าที่เป็นผู้ให้บริการและผู้ใช้โดยที่ผู้ให้บริการซึ่งเป็น Server นั้นจะเป็นผู้ควบคุมระบบว่าจะให้การทำให้การทำงานเป็นเช่นไร และในส่วนของ Server เองจะต้องเป็นเครื่องคอมพิวเตอร์ที่มีสถานะภาพสูง เช่น ทำงานเร็ว สามารถอ้างหน่วยความจำได้มาก มีระดับการประมวลผลที่ดีและจะต้องเป็นเครื่องที่จะต้องมีระยะการทำงานที่ยาวนานเพราะว่า Server จะถูกเปิดให้ทำงานอยู่ตลอดเวลาจึงเป็นสิ่งสำคัญอีกอย่างหนึ่ง (ชาญยศ ปลื้มปิติวิริยะเวช, เอกสิทธิ์เทียมแก้วและคณะ. รอบรู้เรื่องแลน.กรุงเทพฯ : โรงพิมพ์ตะวันออก, 2537, 155 หน้า.)

1.2 MAN (Metropolitan Area Network)

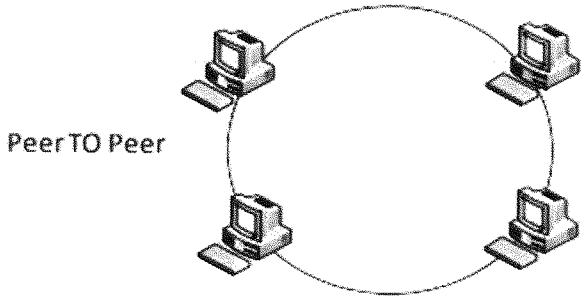
ระบบเครือข่ายในเขตเมือง (Metropolitan Area Network) หมายถึง ระบบเครือข่ายที่มีขนาดใหญ่กว่าเครือข่ายท้องถิ่น แต่อาจเชื่อมต่อกันด้วยระบบการสื่อสารสาหรับสาขาหลาย ๆ แห่งที่อยู่ภายในเขตเมืองเดียวกันหรือหลายเขตเมืองที่อยู่ใกล้กัน ระยะทำงบประมาณ 10 กิโลเมตร เช่น การให้บริการทั้งของรัฐและเอกชนอาจเป็นบริการภายในหน่วยงานหรือเป็นบริการสาธารณะก็ได้รวมถึงการให้บริการระบบโทรทัศน์ทางสาย (Cable Television) เช่น บริษัท UBC ซึ่งเป็นระบบที่มีสายเคเบิลเพียงหนึ่งหรือสองเส้น โดยไม่มีอุปกรณ์สลับช่องสื่อสาร (Switching Element) ทำหน้าที่เก็บกักสัญญาณหรือปล่อยสัญญาณออกไปสู่ระบบอื่น มาตรฐานของระบบ MAN คือ IEEE 802.6 หรือเรียกว่า DQDB (Distributed Queue Dual Bus) ตัวอย่างการใช้งานจริง เช่น ภายในมหาวิทยาลัยหรือในสถานศึกษาจะมีระบบแมนเพื่อเชื่อมต่อระบบแลนของแต่ละคณะวิชาเข้าด้วยกัน เป็นเครือข่ายเดียวกันในวงกว้าง เทคโนโลยีที่ใช้ในเครือข่ายแมน ได้แก่ ATM, FDDI และ SMDS ระบบเครือข่ายแมนที่จะเกิดในอนาคตอันใกล้คือ ระบบที่จะเชื่อมต่อคอมพิวเตอร์ภายในเมืองเข้าด้วยกัน โดยผ่านเทคโนโลยี Wi-Max (http://regelearning.payap.ac.th/docu/mk380/f2.4.6.htm)

2. ประเภทของระบบเครือข่ายตามการใช้งาน

ประเภทของเครือข่ายตามการใช้งานสามารถแบ่งได้เป็น 2 ประเภท ดังนี้

2.1 Peer To Peer

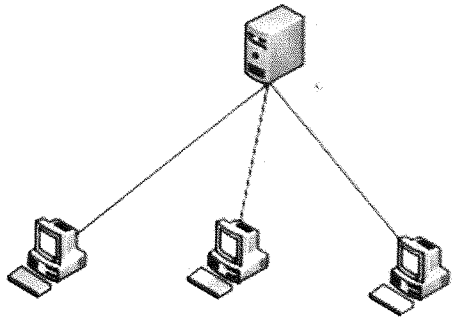
เป็นระบบที่เครื่องคอมพิวเตอร์ทุกเครื่องบนระบบเครือข่ายมีฐานเท่าเทียมกัน คือทุกเครื่องสามารถจะใช้ไฟล์ในเครื่องอื่นได้ และสามารถให้เครื่องอื่นมาใช้ไฟล์ของตนเองได้เช่นกันระบบ Peer To Peer มีการทำงานแบบดิสทริบิวท์ (Distributed System) โดยจะกระจ่ายทรัพยากรต่างๆไปสู่เวิร์กสเตชั่นอื่นๆ แต่จะมี ปัญหาเรื่องการรักษาความปลอดภัย เนื่องจากข้อมูลที่เป็นความลับจะถูกส่งออกไปสู่คอมพิวเตอร์อื่นเช่นกัน โปรแกรมที่ทำงานแบบ Peer To Peer คือ Windows for Workgroupและ Personal Netware



รูปที่ 3.5.1 แสดงการทำงานแบบ Peer To Peer

2.2 Client / Server

เป็นระบบการทำงานแบบ Distributed Processing หรือการประมวลผลแบบกระจ่าย โดยจะแบ่งการประมวลผลระหว่างเครื่องเซิร์ฟเวอร์กับเครื่องไคลเอ็นต์แทนที่แอพพลิเคชั่นจะทำงานอยู่เฉพาะบนเครื่องเซิร์ฟเวอร์ก็แบ่งการคำนวณของโปรแกรมแอพพลิเคชั่น มาทำงานบนเครื่องไคลเอ็นต์ด้วย และเมื่อใดที่เครื่องไคลเอ็นต์ต้องการผลลัพธ์ของข้อมูลบางส่วน จะมีการเรียกใช้ไปยังเครื่องเซิร์ฟเวอร์ให้เฉพาะ ข้อมูลบางส่วนเท่านั้นส่งกลับมาให้เครื่องไคลเอ็นต์เพื่อทำการคำนวณข้อมูลนั้นต่อไป



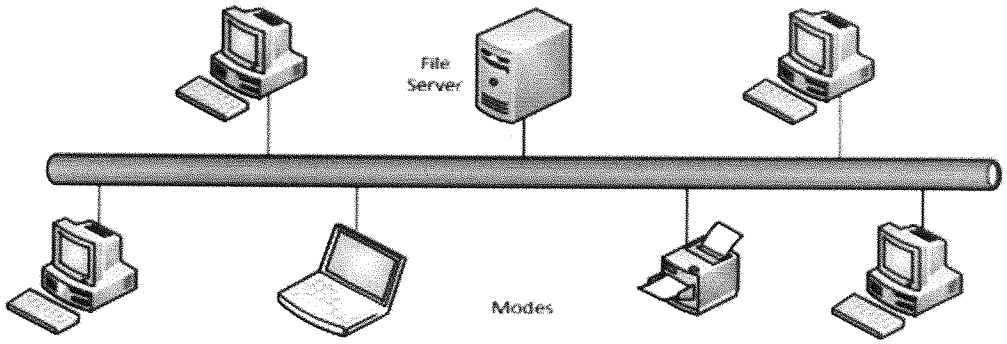
รูปที่ 3.5.2 แสดงการทำงานแบบ Client / Server

3. รูปแบบการเชื่อมต่อของระบบเครือข่าย

รูปแบบการเชื่อมต่อของระบบเครือข่ายแบ่งได้ 5 ประเภท ดังนี้

3.1 ระบบ Bus

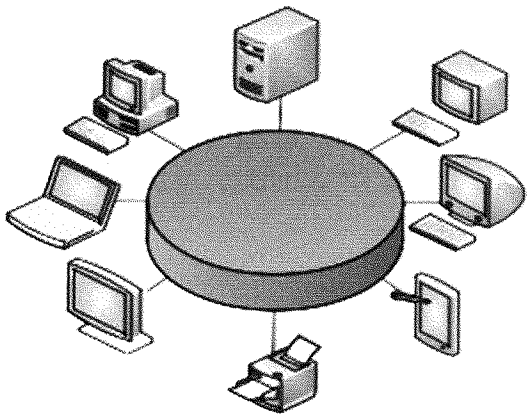
การเชื่อมต่อแบบบัสจะมีสายหลัก1 เส้น เครื่องคอมพิวเตอร์ทั้งเซิร์ฟเวอร์และไคลเอ็นต์ทุกเครื่อง จะต้องเชื่อมต่อสายเคเบิ้ลหลักเส้นนี้โดยเครื่องคอมพิวเตอร์จะถูกมองเป็น Node เมื่อเครื่องไคลเอ็นต์เครื่องที่หนึ่ง (Node A) ต้องการส่งข้อมูลให้กับเครื่องที่สอง (Node C) จะต้องส่งข้อมูลและแอดเดรสของ Node C ลงไปบนบัสสายเคเบิ้ลนี้ เมื่อเครื่องที่ Node C ได้รับข้อมูลแล้วจะนาข้อมูล ไปทำงานต่อทันที



รูปที่ 3.5.3 แสดงการทำงานของระบบ Bus

3.2 ระบบ Ring

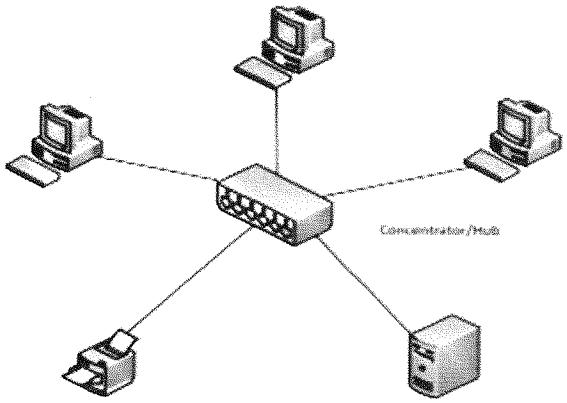
การเชื่อมต่อแบบวงแหวน เป็นการเชื่อมต่อจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งจนครบวงจร ในการส่งข้อมูลจะส่งออกที่สายสัญญาณวงแหวน โดยจะเป็นการส่งผ่านจากเครื่องหนึ่งไปสู่เครื่องหนึ่งจนกว่าจะ ถึงเครื่องปลายทาง ปัญหาของโครงสร้างแบบนี้คือถ้าหากมีสายขาดในส่วนใดจะทำให้ไม่สามารถส่งข้อมูล ได้ระบบ Ring มีการใช้งานบนเครื่องตระกูล IBM กันมากเป็นเครื่องข่าย Token Ring ซึ่งจะใช้รับส่งข้อมูล ระหว่างเครื่องมินิหรือเมนเฟรมของ IBM กับเครื่องลูกข่ายบนระบบ



รูปที่ 3.5.4 แสดงการทำงานของระบบ Ring

3.3 ระบบ Star

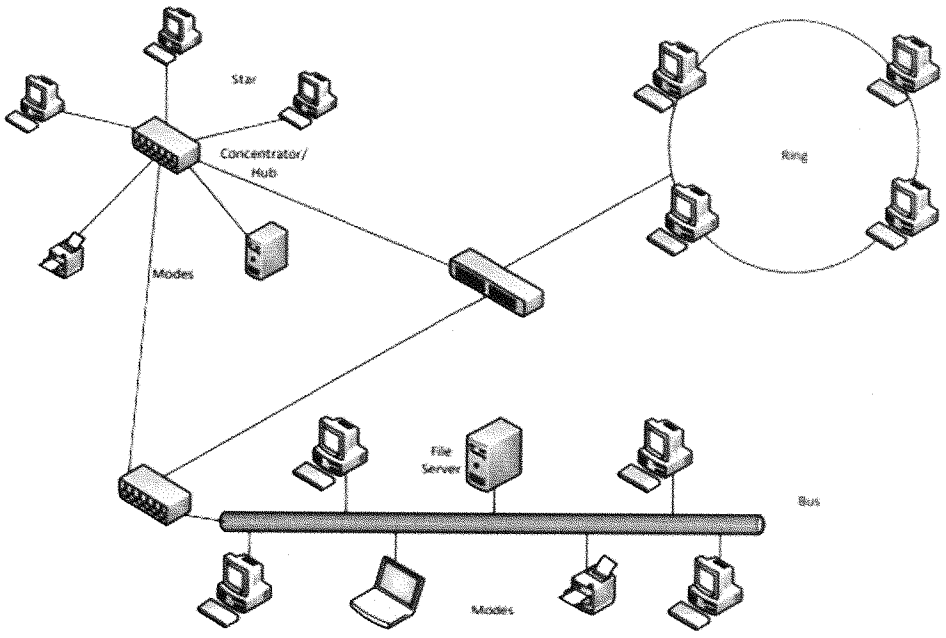
การเชื่อมต่อแบบสตาร์นี้จะใช้อุปกรณ์ Hub เป็นศูนย์กลางในการเชื่อมต่อ โดยที่ทุกเครื่องจะต้อง ผ่าน Hub สายเคเบิ้ลที่ใช้ส่วนมากจะเป็น UTP และ Fiber Optic ในการส่งข้อมูล Hub จะเป็นเสมือนตัวทวนสัญญาณ (Repeater) ปัจจุบันมีการใช้ Switch เป็นอุปกรณ์ในการเชื่อมต่อซึ่งมีประสิทธิภาพการทำงานสูงกว่า



รูปที่ 3.5.5 แสดงการทำงานของระบบ Star

3.4 ระบบ Hybrid

เป็นการเชื่อมต่อที่ผสมผสานเครือข่ายย่อย ๆ หลายส่วนมารวมเข้าด้วยกัน เช่น นำเอาเครือข่ายระบบ Bus, ระบบ Ring และระบบ Star มาเชื่อมต่อเข้าด้วยกัน เหมาะสำหรับบางหน่วยงานที่มีเครือข่ายเก่าและใหม่ให้สามารถทำงานร่วมกันได้ซึ่งระบบ Hybrid Network นี้จะมีโครงสร้างแบบ Hierarchical หรือ Tree ที่มีลำดับชั้นในการทำงาน



รูปที่ 3.5.6 แสดงการทำงานของระบบ Hybrid

3.5 เครือข่ายแบบไร้สาย (Wireless LAN)

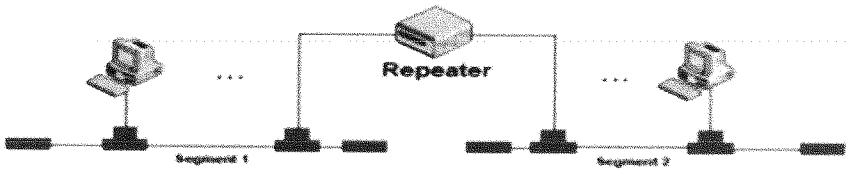
เครือข่ายที่ใช้เป็นระบบแลน (LAN) ที่ไม่ได้ใช้สายเคเบิลในการเชื่อมต่อ นั่นคือระบบเครือข่ายแบบไร้สาย ทำงานโดยอาศัยคลื่นวิทยุในการรับส่งข้อมูล ซึ่งมีประโยชน์ในเรื่องของการไม่ต้องใช้สายเคเบิล เหมาะกับการใช้งานที่ไม่สะดวกในการใช้สายเคเบิล โดยไม่ต้องเจาะผนังหรือเพดานเพื่อวางสาย เพราะคลื่นวิทยุมีคุณสมบัติในการทะลุทะลวงสิ่งกีดขวางอย่างกาแพง หรือพนังห้องได้ดีแต่ก็ต้องอยู่ในระยะทำการ หากเคลื่อนย้ายคอมพิวเตอร์ไปไกลจากรัศมีก็จะขาดการติดต่อได้ การใช้เครือข่ายแบบไร้สายนี้สามารถใช้ได้กับคอมพิวเตอร์พีซีและโน้ตบุ๊ก และต้องใช้การ์ดแลนแบบไร้สายมาติดตั้ง รวมถึงอุปกรณ์ที่เรียกว่า Access Point ซึ่งเป็นอุปกรณ์จ่ายสัญญาณสำหรับระบบเครือข่ายไร้สายมีหน้าที่รับส่งข้อมูลกับการ์ดแลนแบบไร้สาย
(http://www.bcoms.net/network/intro.asp, 2553)

4. อุปกรณ์เครือข่าย

การเชื่อมต่อเครื่องคอมพิวเตอร์ให้กลายเป็น LAN หรือ WAN ได้นั้นจะต้องอาศัยสิ่งที่เรียกว่า "อุปกรณ์เครือข่าย (Network Device)" มีด้วยกันทั้งหมด 6 ชนิด ได้แก่

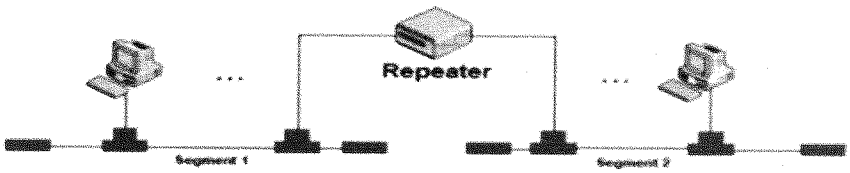
4.1 อุปกรณ์ทวนสัญญาณ (Repeater)

อุปกรณ์ทวนสัญญาณ ทำงานใน Layer ที่ 1 OSI Model เป็นอุปกรณ์ที่ทำหน้าที่รับสัญญาณดิจิตอลเข้ามาแล้วสร้างใหม่ (Regenerate) ให้เป็นเหมือนสัญญาณ (ข้อมูล) เดิมที่ส่งมาจากต้นทาง จากนั้นค่อยส่งต่อออกไปยังอุปกรณ์ตัวอื่น เหตุที่ต้องใช้ Repeater เนื่องจากว่าการ ส่งสัญญาณไปในตัวกลางที่เป็นสายสัญญาณนั้น เมื่อระยะทางมากขึ้นแรงดันของสัญญาณจะลดลงเรื่อย ๆ จึงไม่สามารถส่งสัญญาณในระยะ ทางไกล ๆ ได้ ดังนั้น การใช้ Repeater จะทำให้สามารถส่งสัญญาณไปได้ไกลขึ้น โดยที่สัญญาณไม่สูญหาย



รูปที่ 3.5.7 แสดงการเชื่อมต่อ Repeater เข้ากับเครือข่าย

จากรูปที่ 3.5.7 จะเห็นว่าเครื่องคอมพิวเตอร์ใน Segment 1 (Segment หมายถึงส่วนย่อย ๆ ของ เครือข่าย LAN) เชื่อมต่ออยู่กับคอมพิวเตอร์ใน Segment 2 แต่ทั้งสองเครื่องนี้มีระยะห่างกันมาก จึงต้องใช้ Repeater แต่จะกระจ่ายสัญญาณที่ทวนนั้นออกไปยังคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่ออยู่กับฮับ



รูปที่ 3.5.8 แสดงการเชื่อมต่อคอมพิวเตอร์เข้ากับเครือข่าย โดยใช้ Hub

จากรูปที่ 3.5.8 เป็นการใช้ Hub ในการเชื่อมต่อคอมพิวเตอร์เข้ากับเครือ ข่าย ซึ่งที่ Hub จะมี "พอร์ต (Port)" ใช้สำหรับเป็นช่องทางในการเชื่อมต่อระหว่าง Hub กับเครื่อง คอมพิวเตอร์หรืออุปกรณ์เครือข่ายตัวอื่นๆ จากรูปนี้หากเครื่องคอมพิวเตอร์ใน Segment 1 ต้องการส่งข้อมูลหากันภายใน Segment จะต้องส่งผ่าน Hub

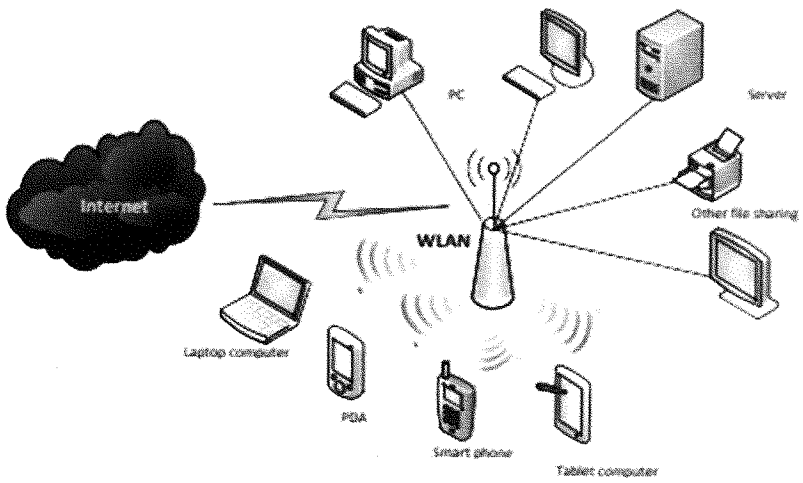
แล้ว Hub จะทวนสัญญาณและส่งต่อข้อมูลนั้นออกไปที่เครื่องคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่ออยู่กับ Hub ทำให้ข้อมูลนั้นถูกส่งไปใน Segment 2 ด้วย แต่ไม่มีเครื่องคอมพิวเตอร์ปลายทางอยู่ใน Segment 2 นี้อยู่แล้ว จึงเป็นการทำให้ความหนาแน่นของข้อมูลในเครือข่ายสูงเกินความจำเป็น ซึ่งเป็นข้อเสียของ Hub

4.2 บริดจ์ (Bridge)

บริดจ์ทำงานใน Layer ที่ 2 ของ OSI Mode เป็นอุปกรณ์ที่ใช้สำหรับเชื่อมต่อ Segment ของเครือข่าย 2 Segment หรือ มากกว่าเข้าด้วยกัน โดยSegment เหล่านั้นจะต้องเป็นเครือข่ายที่ใช้ Data Link Protocol ตัวเดียวกัน และ Network Protocol ตัวเดียวกัน เช่น ต่อ Token RingLAN (LAN ที่ใช้ Topology แบบริง และใช้ โปรโตคอล Token Ring) 2 Segment เข้าด้วยกัน หรือต่อ Ethernet LAN (LAN ที่ใช้ Topology แบบบัส และ ใช้โปรโตคอล Ethernet) 2 Segment เข้าด้วยกันเป็นต้น Bridge มีความสามารถมากกว่า Hub และ Repeater กล่าวคือ สามารถกรองข้อมูลที่จะส่งต่อได้โดยการตรวจสอบว่า ข้อมูลที่ส่งนั้นมีปลายทางอยู่ที่ใด หากเครื่องปลายทางอยู่ภายใน Segment เดียวกันกับเครื่องส่งก็จะส่งข้อมูลนั้นไปใน Segment เดียวกันเท่านั้น ไม่ส่งไป Segment อื่น แต่หากว่าข้อมูลมีปลายทางอยู่ที่ Segment อื่น ก็จะส่งข้อมูลไปใน Segment ที่มีเครื่องปลายทางอยู่เท่านั้น ทำให้สามารถจัดการกับความหนาแน่นของข้อมูลได้มีประสิทธิภาพมากขึ้น ดังรูป ดังต่อไปนี้

4.3 เราเตอร์ (Router)

เราเตอร์จะรับข้อมูลเป็นแพ็กเก็ตเข้ามาตรวจสอบแอดเดรสปลายทาง จากนั้นนำมาเปรียบเทียบกับ ตารางเส้นทางที่ได้รับการโปรแกรมไว้เพื่อหาเส้นทางที่ส่งต่อ หากเส้นทางที่ส่งมาจากอีเทอร์เน็ต และส่ง ต่อออกช่องทางของ Port WAN ที่เป็นแบบจุดไปก็จะมีการปรับปรุงรูปแบบสัญญาณให้เข้ากับมาตรฐานใหม่เพื่อส่งไปยังเครือข่าย WAN ได้ปัจจุบันอุปกรณ์เราเตอร์ได้รับการพัฒนาไปมากทำให้การใช้งานเราเตอร์มีประสิทธิภาพ โดยเฉพาะเมื่อเชื่อมอุปกรณ์เราเตอร์หลาย ๆ ตัวเข้าด้วยกันเป็นเครือข่ายขนาดใหญ่ เราเตอร์สามารถทำงานอย่างมีประสิทธิภาพโดยการหาเส้นทางเดินที่สั้นที่สุดเลือกตามความเหมาะสมและแก้ปัญหาที่เกิดขึ้นเองได้ เมื่อเทคโนโลยีทางด้านอิเล็กทรอนิกส์ได้รับการพัฒนาให้มีขีดความสามารถในการทำงานได้เร็วขึ้น จึงมีผู้พัฒนาอุปกรณ์ที่ทำหน้าที่คัดแยกแพ็กเก็ต หรือเรียกว่า "สวิตช์แพ็กเก็ต ข้อมูล" (Data Switched Packet) โดยลดระยะเวลาการตรวจสอบแอดเดรสลงไป การคัดแยกจะกระทำในระดับวงจร อิเล็กทรอนิกส์ เพื่อให้การทำงานมีประสิทธิภาพ เชิงความเร็วและความแม่นยำสูงสุด อุปกรณ์สวิตช์ข้อมูลจึงมีเวลาหน่วงภายในตัวสวิตช์ต่างมาก จึงสามารถนำมาประยุกต์กับงานที่ต้องการเวลาจริง เช่น การส่งสัญญาณเสียง วิดีโอ ได้ดี



รูปที่ 3.5.9 การทำงานของเราท์เตอร์

4.4 สวิตช์ (Switch)

อุปกรณ์สวิตช์มีหลายแบบ หากแบ่งกลุ่มข้อมูลเป็นแพ็กเก็ตเล็ก ๆ และเรียกใหม่ว่า "เซล" (Cell) กลายเป็น "เซลสวิตช์" (Cell Switch) หรือที่รู้จักกันในนาม "เอทีเอ็มสวิตช์" (ATM Switch) ถ้าสวิตช์ข้อมูลในระดับเฟรมของอีเทอร์เน็ต ก็เรียกว่า "อีเทอร์เน็ตสวิตช์" (Ethernet Switch) และถ้าสวิตช์ตามมาตรฐาน เฟรมข้อมูลที่เป็นกลางและสามารถนาข้อมูลอื่นมาประกอบภายในได้ก็เรียกว่า "เฟรมรีเลย์" (Frame Relay) อุปกรณ์สวิตชิ่งจึงเป็นอุปกรณ์ที่ใช้เทคโนโลยีใหม่ และมีแนวโน้มที่จะพัฒนาให้ใช้กับความเร็วของการ รับส่งข้อมูลจำนวนมาก เช่น เฟรมรีเลย์ (Frame Relay) และเอทีเอ็ม สวิตช์ (ATM Switch) สามารถสวิตช์ข้อมูลขนาดหลายร้อยล้านบิตต่อวินาทีได้ เทคโนโลยีนี้จึงเป็นเทคโนโลยีที่กำลังได้รับความนิยมการออกแบบและจัดรูปแบบเครือข่ายองค์กรที่เป็น "อินทราเน็ต" ซึ่งเชื่อมโยงได้ทั้งระบบ LAN และ WAN จึง ต้องอาศัยอุปกรณ์เชื่อมโยงต่าง ๆ เหล่านี้อุปกรณ์เชื่อมโยง ทั้งหมดนี้รองรับมาตรฐานการเชื่อมต่อได้ หลากหลายรูปแบบ เช่น จากเครือข่ายพื้นฐานเป็นอีเทอร์เน็ต ก็สามารถเชื่อมเข้าสู่ ATM Switch, Frame Relay, or Bridge, Router ได้ทำให้ขนาดของเครือข่ายมีขนาดใหญ่ขึ้น 2.1.4.5 เกตเวย์ (Gateway) เป็นอุปกรณ์ฮาร์ดแวร์ที่เชื่อมต่อเครือข่ายต่างประเภทเข้าด้วยกัน เช่น การใช้เกตเวย์ในการเชื่อมต่อเครือข่ายที่เป็นคอมพิวเตอร์ประเภทพีซี (PC) เข้ากับคอมพิวเตอร์ประเภทแมคอินทอช (MAC) เป็นต้น Gateway ประตูสื่อสารช่องทางสำหรับเชื่อมต่อข่ายงานคอมพิวเตอร์ที่ต่างชนิดกันให้สามารถติดต่อ สื่อสาร กันได้โดยทำให้ผู้ใช้บริการของคอมพิวเตอร์หนึ่งหรือในข่ายงานหนึ่งสามารถติดต่อ เข้าสู่เครื่องบริการหรือข่ายงานที่ต่างประเภทกันได้ ทั้งนี้ โดยการใช้อุปกรณ์ที่เรียกว่า "บริดจ์" (Bridges) โดยโปรแกรมคอมพิวเตอร์จะทำให้การแปลข้อมูลที่จำเป็นให้นอกจากในด้านของข่ายงาน เกตเวย์ยังเป็นอุปกรณ์ในการ เชื่อมต่อข่ายงานบริเวณเฉพาะที่ (LAN) สองข่ายงานที่มีลักษณะไม่เหมือนกันให้สามารถเชื่อมต่อกันได้ หรือจะเป็นการเชื่อมต่อข่ายงาน บริเวณเฉพาะที่เข้ากับข่ายงานบริเวณกว้าง (WAN) หรือต่อเข้ากับมินิคอมพิวเตอร์ หรือต่อเข้ากับเมนเฟรมคอมพิวเตอร์ก็ได้เช่นกัน ทั้งนี้เนื่องจากเกตเวย์มีไมโครโพรเซสเซอร์และหน่วยความจำของตนเอง Gateway จะเป็นอุปกรณ์ที่มีความสามารถมากที่สุดคือ สามารถเครือข่ายต่างชนิดกันเข้าด้วยกัน โดยสามารถเชื่อมต่อ LAN ที่มีหลายๆ โปรโตคอลเข้าด้วยกันได้ และยังสามารถใช้สายส่งที่ต่างชนิดกัน ตัว Gateway จะสามารถสร้างตาราง ซึ่งสามารถบอกได้ว่าเครื่องเซิร์ฟเวอร์ไหนอยู่ภายใต้ Gateway ตัวใด และจะสามารถปรับปรุงข้อมูลตามเวลาที่ตั้งเอาไว้เป็นจุดต่อเชื่อมของเครือข่ายทำหน้าที่เป็นทางเข้าสู่ระบบเครือข่ายต่าง ๆ บนอินเตอร์เน็ตในความหมายของ Router ระบบ เครือข่ายประกอบด้วย Node ของ Gateway และ Node ของ Host เครื่องคอมพิวเตอร์ของผู้ใช้ในเครือข่ายและคอมพิวเตอร์ที่เครื่องแม่ข่ายมีฐานะเป็น Node แบบ Host ส่วนเครื่องคอมพิวเตอร์ที่ควบคุมการจราจรภายในเครือข่าย หรือผู้ให้บริการอินเตอร์เน็ต คือ Node แบบ Gateway ในระบบเครือข่ายของหน่วยธุรกิจ เครื่องแม่ข่ายที่เป็น Node แบบ Gateway มักจะทำหน้าที่เป็นเครื่องแม่ข่ายแบบ Proxy และเครื่องแม่ข่ายแบบ Firewall นอกจากนี้ Gateway ยังรวมถึง Router และ Switch Gateway เป็นอุปกรณ์อิเล็คทรอนิกส์ที่ช่วยในการสื่อสารข้อมูลหน้าที่หลักของเกตเวย์คือช่วยทำให้เครือข่ายคอมพิวเตอร์2 เครือข่ายหรือมากกว่าที่มีลักษณะไม่เหมือนกัน คือลักษณะของการเชื่อมต่อ (Connectivity) ของเครือข่ายที่แตกต่างกัน และมีโปรโตคอลสำหรับการส่ง - รับข้อมูลต่างกัน เช่น LAN เครือหนึ่งเป็นแบบ Ethernet และใช้โปรโตคอล แบบอะซิงโครนัสส่วน LAN อีกเครือข่ายหนึ่งเป็นแบบ Token Ring และใช้โปรโตคอลแบบซิงโครนัส เพื่อให้สามารถติดต่อกันได้เสมือนเป็นเครือข่ายเดียวกัน เพื่อจำกัดวงให้แคบลงมา เกตเวย์โดยทั่วไปจะใช้ เป็นเครื่องมือส่ง -รับ ข้อมูลกันระหว่าง LAN 2 เครือข่ายหรือ LAN กับเครื่องคอมพิวเตอร์เมนเฟรม หรือ ระหว่าง LAN กับ WAN โดยผ่านเครือข่ายโทรศัพท์สาธารณะเช่น X.25 แพ็คเกจสวิตช์เครือข่าย ISDN เทเล็กซ์หรือเครือข่ายทางไกลอื่น ๆ

4) สรุปสาระสำคัญขั้นตอนการดำเนินการและเป้าหมายของงาน

กลุ่มงานคอมพิวเตอร์ เป็นหน่วยงานภายใต้สังกัดสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ได้มีการนำเทคโนโลยีสารสนเทศ เข้ามามีบทบาทสำคัญในการพัฒนาและปรับปรุงการให้บริการด้านสุขภาพ ตั้งแต่การรักษา

ผู้ป่วยจนถึงการจัดการและแลกเปลี่ยนข้อมูลทางการแพทย์ ช่วยเพิ่มประสิทธิภาพในการจัดการข้อมูลและสื่อสารระหว่างหน่วยงานที่เกี่ยวข้องในองค์กร และระหว่างองค์กรที่เกี่ยวข้องต่างๆ ศูนย์ข้อมูลเครือข่ายจึงเป็นหัวใจสำคัญของระบบคอมพิวเตอร์และสารสนเทศขององค์กร ในการรักษาเสถียรภาพ ให้สามารถบริการข้อมูลให้กับผู้รับบริการและบุคลากรในหน่วยงานได้อย่างต่อเนื่อง พัฒนาระบบงานคอมพิวเตอร์และเครือข่าย รวมทั้งให้ คำปรึกษา แนะนำหรือฝึกอบรมการใช้คอมพิวเตอร์และการใช้งานโปรแกรม และดูแลรับผิดชอบ ด้านความมั่นคงปลอดภัยสารสนเทศของสถาบันฯ

ปัจจุบันสถาบันจิตเวชศาสตร์สมเด็จ มีศูนย์ข้อมูลสารสนเทศและระบบเครือข่าย (Data Center) 1 แห่ง ตั้งอยู่ภายในอาคาร 100 ปี ชั้น 6 ซึ่งเป็นสถานที่จัดเก็บอุปกรณ์และระบบต่างๆ ที่จำเป็นในการให้ให้บริการ เช่น เครื่องคอมพิวเตอร์แม่ข่ายของระบบ, อุปกรณ์เครือข่าย และระบบสำรองข้อมูลของสถาบันฯ ซึ่งมีความเสี่ยงที่ระบบจะหยุดทำงานได้จากเหตุภัยพิบัติ เช่น ไฟฟ้าดับ ไฟไหม้ น้ำท่วม ตลอดจนเหตุการณ์ความไม่สงบ ภัยทางการเมือง ภัยคุกคามทางไซเบอร์และปัจจัยอื่นๆ ที่ไม่อาจควบคุมได้ อาจได้รับความเสียหายทำให้การดำเนินงานต้องหยุดชะงัก หรือต้องสูญเสียทั้งข้อมูลหลักและข้อมูลสำรองที่จัดเก็บไว้สถานที่เดียวกันทั้งหมด

จึงมีความจำเป็นในการปรับปรุงศูนย์ข้อมูลสารสนเทศและระบบเครือข่าย (Data Center) และปรับปรุงห้องบริเวณ ชั้น 5 อาคารเจ้าฟ้ามหาจักรีสิรินธร เพื่อสร้างศูนย์ข้อมูลสารสนเทศและระบบเครือข่าย (DR-Site) เพิ่มขึ้นอีกแห่งตั้งอยู่ ให้สามารถรองรับงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยขออนุมัติโครงปรับปรุงห้องเครือข่ายคอมพิวเตอร์ สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา เพื่อให้การบริหารจัดการระบบข้อมูลของคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายมีประสิทธิภาพ มีเสถียรภาพเพิ่มขึ้น และมีศักยภาพในการให้บริการได้อย่างต่อเนื่องปลอดภัยและมีระบบป้องกันพร้อมแก้ไขปัญหา กรณีเกิดความเสียหายรุนแรงหรือเหตุการณ์ฉุกเฉิน

5) ผลสำเร็จของงาน (เชิงปริมาณ/คุณภาพ)

การบริหารจัดการของศูนย์ข้อมูลสารสนเทศและระบบเครือข่าย สามารถเป็นเอกสารอ้างอิง หรือคู่มือปฏิบัติงานห้องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายและพร้อมที่จะให้บริการแก่ผู้บริหารระดับสูง ระดับกลาง ระดับต้นและเจ้าหน้าที่ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา สามารถนำไปเป็นแนวทางการพัฒนาระบบคอมพิวเตอร์และเครือข่ายต่อไปในอนาคต

6) การนำไปใช้ประโยชน์/ผลกระทบ

การบริหารจัดการศูนย์ข้อมูลสารสนเทศและระบบเครือข่าย ใช้ความรู้ความสามารถเฉพาะหรือความชำนาญที่นำไปใช้ประโยชน์ในการปฏิบัติงานหรือแนวทางการพัฒนางานแบบองค์รวม ดังนี้

6.1 ใช้ความรู้ความสามารถในการวิเคราะห์ ตัดสินใจและแก้ปัญหา เมื่อเกิดปัญหาด้านระบบคอมพิวเตอร์และเครือข่าย โดยการพิจารณาจากเอกสารฉบับนี้ ประกอบการดำเนินงานแก้ไขปัญหาในเบื้องต้น

6.2 หน่วยงานหรือผู้ที่เกี่ยวข้องสามารถนำแนวทางดังกล่าวไปประยุกต์ใช้กับระบบงานที่เกี่ยวข้องได้โดยศึกษาจากคู่มือดังกล่าวเป็นแนวทางต่อไปได้

6.3 ทำให้ระบบเครือข่ายภายในองค์กรมีประสิทธิภาพโดยรวมดีขึ้น

6.4 สามารถนำระบบที่พัฒนาและปรับปรุง ไปพัฒนาต่อยอดเพื่อเพิ่มประสิทธิภาพยิ่งขึ้นในอนาคตได้

7) ความยุ่งยากและซับซ้อนในการดำเนินการ

7.1 การตั้งค่าอุปกรณ์ Next-Generation Firewall และกำหนดนโยบายด้านความปลอดภัย (Policy) ต้องทำอย่างระมัดระวัง เพื่อไม่ให้กระทบกับระบบที่มีอยู่ภายในสถาบันฯ ซึ่งอาจจะทำให้ระบบหยุดชะงักได้

7.2 การดำเนินการในการปิดระบบสารสนเทศและโยกย้ายเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่างๆ เพราะมีความเกี่ยวข้องกับการเคลื่อนย้ายอุปกรณ์ที่เกี่ยวข้องกับสถานที่ต่างๆ ภายในอาคาร 100 ปี (Data Center), อาคารเจ้าฟ้ามหาจักรีสิรินธร (DR-Site) ตลอดจนการปรับปรุงระบบเครือข่ายและสารสนเทศทั้งหมดให้ทำงานได้อย่างมีประสิทธิภาพ

8) ปัญหาและอุปสรรคในการการดำเนินการ

ข้อจำกัดด้านจำนวนบุคลากร ไม่สอดคล้องกับปริมาณงานด้านคอมพิวเตอร์และเครือข่าย ทำให้บางครั้งปฏิบัติงานในหน้าที่ไม่ทันเวลาหรือเกิดข้อบกพร่องผิดพลาดจากการปฏิบัติงานอย่างเร่งด่วน ซึ่งส่งผลต่อประสิทธิภาพและประสิทธิผลของงานไม่ดีเท่าที่ควร

9) ข้อเสนอแนะ

9.1 ควรมีนโยบายการบริหารจัดการระบบคอมพิวเตอร์และเครือข่ายอย่างต่อเนื่อง

9.2 ทางผู้จัดทำโครงการ ตั้งใจที่จะพัฒนาระบบเครือข่ายให้มีประสิทธิภาพยิ่งขึ้น เพื่อปิดช่องโหว่ต่างๆ ที่อาจทำให้เกิดความเสี่ยงต่อระบบเครือข่าย และพัฒนาระบบให้มีมาตรฐานสากล ISO27001 ซึ่งจะทำให้ช่วยเพิ่มศักยภาพของระบบสารสนเทศในบริษัทได้มากยิ่งขึ้น

10) การเผยแพร่ (ถ้ามี)

☐ ผลงานแล้วเสร็จและเผยแพร่แล้ว ระบุแหล่งเผยแพร่ .....

☑ ผลงานแล้วเสร็จแต่ยังไม่ได้เผยแพร่

☐ ผลงานยังไม่แล้วเสร็จ

11) การรับรองสัดส่วนของผลงาน ในส่วนที่ตนเองปฏิบัติและผู้มีส่วนร่วมในผลงาน

ผู้สมัครเข้ารับการประเมินบุคคลมีส่วนร่วมในผลงานที่ขอรับการประเมิน ร้อยละ 100 และมีผู้มีส่วนร่วมในผลงาน ดังนี้

รายชื่อผู้มีส่วนร่วมในผลงาน	สัดส่วนมีส่วนร่วมในผลงาน	ลายมือชื่อ
นายรุ่งโรจน์ เหมือนแปลก	100	

ส่วนที่ 4 แบบเสนอข้อเสนอแนวคิดในการปรับปรุงหรือพัฒนางาน

(ข้อเสนอแนวคิดในการปรับปรุงหรือพัฒนางานไม่เกิน 3 หน้ากระดาษA4)

ชื่อผู้สมัครเข้ารับการประเมินบุคคล นายรุ่งโรจน์ เหมือนแปลก

- **ตำแหน่งที่ขอเข้ารับการประเมินบุคคล** นักวิชาการคอมพิวเตอร์ **ระดับ** ชำนาญการ

ตำแหน่งเลขที่ 3938 **กลุ่มงาน** ยุทธศาสตร์และแผนงานโครงการ

กลุ่มภารกิจ ภารกิจพัฒนาสู่ความเป็นเลิศ **หน่วยงาน** สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา กรมสุขภาพจิต

---

1) ชื่อผลงานเรื่อง การออกแบบและพัฒนาระบบเครือข่ายไร้สาย (Somdet-Wifi)

2) หลักการและเหตุผล

สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา เป็นสถาบันฯ ให้บริการบำบัดรักษาผู้ป่วยจิตเวช ประสาทวิทยา ประสาทศัลยศาสตร์ ประสาทจิตเวชศาสตร์ เป็นสถาบันฝึกอบรมทางด้านจิตเวชศาสตร์ สุขภาพจิต ตลอดจนสนับสนุนการพัฒนาวิชาการ การถ่ายทอดความรู้เทคโนโลยีทางการศึกษา วิจัยทางจิตเวช กลุ่มงานคอมพิวเตอร์มีหน้าที่ในการให้บริการระบบสารสนเทศ บริการเครือข่ายแก่ผู้รับบริการและบุคลากร บริการระบบอินเตอร์เน็ต บริการเชื่อมโยงข้อมูลสารสนเทศ อีกทั้งทำการควบคุม ดูแล พัฒนาระบบป้องกันและระบบเครือข่ายคอมพิวเตอร์ เพื่อให้การให้บริการและการสนับสนุนการปฏิบัติงานเป็นไปอย่างต่อเนื่องและมีประสิทธิภาพ

ปัจจุบัน สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ให้บริการเครือข่ายอินเทอร์เน็ตในแบบการเชื่อมต่อบริการผ่านสายสัญญาณ (LAN) แต่ในปัจจุบัน ความต้องการการใช้บริการระบบเครือข่ายคอมพิวเตอร์แบบไร้สายมีจำนวนเพิ่มมากขึ้น ทั้งนี้เนื่องจากแพทย์ พยาบาล และบุคลากรของสถาบันฯ มีการใช้งานอุปกรณ์ Device ที่เป็นลักษณะไร้สายมากขึ้น เช่น Tablet, Smart Phone, Notebook ในการปฏิบัติงานนอกพื้นที่ให้บริการตามจุดเชื่อมต่อผ่านสายสัญญาณ (LAN)

ดังนั้นกลุ่มงานคอมพิวเตอร์ มีความจำเป็นที่จะต้องพัฒนาการให้บริการเครือข่ายคอมพิวเตอร์แบบไร้สาย (Wireless LAN) ให้ครอบคลุมอาคาร สถานที่ และพื้นที่สนับสนุนการปฏิบัติงาน รองรับการปฏิบัติงานของแพทย์ พยาบาล และบุคลากรของสถาบันฯ ได้อย่างมีประสิทธิภาพ และให้สอดคล้องกับมาตรฐานเครือข่ายไร้สาย IEEE 802.11 (Institute of Electrical and Electronics Engineers) และมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

3) บทวิเคราะห์/แนวความคิด/ข้อเสนอ และข้อจำกัดที่อาจเกิดขึ้นและแนวทางแก้ไข

การจัดทำการพัฒนาระบบเครือข่ายไร้สาย (Wireless LAN) จะทำให้มีสัญญาณอินเตอร์เน็ตที่ครอบคลุมพื้นที่การใช้งานภายในสถาบันฯ ได้อย่างมีประสิทธิภาพ และลดข้อจำกัดเรื่องจุดเชื่อมต่ออินเตอร์เน็ตแบบเดิมที่เป็นแบบ LAN ที่ต้องผ่านสายสัญญาณ และลดค่าใช้จ่ายในการจัดซื้อสายสัญญาณอินเตอร์เน็ต รวมทั้งมีการบริหารจัดการระบบเครือข่ายไร้สายที่สามารถควบคุมได้ภายในจุดเดียว เพิ่มช่องทางการสื่อสารระบบเครือข่ายไร้สายที่มีความปลอดภัย และทำให้ระบบเครือข่ายไร้สายของสถาบันฯ สามารถรองรับจำนวนเครื่องคอมพิวเตอร์หรืออุปกรณ์ (Device) ได้มากขึ้นแม้ว่าจะเคลื่อนย้ายก็สามารถเชื่อมต่อกับเครือข่ายตลอดเวลาในระยะการรับ - ส่งข้อมูล และเพื่อพัฒนาระบบเครือข่ายไร้สายให้สามารถรองรับการใช้งานกับอุปกรณ์ใหม่ๆ ในอนาคตได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

3.1 แนวคิด และทฤษฎีที่เกี่ยวกับระบบเครือข่ายไร้สาย

เพื่อให้สามารถวิเคราะห์ออกแบบและจัดทำระบบได้อย่างมีประสิทธิภาพ ตรงตามวัตถุประสงค์ที่กำหนดไว้โดยมีหัวข้อสำคัญในการเรียนรู้ดังต่อไปนี้

- พื้นฐานระบบเครือข่าย อินเตอร์เน็ตโปรโตคอลและอุปกรณ์เครือข่าย
- ระบบเครือข่ายไร้สาย (Wireless LAN)
- เทคโนโลยี Wi-Fi (Wi-Fi Technology)
- มาตรฐานเครือข่ายไร้สาย IEEE 802.11
- ทฤษฎีการวิเคราะห์เพื่อออกแบบและติดตั้งเครือข่ายไร้สายให้มีประสิทธิภาพ
- นิยามระบบเครือข่ายไร้สาย (Somdet-Wi-Fi Hotspot)
- แนวคิดบทความและกรณีศึกษาที่เกี่ยวข้อง

4) ผลที่คาดว่าจะได้รับ

การพัฒนาระบบเครือข่ายไร้สาย (Wireless LAN) มีสัญญาณอินเตอร์เน็ตที่ครอบคลุมพื้นที่การใช้งานภายในสถาบันฯ และสามารถใช้งานระบบเครือข่ายไร้สายได้อย่างต่อเนื่อง พร้อมทั้งสามารถรองรับจำนวนเครื่องคอมพิวเตอร์หรืออุปกรณ์ (Device) ได้มากขึ้น แม้ว่าเคลื่อนย้ายอุปกรณ์ (Device) ก็สามารถเชื่อมต่อกับเครือข่ายตลอดเวลาในระยะการ รับ – ส่ง ข้อมูลที่มีประสิทธิภาพ และมีความปลอดภัย

5) ตัวชี้วัดความสำเร็จ

สถาบันฯ มีระบบเครือข่ายไร้สาย (Wireless LAN) ที่มีความปลอดภัยและมีสัญญาณอินเตอร์เน็ตที่ครอบคลุมพื้นที่การใช้งาน อำนวยความสะดวกให้แก่บุคลากรผู้ใช้บริการ ทั้งจากหน่วยงานภายใน และภายนอก ให้เข้าถึงข้อมูลข่าวสารต่าง ๆ ผ่านทางเครือข่ายอินเตอร์เน็ต (Internet) ได้อย่างมีประสิทธิภาพ