ผลงานวิชาการ

เรื่อง
การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ อาคารศูนย์การแพทย์บางรัก กรมควบคุมโรค

โดย
นายสรายุทธิ์ อินทศร
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
ตำแหน่งเลขที่ ๔๔๐๑
กองโรคเอดส์และโรคติดต่อทางเพศสัมพันธ์
กรมควบคุมโรค

ผลงานวิชาการ

เรื่อง
การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ อาคารศูนย์การแพทย์บางรัก กรมควบคุมโรค

โดย
นายสรายุทธิ์ อินทศร
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
ตำแหน่งเลขที่ ๔๔๐๑
กองโรคเอดส์และโรคติดต่อทางเพศสัมพันธ์
กรมควบคุมโรค

สารบัญ

สารบัญ(ต่อ)

สารบัญตาราง

สารบัญภาพ

สารบัญภาพ(ต่อ)

บทที่ ๑
บทนำ

๑.๑ ความเป็นมาและความสำคัญ

ปัจจุบันระบบเครือข่ายคอมพิวเตอร์เป็นระบบสารสนเทศที่เป็นองค์ประกอบสำคัญในการปฏิบัติงานในองค์กรซึ่งสามารถใช้เป็นสื่อกลางในการแลกเปลี่ยนข้อมูลระหว่างกัน การแบ่งปันทรัพยากรร่วมกันได้ เช่น การใช้เครื่องพิมพ์เอกสาร การใช้พื้นที่สำหรับจัดเก็บข้อมูลหรือฮาร์ดดิสก์ การใช้แฟ้มข้อมูลร่วมกัน และยังเป็นช่องทางสำหรับการใช้ปฏิบัติงานผ่านระบบอินเตอร์เน็ตสำหรับการสืบค้นข้อมูล การศึกษาค้นคว้าวิจัย การบริหารจัดการข้อมูล การติดต่อสื่อสารระหว่างกันผ่านจดหมายอิเล็กทรอนิกส์หรืออีเมล การประชุมทางไกลหรือระบบวิดีโอคอนเฟอร์เรนซ์ได้อย่างสะดวก รวมถึงการรักษาความปลอดภัยของข้อมูล และด้วยกองโรคเอดส์และโรคติดต่อทางเพศสัมพันธ์ ได้รับงบประมาณก่อสร้างอาคารศูนย์ความเป็นเลิศโรคติดต่อทางเพศสัมพันธ์บางรัก (อาคารศูนย์การแพทย์บางรัก กรมควบคุมโรค) เมื่อปี พ.ศ.๒๕๖๐ และสร้างแล้วเสร็จเมื่อปี พ.ศ.๒๕๖๓ เพื่อเป็นสถานที่ในการปฏิบัติหน้าที่ตามภารกิจขององค์กร และให้บริการประชาชนในด้านการตรวจ รักษาและการป้องกันเกี่ยวกับโรคติดต่อทางเพศสัมพันธ์ อีกทั้งเป็นสถานที่ในการให้บริการฉีดวัคซีน การตรวจป้องกันโรคโควิค – 19 และเป็นสถานที่สำหรับศึกษาดูงานทางวิชาการด้านโรคติดต่อทางเพศสัมพันธ์ แต่ยังพบปัญหาเรื่องการใช้งานระบบเครือข่ายที่ไม่ครอบคลุมพื้นที่ มีอุปกรณ์ไม่เพียงพอต่อการใช้งาน และขาดการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ที่ดี ดังนั้นการปรับปรุงระบบเครือข่ายคอมพิวเตอร์ของอาคารศูนย์การแพทย์บางรัก กรมควบคุมโรค ให้สามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพมากขึ้น จึงจำเป็นต้องใช้อุปกรณ์เครือข่ายที่มีความสามารถในการบริหารจัดการระบบเครือข่ายและรักษาความปลอดภัยของระบบเครือข่าย ได้แก่ อุปกรณ์กระจายสัญญาณไร้สาย (Access Point) อุปกรณ์กระจายสัญญาณ (L2 Switch) อุปกรณ์กระจายการทำงานสำหรับเครือข่าย (Link Load Balancer) อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย อุปกรณ์กระจายสัญญาณ (L3 Switch) อุปกรณ์ควบคุมเครือข่ายไร้สาย (Access Point Controller) อุปกรณ์วิเคราะห์การจราจรบนเครือข่าย (Log Analyzer) เครื่องสำรองไฟฟ้า(UPS) อุปกรณ์สำหรับจัดเก็บข้อมูลแบบภายนอก (External Storage) เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) เป็นต้น การนำอุปกรณ์เครือข่ายคอมพิวเตอร์มาใช้ในองค์กรจะช่วยเพิ่มประสิทธิภาพในการทำงานของบุคลากรและมีประโยชน์หลายประการ เช่น

๑. การสื่อสารผ่านระบบเครือข่ายภายในองค์กรได้อย่างมีประสิทธิภาพ ไม่ว่าจะเป็นการส่งข้อมูลผ่าน E-Mail, Chat หรือโทรศัพท์พื้นฐาน ที่จำเป็นสำหรับการปฏิบัติงานและการบริการประชาชนที่เข้ามารับบริการ

๒. การแบ่งปันข้อมูลและทรัพยากรในองค์กร โดยสามารถแบ่งปันข้อมูลและทรัพยากรต่าง ๆ ได้ เช่น การใช้งานไฟล์ร่วมกัน การแชร์เครื่องพิมพ์เอกสาร และอุปกรณ์เก็บข้อมูล เพื่อให้บุคลากรในองค์กรสามารถเข้าถึงและใช้งานได้ตลอดเวลา

๓. รองรับการทำงานแบบออนไลน์ ช่วยให้องค์กรสามารถทำงานแบบออนไลน์ได้มากขึ้น เช่น การทำงานร่วมกันบนเอกสารออนไลน์ การประชุมทางออนไลน์ หรือการบริการประชาชนที่เข้ามารับบริการ

๔. ความปลอดภัยของข้อมูล การใช้อุปกรณ์เครือข่ายเชื่อมต่อกับอุปกรณ์ป้องกัน (Next Generation Firewall) และมีการจัดการความปลอดภัยอย่างเหมาะสมช่วยปกป้องข้อมูลและรักษาความลับขององค์กรได้

๕. การเข้าถึงข้อมูลและการใช้งานอินเทอร์เน็ต สามารถเข้าถึงข้อมูลและบริการต่าง ๆ ในอินเทอร์เน็ตได้อย่างสะดวกและรวดเร็วมากขึ้น

ดังนั้นการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ของอาคารศูนย์การแพทย์บางรัก กรมควบคุมโรค เป็นสิ่งสำคัญที่ช่วยในการสนับสนุนการทำงาน และตรวจสอบความปลอดภัยในการใช้งานบนระบบเครือข่ายคอมพิวเตอร์ สามารถตรวจสอบสาเหตุการเกิดปัญหาและสามารถแก้ไขปัญหาได้ทันท่วงที เพื่อสนับสนุนการปฏิบัติงานของเจ้าหน้าที่ ในการบริการประชาชนด้านการตรวจ ดูแลและรักษา รวมถึงการถ่ายทอดองค์ความรู้ด้านโรคติดต่อทางเพศสัมพันธ์ ให้สอดคล้องกับวัตถุประสงค์และภารกิจขององค์กรที่วางแผนไว้ เพื่อการให้บริการด้านระบบเทคโนโลยีสารสนเทศต่อผู้ใช้งานได้อย่างต่อเนื่อง

๑.๒ วัตถุประสงค์ของการดำเนินงาน

๑.๒.๑ เพื่อปรับปรุงการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ของอาคารศูนย์การแพทย์บางรัก ให้มีประสิทธิภาพมากขึ้น และสามารถรองรับการใช้งานระบบเครือข่ายได้ครอบคลุมพื้นที่ในองค์กร

๑.๒.๒ มีระบบป้องกันการโจมตีและระบบป้องกันความปลอดภัยของระบบเครือข่ายที่มีประสิทธิภาพ สามารถตรวจสอบสถานะอุปกรณ์ได้อย่างรวดเร็ว สามารถป้องกันและแก้ปัญหาได้ทันท่วงที เพื่อความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ในองค์กรมากยิ่งขึ้น

๑.๒.๓ เพิ่มประสิทธิภาพในการทำงาน การให้บริการและระบบทำงานอย่างมีประสิทธิภาพเพื่อรองรับความต้องการของผู้ใช้งาน

๑.๓ ขอบเขตการดำเนินงาน

๑.๓.๑ ทำการศึกษาระบบเครือข่ายเดิมเพื่อออกแบบและวางแผนปรับปรุงประสิทธิภาพการทำงานของระบบเครือข่ายใหม่

๑.๓.๒ ตรวจสอบปัญหาของระบบเครือข่าย เพื่อหาแนวทางการแก้ปัญหาและวางแผนออกแบบสำหรับการนำเอาอุปกรณ์ทางด้านฮาร์ดแวร์มาใช้งาน

๑.๓.๓ จัดหาอุปกรณ์เครือข่ายคอมพิวเตอร์ เพื่อปรับปรุงระบบเครือข่ายของหน่วยงานให้มีประสิทธิภาพมากขั้น

๑.๓.๔ ทดสอบการใช้งานระบบเครือข่าย และความปลอดภัยของระบบเครือข่ายของอาคารศูนย์การแพทย์บางรัก

๑.๔ ประโยชน์ที่คาดว่าจะได้รับ

๑.๔.๑ มีการบริหารจัดการเครือข่ายคอมพิวเตอร์ของอาคารศูนย์การแพทย์บางรัก ที่มีประสิทธิภาพครอบคลุมพื้นที่ของการใช้งานในองค์กร

๑.๔.๒ สามารถตรวจสอบสถานะอุปกรณ์ได้อย่างรวดเร็ว สามารถป้องกันและแก้ปัญหาได้ทันท่วงที

๑.๔.๓ การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์มีรูปแบบที่ดีขึ้นและมีความเสถียรยิ่งขึ้น

๑.๕ นิยามศัพท์

“องค์กร” หมายถึง อาคารศูนย์การแพทย์บางรัก กรมควบคุมโรค

“การบริหารจัดการ” หมายถึง การประสานงานและการบริหารหน้าที่ต่าง ๆ เพื่อให้บรรลุเป้าหมายบางอย่าง ประกอบไปด้วยการวางแผน การบริหารทรัพยากรบุคคล และการควบคุมองค์กร โดยที่การบริหารจัดการครอบคลุมการขยายตัวของธุรกิจตั้งแต่การบริหารจัดการการเงิน การตลาด ทรัพยากรบุคคล กลยุทธ์การผลิต การปฏิบัติการ และการบริการ

“เครือข่ายคอมพิวเตอร์” (Computer Network) หมายถึง เครือข่ายการสื่อสารโทรคมนาคมระหว่างคอมพิวเตอร์จำนวนตั้งแต่สองเครื่องขึ้นไปสามารถแลกเปลี่ยนข้อมูลกันได้ การเชื่อมต่อระหว่างอุปกรณ์คอมพิวเตอร์ในเครือข่าย (โหนดเครือข่าย) จะใช้สื่อที่เป็นสายเคเบิลหรือสื่อไร้สาย เครือข่ายคอมพิวเตอร์ที่รู้จักกันดีคือ อินเทอร์เน็ต

“อุปกรณ์เครือข่าย” (Network hardware) หมายถึง อุปกรณ์เครือข่ายที่เชื่อมต่อกับระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตของอาคารศูนย์การแพทย์บางรัก ได้แก่ อุปกรณ์กระจายสัญญาณ เครื่องควบคุมอุปกรณ์กระจายสัญญาณ อุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์รักษาความปลอดภัยเครือข่าย เครื่องคอมพิวเตอร์ลูกข่าย เป็นต้น

“ผู้รับบริการ” หมายถึง เจ้าหน้าที่หรือประชาชนที่เข้ามารับบริการการตรวจ รักษา ด้านโรคติดต่อทางเพศสัมพันธ์ ณ อาคารศูนย์การแพทย์บางรัก

“ผู้ดูแลระบบ” (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

“แผนผังเครือข่าย” (Network Diagram) หมายถึง แผนภาพการทำงานของเครือข่ายคอมพิวเตอร์ด้วยภาพ เพื่อช่วยลดความซับซ้อนของระบบที่ซับซ้อน แสดงการทำงานอุปกรณ์และการทำงานของระบบเครือข่ายในองค์การที่ทำงานร่วมกัน และเพิ่มการดูแลจัดการ ความเข้าใจ และผลลัพธ์เกี่ยวกับโครงสร้างระบบเครือข่าย การจัดทำแผนภาพเครือข่ายเหล่านี้สามารถแสดงรายละเอียดตามความต้องการและปรับให้เหมาะกับองค์กรได้

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและ สารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่น ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless LAN) เป็นต้น

บทที่ ๒
แนวคิดและทฤษฎีที่เกี่ยวข้อง

ในการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ของอาคารศูนย์การแพทย์บางรัก ผู้จัดทำได้อธิบายและกล่าวถึงทฤษฎีที่เกี่ยวข้องกับการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ รวมถึงงานวิจัยที่เกี่ยวข้องดังต่อไปนี้

๑) แนวคิดวงจรการบริหารงานคุณภาพ PDCA
๒) ทฤษฎีเกี่ยวกับการบริการ
๓) มาตรฐานและเทคโนโลยีของระบบเครือข่าย
๔) แนวทางการพิจารณาจัดหาครุภัณฑ์คอมพิวเตอร์
๕) การดูแลความปลอดภัยในระบบเครือข่ายคอมพิวเตอร์
๖) งานวิจัยที่เกี่ยวข้อง

๒.๑ แนวคิดวงจรการบริหารงานคุณภาพ PDCA[๑]

แนวคิดและความเป็นมาของระบบ

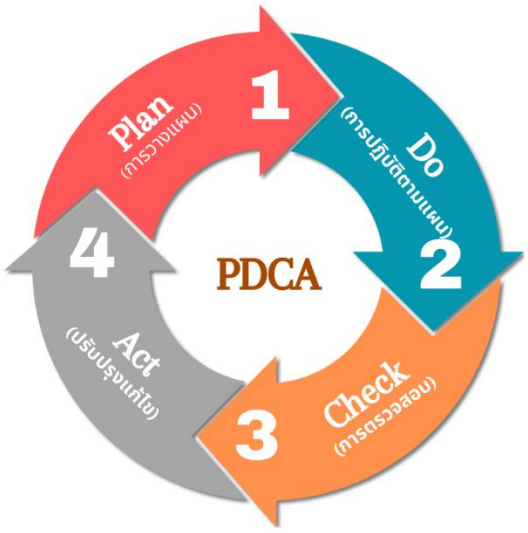
วงจร PDCA เป็นวงจรที่คิดค้นโดย วอลเตอร์ ชูวฮาร์ท ผู้บุกเบิกการใช้สถิติสำหรับแวดวงอุตสาหกรรม ต่อมา PDCA เริ่มเป็นที่รู้จักกันมากขึ้นเมื่อเดมมิ่ง (William Edward Deming) ได้เผยแพร่ให้เป็นกระบวนการทำงานจึงรู้จักในอีกชื่อหนึ่งคือ “วงจรเดมมิ่ง” ซึ่งประกอบด้วย (P : Plan)การวางแผน (D : Do)การปฏิบัติตามแผน (C : Check)การตรวจสอบ และ (A : Action) การดำเนินการให้เหมาะสม ซึ่งการปฏิบัติตาม PDCA นั้นจะปฏิบัติเป็นขั้นตอน โดยเริ่มจาก P จนถึง A และเริ่มกลับ มาปฏิบัติในขั้น P ใหม่ทำวนอยู่อย่างนั้นเป็นวงจรแห่งความสำเร็จ (วีระพล บดีรัฐ, ๒๕๔๓, ๗)

เดมมิ่ง (William Edward Deming) เกิดเมื่อวันที่ ๑๔ ตุลาคม ค.ศ. ๑๙๐๐ ที่เมือง (Sioux) รัฐ (Lowa) สำเร็จการศึกษาปริญญาตรีทางวิทยาศาสตร์จากมหาวิทยาลัย (Wyoming) ปริญญาโททางวิทยาศาสตร์จากมหาวิทยาลัย Colorado และปริญญาเอก สาขาคณิตศาสตร์ฟิสิกส์ (Mathematical Physics) จากมหาวิทยาลัย Yale ในปี ค.ศ. ๑๙๘๒ เริ่มทำงานกับกระทรวงเกษตร (Department of Agriculture) ในปี ค.ศ. ๑๙๓๙ เดมมิ่งย้ายมาเป็นที่ปรึกษาด้านการสุ่มตัวอย่างของสำนักงานสำมะโนประชากร (Bureau of the Census) ปีค.ศ.๑๙๔๖ เริ่มสอนหนังสือที่คณะบริหารธุรกิจ มหาวิทยาลัยนิวยอร์ก (New York University : N.Y.U.) และสอนหนังสือจนถึงปี ค.ศ.๑๙๙๓ และ ตั้งแต่ปีค.ศ.๑๙๕๐ เดมมิ่งเริ่มรับเชิญเป็นวิทยากรและที่ปรึกษาให้กับอุตสาหกรรมในประเทศญี่ปุ่นผ่านสหภาพนักวิทยาศาสตร์และวิศวกรญี่ปุ่น (Japanese Union of Scientists and Engineers : JUSE) ทำให้อุตสาหกรรมของญี่ปุ่นพัฒนาก้าวหน้าไปอย่างรวดเร็วปีค.ศ.๑๙๕๑ เริ่มการมอบรางวัลคุณภาพ Deming (DemingPrize of Quality) ให้แก่ธุรกิจดำเนินงานอย่างมีประสิทธิภาพในประเทศญี่ปุ่น ซึ่งรางวัลที่ทรงเกียรติที่ธุรกิจต่าง ๆ ต้องการและเริ่มต้นก่อนรางวลัคุณภาพ (Malcolm Balding National Quality Award : MBNQA) หรือในสหรัฐอเมริกาหลายสิบปีจนกระทั่งปี ค.ศ. ๑๙๘๐ ดร.เดมมิ่งเริ่มเป็นที่รู้จักกว้างขวางในหมู่ชาวอเมริกันหลังร่วมรายการถ้าญี่ปุ่นทำได้ทำไมเราจะทำไม่ได้ (If Japan Can,Why Can’t We?) ของสถานีโทรทัศน์เอ็นบีซี NBC (สมประสงค์ เสนารัตน์, ๒๕๕๑, ๓)

วีรวิชญ์ เลิศไทยตระกูล (๒๕๕๔) กล่าวถึงปรัชญาวงจร PDCA ว่า (Dr. William Edwards Deming) ได้พัฒนาวงจร PDCA ขึ้นมาจากแนวคิดของ (Dr. W.A. Shewhart) นักควบคุมกระบวนการ เชิงสถิติที่ (J Bell Laboratories) ในสหรัฐอเมริกาที่ได้นำเสนอในหนังสือ Statistical วิธีการจากมุมมองของการควบคุมคุณภาพ (๑๙๓๐) ในระยะแรกรู้จัก วงจร PDCA ในนาม (Shewhart Cycle) จากนั้น ดร.วิลเลี่ยม เอ็ดเวิร์ดเดมมิ่ง ได้นำไปพัฒนาปรับใช้ในการควบคุมคุณภาพในวงการอุตสาหกรรมของญี่ปุ่น จึงมีชื่อเรียกว่า วงจรเดมิ่ง (สมาคมส่งเสริมเทคโนโลยีไทย-ญี่ปุ่น, ๒๕๕๒, ๒๑) เริ่มแรกวงจร PDCA เน้นถึงความสัมพันธ์ของ ๔ ฝ่าย ในการดำเนินธุรกิจเพื่อให้ได้มาซึ่งคุณภาพและความพึงพอใจของลูกค้า ได้แก่ ฝ่ายออกแบบ ฝ่ายผลิต ฝ่ายขาย และฝ่ายวิจัย ความสัมพันธ์ทั้ง ๔ ฝ่าย จะต้องดำเนินต่อไปอย่างต่อเนื่อง เพื่อยกระดับคุณภาพสินค้าตามความต้องการของลูกค้าที่เปลี่ยนแปลงอยู่ตลอดเวลา โดยให้ถือว่าคุณภาพต้องมาก่อนสิ่งใด ต่อมาแนวคิดเกี่ยวกับวงจรเดมมิ่ง ได้ถูกดัดแปลงให้เข้ากับวงจรการบริหารงาน คือขั้นตอน การวางแผน (Plan) ขั้นตอนการปฏิบัติงาน (Do) ขั้นตอนการตรวจสอบ (Check) และขั้นตอนการปรับปรุงแก้ไข (Act)

โครงสร้างของวงจร PDCA

PDCA ย่อมาจาก Plan-Do-Check-Act หรือ วางแผน-ปฏิบัติ-ตรวจสอบ-ปรับปรุง PDCA เป็นเครื่องมือที่ใช้เพื่อปรับปรุงกระบวนการทำงานอย่างเป็นระบบ โดยมีจุดประสงค์เพื่อแก้ไขปัญหาและทำให้เกิดการพัฒนาปรับปรุงให้กระบวนการทำงานมีประสิทธิภาพอย่างต่อเนื่อง (Continuous Improvement – CI) และทำวนลูปแบบนี้ไปเรื่อยๆจนเป็นวงจร (cycle) การทำ PDCA เป็นส่วนหนึ่งของการจัดการคุณภาพ หรือ Quality Management (QM) นั่นคือ กระบวนการในการบ่งชี้และบริหารกิจกรรมต่างๆ ที่มีความจำเป็นอย่างยิ่งต่อการดำเนินการ เพื่อให้สามารถบรรลุวัตถุประสงค์ด้านคุณภาพขององค์กร



ภาพที่ ๑ : วงจรคุณภาพ (PDCA)

การทำ PDCA ๔ ขั้นตอน

๑. ขั้นตอนการวางแผน (Plan)

ขั้นตอนการวางแผนครอบคลุมถึงการกำหนดกรอบหัวข้อที่ต้องการปรับปรุงเปลี่ยนแปลง ซึ่งรวมถึงการพัฒนาสิ่งใหม่ ๆ การแก้ปัญหาที่เกิดขึ้นจากการปฏิบัติงาน ฯลฯ พร้อมกับพิจารณาว่ามีความจำเป็นต้องใช้ข้อมูลใดบ้างเพื่อการปรับปรุงเปลี่ยนแปลงนั้น โดยระบุวิธีการเก็บข้อมูลให้ชัดเจน นอกจากนี้ จะต้องวิเคราะห์ข้อมูลที่รวบรวมได้ แล้วกำหนดทางเลือกในการปรับปรุงเปลี่ยนแปลงดังกล่าว

การวางแผนยังช่วยให้เราสามารถคาดการณ์สิ่งที่เกิดขึ้นในอนาคต และช่วยลดความสูญเสียต่าง ๆ ที่อาจเกิดขึ้นได้ ทั้งในด้านแรงงาน วัตถุดิบ ชั่วโมงการทำงาน เงิน เวลา ฯลฯ โดยสรุปแล้ว การวางแผนช่วยให้รับรู้สภาพปัจจุบัน พร้อมกับกำหนดสภาพที่ต้องการให้เกิดขึ้นในอนาคต ด้วยการผสานประสบการณ์ ความรู้ และทักษะอย่างลงตัว โดยทั่วไปการวางแผนมีอยู่ด้วยกัน ๒ประเภทหลัก ๆ ดังนี้

ประเภทที่๑ การวางแผนเพื่ออนาคต เป็นการวางแผนสำหรับสิ่งที่จะเกิดขึ้นในอนาคตหรือกำลังจะเกิดขึ้น บางอย่างเราไม่สามารถควบคุมสิ่งนั้นได้เลย แต่เป็นการเตรียมความพร้อมของเราสำหรับสิ่งนั้น

ประเภทที่ ๒ การวางแผนเพื่อการปรับปรุงเปลี่ยนแปลง เป็นการวางแผนเพื่อเปลี่ยนแปลงสภาพที่เกิดขึ้นในปัจจุบันเพื่อสภาพที่ดีขึ้น ซึ่งเราสามารถควบคุมผลที่เกิดในอนาคตได้ด้วยการเริ่มต้นเปลี่ยนแปลงตั้งแต่ปัจจุบัน

๒. ขั้นตอนการปฏิบัติ (DO)

ขั้นตอนการปฏิบัติ คือ การลงมือปรับปรุงเปลี่ยนแปลงตามทางเลือกที่ได้กำหนดไว้ในขั้นตอนการวางแผน ในขั้นนี้ต้องตรวจสอบระหว่างการปฏิบัติด้วยว่าได้ดำเนินไปในทิศทางที่ตั้งใจหรือไม่ พร้อมกับสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบด้วย เราไม่ควรปล่อยให้ถึงวินาทีสุดท้ายเพื่อดูความคืบหน้าที่เกิดขึ้น หากเป็นการปรับปรุงในหน่วยงานผู้บริหารย่อมต้องการทราบความคืบหน้าของการดำเนินงาน เพื่อเพิ่มความมั่นใจว่าโครงการปรับปรุงเกิดความผิดพลาดน้อยที่สุด

๓. ขั้นตอนการตรวจสอบ (Check)

ขั้นตอนการตรวจสอบ คือ การประเมินผลที่ได้รับจากการปรับปรุงเปลี่ยนแปลง แต่ขั้นตอนนี้มักจะถูกมองข้ามเสมอการตรวจสอบทำให้เราทราบว่าการปฏิบัติในขั้นที่สองสามารถบรรลุเป้าหมายหรือวัตถุประสงค์ที่ได้กำหนดไว้หรือไม่ สิ่งสำคัญก็คือ เราต้องรู้ว่าจะตรวจสอบอะไรบ้างและบ่อยครั้งแค่ไหน ข้อมูลที่ได้จากการตรวจสอบจะเป็นประโยชน์สำหรับขั้นตอนถัดไป

๔. ขั้นตอนการดำเนินงานให้เหมาะสม (Act)

ขั้นตอนการดำเนินงานให้เหมาะสมจะพิจารณาผลที่ได้จากการตรวจสอบ ซึ่งมีอยู่ ๒ กรณี คือ ผลที่เกิดขึ้นเป็นไปตามแผนที่วางไว้ หรือไม่เป็นไปตามแผนที่วางไว้ หากเป็นกรณีแรก ก็ให้นำแนวทางหรือกระบวนการปฏิบัตินั้นมาจัดทำให้เป็นมาตรฐาน พร้อมทั้งหาวิธีการที่จะปรับปรุงให้ดียิ่งขึ้นไปอีก ซึ่งอาจหมายถึงสามารถบรรลุเป้าหมายได้เร็วกว่าเดิม หรือเสียค่าใช้จ่ายน้อยกว่าเดิม หรือทำให้คุณภาพดียิ่งขึ้นก็ได้แต่ถ้าหากเป็นกรณีที่สอง ซึ่งก็คือผลที่ได้ไม่บรรลุวัตถุประสงค์ตามแผนที่วางไว้ เราควรนำข้อมูลที่รวบรวมไว้มาวิเคราะห์และพิจารณาว่าควรจะดำเนินการอย่างไร เช่น การมองหาทางเลือกใหม่ที่น่าจะเป็นไปได้ การใช้ความพยายามให้มากขึ้นกว่าเดิม การขอความช่วยเหลือจากผู้รู้ หรือกดารเปลี่ยนเป้าหมายใหม่ การวางแผนการดำเนินงาน เราต้องกำหนดเป้าหมายที่ต้องการบรรลุผลสำเร็จ อาจจะเป็นเป้าหมายระยะสั้นหรือเป้าหมายระยะยาว เมื่อปรับปรุงแผนการดำเนินงานเสร็จ เราก็จะกลับเข้าสู่วงจรการทำ PDCA แบบนี้วนไปเรื่อย ๆ

๒.๒ ทฤษฎีเกี่ยวกับการบริการ[๒]

การบริการ (Service) คือ การกระทำกิจกรรมใด ๆ ด้วยร่างกายเพื่อตอบสนองความต้องการของบุคคลอื่น ซึ่งเกี่ยวข้องกับการอำนวยความสะดวก ความสามารถสร้างความพึงพอใจให้กับ ผู้รับบริการได้

SERVICE แต่ละอักษรหมายถึงการให้บริการ ดังนี้

S -----> **Smiling** คือ การยิ้มแย้มแจ่มใส ทั้งใจและวาจา

E -----> **Early Respond** คือ การใส่ใจให้บริการอย่างรวดเร็ว

R -----> **Respectful** คือ การให้ความเคารพ ให้เกียรติ

V -----> **Voluntariness Manner** คือ บริการอย่างเต็มใจ มิได้ฝืนทำ

I -----> **Image Enhancing** คือ การแสดงออกที่เสริมภาพลักษณ์แก่องค์กร

C -----> **Courtesy** คือ กิริยามารยาท สุภาพ อ่อนโยน

E -----> **Enthusiasm** มีความกระตือรือร้น ให้บริการเกินความคาดหมาย

คุณลักษณะเฉพาะในงานบริการ

๑. เป็นสิ่งที่จับต้องไม่ได้ มีความเป็นนามธรรม ไม่มีรูปร่าง ไม่มีตัวตน ผู้รับบริการสามารถสัมผัสการบริการได้ด้วยการรับรู้ผ่านประสาทสัมผัสต่าง ๆ ได้อย่างดี

๒. การบริการมีคุณภาพไม่คงที่ แปรเปลี่ยนไปตามผู้ส่งมอบงานบริการ โดยงานบริการมีการเปลี่ยนแปลงค่อนข้างสูง ขึ้นอยู่กับผู้ให้บริการ หรือพนักงานผู้ทำหน้าที่นั้น หากมีการเปลี่ยนคน คุณภาพงานการบริการ มีการเปลี่ยนแปลงไปตามพฤติกรรมบุคคล ผู้ส่งมอบบริการนั้น ๆ

๓. เก็บรักษาไว้ไม่ได้ การบริการไม่ใช่สินค้าอุปโภค บริโภคใด ๆ ไม่สามารถเก็บรักษา เป็นสินค้าคงคลัง แพคเก็บไว้ได้ ไม่มีวันหมดอายุ ดังนั้นการรักษาการบริการนั้นจึงขึ้นอยู่กับพฤติกรรมเฉพาะตัวของผู้ให้บริการที่ส่งมอบแก่ผู้รับบริการ ด้วยการยื่นการบริการด้วยใจให้ด้วยความสม่ำเสมอ ขึ้นอยู่กับแผนงานนโยบายการธำรงรักษาคุณภาพบริการ

๔. คนเป็นตัวแปรสำคัญในการสร้างและทำลาย คนยังคงเป็นนักบริการที่สำคัญอันดับแรก ไม่ว่าเครื่องมืออุปกรณ์การรักษามีความทันสมัยเพียงใด แต่หากผู้ให้บริการส่งมอบการบริการ แบบไร้ซึ่งสำนึกหน้าที่ มีความบกพร่องหรือมีการเปลี่ยนแปลงโอนย้ายทีมงานเดิม เกิดรอยต่อความไม่สม่ำเสมอคุณภาพงานบริการ การเปรียบเทียบทีมงานเดิมต่อทีมงานใหม่ย่อมส่งผลทำลายชื่อเสียงขององค์กรที่สร้างมานานนับหลายสิบปี ดังนั้น การพิจารณารับบุคลากรเข้าทำงานแต่ละตำแหน่งงานจึงมีความสำคัญ

๕. ต้องใช้แรงงานคนมากกว่าเทคโนโลยี แม้ปัจจุบันความสะดวกด้านเทคโนโลยีเข้ามามีส่วนทำให้คุณภาพชีวิตมนุษย์ดีขึ้นมาก แต่คนคือผู้ให้บริการที่ดีที่สุด มีความอ่อนน้อมถ่อมตน อบอุ่นเข้าใจ หากองค์กรมีคนทำงานที่ดี มีจิตสำนึกในหน้าที่งานบริการมีทัศนคติเชิงบวก มีการฝึกฝนปรับปรุงในหน้าที่ตนเองอย่างสม่ำเสมอ ย่อมส่งผลให้องค์กรมีการเจริญเติบโต มีรากฐานวัฒนธรรมการบริการที่ดี ในทางตรงกันข้ามหากมีคนที่ไร้จิตสำนึกการบริการมาทำงาน องค์กรนั้นย่อมเสียโอกาสสำคัญ และผู้รับบริการกล่าวถึงในแง่ไม่ดีเป็นวงกว้างอย่างต่อเนื่องเช่นกัน

๖. ผลของการบริการเชื่อมโยงถึงศรัทธาในองค์กร การบริการนั้นมีการเปลี่ยนแปลง อย่างรวดเร็วทุกขณะ ไม่มีการจำกัดเวลา สถานที่ เพศ อายุ ดังนั้น หากผู้ให้บริการส่งมอบคุณภาพ งานบริการ อยู่ในระดับต่ำกว่าความคาดหมายของผู้รับบริการ หรือสร้างความไม่พึงพอใจแก่ผู้รับบริการ ย่อมเสี่ยงต่อการถูกร้องเรียนส่งผลต่อหน้าที่ ชื่อเสียงตนเองและเชื่อมโยงมาสู่ความเสียหายหลักต่อองค์กร ทั้งในแง่ของความน่าเชื่อถือความไม่น่าไว้วางใจ ความไม่ประทับใจ รวมถึงมุมมองการไม่พัฒนาปรับปรุงคุณภาพการบริการขององค์กรนั้น ๆ

๗. สร้างภาพลักษณ์และภาพลบเป็นเวลานาน การบริการนับเป็นงานที่มีความสำคัญอย่างมาก จึงควรปลูกฝังผู้ให้บริการมีทัศนคติต่อการส่งมอบบริการที่ดี ไม่ว่าจะสร้างความประทับใจหรือสร้างความไม่พึงพอใจต่อผู้รับบริการจะจดจำฝังใจเป็นเวลานานมีการกล่าวถึงปากต่อปาก การส่งข้อความลงในสังคมออนไลน์ ซึ่งใช้เวลานานหลายสิบปีจึงจะสามารถลบล้างความทรงจำที่ไม่ดีได้

๒.๓ มาตรฐานและเทคโนโลยีของระบบเครือข่าย[๓]

การเชื่อมต่อสายสัญญาณสามารถทำได้หลายวิธี ทำให้เกิดรูปแบบของระบบเครือข่ายขึ้นหลายแบบ รูปร่างของระบบเครือข่ายที่แตกต่างกันนี้เรียกว่า สถาปัตยกรรมระบบเครือข่าย (Network Architecture) หรือโทโปโลยี (Topology) รูปแบบการเชื่อมต่อในเครือข่ายคอมพิวเตอร์ในปัจจุบันมี ๔ รูปแบบหลัก คือ การเชื่อมต่อแบบบัส (Bus Topology) การเชื่อมต่อแบบวงแหวน (Ring Topology) การเชื่อมต่อ แบบดวงดาว (Star Topology) และการเชื่อมต่อแบบผสม (Mixed Topology)

การออกแบบระบบเครือข่ายแบบต่าง ๆ ต้องมีมาตรฐานที่จะเป็นแนวทางในการเลือกใช้อุปกรณ์เครือข่าย ซึ่งมีหลายองค์กรมาตรฐาน เช่น สถาบันมาตรฐานแห่งชาติแห่งสหรัฐอเมริกา (American National Standards Institute : ANSI), Institute of Electrical and Electronics Engineering (IEEE), International Standards Organization (ISO) ซึ่งมีการร่วมกันในการจัดมาตรฐานต่าง ๆ เช่น ISO ร่วมกับ ANSI พัฒนา OSI Model (Open Systems Interconnection Model) ซึ่งแบ่งออกเป็น ๗ ระดับชั้น คือ

๑) ระดับชั้นฟิสิคัล (Physical layer)
๒) ระดับชั้นดาต้าลิงก์ (Data link layer)
๓) ระดับชั้นเน็ตเวิร์ก (Network layer)
๔) ระดับชั้นทรานสปอร์ต (Transport layer)
๕) ระดับชั้นเซสชัน (Session layer)
๖) ระดับชั้นพรีเซนเตชัน (Presentation layer)
๗) ระดับชั้นแอปพลิเคชั่น (Application layer)

สถาปัตยกรรมเครือข่าย TCP/IP จะต่างจาก OSI คือมีการแบ่งออกเป็น ๔ ระดับชั้น คือ

๑) ระดับชั้นโฮสต์-ทู-เน็ตเวิร์ก Host-to-Network
๒) ระดับชั้นอินเทอร์เน็ต (Internet layer)
๓) ระดับชั้นทรานสปอร์ต (Transport layer)
๔) ระดับชั้นแอปพลิเคชัน (Application layer)

โทโปโลยี

สถาปัตยกรรมการเชื่อมต่อของระบบเครือข่ายคอมพิวเตอร์มีหลายแบบสามารถเลือกใช้ให้เหมาะสมกับการใช้งานช่วยเพิ่มประสิทธิภาพการทำงานและประหยัดค่าใช้จ่าย รวมทั้งวางแผนระบบเครือข่ายในอนาคต โดยส่วนใหญ่คอมพิวเตอร์ภายในองค์กรใหญ่จะติดต่อสื่อสารผ่านระบบ LAN (Local Area Network) โดยมี backbone เป็นส่วนประกอบหลัก เป็นจุดที่จะทำการสื่อสารภายในองค์กรผ่าน backbone เทคโนโลยี LAN มีหลายประเภท เช่น Ethernet, Token Ring, FDDI และ Wireless LAN เป็นต้น แต่นิยมกันมากที่สุดในปัจจุบันคือ อีเธอร์เน็ต (Ethernet) ซึ่งอีเธอร์เน็ตเองยังจำแนกออกได้หลายประเภทย่อย ขึ้นอยู่กับความเร็ว

โทโปโลยี (Topology) และสายสัญญาณที่ใช้เทคโนโลยี LAN แต่ละประเภทมีทั้งข้อดีและข้อเสียที่แตกต่างกัน การเลือกใช้เทคโนโลยีเหล่านี้ควรให้เหมาะสมกับลักษณะการใช้งานเครือข่ายขององค์กร โทโปโลยีของเครือข่ายอาจจะมีผลต่อสมรรถนะของเครือข่ายได้

การเลือกโทโปโลยีอาจมีผลต่อประเภทของอุปกรณ์ที่ใช้ในเครือข่าย ดังนี้

- สมรรถนะของอุปกรณ์เหล่านั้น
- ความสามารถในการขยายของเครือข่าย
- วิธีการดูแลและจัดการเครือข่าย การรู้จักและเข้าใจโทโปโลยีประเภทต่าง ๆ

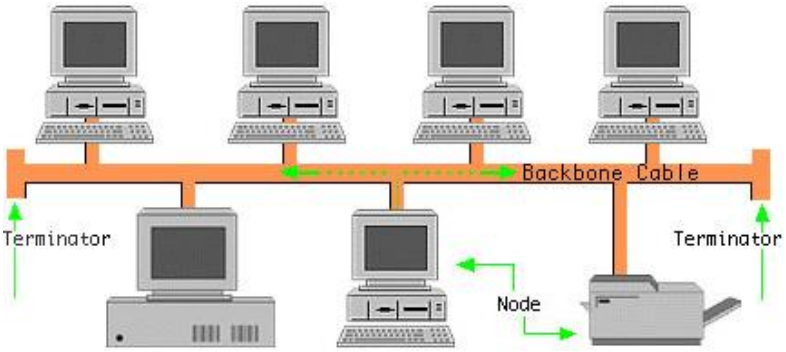
โทโปโลยีแต่ละประเภทมีดังต่อไปนี้

โทโปโลยีแบบบัส (Bus Topology)

เป็นรูปแบบการเชื่อมต่อกันโดยผ่ายสายสัญญาณแกนหลัก ที่เรียกว่า BUS หรือ แบ็คโบน (Backbone) คือ สายรับส่งสัญญาณข้อมูลหลักใช้เป็นทางเดินข้อมูลของทุกเครื่องภายในระบบเครือข่ายและจะมีสายแยกย่อยออกไปในแต่ละจุดเพื่อเชื่อมต่อเข้ากับคอมพิวเตอร์เครื่องอื่น ๆ ซึ่งเรียกว่าโหนด (Node)

ข้อมูลจากโหนดผู้ส่งจะถูกส่งเข้าสู่สายบัสในรูปของแพ็กเกจ ซึ่งแต่ละแพ็กเกจจะประกอบไปด้วยข้อมูลของผู้ส่ง ผู้รับ และข้อมูลที่จะส่งการสื่อสารภายในสายบัสจะเป็นแบบ ๒ ทิศทางแยกไปยังปลายทั้ง ๒ ด้านของบัส โดยตรงปลายทั้ง ๒ ด้านของบัสจะมีเทอร์มิเนเตอร์ (Terminator) ทำหน้าที่ลบล้างสัญญาณที่ส่งมาถึง เพื่อป้องกันไม่ให้สัญญาณข้อมูลนั้นสะท้อนกลับ เข้ามายังบัสอีก เพื่อเป็นการป้องกันการชนกันของข้อมูลอื่น ๆ ที่เดินทางอยู่บนบัสในขณะนั้น

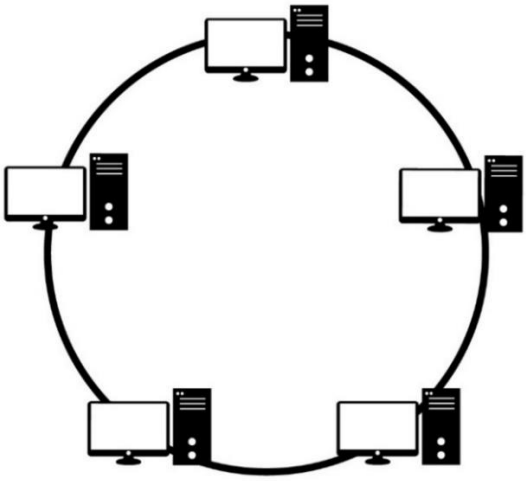
สัญญาณข้อมูลจากโหนดผู้ส่งเมื่อเข้าสู่บัส ข้อมูลจะไหลผ่านไปยังปลายทั้ง ๒ ด้านของบัส แต่ละโหนดที่เชื่อมต่อเข้ากับบัสจะคอยตรวจดูว่าตำแหน่งปลายทางที่มากับแพ็กเกจข้อมูลนั้นตรงกับตำแหน่งของตนหรือไม่ถ้าตรงก็จะรับข้อมูลนั้นเข้ามาสู่โหนดตนแต่ถ้าไม่ใช่ก็จะปล่อยให้สัญญาณข้อมูลนั้นผ่านไป จะเห็นว่าทุก ๆ โหนด ภายในเครือข่ายแบบ BUS นั้นสามารถรับรู้สัญญาณข้อมูลได้ แต่จะมีเพียงโหนดปลายทางเพียงโหนดเดียวเท่านั้นที่จะรับข้อมูลนั้นไปได้



ภาพที่ ๒ : โทโปโลยีแบบบัส (Bus Topology)

โทโปโลยีแบบวงแหวน (Ring Topology)

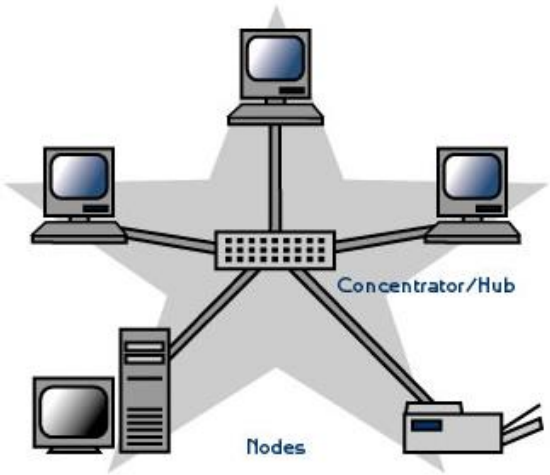
เป็นรูปแบบที่เครื่องคอมพิวเตอร์ทุกเครื่องในระบบเครือข่าย ทั้งเครื่องที่เป็นผู้ให้บริการ (Server) และเครื่องที่เป็นผู้ขอใช้บริการ (Client) ทุกเครื่องถูกเชื่อมต่อกันเป็นวงกลม ข้อมูลข่าวสารที่ส่งระหว่างกันจะไหลวนอยู่ในเครือข่ายไปในทิศทางเดียวกันโดยไม่มีจุดปลายหรือเทอร์มิเนเตอร์เช่นเดียวกับเครือข่ายแบบ BUS ในแต่ละโหนด หรือแต่ละเครื่องจะมีรีพีตเตอร์ (Repeater) ประจำแต่ละเครื่อง ๑ ตัว ซึ่งจะทำหน้าที่เพิ่มเติมข้อมูลที่จำเป็นต่อการติดต่อสื่อสารเข้าในส่วนหัวของแพ็กเกจที่ส่ง และตรวจสอบข้อมูลจากส่วนหัวของ Packet ที่ส่งมาถึง ว่าเป็นข้อมูลของตนหรือไม่ แต่ถ้าไม่ใช่ก็จะปล่อยข้อมูลนั้นไปยัง Repeater ของเครื่องถัดไป



ภาพที่ ๓ : โทโปโลยีแบบวงแหวน (Ring Topology)

โทโปโลยีแบบดาว (Star Topology)

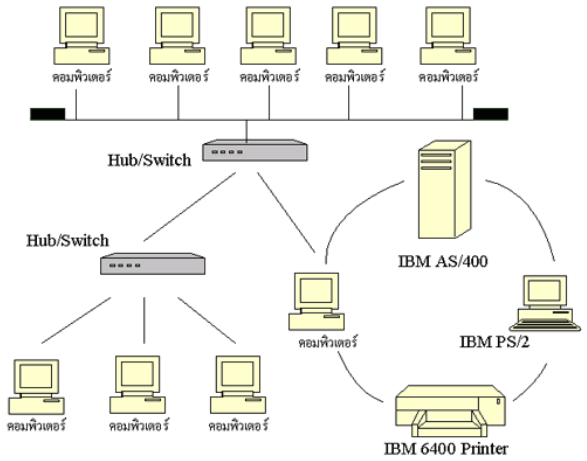
เป็นรูปแบบที่เครื่องคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่อเข้าด้วยกันในเครือข่าย จะต้องเชื่อมต่อกับอุปกรณ์ตัวกลางตัวหนึ่งที่เรียกว่า ฮับ (HUB) หรือสวิตช์ (Switch) หรือเครื่อง ๆ หนึ่ง ซึ่งทำหน้าที่เป็นศูนย์กลางของการเชื่อมต่อสายสัญญาณที่มาจากเครื่องต่าง ๆ ในเครือข่าย และควบคุมเส้นทางการสื่อสารทั้งหมด เมื่อมีเครื่องที่ต้องการส่งข้อมูลไปยังเครื่องอื่น ๆ ที่ต้องการในเครือข่าย เครื่องนั้นก็จะต้องส่งข้อมูลมายัง HUB หรือเครื่องศูนย์กลางก่อน แล้ว HUB ก็จะทำหน้าที่กระจายข้อมูลนั้นไปในเครือข่ายต่อไป



ภาพที่ ๔ : โทโปโลยีแบบดาว (Star Topology)

โทโพโลยีแบบผสม (Hybrid Topology)

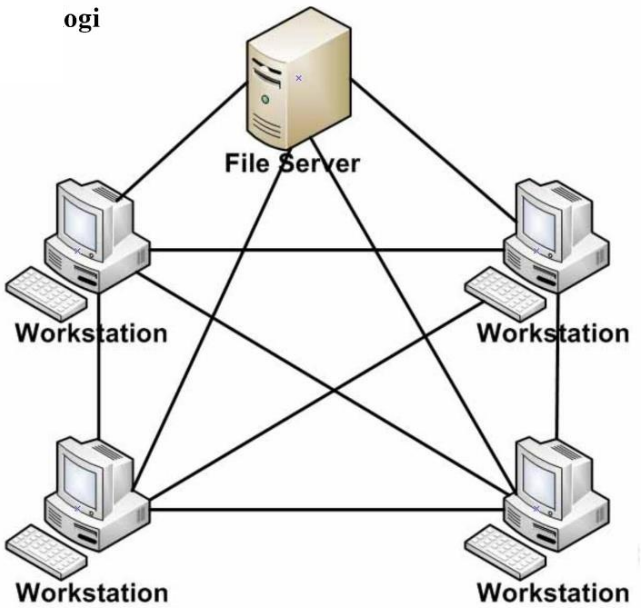
เป็นรูปแบบใหม่ ที่เกิดจากการผสมผสานกันของโทโปโลยีแบบ STAR , BUS , RING เพื่อเป็นการลดข้อเสียของรูปแบบที่กล่าวมาและเพิ่มข้อดีขึ้นมาและมักจะนำมาใช้กับระบบ WAN (Wide Area Network) ซึ่งการเชื่อมต่อกันของแต่ละรูปแบบนั้น ต้องใช้ Router เป็นตัวเชื่อมการติดต่อระหว่างกัน



ภาพที่ ๕ : โทโพโลยีแบบผสม (Hybrid Topology)

โทโปโลยีแบบเมซหรือแบบตาข่าย (Mesh Topology)

เป็นรูปแบบที่ถือว่า สามารถป้องกันการผิดพลาดที่อาจจะเกิดขึ้นกับระบบได้ดีที่สุด เป็นรูปแบบที่ใช้วิธีการเดินสายเชื่อมการติดต่อกับทุกเครื่องในระบบเครือข่าย คือ เครื่องทุกเครื่องในระบบเครือข่ายนี้ต้องมีสายไปเชื่อมกับทุก ๆ เครื่อง ระบบนี้ยากต่อการเดินสายและมีราคาแพง จึงไม่ค่อยมีผู้นิยม

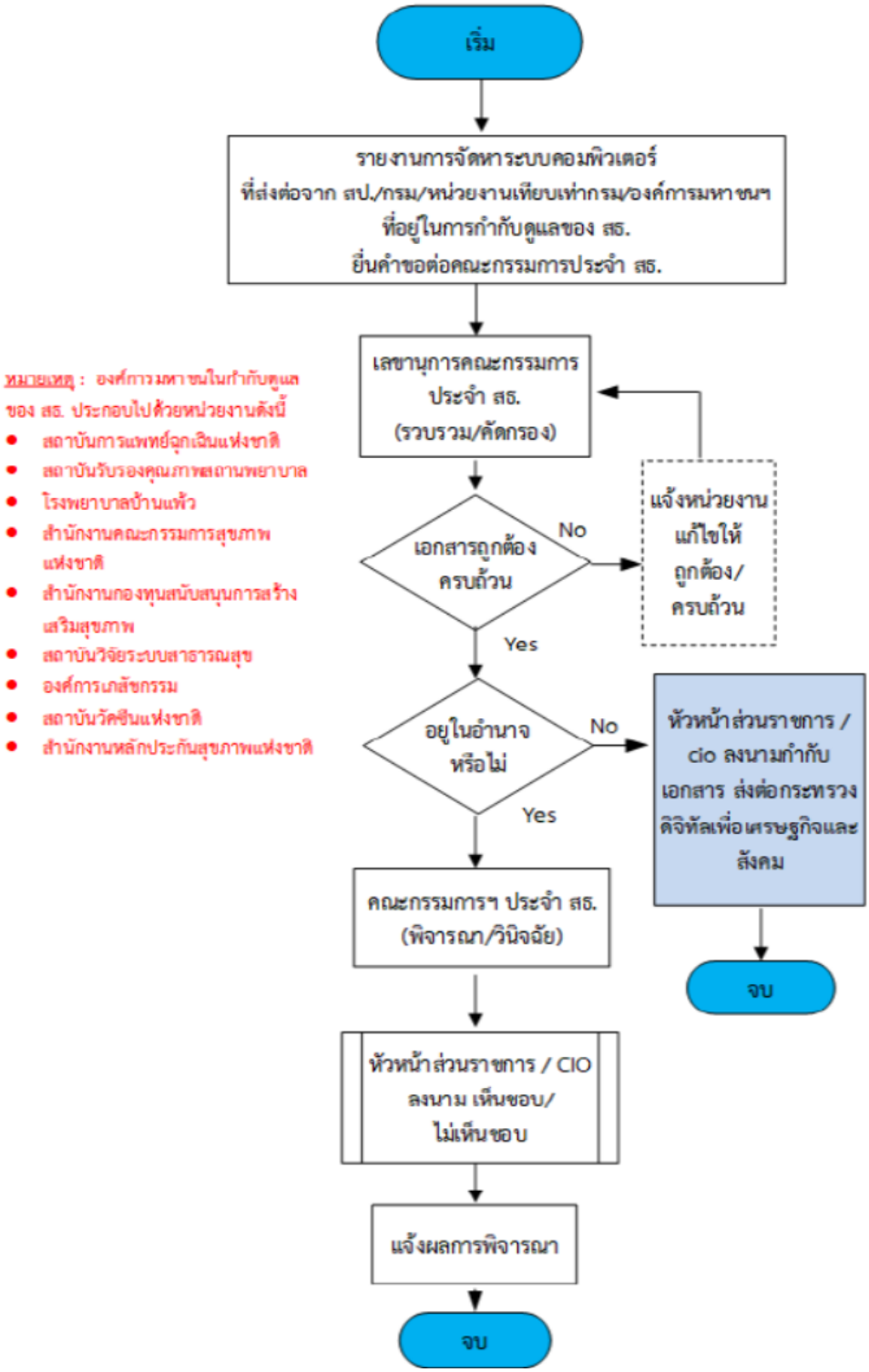


ภาพที่ ๖ : โทโปโลยีแบบเมซหรือแบบตาข่าย (Mesh Topology)

๒.๔ แนวทางการพิจารณาจัดหาครุภัณฑ์คอมพิวเตอร์[๔]

การคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ ประจำกระทรวงสาธารณสุข ได้จัดทำแนวทางการพิจารณาจัดหาครุภัณฑ์คอมพิวเตอร์ปฏิบัติของกระทรวงสาธารณสุข ภายใต้ระเบียบกระทรวงสาธารณสุข ว่าด้วยการบริหารและจัดหาระบบคอมพิวเตอร์ของกระทรวงสาธารณสุข ปี พ.ศ.๒๕๖๓ โดยมีวัตถุประสงค์เพื่อเป็นแนวทางให้แก่ คณะกรรมการในการบริหารและจัดหาระบบคอมพิวเตอร์ของกระทรวงสาธารณสุขเป็นไปในทิศทางเดียวกัน โดยมีสาระสำคัญดังนี้

๑. คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์พิจารณาเห็นชอบในหลักการ
๒. อำนาจการพิจารณาของคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์
๓. กรอบการพิจารณาครุภัณฑ์คอมพิวเตอร์ตรงเกณฑ์/ไม่ตรงเกณฑ์
๔. ประเภทครุภัณฑ์/วัสดุอุปกรณ์ ที่ใช้งานร่วมกับระบบคอมพิวเตอร์ ที่ไม่ต้องเสนอขอความเห็นชอบ ต่อคณะกรรมการฯ
๕. การจัดหาสิทธิ์การใช้งาน Hardware และ Software ที่ใช้ร่วมกับอุปกรณ์ทางการแพทย์ให้ถือเป็นครุภัณฑ์ทางการแพทย์
๖. ประเด็นสำคัญที่ต้องพิจารณา ต้องคำนึงถึงประเด็นสำคัญต่อไปนี้
   ๖.๑. ความคุ้มค่า
   ๖.๒. ความเหมาะสม
   ๖.๓. ความจำเป็น
   ๖.๔. ความซ้ำซ้อน
๗. แนวทางพิจารณารายงานการจัดหา Hardware และ Software
๘. แนวทางพิจารณาการเช่า และการซื้อบริการดิจิทัล ได้แก่
   ๘.๑. การเช่าครุภัณฑ์คอมพิวเตอร์ เช่น การเช่า Notebook, Printer เป็นต้น
   ๘.๒. การซื้อบริการดิจิทัล ประกอบด้วย
      ๘.๒.๑. การซื้อบริการดิจิทัลแบบต่อเนื่อง ที่มีผลผูกพันระยะยาว เช่น การซื้อบริการระบบ Cloud Server หรือ การซื้อบริการระบบงานบน Cloud Serve
      ๘.๒.๒. การซื้อบริการ สิทธิ์การใช้งานระบบ หรือ Software แบบจำกัดระยะเวลา เช่น Office365, Antivirus, Domain name เป็นต้น
      ๘.๒.๓. การซื้อบริการดิจิทัลที่ไม่มีผลผูกพันระยะยาว เช่น การซื้อบริการพิสูจน์ตัวตน (e-KYC) บริการ วิเคราะห์ข้อมูล โดย AI อ่านภาพ x-ray เป็นต้น ซึ่งมักจะเป็นการซื้อบริการเป็นรายครั้ง
๙. แนวทางการเสนอรายงานการจัดหาครุภัณฑ์คอมพิวเตอร์ เพื่อจัดทำคำของบประมาณรายจ่ายประจำปี (งบลงทุน: ค่าครุภัณฑ์คอมพิวเตอร์)
๑๐. ผลการพิจารณาของคณะกรรมการจัดหาฯ ไม่ผูกมัดวงเงินที่เห็นชอบในหลักการ
๑๑. แนวทางการจัดหาระบบซอฟต์แวร์ของหน่วยงาน การจัดหาระบบซอฟต์แวร์ของหน่วยงานมีข้อควรพิจารณาใน ประเด็นต่าง ๆ ดังนี้
   ๑๑.๑. กระบวนการทางพัสดุ ให้พิจารณาว่าประเภทงบประมาณ เช่น งบลงทุน งบดำเนินงาน เป็นต้น
   ๑๑.๒. กระบวนการทางนิติกรรมสัญญา
   ๑๑.๓. การอ้างสิทธิผูกพันข้อมูล
   ๑๑.๔. การปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๑๒. การรายงานผลการจัดหาหลังเสร็จสิ้นกระบวนการทางพัสดุ
๑๓. การประกาศเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์



ภาพที่ ๗ : กระบวนการจัดหาระบบคอมพิวเตอร์ของหน่วยงาน สังกัดกระทรวงสาธารณสุข

๒.๕ การดูแลความปลอดภัยในระบบเครือข่ายคอมพิวเตอร์[๕]

การใช้งานเครือข่ายแม้ว่าจะมีประโยชน์ต่อการสื่อสารข้อมูล แต่ยังคงมีความเสี่ยงหากไม่มีการควบคุมหรือการป้องกันที่ดีการโจมตีหรือบุกรุกเครือข่าย หมายถึง ความพยายามของผู้บุกรุกหรือผู้ประสงค์ร้ายที่จะเข้าใช้ระบบ (Access Attack) การแก้ไขข้อมูลหรือระบบ (Modification Attack) การทำให้ระบบไม่สามารถใช้งานได้ (Deny of Service Attack) และการบิดเบือนข้อมูล (Repudiation Attack) เพื่อลักลอบนำข้อมูลที่สำคัญหรือเข้าใช้ระบบโดยไม่ได้รับอนุญาต

๒.๕.๑ รูปแบบการโจมตีเครือข่าย

- Packet Sniffer
- IP Spoofing
- Password Attacks
- Man in the Middle
- Denial of Service
- Trojan Horse & Virus

Packet Sniffer คือ ความพยายามของผู้บุกรุกโดยการใช้โปรแกรมที่มีความสามารถในการตรวจจับ Packet ที่เคลื่อนที่อยู่บนเครือข่าย โดยฉพาะอย่างยิ่ง Packet ของข้อมูลที่ไม่มีการเข้ารหัส (Clear text) ซึ่งอาจจะนำไปสู่การโจมตีเครือข่ายในรูปแบบอื่น ๆ ต่อไป เช่น ชื่อผู้ใช้และรหัสผ่าน Packet Sniffer อาจโจมตีโดยใช้ชื่อผู้ใช้และรหัสผ่านที่ตรวจจับได้ เข้าใช้งานระบบ

IP Spoofing คือ การปลอมแปลงหมายเลข IP Address ให้เป็นหมายเลขซึ่งได้รับอนุญาตให้เข้าใช้งานเครือข่ายนั้น ๆ ได้ เพื่อบุกรุกเข้าไปขโมยหรือทำลายข้อมูล หรือกระทำการอื่น ๆ อันเป็นการโจมตีเครือข่าย เช่น การเข้าไปลบค่า Routing table ทิ้งเพื่อให้สามารถส่งข้อมูลผ่านไปยังภายนอกได้การได้มาซึ่งหมายเลข IP Address ที่ได้รับอนุญาตอาจได้มาจากการ Sniffer ดูแพคเกจข้อมูลจากหมายเลข IP ต่าง ๆ ที่วิ่งผ่านเพื่อจับสังเกตหาหมายเลข IP Address ที่คาดว่าจะเป็นไปได้หรือใช้วิธีการอื่น ๆ ที่ได้มาซึ่งหมายเลข IP Address

Password Attacks คือ ความพยายามบุกรุกเข้าสู่เครือข่ายเพื่อโจมตีเครือข่ายรูปแบบอื่น ๆ ต่อไปโดยการใช้วิธีการต่าง ๆ เพื่อให้ได้มาซึ่งรหัสผ่านสำหรับเข้าสู่เครือข่าย เช่น Packet Sniffer, IP Spoofing หรือใช้วิธีการเข้ารหัสผ่าน (Brute-Force)

Man in the Middle คือ ผู้โจมตีที่ทำตัวเป็นตัวกลาง หรือ ปลอมตัวเป็นตัวกลางระหว่างเครือข่าย เช่น ปลอมเป็นผู้ให้บริการอินเทอร์เน็ต IP ที่ทำหน้าที่ให้บริการเชื่อมโยงเครือข่ายระหว่างองค์กรเพื่อโจมตีเครือข่ายองค์กรใด ๆ โดยการอาศัยวิธีการต่าง ๆ เช่น Packet Sniffer ในการขโมยข้อมูล

Denial of Service คือ ความพยายามของผู้บุกรุกในการทำให้เครือข่าย หรือ Server นั้นไม่สามารถให้บริการได้ด้วยวิธีการต่าง ๆ เช่น การใช้ทรัพยากรของ Server จนหมด ถือเป็นการโจมตีจุดอ่อนหรือข้อจำกัดของระบบ เช่น การส่ง Packet จำนวนมากอย่างต่อเนื่องเพื่อให้ Traffic เต็ม

Trojan Horse & Virus คือ ความพยายามในการทำลายระบบโดยการส่ง Trojan horse, Worm หรือ Virus เข้าโจมตีเครือข่าย

- Trojan horse คือ โปรแกรมทำลายระบบที่แฝงมากับโปรแกรมอื่น ๆ เช่น Screen Saver

- Worm คือ โปรแกรมที่แพร่กระจายตัวเองไปยังเครื่องอื่น ๆ ในเครือข่าย
- Virus คือ โปรแกรมที่ทำลายระบบและ โปรแกรมภายในเครื่องคอมพิวเตอร์

๒.๕.๒ การรักษาความปลอดภัยของเครือข่าย

แม้ว่าการปกป้องข้อมูลเป็นสิ่งที่มีลำดับความสำคัญสูงสุด แต่การรักษาเครือข่ายให้ทำงานอย่างถูกต้องก็เป็นปัจจัยที่สำคัญในการปกป้องข้อมูลที่อยู่ในเครือข่ายนั้น ถ้ามีช่องโหว่ของระบบเครือข่ายที่อนุญาตให้โจมตีได้ ความเสียหายที่เกิดขึ้นอาจใช้ทั้งเวลาและความพยายามอย่างมากที่จะทำให้ระบบกลับมาทำงานได้เหมือนเดิม

<u>รูปแบบการรักษาความปลอดภัยของเครือข่าย</u>

๑. Firewall คือ ฮาร์ดแวร์ และซอฟต์แวร์ ที่ใช้เพื่อให้ผู้ใช้ที่อยู่ภายในสามารถใช้บริการเครือข่ายภายในได้เต็มที่และใช้บริการเครือข่ายภายนอก เช่น อินเตอร์เน็ต และ ในขณะเดียวกันจะป้องกันมิให้ผู้อื่นเข้าใช้บริการเครือข่ายที่อยู่ข้างในได้ โดยการควบคุมและกำหนดนโยบายการใช้เครือข่าย โดยขออนุญาตหรือไม่อนุญาตให้แพ็กเกจผ่านได้ Firewall แบ่งออกเป็น ๒ ประเภท คือ

๑.๑. Application Layer Firewall หรือเรียกว่า Proxy Firewall ทำหน้าที่ควบคุมและกำหนดนโยบายการใช้งาน Application ต่าง ๆ โดยทำหน้าที่เชื่อมต่อกับ Client แทน Server

๑.๒. Packet Filtering Firewall ทำหน้าที่กรองแพ็คเกจที่ผ่านเข้า - ออกเครือข่ายและอนุญาต / ไม่อนุญาตให้ผ่าน Firewall ได้ตามนโยบายที่กำหนดไว้

๒. Intrusion Detection System (IDS) เป็นเครื่องมือสำหรับการรักษาความปลอดภัยอีกประเภทหนึ่งที่ใช้สำหรับตรวจจับความพยายามที่จะบุกรุกเครือข่าย โดยระบบจะแจ้งเตือนผู้ดูแลระบบเมื่อการบุกรุกหรือพยายามที่จะบุกรุกเครือข่าย IDS ไม่ใช่ระบบป้องกันผู้บุกรุก แต่มีหน้าที่เตือนภัยในการเข้าใช้เครือข่ายที่ผิดปกติเท่านั้น ดังนั้นจะต้องมีความสามารถในการระบุได้ว่าเหตุการณ์ใดผิดปกติ และผิดปกติอย่างไร โดยส่วนใหญ่จะจำแนกประเภทความผิดปกติออกเป็น ๓ ระดับ

๒.๑. การสำรวจเครือข่าย : ความพยายามในการรวบรวมข้อมูลก่อนการ โจมตีของผู้บุกรุก เช่น การสแกนหา IP Address (IP Scans), การสแกนหาพอร์ต (Port Scans), การสแกนหาพอร์ตที่สามารถส่ง โทรจันเข้าสู่เครือข่ายได้ (Trojan Scans), การสแกนหาจุดอ่อนของระบบ (Vulnerability Scans) และการทดสอบสิทธิ์การใช้งานไฟล์ต่าง ๆ (File Snooping)

๒.๒. การโจมตี : ความพยายามในการโจมตีเครือข่าย ซึ่งควรให้ระดับความสำคัญสูงสุด เช่น การพบความผิดปกติของการส่ง packet ซ้ำ ๆ เข้าสู่เครือข่าย หรือ ลักษณะของ Packet บนเครือข่ายจากคนละผู้ส่ง แต่มี signature เดียวกัน

๒.๓. เหตุการณ์น่าสงสัยหรือผิดปกติ : เหตุการณ์อื่น ๆ ที่ผิดปกติที่ไม่ได้จัดอยู่ในประเภทต่าง ๆ

๓. Cryptography คือ การเข้ารหัสข้อมูลเพื่อป้องกันการดักดูข้อมูลจาก Sniffer โดยปัจจุบันการเข้ารหัสข้อมูลจะแบ่งออกเป็น ๒ ประเภทคือ

- Symmetric Key Cryptography
- Public Key

๔. Authorized คือ การพิสูจน์ตัวตนบนเครือข่าย เป็นการระบุถึงผู้ส่งและผู้รับข้อมูลบนเครือข่ายว่าเป็นตัวจริงหรือไม่ โดยมีวิธีการ ๒ วิธีคือ

๔.๑. Digital Signature คือ ลายเซ็นอิเล็กทรอนิกส์ที่ลงท้ายไปกับข้อมูลที่ส่งไปบนเครือข่าย โดยขึ้นอยู่กับนโยบายการใช้งานของแต่ละเครือข่ายดังนั้น Digital Signature อาจเป็นรหัสผ่าน ลายนิ้วมือหรือ Private Key เป็นต้น

๔.๒. Certificate Authority คือ หน่วยงานหรือองค์กรที่ตั้งขึ้นเพื่อรับรองสิทธิการเข้าถึงเครือข่ายและข้อมูลบนเครือข่ายของทั้งผู้ให้บริการและผู้ใช้บริการ ซึ่งจะเกี่ยวข้องกับธุรกรรมต่าง ๆ บนเครือข่ายอินเตอร์เน็ต

๕. Secure Socket Layer คือ เทคโนโลยีที่พัฒนาขึ้นเพื่อความปลอดภัยในการทำธุรกรรมต่าง ๆ ผ่านเครือข่าย โดยเฉพาะอย่างยิ่งเครือข่ายอินเตอร์เน็ตถือเป็นโปรโตคอลตัวหนึ่งและมีหน้าที่หลัก ๆ คือ

๕.๑. Server Authentication คือการพิสูจน์ตัวตนของผู้ให้บริการ โดยติดต่อกับ CA : Certificate Authority เพื่อตรวจสอบความมีอยู่จริง

๕.๒. Client Authentication คือ ผู้ให้บริการติดต่อกับใครอยู่หรือข้อมูลที่เกี่ยวข้องสามารถพิสูจน์ตัวตนได้จริง

๕.๓. Encrypted Session คือการเข้ารหัสข้อมูล ที่อยู่ในระหว่างการทำธุรกรรมครั้งนั้น ๆ

๖. Virtual Private Network คือ เครือข่ายส่วนบุคคลเสมือนหรืออุโมงค์ข้อมูลที่ทำงานอยู่บนเครือข่ายสาธารณะ สามารถแบ่งออกตามลักษณะการใช้งานได้ ๓ ประเภท

๖.๑. Access VPN คือ VPN สำหรับผู้ที่เชื่อมต่อระยะไกล

๖.๒. Intranet VPN คือ VPN ที่ใช้ส่งข้อมูลที่เป็นความลับระหว่างบุคคล หรือหน่วยงานภายในองค์กร

๖.๓. Extranet VPN คือ VPN ที่ใช้ในการเชื่อมโยงข้อมูลสำคัญระหว่างองค์กร

๒.๖ งานวิจัยที่เกี่ยวข้อง

ณัฏฐ์ณพัชร์ อ่อนตาม(อ้างถึงใน เรืองวิทย์ เกษสุวรรณ)[๖] กล่าวว่า ประวัติของเดมมิ่งว่าเป็นที่รู้จักกันแพร่หลายในหลักการบริหารที่เรียกว่า วงจรคุณภาพ (PDCA) หรือ วงจรเดมมิ่ง ซึ่งเป็นชื่อที่ใช้แทนกันกับการจัดการคุณภาพ เขาเป็นคนผลักดันให้ผู้บริหารญี่ปุ่นยอมรับแนวคิด ในการจัดการคุณภาพ และเป็นคนแรกที่มองว่าการจัดการคุณภาพเป็นกิจกรรมขององค์กรทั้งหมด ไม่ใช่แค่งานตรวจคุณภาพตามที่กำหนดหรือเป็นงานของกลุ่มใดกลุ่มหนึ่ง และเป็นคนแรกที่ระบุว่าคุณภาพเป็นความรับผิดชอบทางการบริหารของผู้บริหารวงล้อเดมมิ่งถูกพัฒนาขึ้นโดย ดร. ชิวฮาร์ท นักวิทยาศาสตร์ชาวอเมริกัน ซึ่งต่อมา ดร. เดมมิ่งได้นำไปเผยแพร่ที่ประเทศญี่ปุ่นจนประสบความสำเร็จและเป็นที่รู้จักกันอย่างแพร่หลาย โดยมีกิจกรรมที่เกี่ยวข้อง ๔ ขั้นตอน คือ PDCA (Plan, Do, Check and Act) ที่เป็นกิจกรรมพื้นฐานในการพัฒนาประสิทธิภาพและคุณภาพในการดำเนินงานขององค์กร

สุขสันต์ สุขสงคราม[๗] กล่าวว่า หลักการของวงจรคุณภาพ (PDCA) เดมมิ่ง (Deming in Mycoted, 2004) กล่าวว่า การจัดการอย่างมีคุณภาพเพื่อให้เกิดผลผลิตและบริการที่มีคุณภาพขึ้น โดยหลักการที่เรียกว่าวงจรคุณภาพ (PDCA) หรือวงจรเดมมิ่ง ซึ่งประกอบด้วย 4 ขั้นตอน คือ การวางแผน การปฏิบัติตามแผน การตรวจสอบ และการปรับปรุงแก้ไขดังนี้

๑) Plan คือ กำหนดสาเหตุของปัญหา จากนั้นวางแผนเพื่อการเปลี่ยนแปลงหรือทดสอบเพื่อการปรับปรุงให้ดีขึ้น

๒) Do คือ การปฏิบัติตามแผนหรือทดลองปฏิบัติเป็นการนำร่อง
๓) Check คือ ตรวจสอบเพื่อทราบว่าบรรลุผลตามแผนหรือหากมีสิ่งใดที่ทำผิดพลาดหรือได้เรียนรู้อะไรมาแล้วบ้าง
4) Act คือ ยอมรับการเปลี่ยนแปลง หากบรรลุผลเป็นที่น่าพอใจหรือหากผลการปฏิบัติไม่เป็นไปตามแผน ให้ทำซ้ำวงจรโดยใช้การเรียนรู้จากการกระทำในวงจรที่ได้ปฏิบัติไปแล้ว

พีรพันธ์ รุจิพงษ์กุล และ เกียรติศักดิ์ โยชะนัง (๒๕๕๙)[๓] การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ ๑) ศึกษาแนวโน้มของระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ ภายในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ๒) วิเคราะห์หาแนวทางของระบบรักษาความปลอดภัยบนระบบ เครือข่ายคอมพิวเตอร์ภายใน มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ โดยแบ่งออกเป็น ๕ ด้าน คือ ด้านนโยบาย ด้านฮาร์ดแวร์ ด้านซอฟต์แวร์ ด้านบุคลากร และด้านกระบวนการ กลุ่มตัวอย่างที่ใช้ในการวิจัย ประกอบด้วยผู้บริหาร จำนวน ๑๐ คน ผู้เชี่ยวชาญและผู้ปฏิบัติงานด้านการรักษาความปลอดภัยของระบบเครือข่าย คอมพิวเตอร์ ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ จำนวน ๓๐ คน รวม ๔๐ คน เครื่องมือที่ใช้ในการเก็บ รวบรวมข้อมูล เป็นแบบสอบถาม จำนวน ๓ รอบ สถิติที่ใช้ ได้แก่ ค่ามัธยฐาน ค่าฐานนิยม และค่าพิสัยระหว่างควอไทล์ ผลการวิจัยพบว่าระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้า พระนครเหนือ ฮาร์ดแวร์และซอฟแวร์ต้องมีประสิทธิภาพสูง มีมาตรฐาน ราคาต้องคุ้มค่า มีการกำหนดนโยบายที่ชัดเจน เป็นลายลักษณ์อักษรพร้อมบทลงโทษ บุคลากรต้องมีความรู้ความสามารถมีการฝึกอบรมอยู่เสมอ มีกระบวนการทำงาน ที่เป็นขั้นตอน ชัดเจน พร้อมจัดทำคู่มือและขั้นตอนการปฏิบัติงานให้ทันสมัยอยู่เสมอ

วารสาร มจร อุบลปริทรรศน์ มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย (2560)[๔] การพัฒนาระบบบริหารจัดการรักษาความปลอดภัย ของระบบเครือข่ายสารสนเทศภาครัฐ โดยการวิจัยครั้งนี้มีวัตถุประสงค์ ดังนี้ ๑) เพื่อหาแนวทางในการบริหารจัดการการป้องกันภัยคุกคาม ระบบเครือข่ายสารสนเทศภาครัฐ ๒) เพื่อพัฒนาระบบบริหารจัดการรักษาความปลอดภัยของระบบเครือข่าย สารสนเทศภาครัฐ ประชากรและกลุ่มตัวอย่างเป็นบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏชัยภูมิที่มาใช้ บริการอินเทอร์เน็ตบริเวณลานพวงชมพู อาคารศูนย์ภาษาและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏชัยภูมิ จำนวน ๓๐ คน เครื่องมือที่ใช้ในการวิจัยไฟร์วอลล์โอเพ้นซอร์สพีเอฟเซนต์และแบบสอบถามเพื่อวัด ความพึงพอใจ สถิติที่ใช้ในงานวิจัยได้แก่จำนวน ร้อยละ ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ผลการวิจัยมี ดังนี้ ส่วนใหญ่ผู้ใช้เครือข่ายสารสนเทศเป็นนักศึกษาเพศหญิง ช่วงอายุ ๒๐-๓๐ ปี มีวัตถุประสงค์เพื่อเช็ค Mail /Chat ความถี่ที่ใช้งานจะอยู่ที่ ๕ วันต่อสัปดาห์ ความเร็วที่ใช้เครือข่ายอยู่ในระดับเร็ว มีความพึงพอใจใน ภาพรวมต่อการพัฒนาระบบบริหารจัดการรักษาความปลอดภัยของระบบเครือข่ายสารสนเทศภาครัฐ อยู่ใน ระดับมาก (X= 4.27, S.D. = 0.68)

บทที่ ๓
วิธีการดำเนินงาน

วิธีการดำเนินงานในการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์อาคารศูนย์การแพทย์บางรัก มีองค์ประกอบดังนี้

๓.๑ รูปแบบการดำเนินงาน
๓.๒ ขั้นตอนการดำเนินงาน
๓.๓ การบำรุงรักษาอุปกรณ์เครือข่ายคอมพิวเตอร์

สามารถอธิบายวิธีการดำเนินงานได้ดังนี้

๓.๑ รูปแบบการดำเนินงาน

การดำเนินงานการพัฒนาการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ขององค์กร โดยศึกษากระบวนการทำงานจากระบบเครือข่ายคอมพิวเตอร์ของอาคารศูนย์การแพทย์บางรัก กรมควบคุมโรค เพื่อพัฒนาการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ให้มีประสิทธิภาพมากยิ่งขึ้น ตามวงจรคุณภาพ PDCA ด้วยการศึกษาเอกสารงานวิจัยที่เกี่ยวข้อง แล้วสังเคราะห์องค์ความรู้เพื่อสร้างเป็นแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรต่อไป

๓.๒ ขั้นตอนการดำเนินงาน

ขั้นตอนการดำเนินงานด้านการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ของอาคารศูนย์การแพทย์บางรัก กรมควบคุมโรคได้ มีขั้นตอนดังนี้

๓.๒.๑ การวางแผนและการวิเคราะห์ความต้องการของระบบเครือข่ายในองค์กร ขั้นตอนและข้อควรระวังที่สำคัญสำหรับการวางแผนและการวิเคราะห์ความต้องการของระบบเครือข่าย ได้แก่

๑) สำรวจและวิเคราะห์ความต้องการ ให้การสำรวจและวิเคราะห์ความต้องการขององค์กรเพื่อเข้าใจความต้องการที่แท้จริง เช่น จำนวนผู้ใช้งาน การใช้งานแอปพลิเคชัน ความต้องการในเรื่องของความปลอดภัยและความเสถียรของการใช้งานระบบเครือข่าย
๒) กำหนดขอบเขตของระบบเครือข่ายโดยรวม รวมถึงการกำหนดเส้นทางการเชื่อมต่อ การระบุความจำเป็นของการสนับสนุนเทคโนโลยี และบริการอื่น ๆ ที่เกี่ยวข้องกับการปฏิบัติงานของเจ้าหน้าที่ในองค์กร
๓) วางแผนการปรับปรุงหรือการเปลี่ยนแปลงของระบบเครือข่ายโดยใช้ข้อมูลที่เกี่ยวข้อง เช่น การเปลี่ยนแปลงโครงสร้างระบบเครือข่าย การอัพเกรดฮาร์ดแวร์หรือซอฟต์แวร์ หรือการเปลี่ยนแปลงการตั้งค่าและการทดสอบใหม่
๔) วิเคราะห์และวางแผนความปลอดภัย การให้ความสำคัญกับการวิเคราะห์และวางแผนเรื่องความปลอดภัยของระบบเครือข่าย รวมถึงการกำหนดมาตรการความปลอดภัย การประเมินความเสี่ยงกับสถานการณ์

๕) กำหนดและการจัดสรรทรัพยากรที่เกี่ยวข้องกับระบบเครือข่าย รวมถึงการกำหนดงบประมาณที่เหมาะสม และการจัดการเทคโนโลยีและอุปกรณ์เครือข่าย

๖) วางแผนและการวิเคราะห์การดำเนินงานเพื่อให้ระบบเครือข่ายมีประสิทธิภาพและมีความเสถียร รวมถึงการกำหนดวิธีการตรวจสอบและวิเคราะห์ประสิทธิภาพของระบบ

๓.๒.๒ การสำรวจอุปกรณ์เครือข่ายในองค์กร และพื้นที่สำหรับใช้ในการติดตั้ง เพื่อเพิ่มประสิทธิภาพของระบบเครือข่ายในองค์กรและเป็นกระบวนการที่สำคัญในการดูแลและบริหารจัดการเครือข่ายคอมพิวเตอร์ให้มีประสิทธิภาพและปลอดภัย มีขั้นตอนและวัตถุประสงค์ในการดำเนินงานดังนี้

๑) การสำรวจอุปกรณ์เครือข่าย

วัตถุประสงค์

- การระบุปัญหาที่เกิดขึ้นในเครือข่าย เช่น ปัญหาในประสิทธิภาพการทำงาน ปัญหาในความปลอดภัย หรือปัญหาการปรับปรุงแก้ไขเครือข่ายให้มีประสิทธิภาพมากขึ้น
- การปรับปรุงแก้ไขปัญหาที่พบ เพื่อให้เครือข่ายสามารถทำงานได้ดียิ่งขึ้น และมีการประสิทธิภาพสูงขึ้น
- เพิ่มความปลอดภัยในระบบ เช่น การตรวจสอบช่องโหว่ในระบบ การตรวจสอบการเข้าถึงที่มีอันตราย หรือการตรวจสอบการปฏิบัติตามนโยบายความปลอดภัยขององค์กร

ขั้นตอนการสำรวจ

- การเก็บรวบรวมข้อมูลเกี่ยวกับเครือข่าย เช่น โครงสร้างของเครือข่าย การกำหนด IP addressการใช้งานของบริการและ แอปพลิเคชันต่าง ๆ และข้อมูลที่เกี่ยวข้องกับความปลอดภัย
- การสำรวจเครือข่ายเพื่อตรวจสอบเครื่องมือและเครื่องมือที่ใช้งานอยู่บนเครือข่าย รวมถึงการตรวจสอบรูปแบบการเชื่อมต่อและแพ็กเก็ตที่ถูกส่งไปยังและจากเครือข่าย
- การวิเคราะห์ข้อมูลที่เก็บรวบรวมและตรวจสอบ เพื่อระบุปัญหาและความเสี่ยงที่อาจเกิดขึ้นในเครือข่าย
- การรายงานผลการสำรวจ รวมถึงการแนะนำแนวทางในการแก้ไขปัญหาและเพิ่มประสิทธิภาพของเครือข่าย

๒) การสำรวจพื้นที่ในการติดตั้งอุปกรณ์ ประกอบด้วย

วัตถุประสงค์ของการสำรวจ

- การระบุพื้นที่ที่เหมาะสมสำหรับติดตั้งอุปกรณ์เครือข่าย
- การตรวจสอบความพร้อมทางพื้นที่ เช่น การตรวจสอบการเชื่อมต่อระบบไฟฟ้า การเชื่อมต่อเครือข่าย เป็นต้น

- การประเมินความต้องการในการใช้งาน เช่น การตรวจสอบว่าต้องการการเชื่อมต่อ WiFi การเชื่อมต่อแบบไร้สาย หรือการใช้งานที่ต้องการความเร็วในการส่งข้อมูลเพื่อกำหนดพื้นที่ที่เหมาะสม
- การตรวจสอบโครงสร้างพื้นที่
  - การตรวจสอบโครงสร้างและขนาดของพื้นที่ เพื่อให้มีพื้นที่ที่เหมาะสมสำหรับติดตั้งอุปกรณ์เครือข่าย
  - การตรวจสอบความเหมาะสมของสิ่งก่อสร้าง เช่น ระบบระบายน้ำ ระบบระบายอากาศ และระบบไฟฟ้า
- การตรวจสอบความปลอดภัยของพื้นที่ เช่น การตรวจสอบความปลอดภัยจากภัยธรรมชาติ การป้องกันการเข้าถึงที่ไม่พึงประสงค์ และการตรวจสอบความปลอดภัยกับการเข้าถึงที่เกี่ยวข้องกับเครือข่าย
- การวางแผนการติดตั้ง
  - การวางแผนการติดตั้งอุปกรณ์เครือข่ายโดยพิจารณาความต้องการและโครงสร้างของพื้นที่
  - การกำหนดตำแหน่งที่ติดตั้งอุปกรณ์เครือข่ายให้เหมาะสมเพื่อความสะดวกในการบริหารจัดการและการบำรุงรักษา

การจัดทำแผนการติดตั้งอุปกรณ์เครือข่าย

ตารางที่ ๑ แผนการดำเนินงานการติดตั้งอุปกรณ์เครือข่ายคอมพิวเตอร์อาคารศูนย์การแพทย์บางรัก

แผนการดำเนินงานการติดตั้งอุปกรณ์เครือข่ายคอมพิวเตอร์อาคารศูนย์การแพทย์บางรัก

รายการ	พ.ศ. 2565			พ.ศ. 2566						ผลการดำเนินงาน	หมายเหตุ
	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.		
1. การเตรียมสถานที่สำหรับการติดตั้งอุปกรณ์											
1.1 สำรวจพื้นที่สำหรับติดตั้งตู้เก็บอุปกรณ์ ชั้น 12 และชั้น 13			→								
1.2 สำรวจจุดติดตั้งอุปกรณ์ Access Point				→							
1.3 สำรวจระบบไฟฟ้าเพื่อรองรับการใช้งานกับอุปกรณ์เครือข่ายคอมพิวเตอร์				→							
1.4 สำรวจอุปกรณ์อุปกรณ์เครือข่ายและอุปกรณ์ที่เกี่ยวข้อง ที่มีอยู่เดิม				→							
1.5 ประชาสัมพันธ์การปิดระบบเครือข่ายของอาคารให้กับเจ้าหน้าที่					→						
2. การติดตั้งอุปกรณ์											
2.1 เครื่องคอมพิวเตอร์แม่ข่าย					→						
2.2 อุปกรณ์กระจายสัญญาณไร้สาย (Access Point)						→					
2.3 อุปกรณ์กระจายสัญญาณ (L2 Switch) ขนาด 24 ช่อง						→					
2.4 อุปกรณ์กระจายการทางานสำหรับเครือข่าย (Link Load Balancer)						→					
2.5 อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall)					→						
2.6 อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System)						→					
2.7 อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย					→						
2.8 อุปกรณ์กระจายสัญญาณ (L3 Switch) ขนาด 24 ช่อง						→					
2.9 อุปกรณ์ควบคุมเครือข่ายไร้สาย (Access Point Controller)						→					
2.10 อุปกรณ์วิเคราะห์การจราจรบนเครือข่าย (Log Analyzer)						→					
2.11 เครื่องสำรองไฟฟ้าขนาด 40 KVA					→						
2.12 โปรแกรมแม่ข่ายเสมือน (VMware)					→						
2.13 อุปกรณ์สำหรับจัดเก็บข้อมูลแบบภายนอก (External Storage)					→						
2.14 การออกแบบและติดตั้งอุปกรณ์เครือข่าย						→					
3. การ Config อุปกรณ์											
3.1 การ Config อุปกรณ์เน็ตเวิร์ค และอุปกรณ์อื่น ๆ						→					
4. การทดสอบระบบ											
4.1 การทดสอบการทำงานของอุปกรณ์					→	→					

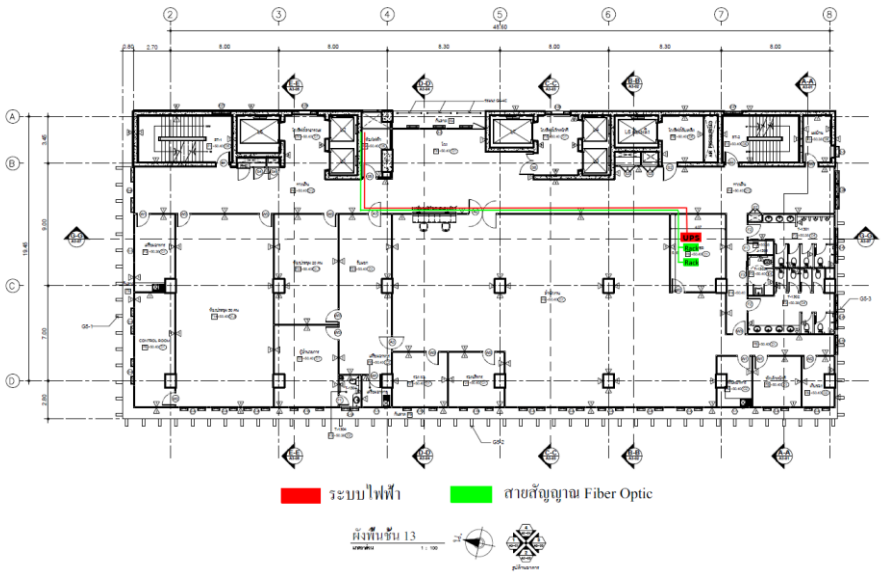
การเคลื่อนย้ายอุปกรณ์

เคลื่อนย้ายตู้จัดเก็บอุปกรณ์เครือข่ายเดิม และเครื่องคอมพิวเตอร์แม่ข่ายไปติดตั้งบริเวณห้อง Server ชั้น ๑๓ ที่ได้มีการปรับปรุงห้องสำหรับติดตั้งอุปกรณ์เครือข่ายของอาคาร เพื่อความสะดวกในการบริหารจัดการและการดูแลรักษาอุปกรณ์เครือข่าย

ภาพที่ ๘ : ปรับปรุงเคลื่อนย้ายอุปกรณ์ห้อง Server

การเดินสายสัญญาณเครือข่ายคอมพิวเตอร์

เดินสายสัญญาณเครือข่าย Fiber Optic ระหว่างชั้น ๑๒ และชั้น ๑๓ เนื่องจากบริเวณห้องติดตั้งอุปกรณ์เครือข่ายเดิมชั้น ๑๒ มีพื้นที่ไม่เหมาะสมสำหรับการติดตั้งอุปกรณ์เครือข่ายใหม่ ด้วยมีพื้นที่จำกัดและขาดอุปกรณ์ดูแลความปลอดภัย เช่น ระบบดับเพลิง เครื่องปรับอากาศ และอุปกรณ์ดูดความชื้น เพื่อให้เกิดความเหมาะสมจึงจำเป็นต้องนำอุปกรณ์เครือข่ายที่จัดหาใหม่ไปติดตั้ง ณ บริเวณพื้นที่ที่จัดเตรียมไว้สำหรับติดตั้งอุปกรณ์เครือข่าย ชั้น ๑๓ โดยการเดินสายสัญญาณ Fiber Optic จากชั้น ๑๒ ไปยัง ชั้น ๑๓ เพิ่มเติมนั้น เพื่อเชื่อมต่อกับ Core Switch ที่มีการเชื่อมต่อกับอุปกรณ์กระจายสัญญาณแต่ละชั้นภายในอาคาร ระบบกล้องวงจรปิด (CCTV) และระบบโทรศัพท์ IP Phone ให้สามารถใช้งานร่วมกับอุปกรณ์เครือข่ายที่ติดตั้งใหม่ได้ปกติ อีกทั้งยังสามารถลดค่าใช้จ่ายในการเดินสายสัญญาณใหม่ทั้งระบบ



ภาพที่ ๙ : แบบเดินสายสัญญาณ Fiber Optic ระหว่างห้อง Server ชั้น ๑๒ และชั้น ๑๓

แผงกระจายไฟเบอร์ ชั้น ๑๒ แผงกระจายไฟเบอร์ ชั้น ๑๓

ภาพที่ ๑๐ : แผงกระจาย Fiber Optic ห้อง Server ชั้น ๑๒ และชั้น ๑๓

๓.๒.๓ การจัดหาระบบคอมพิวเตอร์ เป็นกระบวนการที่สำคัญในการสร้างและบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ให้มีประสิทธิภาพและสอดคล้องกับความต้องการขององค์กรหรือผู้ใช้งาน โดยใช้เกณฑ์ราคากลางและคุณลักษณะพื้นฐานการจัดหาอุปกรณ์และระบบคอมพิวเตอร์ ฉบับเดือน ธันวาคม ๒๕๖๔ เป็นเกณฑ์ในการจัดหาระบบคอมพิวเตอร์[๘] มีขั้นตอนการจัดหาระบบคอมพิวเตอร์ ดังนี้

(๑) การสำรวจความต้องการใช้งานระบบเครือข่ายคอมพิวเตอร์ขององค์กรเพื่อดำเนินการจัดทำคำของบประมาณรายจ่ายประจำปี

(๒) จัดทำโครงการเพื่อขออนุมัติดำเนินการจัดทำคำขอครุภัณฑ์คอมพิวเตอร์ตามแผนงาน/โครงการ/กิจกรรมที่กำหนดไว้

(๓) จัดทำรายงานการจัดห่าระบบคอมพิวเตอร์ในภาพรวมของกองโรคเอดส์และโรคติดต่อทางเพศสัมพันธ์

(๔) ตรวจสอบรายการและจัดทำรายงานจัดหาครุภัณฑ์คอมพิวเตอร์ตามแบบฟอร์มที่เกี่ยวข้องในการจัดทำรายงานการจัดหาระบบคอมพิวเตอร์ทั้งหมด

(๕) จัดทำหนังสือนำส่งเสนอหัวหน้ากลุ่มบริหารทั่วไปลงนาม

(๖) จัดทำหนังสือส่งเสนอต่อผู้อำนวยการกองโรคเอดส์และโรคติดต่อทางเพศสัมพันธ์ และกองดิจิทัลเพื่อการควบคุมโรค กรมควบคุมโรค

(๗) เลขาคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ประจำกรมควบคุมโรค กองดิจิทัลเพื่อการควบคุมโรค ตรวจสอบความถูกต้องของรายงานการจัดหาระบบคอมพิวเตอร์

(๘) คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ประจำกรมควบคุมโรค กองดิจิทัลเพื่อการควบคุมโรค พิจารณาให้ความเห็นชอบและอนุมัติ

(๙) เลขาคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ประจำกรมควบคุมโรค กองดิจิทัลเพื่อการควบคุมโรค ทำหนังสือส่งต่อไปยังผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข

(๑๐) คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ประจำกระทรวงสาธารณสุข พิจารณาให้ความเห็นและอนุมัติ ทำหนังสือแจ้งผลการอนุมัติไปยังคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ประจำกรมควบคุมโรค กองดิจิทัลเพื่อการควบคุมโรค

(๑๑) เลขาคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ประจำกรมควบคุมโรค กองดิจิทัลเพื่อการควบคุมโรค ทำหนังสือแจ้งผลรายงานการจัดหาระบบคอมพิวเตอร์ ที่ผ่านการอนุมัติไปยังกองโรคเอดส์และโรคติดต่อทางเพศสัมพันธ์

(๑๒) กองโรคเอดส์และโรคติดต่อทางเพศสัมพันธ์ รับหนังสือแจ้งผลรายงานการจัดหาระบบคอมพิวเตอร์ และผลการอนุมัติฉบับจริง และส่งหนังสือไปยังกลุ่มงานที่เกี่ยวข้องคือ กลุ่มบริหารทั่วไป (งานสารสนเทศ งานพัสดุและยานพาหนะ และงานการเงินและบัญชี) ศูนย์อำนวยการบริหารจัดการปัญหาเอดส์แห่งชาติ (งานยุทธศาสตร์และแผนงาน) โดยส่งเอกสารฉบับจริงให้กับกลุ่มบริหารทั่วไป

(๑๓) กลุ่มบริหารทั่วไป ดำเนินการโดยงานสารสนเทศ รับหนังสือรายงานฉบับจริง และทำการสอบทานกับกลุ่มงานที่เกี่ยวข้องว่าได้รับเอกสารแจ้งผลรายงานการจัดหาระบบคอมพิวเตอร์หรือไม่ หากไม่ทราบแจ้งเวียนไฟล์เอกสารส่งให้ผู้เกี่ยวข้องทราบอีกครั้ง

(๑๔) งานพัสดุและยานพาหนะ กลุ่มบริหารทั่วไป ประสานแจ้งกลุ่มที่เกี่ยวข้องจัดทำขออนุมัติหลักการจัดซื้อจัดจ้างครุภัณฑ์คอมพิวเตอร์

(๑๕) จัดทำหนังสืออนุมัติในหลักการจัดซื้อจัดจ้างครุภัณฑ์คอมพิวเตอร์ นำเสนอผู้อำนวยการกองโรคเอดส์และโรคติดต่อทางเพศสัมพันธ์ พิจารณาเห็นชอบ

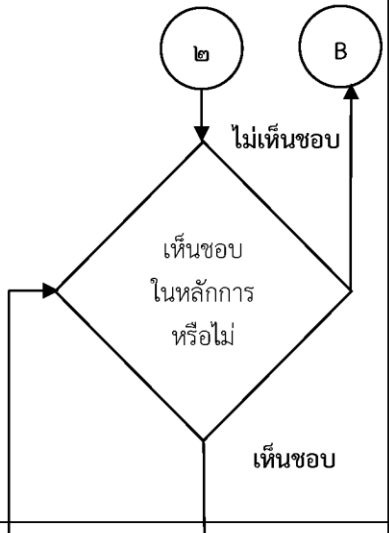
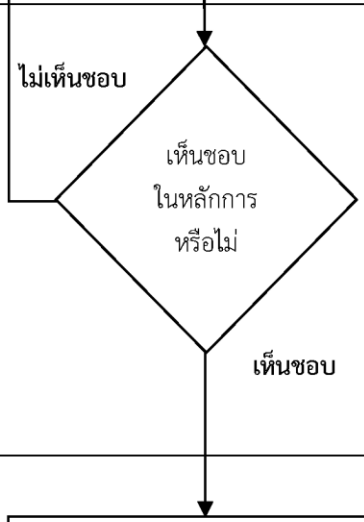
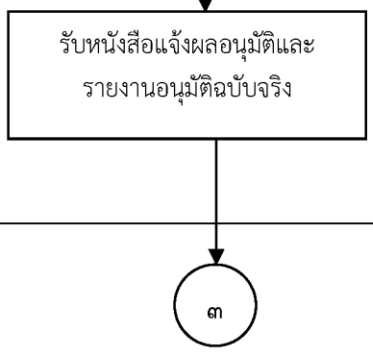
(๑๖) ดำเนินการจัดซื้อจัดจ้างตามระเบียบพัสดุและหนังสือขออนุมัติแต่งตั้งคณะกรรมการกำหนดคุณลักษณะเฉพาะและราคากลาง

(๑๗) กองดิจิทัลเพื่อการควบคุมโรค รับรายงานผลการจัดซื้อจัดหาระบบคอมพิวเตอร์ของกองโรคเอดส์และโรคติดต่อทางเพศสัมพันธ์

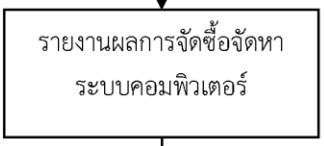
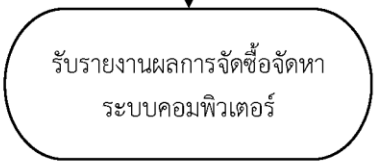
ขั้นตอนการปฏิบัติกระบวนการจัดซื้อ/จัดทำคำขอครุภัณฑ์คอมพิวเตอร์

ผู้รับผิดชอบ	ขั้นตอนการปฏิบัติงาน	ระยะเวลา	เอกสารที่เกี่ยวข้อง
งานยุทธศาสตร์และแผนงาน ศบ.จอ ของ กองโรคเอดส์ฯ กรมควบคุมโรค	แจ้งเวียนรายการจัดทำคำขอครุภัณฑ์คอมพิวเตอร์	๑ วัน	แบบคำของบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ..... งบลงทุน:ค่าครุภัณฑ์คอมพิวเตอร์
กลุ่ม/ศูนย์ กองโรคเอดส์ฯ กรมควบคุมโรค	จัดทำคำขอรายการครุภัณฑ์คอมพิวเตอร์ส่งกลุ่มยุทธศาสตร์	๗ วัน	๑.แบบคำของบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ..... งบลงทุน:ค่าครุภัณฑ์คอมพิวเตอร์ของกลุ่ม/ศูนย์..... ๒.ใบเสนอราคากรณีไม่ตรงกับรายการมาตรฐานกลาง
งานสารสนเทศ กลุ่มบริหารทั่วไป กองโรคเอดส์ฯ กรมควบคุมโรค	ตรวจสอบรายการคำขอมีแก้ไข **แก้ไข**	๗ วัน	๑.แบบคำของบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ..... งบลงทุน:ค่าครุภัณฑ์คอมพิวเตอร์ของกลุ่ม/ศูนย์..... ๒.แบบคำของบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ..... งบลงทุน:ค่าครุภัณฑ์คอมพิวเตอร์ของกองโรคเอดส์ฯ ๓.ใบเสนอราคากรณีไม่ตรงกับรายการมาตรฐานกลาง
งานสารสนเทศ กลุ่มบริหารทั่วไป กองโรคเอดส์ฯ กรมควบคุมโรค	**ไม่แก้ไข** A จัดทำรายงานจัดหาคอมพิวเตอร์ ๑	๕ วัน	๑.แบบคำของบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ..... งบลงทุน:ค่าครุภัณฑ์คอมพิวเตอร์ของ กองโรคเอดส์ฯ ๒.แบบสำรวจจำนวนครุภัณฑ์คอมพิวเตอร์ทั้งหมด ๓.แบบสำรวจความต้องการเพิ่มเติมครุภัณฑ์คอมพิวเตอร์ ๔.แบบฟอร์มรายงานการจัดหาระบบคอมพิวเตอร์ภาครัฐที่มีมูลค่าเกิน หรือไม่เกิน ๕ ล้านบาท ๕.แบบฟอร์มสรุปรายงานการจัดหาระบบคอมพิวเตอร์ไม่ตรงเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ผู้รับผิดชอบ	ขั้นตอนการปฏิบัติงาน	ระยะเวลา	เอกสารที่เกี่ยวข้อง
A	๑		๖.เอกสารแนบประกอบการพิจารณาจำนวนบุคลากร (คน) ๗.เอกสารแนบประกอบการพิจารณาครุภัณฑ์คอมพิวเตอร์ภายในหน่วยงาน ๘.แบบบัญชีราคากลางงานพัฒนาระบบประเภทโปรแกรมประยุกต์ (Application Software Development) ๙.แบบฟอร์มแนวคิดของโครงการการพัฒนาระบบ Application and Digital Solution
งานสารสนเทศ กลุ่มบริหารทั่วไป	เสนอหัวหน้ากลุ่มบริหารทั่วไป ลงนาม	๑ วัน	๑.หนังสือนำส่งรายงานจัดหาคอมพิวเตอร์ของกองโรคเอดส์ฯ ๒.สรุปรายงานจัดหาคอมพิวเตอร์ ที่มีลายเซ็นหัวหน้ากลุ่มพัฒนานวัตกรรมวิจัย และดิจิทัล ลงนามตามเอกสารที่เกี่ยวข้อง ๑ - ๘
งานธุรการ กองโรคเอดส์ฯ	เสนอ ผอ.กองโรคเอดส์ฯ ลงนาม	๓ วัน	๑.หนังสือนำส่งรายงานจัดหาคอมพิวเตอร์ของกองโรคเอดส์ ๒.สรุปรายงานจัดหาคอมพิวเตอร์ ที่มีลายเซ็นหัวหน้ากลุ่มบริหารทั่วไป และผู้อำนวยการกองโรคเอดส์ฯ ลงนามตามเอกสารที่เกี่ยวข้อง ๑ - ๘
งานธุรการ กองโรคเอดส์ฯ กรมควบคุมโรค	รับ - ส่ง หนังสือรายงานจัดหาฯ	๑ วัน	๑.หนังสือนำส่งรายงานจัดหาคอมพิวเตอร์ของกองโรคเอดส์ฯ ที่ลงนามแล้ว
กองดิจิทัลเพื่อการควบคุมโรค	ตรวจรายงานจัดหาคอมพิวเตอร์ถูกต้องหรือไม่ B ไม่ถูกต้อง ถูกต้อง	๗ วัน	๑.หนังสือนำส่งรายงานจัดหาคอมพิวเตอร์ของกองโรคเอดส์ฯ ๒.สรุปรายงานจัดหาคอมพิวเตอร์ที่มีลายเซ็นหัวหน้ากลุ่มบริหารทั่วไป และผู้อำนวยการกองโรคเอดส์ฯ ลงนาม ๓.หนังสือนำส่งรายงานจัดหาคอมพิวเตอร์ของกองดิจิทัลเพื่อการควบคุมโรค
	๒		

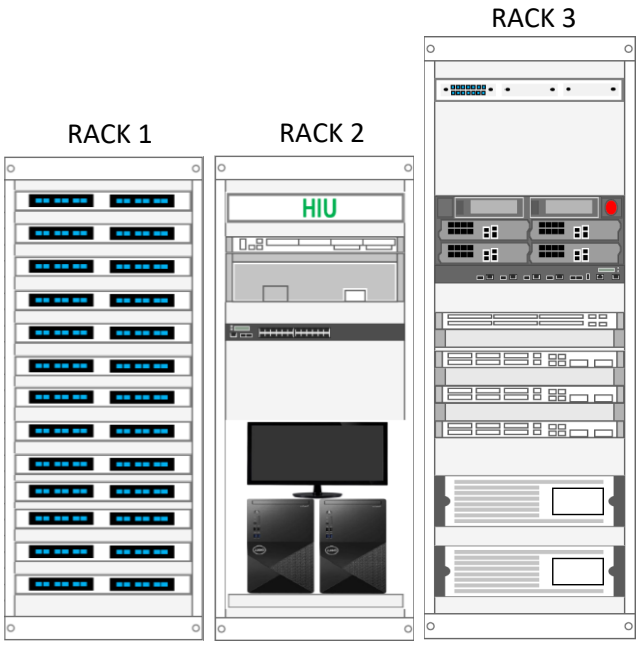
ผู้รับผิดชอบ	ขั้นตอนการปฏิบัติงาน	ระยะเวลา	เอกสารที่เกี่ยวข้อง
คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ประจำกรมควบคุมโรค		๕ วัน	๑.หนังสือนำส่งรายงานจัดหาคอมพิวเตอร์ของกองดิจิทัลเพื่อการควบคุมโรคถึงผู้อำนวยการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ๒.สรุปรายงานจัดหาคอมพิวเตอร์ที่มีลายเซ็นหัวหน้ากลุ่มบริหารทั่วไป และผู้อำนวยการกองโรคเอดส์ฯ ลงนามตามเอกสารที่เกี่ยวข้อง ๑ – ๘
คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ประจำกระทรวงสาธารณสุข		๗ วัน	๑.หนังสือนำส่งรายงานจัดหาคอมพิวเตอร์ของกองดิจิทัลเพื่อการควบคุมโรคถึงผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ๒.สรุปรายงานจัดหาคอมพิวเตอร์ที่มีลายเซ็นหัวหน้ากลุ่มบริหารทั่วไป และผู้อำนวยการกองโรคเอดส์ฯ ลงนามตามเอกสารที่เกี่ยวข้อง ๑ – ๘
กองดิจิทัลเพื่อการควบคุมโรค	 	๓ วัน	๑.หนังสือแจ้งผลอนุมัติรายงานจัดหาคอมพิวเตอร์จากสำนักงานปลัดกระทรวงสาธารณสุข ๒.รายงานจัดหาคอมพิวเตอร์ที่ผ่านการอนุมัติ

ผู้รับผิดชอบ	ขั้นตอนการปฏิบัติงาน	ระยะเวลา	เอกสารที่เกี่ยวข้อง
กองดิจิทัลเพื่อการควบคุมโรค	๓ ↓ ทำหนังสือแจ้งผลอนุมัติและรายงานอนุมัติฉบับจริง	๑ วัน	๑.หนังสือแจ้งผลอนุมัติรายงานจัดหาคอมพิวเตอร์จากกองดิจิทัลเพื่อการควบคุมโรค ๒.รายงานจัดหาคอมพิวเตอร์ที่ผ่านการอนุมัติ
งานธุรการ กองโรคเอดส์ฯ กรมควบคุมโรค	↓ รับหนังสือแจ้งผลอนุมัติและรายงานอนุมัติฉบับจริง	๑ วัน	๑.หนังสือแจ้งผลอนุมัติรายงานจัดหาคอมพิวเตอร์จากกองดิจิทัลเพื่อการควบคุมโรค ๒.รายงานจัดหาคอมพิวเตอร์ที่ผ่านการอนุมัติ
งานธุรการ กลุ่มบริหารทั่วไป กองโรคเอดส์ฯ กรมควบคุมโรค	↓ แจ้งผู้เกี่ยวข้องรายงานทราบผลการอนุมัติ	๑ วัน	ไฟล์สำเนาหนังสือรายงานจัดหาคอมพิวเตอร์ที่ผ่านการอนุมัติ
งานสารสนเทศ กลุ่มบริหารทั่วไป กองโรคเอดส์ฯ	↓ จัดทำขออนุมัติหลักการจัดซื้อจัดจ้างครุภัณฑ์คอมพิวเตอร์	๑ วัน	หนังสือขออนุมัติหลักการจัดซื้อจัดจ้างครุภัณฑ์คอมพิวเตอร์
ผู้อำนวยการ กองโรคเอดส์ฯ กรมควบคุมโรค	↓ อนุมัติในหลักการจัดซื้อจัดจ้างครุภัณฑ์คอมพิวเตอร์ ↓ ๔	๑ วัน	หนังสือขออนุมัติหลักการจัดซื้อจัดจ้างครุภัณฑ์คอมพิวเตอร์ ที่ผ่านการอนุมัติ

ผู้รับผิดชอบ	ขั้นตอนการปฏิบัติงาน	ระยะเวลา	เอกสารที่เกี่ยวข้อง
งานพัสดุและยานพาหนะ กลุ่มบริหารทั่วไป กองโรคเอดส์ฯ		๙๐ วัน	๑. แผนการจัดซื้อจัดจ้าง ๒. หนังสือขออนุมัติแต่งตั้งคณะกรรมการกำหนดคุณลักษณะและราคากลาง ๓. หนังสือรายงานคุณลักษณะเฉพาะและราคากลาง ๔. หนังสือรายงานการจัดซื้อ ๕. ร่างประกาศ ร่างเอกสารประกวด ๖. หนังสือขออนุมัติแต่งตั้งคณะกรรมการพิจารณาประกวดราคาและคณะกรรมการตรวจรับ ๗. หนังสือรายงานผลการพิจารณาประกวดราคา ๘. หนังสือแจ้งลงนามในสัญญา ๙. หนังสือสัญญา ๑๐. รายงานผลการตรวจรับพัสดุ ๑๑. หนังสือเบิก-จ่าย
งานพัสดุและยานพาหนะ กลุ่มบริหารทั่วไป กองโรคเอดส์ฯ		นับจากจัดหาเสร็จสิ้นภายใน ๓๐ วัน	รายงานผลการจัดซื้อจัดหาระบบคอมพิวเตอร์
กองดิจิทัลเพื่อการควบคุมโรค		๑ วัน	รายงานผลการจัดซื้อจัดหาระบบคอมพิวเตอร์ ของ กองโรคเอดส์ฯ

๓.๒.๔ การออกแบบระบบเครือข่าย ตามความต้องการขององค์กร และติดตั้งอุปกรณ์ต่าง ๆ เช่น เซิร์ฟเวอร์ สวิตช์ ระบบสำรองข้อมูล ระบบไฟฟ้า เป็นต้น

ออกแบบการติดตั้งอุปกรณ์



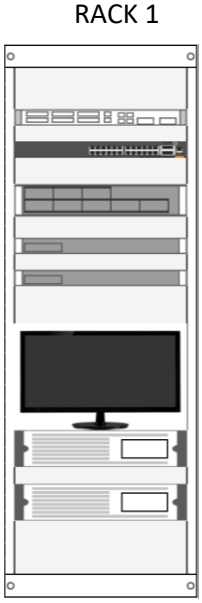
อุปกรณ์ที่ติดตั้งในตู้_Rack 1
- ติดตั้ง fiber patch panel สำหรับเชื่อมต่อระบบแต่ละชั้นภายในอาคาร

อุปกรณ์ที่ติดตั้งในตู้_Rack 2
- Router
- NextGen Fiwall
- SW L2 สำหรับเครื่องควบคุม IP Phone

อุปกรณ์ที่ติดตั้งในตู้_Rack 3
- fiber patch panel เชื่อมต่อระบบเครือข่ายกับชั้น 13
- ติดตั้งเครื่องควบคุมระบบ IP Phone
- SW L2 x 3
- UPS x 2

ภาพที่ ๑๑ : แบบการติดตั้งอุปกรณ์เครือข่ายชั้น ๑๒

ออกแบบการติดตั้งอุปกรณ์ในตู้จัดเก็บอุปกรณ์ (Rack) ขนาด 27U บริเวณห้อง Server ชั้น ๑๓

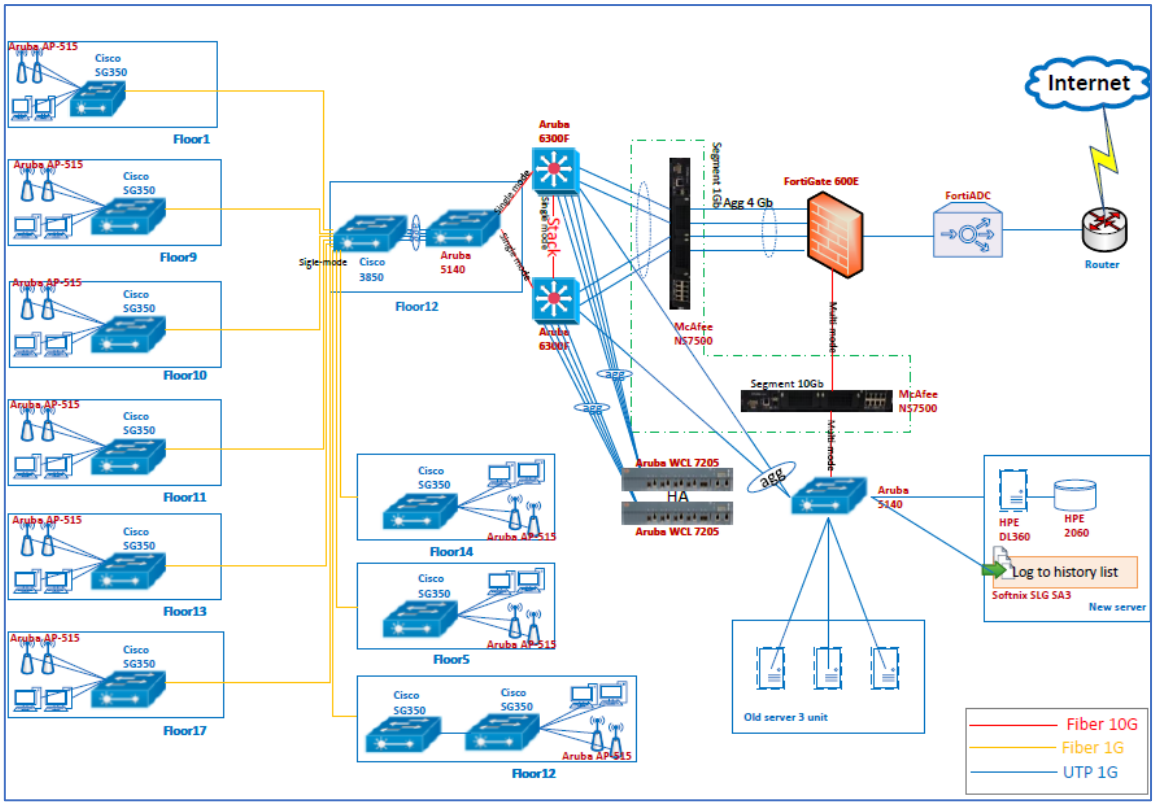


อุปกรณ์ที่ติดตั้งในตู้
(ระบบเครือข่ายเดิม)
- SW L3 Managed
- SW L2
- HP Server (HIS VPM)
- Server Repicate VPM
- Server ระบบ LIS
- NAS Box สำหรับเก็บข้อมูลภาพถ่าย

อุปกรณ์ที่ติดตั้งในตู้
- Fiber Optic Panal
- Link Load Balance
- SW L2 Link to F12
- SW L3 Managed
- AP Controller
- Log File
- IPS
- HP Server
- HP External Storage

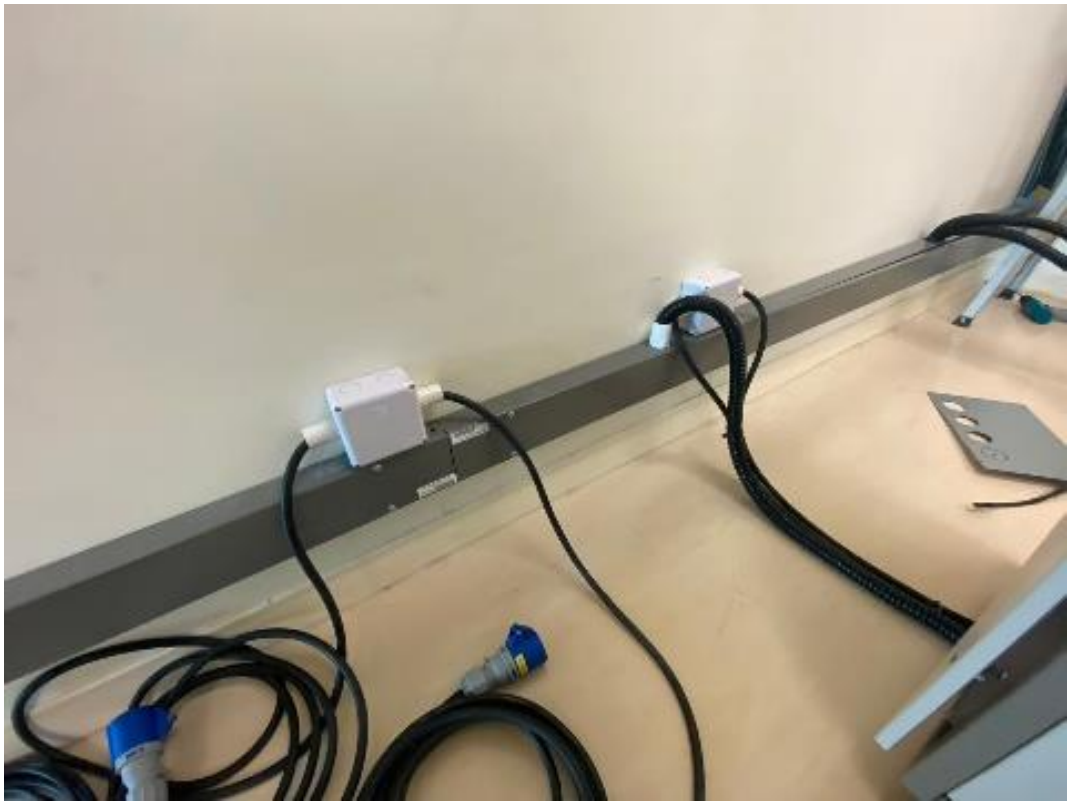
ภาพที่ ๑๒ : แบบการติดตั้งอุปกรณ์เครือข่ายชั้น ๑๓

แผนผังระบบเครือข่าย (Network Diagram)



ภาพที่ ๑๓ : แผนผังระบบเครือข่าย (Network Diagram)

การปรับปรุงระบบไฟฟ้าสำหรับอุปกรณ์เครือข่ายบริเวณ ชั้น ๑๓ ของอาคาร



ภาพที่ ๑๔ : การปรับปรุงระบบไฟฟ้า

๓.๒.๕ การติดตั้งอุปกรณ์เครือข่ายคอมพิวเตอร์ เป็นขั้นตอนที่สำคัญเพื่อสร้างระบบเครือข่ายคอมพิวเตอร์ภายในองค์กร ให้สามารถเชื่อมต่อกันและแบ่งปันข้อมูล ทรัพยากร และบริการต่าง ๆ ได้ระหว่างกันอย่างมีประสิทธิภาพและปลอดภัย โดยดำเนินการติดตั้งอุปกรณ์ตามแผนการดำเนินงานที่กำหนดไว้ และผู้จัดทำได้นำอุปกรณ์ที่ผ่านกระบวนการจัดซื้อจัดจ้างตามระเบียบเรียบร้อยแล้วจำนวน ๑๒ รายการ ติดตั้ง ณ อาคารศูนย์การแพทย์บางรักกรมควบคุมโรค ซึ่งคุณลักษณะของอุปกรณ์มีความสามารถในการทำงานดังนี้

๑) อุปกรณ์กระจายสัญญาณไร้สาย (Access Point) คือ อุปกรณ์ที่ใช้ในเครือข่ายไร้สาย (Wireless Network) เพื่อเชื่อมต่ออุปกรณ์ต่าง ๆ เข้ากับเครือข่ายไร้สาย เช่น เครื่องคอมพิวเตอร์พกพา สมาร์ทโฟน แท็บเล็ต และอุปกรณ์อื่น ๆ เพื่อให้ผู้ใช้งานสามารถเข้าถึงข้อมูลหรือบริการในเครือข่ายได้

๒) อุปกรณ์กระจายสัญญาณ (L2 Switch) คือ อุปกรณ์ที่ใช้ในระบบเครือข่ายแบบมีสายต่อสัญญาณในเชื่อมต่อกับอุปกรณ์อื่นโดยใช้สาย LAN เป็นตัวกลางในการส่ง-รับข้อมูล ซึ่งสวิตช์ช่วยให้อุปกรณ์ที่เชื่อมต่อแต่ละเครื่องสามารถดำเนินการทำงานในระบบเครือข่ายได้เสถียรสูงและแจกจ่ายสัญญาณให้กับอุปกรณ์ต่าง ๆ

๓) อุปกรณ์กระจายการทำงานสำหรับเครือข่าย (Link Load Balancer) คือ อุปกรณ์ที่ใช้ในโครงข่ายคอมพิวเตอร์เพื่อกระจายการทำงานและการโหลดของผู้ใช้หรือบริการให้สมดุลกันบนหลาย ๆ เส้นทางเครือข่าย ช่วยลดการซ้อนทับ (congestion) ในเส้นทางเครือข่ายและเพิ่มประสิทธิภาพของ การใช้งานโดยการแบ่งการทำงานหรือการโหลดของผู้ใช้ให้กระจายไปยังเซิร์ฟเวอร์หลาย ๆ เครื่องพร้อมกัน ทำให้เส้นทางเครือข่ายไม่ต้องทำงานหนักเพียงเพียงเส้นทางเดียว

๔) อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) คือ เป็นอุปกรณ์ที่ใช้ในการป้องกันและควบคุมการเข้าถึงเครือข่ายขององค์กร โดยมีความสามารถในการตรวจจับและป้องกันการโจมตี

ที่มีความหลากหลาย เช่น การโจมตีด้วยมัลแวร์ (Malware) การโจมตีด้วยแฝดเอนจิเนียริ่ง (Distributed Denial of Service - DDoS) การโจมตีแบบสแปม (Spam) การโจมตีแบบฝังลึก (Intrusion) การละเมิดข้อมูล (Data Breach) เป็นต้น

๕) อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย คือ เป็นอุปกรณ์หรือโปรแกรมที่ใช้ในการวิเคราะห์ข้อมูลการจราจรที่ถูกบันทึกไว้ในไฟล์ล็อก (log files) ของระบบเครือข่าย โดยทั่วไปแล้ว Log Analyzer จะทำหน้าที่ดึงข้อมูลจากไฟล์ล็อกเหล่านั้นและนำมาวิเคราะห์เพื่อให้ผู้ดูแลระบบหรือผู้ใช้งานเข้าใจถึงสถานะและปัญหาต่าง ๆ ที่เกิดขึ้นในระบบเครือข่ายได้ เช่น ปัญหาในการเชื่อมต่อ การโจมตีจากภัยคุกคาม การทำงานของแอปพลิเคชัน เป็นต้น

๖) อุปกรณ์กระจายสัญญาณ (L3 Switch) คือ เป็นอุปกรณ์ที่มีความสามารถในการทำงานทั้งในระดับ Layer 2 และ Layer 3 ของโมเดล OSI ซึ่งช่วยเพิ่มประสิทธิภาพและความยืดหยุ่นในการบริหารจัดการเครือข่ายในองค์กรหรือสถานประกอบการต่าง ๆ ที่มีความซับซ้อนในโครงสร้างของเครือข่ายขององค์กร โดยสามารถกำหนดแส้นทางการส่งข้อมูลในเครือข่าย สามารถสร้างเส้นทางการส่งข้อมูลระหว่าง VLAN หรือเครือข่ายย่อยต่าง ๆ ในองค์กรได้

๗) อุปกรณ์ควบคุมเครือข่ายไร้สาย (Access Point Controller) คือ อุปกรณ์ที่ใช้ในระบบเครือข่ายไร้สายเพื่อบริหารจัดการและควบคุมการทำงานของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point : AP) ที่มีจำนวนมากในเครือข่ายเดียวกันได้อย่างมีประสิทธิภาพ ซึ่ง Access Point Controller จะเป็นหน่วยควบคุมที่ทำหน้าที่สำคัญในการจัดการการเชื่อมต่อของอุปกรณ์ต่าง ๆ ในเครือข่ายไร้สาย เช่น การกำหนดค่าการเชื่อมต่อของผู้ใช้งาน การจัดการแบนด์วิธ การจัดการความปลอดภัย และการตรวจสอบปัญหาและการดูแลรักษา การใช้อุปกรณ์ควบคุมเครือข่ายไร้สายช่วยให้การดูแลระบบเครือข่ายไร้สายเป็นไปอย่างมีประสิทธิภาพโดยทำให้การจัดการและการดูแลรักษาเครือข่ายง่ายขึ้นและมีประสิทธิภาพมากขึ้นในขณะเดียวกัน

๘) อุปกรณ์วิเคราะห์การจราจรบนเครือข่าย (Log Analyzer) คือ เป็นอุปกรณ์หรือโปรแกรมที่สำคัญในการดูแลและบริหารจัดการเครือข่ายให้มีประสิทธิภาพและปลอดภัย สำหรับใช้ในการวิเคราะห์ข้อมูลการจราจรที่ถูกบันทึกไว้ในไฟล์ล็อก (log files) ของระบบเครือข่ายขององค์กร Log Analyzer จะทำหน้าที่ดึงข้อมูลจากไฟล์ล็อกเหล่านั้นและนำมาวิเคราะห์เพื่อให้ผู้ดูแลระบบหรือผู้ใช้งานเข้าใจถึงสถานะและปัญหาต่าง ๆ ที่เกิดขึ้นในระบบเครือข่ายได้ เช่น ปัญหาในการเชื่อมต่อ การโจมตีจากภัยคุกคาม การทำงานของแอปพลิเคชัน และระบบอื่น ๆ ที่ถูกใช้งานผ่านระบบเครือข่ายขององค์กร

๙) เครื่องสำรองไฟฟ้าขนาด 40 KVA (UPS 40 KVA) คือ อุปกรณ์อิเล็คทรอนิคส์ที่ทำหน้าที่จ่ายพลังงานไฟฟ้าให้แก่อุปกรณ์ไฟฟ้าและอุปกรณ์อิเล็กทรอนิกส์ได้อย่างต่อเนื่องแม้ในเวลาที่เกิดไฟดับหรือแม้แต่กรณีที่เกิดปัญหาแรงดันไฟฟ้าผันผวนผิดปกติ หรือไฟกระชาก โดยหน้าที่ของ UPS หรือเครื่องสำรองไฟฟ้าจะทำการปรับแรงดันให้ระดับอยู่คงที่ปลอดภัยต่ออุปกรณ์ไฟฟ้าและอุปกรณ์อิเล็คทรอนิคส์ไม่ให้เกิดความเสียหาย ในกรณีที่เกิดเหตุการณ์ ไฟตก ไฟดับ ไฟเกิน หรือ ไฟกระชาก เป็นต้น

๑๐) อุปกรณ์สำหรับจัดเก็บข้อมูลแบบภายนอก (External Storage) คือ อุปกรณ์ที่ใช้เก็บข้อมูลที่ไม่ต้องการเก็บไว้ในอุปกรณ์ภายใน เช่น ฮาร์ดดิสก์พอร์ตเบล (Hard Disk Portable) หรือ ฮาร์ดดิสก์แอกซ์เทอร์นอล (External Hard Disk) แฟลชไดร์ฟ (Flash Drive) การ์ดหน่วยความจำ (Memory Card) เป็นต้น โดยอุปกรณ์เหล่านี้สามารถเชื่อมต่อกับคอมพิวเตอร์หรืออุปกรณ์อื่นๆ ผ่านพอร์ตต่างๆ เช่น USB, Thunderbolt หรือ FireWire เพื่อทำการถ่ายโอนข้อมูล หรือการสำรองข้อมูลออกไปนอกอุปกรณ์หลักได้

๑๑) เครื่องคอมพิวเตอร์แม่ข่าย คือ เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นแม่ข่ายหรือเซิร์ฟเวอร์ในระบบเครือข่ายคอมพิวเตอร์ ซึ่งมีหน้าที่ในการจัดการและควบคุมการสื่อสารระหว่างอุปกรณ์คอมพิวเตอร์ต่าง ๆ ในเครือข่าย รวมถึงการให้บริการแก่ผู้ใช้งานต่าง ๆ ในเครือข่ายด้วย เช่น การแชร์ไฟล์ การพิมพ์เครื่องพิมพ์ที่ใช้ร่วมกัน การเก็บข้อมูล และบริการอื่น ๆ ตามที่ต้องการขององค์กรหรือระบบเครือข่ายนั้น ๆ อาจมีหลายประเภทขึ้นอยู่กับลักษณะงานและความต้องการของผู้ใช้งาน เช่น เซิร์ฟเวอร์ไฟล์ (File Server) เซิร์ฟเวอร์อีเมล (Email Server) เซิร์ฟเวอร์ฐานข้อมูล (Database Server) เป็นต้น

๑๒) อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) คือเป็นเครื่องมือที่ใช้ในระบบคอมพิวเตอร์เพื่อตรวจจับและป้องกันการบุกรุกหรือการโจมตีที่เป็นอันตรายต่อระบบขององค์กร ซึ่ง IPS มักจะถูกใช้ร่วมกับระบบป้องกันไวรัสและไฟร์วอลล์ (Firewall) เพื่อเสริมสร้างความปลอดภัยให้กับเครือข่ายคอมพิวเตอร์และระบบสารสนเทศขององค์กร

การติดตั้งอุปกรณ์เครือข่ายคอมพิวเตอร์

ภาพที่ ๑๕ : การติดตั้งอุปกรณ์เครือข่าย ห้อง Server ชั้น ๑๓

การติดตั้งเครื่องสำรองไฟฟ้า

ระบบไฟฟ้า ๒ ระบบให้กับตู้ติดตั้งอุปกรณ์เครือข่าย คือ ระบบไฟฟ้าของอาคารที่เชื่อมต่อกับระบบเครื่องสำรองไฟ Generator และระบบไฟฟ้าสำรองจากตู้แบตเตอร์รี่ ขนาด 12V จำนวน ๗๒ ก้อน

ภาพที่ ๑๖ : การติดตั้งเครื่องสำรองไฟฟ้าและตู้แบตเตอรี่

ตู้แบตเตอรี่ (12V จำนวน ๗๒ ก้อน)

เครื่องสำรองไฟฟ้า

ภาพที่ ๑๗ : การติดตั้งเครื่องสำรองไฟฟ้าและตู้แบตเตอรี่

เชื่อมต่อระบบไฟฟ้า ๒ ระบบ ให้กับอุปกรณ์เครือข่ายและเครื่อง Server

ภาพที่ ๑๘ : การเชื่อมต่อระบบไฟฟ้า ๒ ระบบ

การติดตั้งอุปกรณ์กระจายสัญญาณ Access Point

ภาพที่ ๑๙ : การติดตั้งอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point)

๓.๒.๖ การประเมินประสิทธิภาพของเครือข่าย มีเกณฑ์การประเมินพื้นฐานของระบบเครือข่ายสิ่งสำคัญในการเลือกระบบเครือข่ายเป็นที่จะต้องพิจารณาสำหรับการปรับปรุงการทำงานของเครือข่าย เกณฑ์ประสิทธิภาพพื้นฐานของระบบเครือข่ายที่สำคัญ คือ สมรรถนะ (Performance), ความน่าเชื่อถือ (Reliability) และความปลอดภัย (Security)

๑) สมรรถนะ (Performance) ขึ้นกับปัจจัยดังต่อไปนี้

๑.๑) จำนวนผู้ใช้ (Number of Users) ผู้ใช้จำนวนมากในเครือข่ายทำให้การตอบสนองช้าลง ถ้ามันถูกออกแบบมาเพื่อรองรับการใช้และ

เข้าถึงจำนวนมากในช่วงการใช้สูงสุดอาจทำให้การทำงานในระบบเครือข่ายช้าลง นั่นเป็นประสิทธิภาพและสมรรถนะของระบบเครือข่าย

๑.๒) ตัวกลางการสื่อสารที่ใช้ในระบบเครือข่ายเป็นปัจจัยสำคัญสำหรับประสิทธิภาพการส่งผ่านข้อมูลซึ่ง สายใยแก้วนำแสง (Fiber Optic) เป็นตัวกลางการสื่อสารที่ส่งข้อมูลได้เร็วที่สุด

๑.๓) อุปกรณ์ที่ใช้ในระบบเครือข่ายมีผลต่อความเร็วและอัตราการส่งผ่านข้อมูลคอมพิวเตอร์ที่มีประสิทธิภาพและพื้นที่การจัดเก็บขนาดใหญ่ทำให้การทำงานมีประสิทธิภาพมากขึ้น

๑.๔) ซอฟต์แวร์ที่ใช้สำหรับโปรแกรมและการประมวลผลข้อมูลที่ผู้ส่งและผู้รับและเครื่องตัวกลางเป็นผลกับสมรรถนะของระบบเครือข่าย

๒) ความเชื่อถือได้ (Reliability) ขึ้นกับปัจจัยดังต่อไปนี้

๒.๑) ความถี่ของความล้มเหลว (Frequency of Failure) ทุกระบบเครือข่ายมีโอกาสล้มเหลว แต่ระบบเครือข่ายที่ล้มเหลวบ่อยครั้งเป็นระบบเครือข่ายที่ไม่มีประสิทธิภาพ

๒.๒) เวลาการกู้คืน (Recovery Time) เวลาที่ใช้ในการกู้คืนสภาพหลังจากความล้มเหลว ระบบเครือข่ายที่สามารถกู้คืนได้รวดเร็วจะมีประสิทธิภาพและเป็นประโยชน์มากกว่าระบบที่ใช้เวลานานในการกู้คืน

๒.๓) ภัยพิบัติ (Catastrophe) ระบบเครือข่ายต้องสามารถป้องกันภัยจากไฟไหม้ แผ่นดินไหว หรือการโจรกรรมซึ่งระบบเครือข่ายอาจมีระบบในการสำรองไฟล์ (back up)

๓) ความปลอดภัย (Security) สำคัญมากสำหรับประสิทธิภาพของเครือข่าย

๓.๑) การเข้าถึงที่ไม่ได้รับอนุญาต (Unauthorized Access) ในเครือข่ายอาจมีข้อมูลที่สำคัญจึงต้องได้รับการคุ้มครองจากการเข้าถึงที่ไม่ได้รับอนุญาต ซึ่งอาจเป็นการระบุผู้ใช้และรหัสผ่านหรือเทคนิคการเข้ารหัสที่สูงขึ้น

๓.๒) ไวรัส (Viruses) ระบบเครือข่ายสามารถเข้าถึงจากหลายจุดซึ่งอาจมีไวรัสคอมพิวเตอร์อยู่ ซึ่งไวรัสเป็นโปรแกรมที่ก่อให้เกิดความเสียหายต่อระบบ ซึ่งระบบเครือข่ายที่ดีต้องมีการป้องกันไวรัสคอมพิวเตอร์ทั้งจากโปรแกรมหรืออุปกรณ์ (software or hardware)

๓.๓ การบำรุงรักษาอุปกรณ์เครือข่ายคอมพิวเตอร์

การบำรุงรักษาอุปกรณ์เครือข่ายคอมพิวเตอร์เป็นกระบวนการที่สำคัญในการรักษาประสิทธิภาพและความเสถียรของระบบเครือข่าย โดยมีวัตถุประสงค์ในการบำรุงรักษาอุปกรณ์เครือข่ายคอมพิวเตอร์ดังนี้

วัตถุประสงค์

๑. เพื่อการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ ให้สามารถใช้งานได้อย่างปกติ รวมถึงการกระทำใด ๆ เพื่อป้องกันความชำรุดเสียหายของเครื่องคอมพิวเตอร์แม่ข่ายระบบเครือข่ายและอุปกรณ์ ให้สามารถใช้งานได้อย่างต่อเนื่องและลดความเสี่ยงในการเกิดปัญหาจากการใช้งาน

๒. เพื่อตรวจสอบการทำงานของระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ของอาคารศูนย์การแพทย์บางรัก ให้อยู่ในสภาพพร้อมใช้งาน

๓. เพื่อให้ระบบเครื่อข่ายคอมพิวเตอร์และอุปกรณ์ของของอาคารศูนย์การแพทย์บางรัก มีเสถียรภาพ และมีการใช้งานอินเทอร์เน็ตที่รวดเร็ว รวมทั้งลดความเสียหายจากการที่ข้อมูลถูกทำลายจากไวรัสคอมพิวเตอร์

การบำรุงรักษาอุปกรณ์เครือข่ายคอมพิวเตอร์

การบำรุงรักษาอุปกรณ์ที่นำมาใช้ในองค์กรมีวิธีดำเนินการดังนี้

๑. การบำรุงรักษาอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ได้แก่

- ๑.๑ การตรวจสอบสถานะของ Access Point เพื่อให้ทราบถึงประสิทธิภาพในการทำงาน รวมถึงความเสถียรภาพของการเชื่อมต่อและประสิทธิภาพของสัญญาณ Wi-Fi
- ๑.๒ การตรวจสอบสภาพของอุปกรณ์ฮาร์ดแวร์ของ Access Point เช่น อุปกรณ์ภายใน Access Point เสาอากาศและการเชื่อมต่อสายแลนหรือสายไร้สาย เพื่อให้มั่นใจว่าอุปกรณ์ทำงานได้อย่างเหมาะสมและมีประสิทธิภาพสูง
- ๑.๓ การตรวจสอบการรักษาความปลอดภัย ตรวจสอบและปรับแต่งการตั้งค่าความปลอดภัยของ Access Point เพื่อป้องกันการเข้าถึงที่ไม่มีอำนาจและการบุกรุกที่อาจเกิดขึ้น รวมถึงการตรวจสอบการใช้งานของระบบรักษาความปลอดภัย เช่น การใช้งานระบบรหัสผ่านและการเข้ารหัสข้อมูล
- ๑.๔ การดูแลรักษาซอฟต์แวร์ อัปเดตซอฟต์แวร์ของ Access Point เพื่อให้ได้รับการแก้ไขข้อบกพร่อง (patches) และคุณสมบัติใหม่ ๆ ที่สำคัญ เพื่อปรับปรุงประสิทธิภาพและความปลอดภัยของอุปกรณ์
- ๑.๕ การจัดการการใช้งาน ตรวจสอบและบันทึกการใช้งานของ Access Point เพื่อวิเคราะห์ปัญหาที่อาจเกิดขึ้น และใช้ข้อมูลเหล่านั้นในการปรับปรุงและป้องกันปัญหาในอนาคต

๒. การบำรุงรักษาอุปกรณ์กระจายสัญญาณ (L2 Switch) ได้แก่

- ๒.๑ อัปเดตซอฟต์แวร์ของอุปกรณ์เป็นระยะเพื่อรับการแก้ไขปรับปรุงความปลอดภัย
- ๒.๒ สำรองข้อมูลการกำหนดค่าอุปกรณ์เพื่อใช้ในกรณีเกิดภัยความเสียหายหรือข้อมูลสูญหาย และตรวจสอบการทำงานของการกู้คืนข้อมูลเป็นระยะ
- ๒.๓ ตรวจสอบและเช็คความสมบูรณ์ของฮาร์ดแวร์ เช่น พอร์ตเสียหาย หรือการทำงานของพัดลมที่ไม่ปกติ เพื่อป้องกันการฉีกขาดในการทำงาน

๒.๔ ทำความสะอาดอุปกรณ์ เช่น ทำความสะอาดพอร์ต ทำความสะอาดตัวเครื่อง และเช็คการทำงานของพัดลม เพื่อให้การทำงานเครื่องไม่มีปัญหา

๒.๕ ตรวจสอบและเปลี่ยนอุปกรณ์ที่ชำรุด เช่น หลอดไฟ LED ที่เสีย หรือพอร์ตเครือข่ายที่ไม่ทำงาน

๒.๖ ตรวจสอบและลบข้อมูลที่เก็บไว้ในอุปกรณ์ เพื่อป้องกันการทำลายข้อมูลที่มีความลับหรือที่มีค่า

๒.๗ ตรวจสอบและติดตามประสิทธิภาพของอุปกรณ์ โดยระบุปัจจัยที่ส่งผลต่อประสิทธิภาพ เช่น การใช้งานแบนด์วิดธ์และความเร็วของการส่งข้อมูล

๓. การบำรุงรักษาอุปกรณ์กระจายการทำงานสำหรับเครือข่าย (Link Load Balancer) ได้แก่

๗) ตรวจสอบสมรรถภาพของอุปกรณ์ Link Load Balancer เป็นประจำเพื่อตรวจสอบว่าทุกฟังก์ชันทำงานอย่างถูกต้อง การทำงานของการแบ่งโหลด (load balancing) การเชื่อมต่อ เป็นต้น

๘) ดำเนินการอัปเดตซอฟต์แวร์และฮาร์ดแวร์เมื่อมีเวอร์ชันใหม่ออกสู่ตลาดหรือเมื่อมีความต้องการปรับปรุงเพื่อประสิทธิภาพของระบบ

๙) การสำรองข้อมูลและวางแผนการกู้คืนข้อมูลในกรณีเกิดภัยคุกคามหรือความสูญเสียข้อมูล เพื่อให้ระบบสามารถกลับคืนสู่สภาพปกติได้รวดเร็ว

๑๐) ตรวจสอบและปรับปรุงความปลอดภัยของอุปกรณ์ Link Load Balancer เพื่อป้องกันการบุกรุกและความเสี่ยงต่อข้อมูลและระบบเครือข่าย

๑๑) การจัดการการจัดเก็บข้อมูลเชิงประจำ เช่น บันทึกการทำงาน ข้อมูลการเชื่อมต่อและสถิติ เพื่อให้มีข้อมูลสำหรับการวิเคราะห์และการตรวจสอบปัญหาในอนาคต

๑๒) การสังเกตการณ์ ติดตามและวิเคราะห์ข้อมูลการทำงานของ Link Load Balancer เพื่อตรวจสอบประสิทธิภาพและความเสถียรของระบบ เพื่อให้สามารถรับมือกับปัญหาและปรับปรุงประสิทธิภาพได้อย่างเหมาะสม

๔. การบำรุงรักษาอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) ได้แก่

๔.๑ อัปเดตซอฟต์แวร์และเซ็นเซอร์ของ NGFW เพื่อให้ระบบมีความปลอดภัยต่อการโจมตีล่าสุดและช่องโหว่ที่มีการเผยแพร่ ซึ่งอัปเดตนี้ควรทำเป็นประจำเพื่อรักษาความปลอดภัยและประสิทธิภาพของระบบ

๔.๒ การตรวจสอบและบล็อกการโจมตีที่เกิดขึ้นในระบบเครือข่ายโดย NGFW อย่างสม่ำเสมอ เช่น การตรวจจับและบล็อกการโจมตีด้วยมัลแวร์หรือการโจมตี

๔.๓ การตรวจสอบและบันทึกเหตุการณ์ที่เกิดขึ้นในระบบเครือข่ายเพื่อตรวจสอบการกระทำที่เป็นไปในระบบ เช่น การบันทึกการเข้าถึงที่ถูกปฏิเสธหรือการสแกนการโจมตี

๔.๔ ทดสอบความสามารถในการตอบสนองของ NGFW และปรับปรุงการกำหนดค่าหรือนโยบายตามความเหมาะสม เพื่อให้สามารถป้องกันการโจมตีได้อย่างมีประสิทธิภาพ

๔.๕ การบำรุงรักษาฐานข้อมูลของ NGFW เช่น ลิขสิทธิ์และรายชื่อที่ระบุมัลแวร์ เพื่อให้สามารถตรวจจับและบล็อกการโจมตีได้อย่างมีประสิทธิภาพ

๔.๖ การดูแลและซ่อมบำรุงอุปกรณ์ NGFW เพื่อให้สามารถทำงานอย่างเสถียรและมีประสิทธิภาพตลอดเวลา

๕. การบำรุงรักษาอุปกรณ์จัดเก็บ Log File ระบบเครือข่าย ได้แก่

๕.๑ การตรวจสอบความพร้อมใช้งาน (Monitoring) ตรวจสอบสถานะและประสิทธิภาพของอุปกรณ์จัดเก็บ Log File เพื่อแน่ใจว่าทำงานอย่างถูกต้องและมีประสิทธิภาพที่เพียงพอในการรองรับภาระการใช้งาน

๕.๒ การสำรองข้อมูล Log File เพื่อป้องกันข้อมูลจากการสูญหายหรือเสื่อมสภาพ และให้สามารถกู้คืนข้อมูลได้เมื่อเกิดภัยคุกคามหรือการล้มเหลวของระบบ

๕.๓ การควบคุมการเข้าถึง (Access Control) ให้กำหนดสิทธิ์การเข้าถึงข้อมูล Log File เพื่อป้องกันการเข้าถึงโดยไม่มีอำนาจหรือการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

๕.๔ ตรวจสอบข้อมูล Log File เพื่อตรวจสอบประสิทธิภาพของระบบ เช่น ตรวจสอบการเข้าถึงที่ไม่มีอำนาจหรือการกระทำที่ไม่เหมาะสม และวิเคราะห์ข้อมูลเพื่อค้นหาต้นเหตุของปัญหา

๕.๕ อัปเดตซอฟต์แวร์และระบบปฏิบัติการของอุปกรณ์เพื่อรักษาความปลอดภัยและป้องกันการโจมตี โดยใช้มาตรการรักษาความปลอดภัยเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่มีอำนาจหรือการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

๕.๖ การบริหารจัดการพื้นที่เก็บข้อมูล Log File ให้เพียงพอและมีประสิทธิภาพเพื่อรองรับการเก็บข้อมูลในระยะยาวโดยไม่มีการขาดทรัพยากรหรือการล้มเหลวในการบันทึกข้อมูล

๕.๗ การสร้างรายงานเกี่ยวกับข้อมูล Log เพื่อช่วยในการวิเคราะห์และตรวจสอบสถานะของระบบ เช่น รายงานแนวโน้มของเหตุการณ์ที่เกิดขึ้นในเวลาที่กำหนด การสร้างแผนภูมิและรายงานความผิดปกติ

๖. การบำรุงรักษาอุปกรณ์กระจายสัญญาณ (L3 Switch) ได้แก่

๖.๑ การสำรองข้อมูล (Backup) ของการตั้งค่า (Configuration) และระบบปฏิบัติการของ L3 Switch เพื่อป้องกันข้อมูลไม่ได้หายไปเมื่อเกิดเหตุฉุกเฉินหรือความเสียหาย เช่นการใช้งานผิดพลาดหรือเหตุสูญเสียข้อมูล

๖.๒ ปรับปรุงซอฟต์แวร์และเฟิร์มแวร์ของ L3 Switch เพื่อให้มันมีประสิทธิภาพและปลอดภัยตลอดเวลา โดยการอัพเกรดหรืออัปเดตอย่างต่อเนื่องตามคำแนะนำจากผู้ผลิตและผู้จัดจำหน่าย

๖.๓ ตรวจสอบปัญหาที่เกิดขึ้นบน L3 Switch เพื่อแก้ไขปัญหาทันที รวมถึงการดีบัก (Debugging) และการวิเคราะห์ข้อมูลเพื่อหาสาเหตุของปัญหา

๖.๔ การควบคุมการเข้าถึงและความปลอดภัยปรับการตั้งค่าการเข้าถึงและความปลอดภัยบน L3 Switch เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและการโจมตีต่าง ๆ เช่นการใช้งานไม่ชอบด้วย

๖.๕ การจัดการและการตรวจสอบการใช้งานของทรัพยากรเครือข่ายและวิเคราะห์การใช้งานของทรัพยากรเครือข่ายบน L3 Switch เช่นการใช้งานแบนด์วิชท์ และการเชื่อมต่อของผู้ใช้ เพื่อปรับปรุงประสิทธิภาพและการจัดสรรทรัพยากรอย่างเหมาะสม

๖.๖ การควบคุมการจัดการและการติดตามโดยใช้เครื่องมือและระบบจัดการเครือข่าย (Network Management Systems) เพื่อควบคุมการดูแลรักษาและติดตามสถานะของ L3 Switch เพื่อให้การบริหารจัดการเครือข่ายเป็นไปอย่างมีประสิทธิภาพ

๗. การบำรุงรักษาอุปกรณ์ควบคุมเครือข่ายไร้สาย (Access Point Controller) ได้แก่

๗.๑ การตรวจสอบและบำรุงรักษาอุปกรณ์ควบคุมเครือข่ายไร้สาย เช่น Access Point Controller รวมถึงการตรวจสอบสถานะของอุปกรณ์ เช็คการทำงานและประสิทธิภาพ การดำเนินการบำรุงรักษาอย่างเป็นระบบ เช่น การอัพเกรดซอฟต์แวร์หรือการทำความสะอาดอุปกรณ์

๗.๒ การกำหนดค่าและการปรับแต่งต่าง ๆ ของอุปกรณ์ควบคุม เช่น การตั้งค่าการเชื่อมต่อเครือข่าย การกำหนดค่าความปลอดภัย เป็นต้น

๗.๓ การดูแลรักษาความปลอดภัย เช่น การตรวจสอบและการป้องกันการบุกรุก การจัดการการเข้าถึงที่มีความปลอดภัย การอัปเดตโปรแกรมและการแก้ไขช่องโหว่ที่อาจเกิดขึ้น

๗.๔ การจัดการเครือข่ายเพื่อให้สอดคล้องกับความต้องการและการใช้งานขององค์กร รวมถึงการจัดการการขยายเครือข่ายหรือการเพิ่มอุปกรณ์ใหม่ในเครือข่าย

๗.๕ การตรวจสอบปัญหาและการแก้ไข เช่น Access Point Controller จะต้องสามารถตรวจสอบปัญหาที่เกิดขึ้นในระบบและดำเนินการแก้ไขให้เร็วที่สุดเพื่อลดอันตรายที่อาจเกิดขึ้นจากปัญหาดังกล่าว

๗.๖ การสำรวจและวิเคราะห์ประสิทธิภาพของระบบ เพื่อพัฒนาและปรับปรุงเครือข่ายให้มีประสิทธิภาพมากขึ้นในอนาคต

๘. การบำรุงรักษาอุปกรณ์วิเคราะห์การจราจรบนเครือข่าย (Log Analyzer) ได้แก่

๘.๑ การตั้งค่าอุปกรณ์ ตรวจสอบและปรับปรุงการตั้งค่าของ Log Analyzer เพื่อให้สอดคล้องกับความต้องการและการใช้งานของระบบ เช่น การตั้งค่าการวิเคราะห์ข้อมูล การตั้งค่าการแจ้งเตือน และการกำหนดเกณฑ์การค้นหาข้อมูล

๘.๒ ตรวจสอบและดำเนินการอัปเดตซอฟต์แวร์ Log Analyzer เพื่อรับการปรับปรุงและแก้ไขข้อบกพร่องต่าง ๆ ที่อาจจะมีอยู่ เพื่อให้การทำงานมีประสิทธิภาพสูงสุดและปลอดภัย

๘.๓ สำรองข้อมูลของ Log Analyzer เพื่อป้องกันข้อมูลที่สำคัญจากการสูญหายหรือความเสียหายที่อาจเกิดขึ้น นอกจากนี้ยังสามารถใช้ข้อมูลสำรองเพื่อกู้คืนข้อมูลในกรณีที่จำเป็น

๘.๔ การจัดการความปลอดภัยโดยการตรวจสอบและจัดการระบบรักษาความปลอดภัย เช่น การใช้งานระบบการตรวจจับการบุกรุก และระบบการตรวจสอบระบบการเข้าถึง

๘.๕ การตรวจสอบและการวิเคราะห์ข้อมูลและการรายงานการดำเนินการของ Log Analyzer เพื่อตรวจสอบปัญหาและข้อผิดพลาดที่อาจเกิดขึ้น และดำเนินการปรับปรุงตามได้เมื่อจำเป็น

๘.๖ การตรวจสอบประสิทธิภาพการทำงานของ Log Analyzer เพื่อให้มั่นใจว่ามันทำงานอย่างมีประสิทธิภาพและมีประสิทธิภาพที่สูงสุด

๙. การบำรุงรักษาอุปกรณ์เครื่องสำรองไฟฟ้า ได้แก่

๙.๑ ทำการตรวจสอบและทดสอบเครื่องสำรองไฟฟ้าอย่างเป็นระยะเวลาเพื่อตรวจสอบความพร้อมใช้งานและประสิทธิภาพในการทำงาน รวมถึงการทดสอบระบบเครื่องสำรองไฟฟ้าในสถานการณ์ฉุกเฉิน เพื่อให้มั่นใจว่ามันทำงานได้อย่างถูกต้อง

๙.๒ บำรุงรักษาเครื่องสำรองไฟฟ้าอย่างสม่ำเสมอตามคำแนะนำจากผู้ผลิต โดยรวมถึงการทำความสะอาด การตรวจสอบสายไฟและสวิตช์ การตรวจสอบและเปลี่ยนอะไหล่ที่ชำรุดหรือเสื่อมสภาพ เป็นต้น

๙.๓ รักษาความสะอาดของเครื่องสำรองไฟฟ้าเพื่อป้องกันการสะสมของฝุ่นและสิ่งสกปรกอื่นที่อาจทำให้เครื่องทำงานไม่สมบูรณ์

๙.๔ ตรวจสอบและบันทึกประวัติการทำงานของเครื่องสำรองไฟฟ้า เช่น การทดสอบ การบำรุงรักษา และปัญหาที่เกิดขึ้น เพื่อให้สามารถติดตามและวิเคราะห์ปัญหาได้อย่างมีประสิทธิภาพ

๙.๕ การเตรียมการและการทดสอบแผนฉุกเฉินเพื่อให้การทำงานของเครื่องสำรองไฟฟ้ามีประสิทธิภาพและปลอดภัย

๑๐. การบำรุงรักษาอุปกรณ์สำหรับจัดเก็บข้อมูลแบบภายนอก (External Storage) ได้แก่

๑๐.๑ การเก็บอยู่ในสภาพแวดล้อมที่เหมาะสม ในอุณหภูมิสูงมากหรือต่ำมากเกินไป เพราะอุปกรณ์อาจเสียหายได้ ควรเก็บในที่ที่มีอุณหภูมิและความชื้นเหมาะสม

๑๐.๒ รักษาความสะอาดของอุปกรณ์อย่าให้มีฝุ่นหรือสิ่งสกปรกที่อาจทำให้อุปกรณ์เสียหาย

๑๐.๓ ตรวจสอบสภาพของอุปกรณ์อย่างสม่ำเสมอ เช่น ตรวจสอบสายเชื่อมต่อ สภาพเสียงของอุปกรณ์ และสภาพการทำงานของอุปกรณ์

๑๐.๔ ทำการสำรองข้อมูลอย่างสม่ำเสมอเพื่อป้องกันข้อมูลไม่สูญหายในกรณีที่เกิดเหตุฉุกเฉิน เช่น การสำรองข้อมูลไปยังอุปกรณ์ภายนอกเสริม

๑๐.๕ การซื้อประกันสำหรับอุปกรณ์ภายนอกเพื่อป้องกันการเสียหายหรือสูญหายของข้อมูล

๑๐.๖ การป้องกันจากการสูญหายโดยใช้เทคโนโลยีการเข้ารหัสข้อมูลเพื่อป้องกันการถูกเข้าถึงโดยไม่พึงประสงค์ และหลีกเลี่ยงการสูญหายของข้อมูลด้วยการสำรองข้อมูลในที่ที่ปลอดภัย

๑๑. การบำรุงรักษาอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย ได้แก่

๑๑.๑ ตรวจสอบการทำงานของระบบเครือข่ายอย่างสม่ำเสมอ โดยรวบรวมข้อมูลการใช้งานประสิทธิภาพและเหตุการณ์ต่าง ๆ เพื่อตรวจสอบปัญหาและอุบัติเหตุที่อาจเกิดขึ้น

๑๑.๒ การป้องกันและตรวจจับการบุกรุก ใช้เครื่องมือเพื่อเพิ่มการป้องกันการกระทำที่ไม่เหมาะสมในระบบ เช่น การใช้ระบบไฟร์วอลล์ (Firewall) และระบบตรวจจับการบุกรุก (IPS) เป็นต้น

๑๑.๓ การอัปเดตและปรับปรุงซอฟต์แวร์และฮาร์ดแวร์ให้เป็นระยะ เพื่อให้ระบบมีความปลอดภัย และมีประสิทธิภาพที่ดีที่สุด

๑๑.๔ การจัดการข้อมูลและการสำรองข้อมูล เพื่อป้องกันข้อมูลจากการสูญหายหรือเสียหาย

๑๑.๕ การจัดการความปลอดภัยด้านการจำกัดสิทธิ์ในการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย เช่น การใช้ระบบการรับรองตัวตน (Authentication) การใช้ระบบการเข้ารหัส (Encryption) เป็นต้น

๑๒. การบำรุงรักษาอุปกรณ์ป้องกันและตรวจจับการบุกรุก (IPS) ได้แก่

๑๒.๑ การตรวจสอบความถูกต้องของการตั้งค่าและการทำงานของ IPS เพื่อให้มั่นใจว่าระบบทำงานอย่างมีประสิทธิภาพ และป้องกันการบุกรุกได้อย่างมีประสิทธิภาพ

๑๒.๒ การอัปเดตซอฟต์แวร์และลิขสิทธิ์ของ IPS เพื่อให้มีความสามารถในการตรวจจับและป้องกันการโจมตีที่สมบูรณ์และปรับปรุงประสิทธิภาพในการป้องกัน

๑๒.๓ การวิเคราะห์ข้อมูล การตรวจสอบข้อมูลและบันทึกการเหตุการณ์ที่เกี่ยวข้องกับการโจมตีหรือการบุกรุก เพื่อทบทวนและวิเคราะห์แหล่งกำเนิดของปัญหาและการวางแผนในการป้องกันเหตุการณ์ในอนาคต

๑๒.๔ การตรวจสอบการทำงาน การตรวจสอบความถูกต้องของระบบ IPS โดยตรวจสอบรายงานและการแจ้งเตือนเพื่อตรวจสอบว่าระบบทำงานตามที่คาดหวังหรือไม่ และทำการแก้ไขปรับปรุงตามความต้องการเพื่อให้ระบบทำงานอย่างมีประสิทธิภาพ

๑๒.๕ การเฝ้าระวังระบบและการตรวจสอบการทำงานของ IPS เพื่อตรวจจับและระบุการฝ่าฝืนหรือการขาดความสามารถของระบบในการป้องกัน

การทำตามขั้นตอนเหล่านี้จะช่วยให้ระบบเครือข่ายคอมพิวเตอร์ทำงานอย่างเสถียรและป้องกันปัญหาที่อาจเกิดขึ้นได้ในอนาคต นอกจากนี้ การบำรุงรักษาเป็นสิ่งสำคัญที่ช่วยให้ระบบเครือข่ายมีอายุการใช้งานที่ยาวนานและประสิทธิภาพสูงขึ้นในระยะยาว

บทที่ ๔
ผลการดำเนินงาน

จากวิธีการดำเนินงานเพื่อปรับปรุงการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ ให้มีประสิทธิภาพมากยิ่งขึ้น สามารถสรุปการดำเนินงานได้ดังนี้

๔.๑ ขั้นตอนการดำเนินงาน

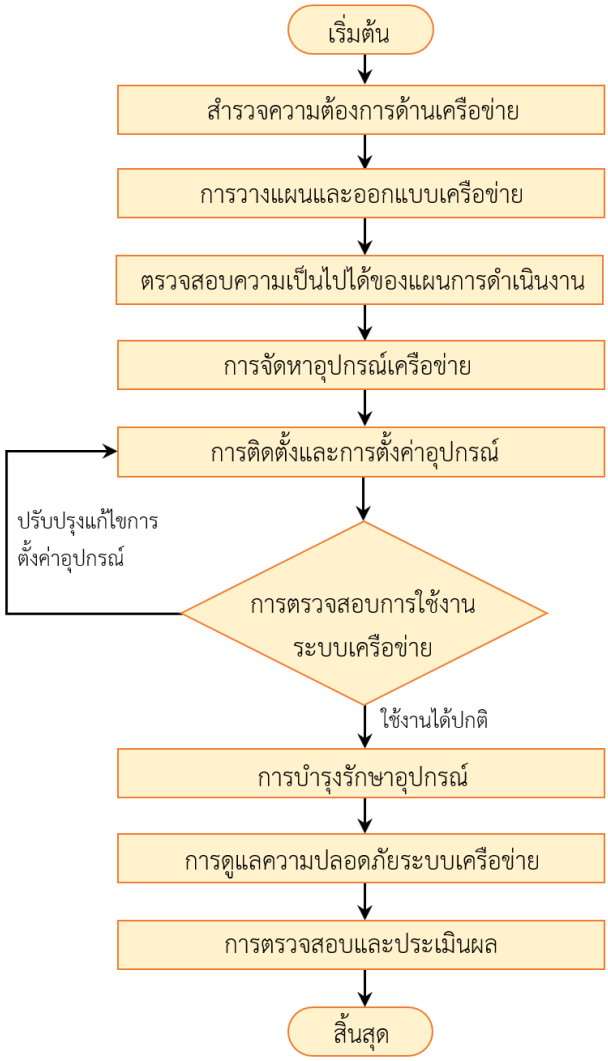
๔.๒ ผลการนำอุปกรณ์เครือข่ายมาปรับปรุงการบริหารจัดการเครือข่ายในองค์กร

๔.๓ แผนการดูแลบำรุงรักษาระบบสารสนเทศ

๔.๔ แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ

๔.๑ ขั้นตอนการดำเนินงาน

การดำเนินงานปรับปรุงระบบเครือข่ายเป็นกระบวนการที่มีขั้นตอนการดำเนินงานที่สำคัญที่จะช่วยให้การบริหารจัดการเครือข่ายเป็นไปอย่างมีประสิทธิภาพ ในการปรับปรุงการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ของอาคารศูนย์การแพทย์บางรัก ผู้จัดทำได้นำทฤษฎีวงจรคุณภาพ PDCA มาประกอบกับการวิเคราะห์ขั้นตอนการดำเนินงานมีขั้นตอนดังนี้



ตารางที่ ๒ นำทฤษฎีวงจรคุณภาพ PDCA ประกอบการวิเคราะห์ขั้นตอนการดำเนินงาน

วงจรคุณภาพ PDCA	ขั้นตอนการดำเนินงาน
การวางแผนปฏิบัติงาน (Plan)	**การสำรวจความต้องการด้านเครือข่าย** - เพื่อทราบปัญหาปัจจุบันของเครือข่ายที่มีอยู่ การประเมินความต้องการของผู้ใช้จริง การพิจารณาเทคโนโลยีที่เหมาะสมกับความต้องการ - เพื่อการเก็บรวบรวมข้อมูลทรัพยากรระบบเครือข่ายที่มีอยู่ในองค์กร - เพื่อทำความเข้าใจความต้องการและความพึงพอใจต่อการใช้งานเครือข่ายคอมพิวเตอร์ เช่น อินเทอร์เน็ต ระบบเครือข่ายภายในองค์กร เป็นต้น - เพื่อการวิเคราะห์ข้อมูล สำหรับจัดทำแผนดำเนินงานและการออกแบบเครือข่ายที่เหมาะสมกับงบประมาณที่ได้รับและตอบสนองต่อความต้องการของบุคลากรในองค์กร **การวางแผนและออกแบบเครือข่าย** - วางแผนการเชื่อมต่อระหว่างอุปกรณ์เครือข่าย เช่น เซิร์ฟเวอร์ สวิตช์ ระบบเก็บข้อมูล เป็นต้น - กำหนดความต้องการด้านประสิทธิภาพ เช่น การรองรับผู้ใช้พร้อมกันจำนวนมาก การควบคุมการใช้งานแบนด์วิดธ์ เป็นต้น - ออกแบบโครงสร้างและสถาปัตยกรรมของระบบเครือข่ายที่เหมาะสมกับความต้องการและเป้าหมาย - เลือกใช้เทคโนโลยีและอุปกรณ์ที่เหมาะสมและทันสมัยสำหรับการบริหารจัดการระบบเครือข่ายขององค์กร **ตรวจสอบความเป็นไปได้ของแผนการดำเนินงาน** - วิเคราะห์และประเมินความเป็นไปได้ของแผนการดำเนินงาน เช่น การตรวจสอบความเสี่ยง การประมาณการค่าใช้จ่าย และการแสดงผลกระทบในการดำเนินงาน
การดำเนินงานตามแผน (Do)	**การจัดหาอุปกรณ์เครือข่าย** - การเลือกและจัดซื้ออุปกรณ์เครือข่ายตามความเหมาะสมกับความต้องการ และงบประมาณที่ได้รับ - การตรวจสอบคุณภาพและประสิทธิภาพของอุปกรณ์เครือข่ายที่สอดคล้องกับมาตรฐาน

วงจรคุณภาพ PDCA	ขั้นตอนการดำเนินงาน
	การติดตั้งและการตั้งค่าอุปกรณ์เครือข่าย - การติดตั้งอุปกรณ์เครือข่ายตามแผนการดำเนินงานที่ออกแบบ - การกำหนดค่าเริ่มต้นของอุปกรณ์ เช่น การกำหนดวงเน็ตเวิร์ค การกำหนด IP Address การกำหนดค่าเร้าเตอร์ การตั้งค่าการรักษาความปลอดภัย เป็นต้น
การตรวจสอบ (Check)	**การตรวจสอบการใช้งานระบบเครือข่าย** - ทดสอบระบบเครือข่ายเพื่อตรวจสอบความถูกต้องและประสิทธิภาพในการใช้งาน - ตรวจสอบความปลอดภัยของระบบเครือข่าย ปรับปรุงแก้ไขปัญหาหรือข้อบกพร่องที่พบ - ทดสอบซอฟต์แวร์และแอปลิเคชั่นเพื่อให้แน่ใจว่าสามารถใช้งานร่วมกับระบบหรืออุปกรณ์ที่มีอยู่เดิมในองค์กรได้ **การบำรุงรักษาอุปกรณ์เครือข่าย** - การทำความสะอาดที่บ่อยป้องกันการสะสมของฝุ่นและอุภูมิที่สามารถทำให้เกิดปัญหาได้ เช่น การทำความสะอาดที่ระบบระบายความร้อน หรือการใช้เครื่องเป่าลม เป็นต้น - การตรวจสอบสภาพฮาร์ดแวร์หรือซอฟต์แวร์เพื่อช่วยในการป้องกันการรั่วไหลของข้อมูล - การสำรองข้อมูลเพื่อป้องกันข้อมูลศูนย์หาย
การนำผลการประเมินมาปรับปรุงงาน (Action)	**การดูแลความปลอดภัยระบบเครือข่ายคอมพิวเตอร์** - การวางแผนและการดำเนินงานเพื่อป้องกันการบุกรุกและการละเมิดความปลอดภัยของเครือข่าย - การพัฒนานโยบายและมาตรการเพื่อรักษาความปลอดภัยของข้อมูลและระบบที่ใช้ปฏิบัติงานในองค์กร **การปรับปรุงและพัฒนา** - การตรวจสอบและปรับปรุงโครงสร้างเครือข่ายเพื่อให้เหมาะสมกับความต้องการและเทคโนโลยีใหม่ ๆ เพื่อให้ระบบเครือข่ายมีประสิทธิภาพและมีความสามารถในการรองรับการเปลี่ยนแปลงขององค์กรในอนาคต

๔.๒ ผลการนำอุปกรณ์เครือข่ายมาปรับปรุงการบริหารจัดการเครือข่ายในองค์กร

การนำอุปกรณ์เครือข่ายมาปรับปรุงการบริหารจัดการเครือข่ายในองค์กร ช่วยเพิ่มประสิทธิภาพในการทำงานของบุคลากร ช่วยลดค่าใช้จ่าย และเพิ่มความเสถียรภาพของเครือข่าย ประโยชน์ของการนำอุปกรณ์เครือข่ายมาใช้ในการบริหารจัดการระบบเครือข่ายในองค์กรมีดังนี้

๑) มีระบบบริหารจัดการเครือข่ายที่มีประสิทธิภาพ รองรับการใช้งานระบบเครือข่ายได้ครอบคลุมพื้นที่ขององค์กร ได้แก่

๑.๑) การนำอุปกรณ์กระจายสัญญาณ (L3 Switch) มาเป็นตัวกลางในการส่งข้อมูลระหว่างเครือข่ายในองค์กร โดยดำเนินการดังนี้

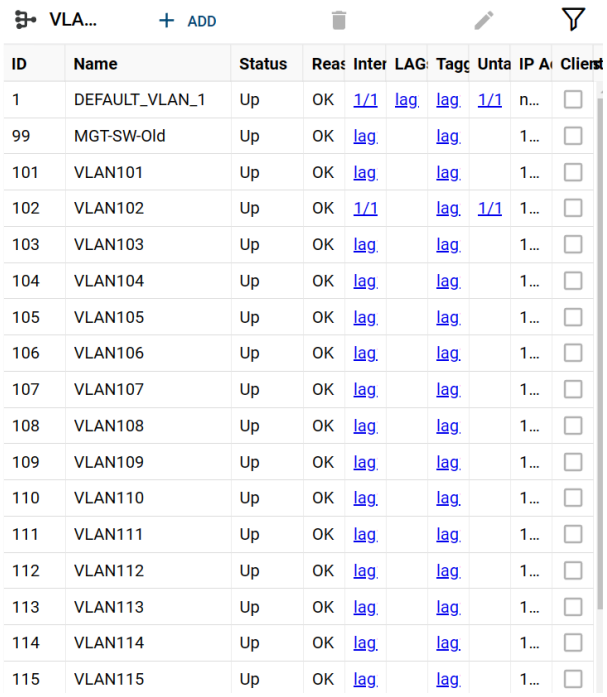
๑.๑.๑) การทำเราท์ (Routing) สำหรับใช้ในการตรวจสอบเส้นทางที่เหมาะสมสำหรับการส่งข้อมูล จากนั้นจึงทำการส่งข้อมูลไปยังเครื่องปลายทางตามเส้นทางที่กำหนด

VRF: default

Prefix	Nexthop	Interface	VRF(egress)	Origin/ Type	Distance/ Metric	Age
0.0.0.0/0	10.0.1.1	vlan198	-	S	[1/0]	00m:02w:02d
10.0.1.0/29	-	vlan198	-	C	[0/0]	-
10.0.1.2/32	-	vlan198	-	L	[0/0]	-
10.0.86.0/29	10.0.1.1	vlan198	-	O	[110/101]	00m:02w:01d
10.0.250.0/23	10.0.1.1	vlan198	-	O/E2	[110/10]	00m:02w:01d
10.0.252.0/23	-	vlan252	-	C	[0/0]	-
10.0.252.254/32	-	vlan252	-	L	[0/0]	-
10.0.254.0/24	10.0.1.1	vlan198	-	O/E2	[110/10]	00m:02w:00d
10.0.255.0/24	10.0.1.1	vlan198	-	O/E2	[110/10]	00m:02w:00d
10.212.134.0/24	10.0.1.1	vlan198	-	O/E2	[110/10]	00m:02w:01d
192.168.1.0/24	10.0.1.1	vlan198	-	O	[110/101]	00m:02w:00d
192.168.99.0/24	-	vlan99	-	C	[0/0]	-
192.168.99.1/32	-	vlan99	-	L	[0/0]	-
192.168.101.0/24	-	vlan101	-	C	[0/0]	-
192.168.101.1/32	-	vlan101	-	L	[0/0]	-
192.168.102.0/24	-	vlan102	-	C	[0/0]	-
192.168.102.1/32	-	vlan102	-	L	[0/0]	-
192.168.103.0/24	-	vlan103	-	C	[0/0]	-
192.168.103.1/32	-	vlan103	-	L	[0/0]	-
192.168.104.0/24	-	vlan104	-	C	[0/0]	-
192.168.104.1/32	-	vlan104	-	L	[0/0]	-
192.168.105.0/24	-	vlan105	-	C	[0/0]	-
192.168.105.1/32	-	vlan105	-	L	[0/0]	-
192.168.106.0/24	-	vlan106	-	C	[0/0]	-
192.168.106.1/32	-	vlan106	-	L	[0/0]	-
192.168.107.0/24	-	vlan107	-	C	[0/0]	-
192.168.107.1/32	-	vlan107	-	L	[0/0]	-
192.168.108.0/24	-	vlan108	-	C	[0/0]	-
192.168.108.1/32	-	vlan108	-	L	[0/0]	-
192.168.109.0/24	-	vlan109	-	C	[0/0]	-
192.168.109.1/32	-	vlan109	-	L	[0/0]	-
192.168.110.0/24	-	vlan110	-	C	[0/0]	-
192.168.110.1/32	-	vlan110	-	L	[0/0]	-
192.168.111.0/24	-	vlan111	-	C	[0/0]	-
192.168.111.1/32	-	vlan111	-	L	[0/0]	-
192.168.112.0/24	-	vlan112	-	C	[0/0]	-
192.168.112.1/32	-	vlan112	-	L	[0/0]	-
192.168.113.0/24	-	vlan113	-	C	[0/0]	-
192.168.113.1/32	-	vlan113	-	L	[0/0]	-
192.168.114.0/24	-	vlan114	-	C	[0/0]	-
192.168.114.1/32	-	vlan114	-	L	[0/0]	-
192.168.115.0/24	-	vlan115	-	C	[0/0]	-
192.168.115.1/32	-	vlan115	-	L	[0/0]	-
192.168.116.0/24	-	vlan116	-	C	[0/0]	-

ภาพที่ ๒๐ : IP Route

๑.๑.๒) การแบ่งแยกเครือข่ายโดยการสร้าง Virtual LANs (VLANs) เพื่อแบ่งเครือข่ายออกเป็นกลุ่มเพื่อความสะดวกในการบริหารจัดการและความปลอดภัยของเครือข่ายในองค์กร



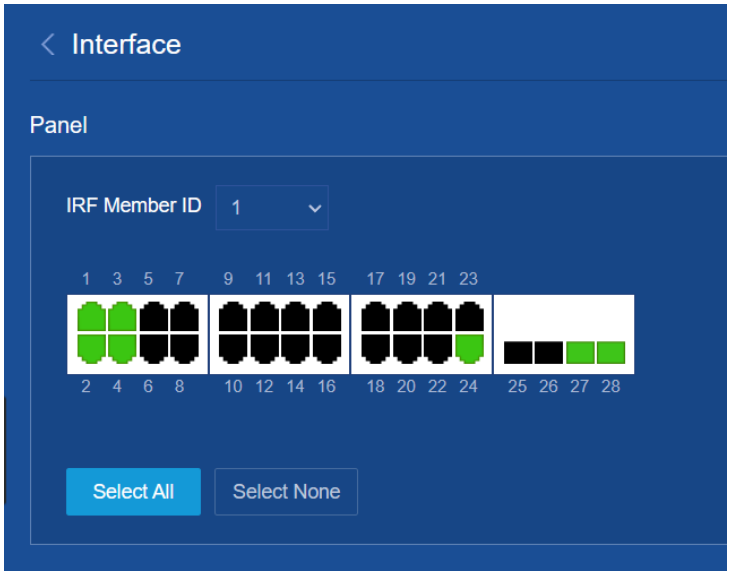
ID	Name	Status	Reas	Inter	LAG	Tagg	Unta	IP A	Client
1	DEFAULT_VLAN_1	Up	OK	1/1	lag	lag	1/1	n...	
99	MGT-SW-Old	Up	OK	lag		lag		1...	
101	VLAN101	Up	OK	lag		lag		1...	
102	VLAN102	Up	OK	1/1		lag	1/1	1...	
103	VLAN103	Up	OK	lag		lag		1...	
104	VLAN104	Up	OK	lag		lag		1...	
105	VLAN105	Up	OK	lag		lag		1...	
106	VLAN106	Up	OK	lag		lag		1...	
107	VLAN107	Up	OK	lag		lag		1...	
108	VLAN108	Up	OK	lag		lag		1...	
109	VLAN109	Up	OK	lag		lag		1...	
110	VLAN110	Up	OK	lag		lag		1...	
111	VLAN111	Up	OK	lag		lag		1...	
112	VLAN112	Up	OK	lag		lag		1...	
113	VLAN113	Up	OK	lag		lag		1...	
114	VLAN114	Up	OK	lag		lag		1...	
115	VLAN115	Up	OK	lag		lag		1...	

ภาพที่ ๒๑ : การสร้าง VLANs

๑.๑.๓) สามารถสนับสนุนการทำงานของหลายเครือข่ายพร้อมกันได้ โดยรองรับการทำเราท์แยกและจัดการของแต่ละเครือข่ายโดยอิสระ เช่น ระบบกล้องวงจรปิด ระบบโทรศัพท์ IP Phone และระบบเครือข่าย สามารถใช้งานร่วมกันได้

๑.๒) การนำอุปกรณ์กระจายสัญญาณ (L2 Switch) มาใช้ในการส่งข้อมูลภายในเครือข่ายขององค์กรโดยดำเนินการดังนี้ โดยดำเนินการดังนี้

๑.๒.๑) ทำการสร้างและจัดการ VLAN ให้สามารถแยกและจัดกลุ่มอุปกรณ์ต่าง ๆ ในเครือข่ายแต่ละชั้นขององค์กร เช่น ระบบโทรศัพท์ IP Phone และระบบเครือข่าย และอุปกรณ์กระจายสัญญาณแบบไร้สาย



ภาพที่ ๒๒ : การสร้าง Interface

๑.๒.๒) ช่วยในการสร้างเครือข่ายที่ยืดหยุ่น ทำให้ง่ายต่อการขยายเครือข่ายในอนาคต โดยการเพิ่มหรือลดอุปกรณ์ในเครือข่ายได้ง่าย

๑.๒.๓) จัดการและดูแลรักษาเครือข่ายได้อย่างมีประสิทธิภาพ เช่น การสำรองข้อมูลการกำหนดค่าและการตรวจสอบประสิทธิภาพของเครือข่าย และมีระบบสำหรับการตรวจสอบการทำงานของอุปกรณ์

๑.๓) การนำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาเพิ่มประสิทธิภาพในการใช้งานระบบเครือข่ายได้ครอบคลุมพื้นที่ในองค์กร โดยดำเนินการดังนี้

๑.๓.๑) ดำเนินการติดตั้งอุปกรณ์ AP ในตำแหน่งที่ไม่มีจุดเชื่อมต่อระบบเครือข่าย

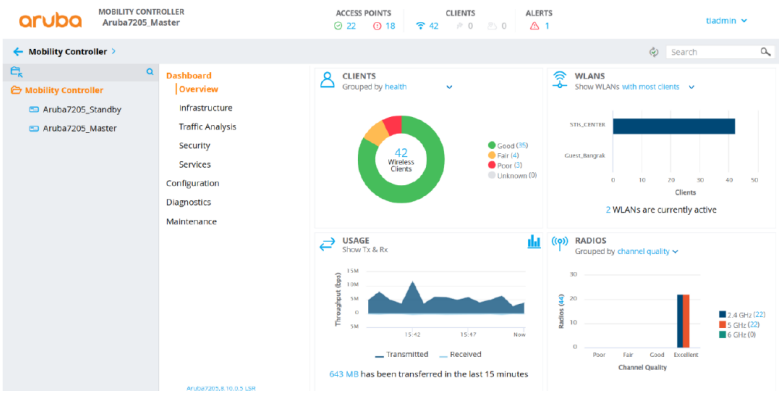
๑.๓.๒) ตั้งค่าการรับสัญญาณเครือข่ายและระบบอินเตอร์เน็ต

๑.๓.๓) กำหนดสิทธิ์การเข้าใช้งานระบบเครือข่ายในองค์กร

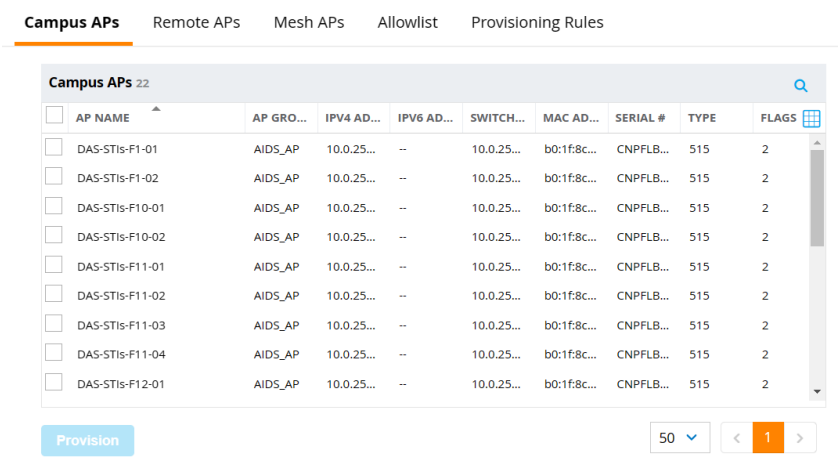
๑.๔) การนำอุปกรณ์ควบคุมเครือข่ายไร้สาย (Access Point Controller) มาใช้ในองค์กรเพื่อเพิ่มประสิทธิภาพในการใช้งานระบบเครือข่าย โดยดำเนินการดังนี้

๑.๔.๑) สำหรับการบริหารจัดการอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) จำนวน หลาย ๆ ตัว

๑.๔.๒) สำหรับการจัดการการเชื่อมต่อของอุปกรณ์ต่าง ๆ ในเครือข่ายไร้สาย เช่น การหนดค่าการเชื่อมต่อของผู้ใช้งาน การจัดการแบนด์วิชท์ การจัดการความปลอดภัย และการตรวจสอบปัญหา เป็นต้น



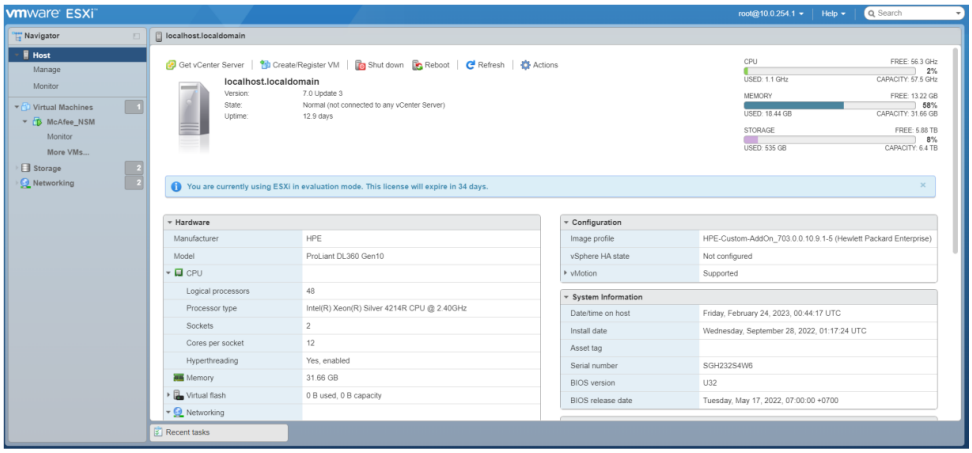
ภาพที่ ๒๓ : การสร้าง Interface



ภาพที่ ๒๔ : แสดงสถานะการทำงานของ AP (Access Point)

๑.๕) การนำเครื่องคอมพิวเตอร์แม่ข่าย (Server) มาใช้ในการจัดการระบบข้อมูลโดยดำเนินการดังนี้

๑.๕.๑) ติดตั้งซอฟต์แวร์แม่ข่ายเสมือน เพื่อใช้สำหรับบริหารจัดการระบบข้อมูลและซอฟต์แวร์ที่ใช้ภายในและภายนอกองค์กร



ภาพที่ ๒๕ : คุณลักษณะเครื่องคอมพิวเตอร์แม่ข่าย

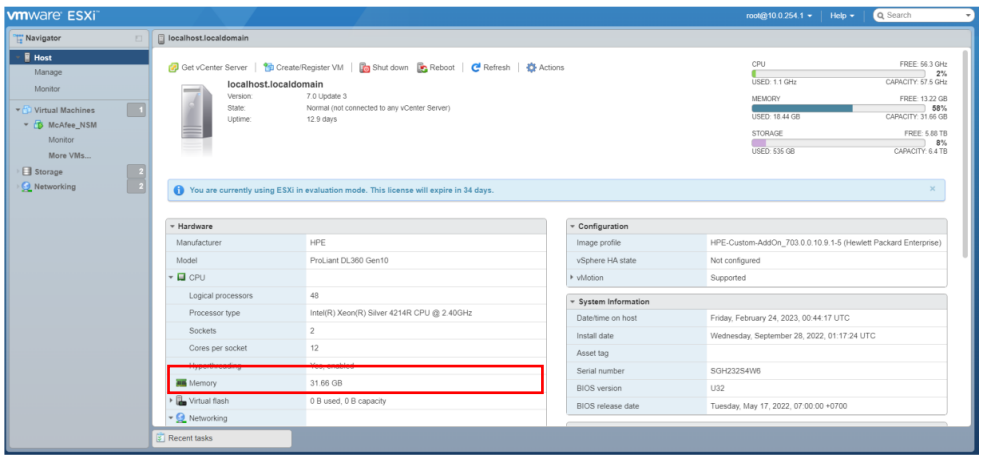
๑.๕.๒) ติดตั้งโปรแกรม HIS ของศูนย์บริการคลินิกขององค์กร เพื่อใช้ในการบริการตรวจ ดูแลรักษาโรคติดต่อทางเพศสัมพันธ์

๑.๕.๓) ติดตั้งระบบ API (Application Programming Interfaces) สำหรับเชื่อมต่อข้อมูลกับหน่วยงานภายนอก

๑.๕.๔) เพื่อใช้ในการจัดเก็บข้อมูล สำหรับการนำมาการวินิจฉัย หรือนำข้อมูลมาทำการวิเคราะห์ด้านการรักษา หรือข้อมูลด้านสถิติ เป็นต้น

๑.๕.๕) กำหนดให้เครื่องคอมพิวเตอร์แม่ข่าย สามารถสำรองข้อมูลแบบอัตโนมัติ ซึ่งช่วยลดความเสี่ยงในกรณีข้อมูลสูญหายหรือเกิดเหตุฉุกเฉิน

๑.๕.๖) การบริหารจัดการทรัพยากร เช่น การใช้งาน CPU, หน่วยความจำ (RAM) และพื้นที่จัดเก็บข้อมูล



ภาพที่ ๒๖ : หน้าจอแสดงผลหน่วยความจำ

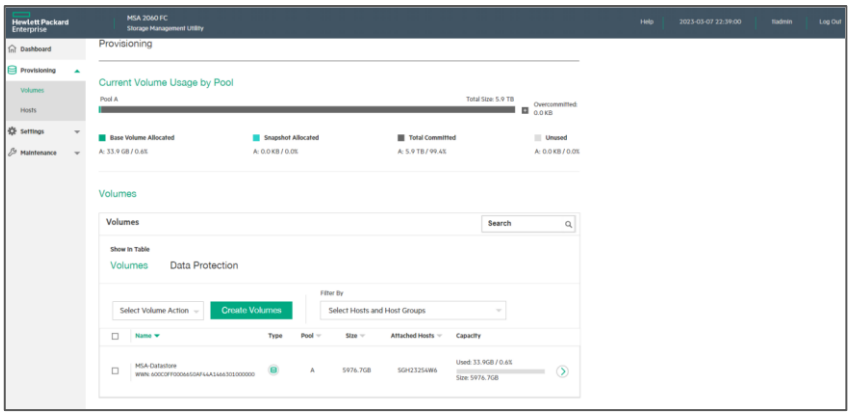
๑.๖) การนำอุปกรณ์สำหรับจัดเก็บข้อมูลแบบภายนอก (External Storage) สำหรับใช้ในการจัดเก็บ และบริหารจัดการข้อมูล

๑.๖.๑) อุปกรณ์สำหรับจัดเก็บข้อมูลแบบภายนอกช่วยเพิ่มพื้นที่จัดเก็บข้อมูลให้กับเครื่องคอมพิวเตอร์แม่ข่าย การสำรองข้อมูล log file และอุปกรณ์อื่น ๆ ซึ่งช่วยให้เก็บข้อมูลได้มากขึ้นโดยไม่ต้องเสียพื้นที่บนอุปกรณ์หลัก

๑.๖.๒) สามารถเข้าใช้งานข้อมูลผ่านระบบเครือข่ายได้อย่างสะดวก

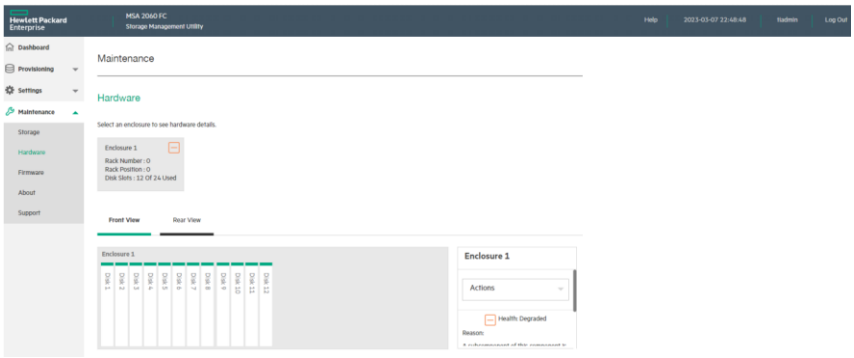
๑.๖.๓) มีระบบตรวจสอบสถานะระบบเครือข่ายขององค์กรตลอดเวลาช่วยเพิ่มความปลอดภัยของข้อมูล

๑.๖.๔) มีระบบแสดงสถานะการทำงานของอุปกรณ์ สำหรับใช้ในการบริหารจัดการอุปกรณ์ เช่น การแจ้งเตือน, Performance Data และสามารถตรวจสอบประวัติการใช้งาน



ภาพที่ ๒๗ : หน้าจอแสดงสถานะการทำงาน

๑.๖.๕) มีความยืดหยุ่นในการใช้งาน สามารถเพิ่มความจุให้กับอุปกรณ์ได้ในภายหลัง โดยไม่มีผลกระทบกับข้อมูล



ภาพที่ ๒๘ : หน้าจอแสดงสถานะของ Storage

๒) การปรับปรุงระบบไฟฟ้า เป็นปัจจัยที่สำคัญอย่างหนึ่งของการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ขององค์กรให้มีความเสถียรและประสิทธิภาพมากขึ้น โดยมีการคำนวณขนาดเครื่องสำรองไฟฟ้าและได้ดำเนินการติดตั้งเครื่องสำรองไฟฟ้าขนาด 40 KVA ให้กับตู้ติดตั้งอุปกรณ์เครือข่ายภายในห้อง Server ชั้น ๑๓ และรองรับอุปกรณ์เครือข่ายที่จะมีการดำเนินงานเข้ามาติดตั้งภายในห้อง Server ในอนาคต

การคำนวณเบื้องต้น ของ UPS[๙]

การแปลงค่า VA เป็น Watt

VA = Voltage (RMS) x Current (RMS) = V x A

VA = Watt x 1.4

คำอธิบายเพิ่มเติม

- Voltage (RMS) (Root Mean Square Voltage) คือ ค่าของแรงดันไฟฟ้าที่คำนวณจากค่ากำลังเฉลี่ยที่เกิดขึ้นเมื่อมีการใช้แรงดันไฟฟ้านั้นในการทำงานของวงจรไฟฟ้า RMS เป็นค่าที่สำคัญในไฟฟ้ากระแสสลับ (AC) และมีความหมายตรงข้ามกับแรงดันไฟฟ้ากระแสตรง (DC) ที่มีค่าคงที่
  - ตัวอย่าง
    - แรงดันไฟฟ้าภายในบ้านทั่วไปที่ใช้ในหลายประเทศมีค่า RMS ประมาณ 220-240 โวลต์ สำหรับไฟฟ้ากระแสสลับ 50 เฮิร์ตซ์
    - อุปกรณ์วัดไฟฟ้ากระแสสลับ เช่น มัลติมิเตอร์ มักจะให้ค่าแรงดันไฟฟ้าในรูปแบบ RMS เป็นต้น
- Current (RMS) (Root Mean Square Current) คือ ค่าของกระแสไฟฟ้าที่คำนวณจากค่ากำลังเฉลี่ยที่เกิดขึ้นเมื่อมีการใช้กระแสไฟฟ้านั้นในการทำงานของวงจรไฟฟ้า RMS เป็นค่าที่สำคัญในไฟฟ้ากระแสสลับ (AC) และมีความหมายตรงข้ามกับกระแสไฟฟ้ากระแสตรง (DC) ที่มีค่าคงที่
  - ตัวอย่าง
    - กระแสไฟฟ้าในวงจรภายในบ้านมักจะถูกวัดในรูปแบบ RMS เพื่อให้แน่ใจว่าอุปกรณ์ไฟฟ้าต่างๆ สามารถทำงานได้อย่างปลอดภัยและมีประสิทธิภาพ
    - อุปกรณ์วัดไฟฟ้ากระแสสลับ เช่น มัลติมิเตอร์ มักจะให้ค่ากระแสไฟฟ้าในรูปแบบ RMS เป็นต้น
- วัตต์ (Watt) เป็นหน่วยวัดกำลังไฟฟ้าในระบบหน่วยสากล (SI) โดยมีสัญลักษณ์คือ W หน่วยวัตต์ถูกใช้เพื่อวัดอัตราการใช้พลังงานหรือการผลิตพลังงานของอุปกรณ์ไฟฟ้าหรือเครื่องจักร
  - ตัวอย่าง
    - หลอดไฟที่มีค่า 60 Watt หมายถึงหลอดไฟนั้นใช้พลังงาน 60 Watt ต่อชั่วโมง
    - เครื่องปรับอากาศที่ระบุว่าใช้พลังงาน 2000 Watt หมายถึงการใช้พลังงาน 2000 Watt ในหนึ่งชั่วโมง เป็นต้น

การคำนวณขนาดกำลังจ่ายของ UPS ที่เหมาะสมกับอุปกรณ์ไฟฟ้า ปฏิบัติดังนี้

๑. ทำรายการอุปกรณ์ไฟฟ้าที่จะต่อพ่วงกับระบบ UPS ทั้งหมด เช่น เครื่องคอมพิวเตอร์ อุปกรณ์กระจายสัญญาณ จอภาพ หรืออุปกรณ์ที่จำเป็นอื่น ๆ โดยอุปกรณ์ไฟฟ้าแต่ละชนิดจะมีป้ายแสดงค่ากำลัง (Nameplate) เพื่อระบุถึงแรงดันไฟฟ้าและกระแสไฟฟ้าที่ต้องการสำหรับใช้งานโดยทั่วไปจะอยู่ที่ด้านหลังของเครื่อง
   - ให้คำนวณค่า VA โดยคูณค่า Volt และ Amps เข้าด้วยกัน
   - อุปกรณ์ไฟฟ้าบางชนิดอาจให้ค่ามาในรูปของพลังงานไฟฟ้าในหน่วยวัตต์ (Watt-W) ให้แปลงกลับเป็นค่า VA โดยการคูณค่าวัตต์ด้วย 1.4

๒. รวมค่า VA ของอุปกรณ์ไฟฟ้าทั้งหมดในรายการที่จะต่อพ่วงกับระบบ UPS

๓. เลือก UPS ที่จะสามารถจ่ายไฟได้พอเพียงต่อระดับค่า VA ของอุปกรณ์ไฟฟ้าทั้งหมด

ตัวอย่างการคำนวณ

การคำนวณขนาดของ UPS ที่สามารถใช้กับเครื่องคอมพิวเตอร์ ขนาด 220V 1.5A, เครื่องพิมพ์ Inkjet ขนาด 50 Watt และโมเด็ม ขนาด 20 Watt มีวิธีคำนวณดังนี้

- VA ของเครื่องคอมพิวเตอร์ ขนาด 220V 1.5A = 220 x 1.5 = 330 VA
- VA ของเครื่องพิมพ์ Inkjet ขนาด 50 Watt = 50 x 1.4 = 70 VA
- VA ของโมเด็ม ขนาด 20 Watt = 20 x 1.4 = 28 VA
- VA รวม = 330 + 70 + 28 = 428 VA

ดังนั้น ขนาดของ UPS ที่สามารถต่อพ่วงกับเครื่องคอมพิวเตอร์และอุปกรณ์ดังกล่าวได้อย่างปลอดภัย ต้องมีขนาด 428 VA ขึ้นไป

หมายเหตุ : โดยทั่วไปหากเลือก UPS ที่มีกำลัง VA เท่ากับค่า VA รวมของอุปกรณ์ไฟฟ้าที่จะนำไปต่อพ่วงทั้งหมด UPS จะจ่ายไฟที่ Full Load และจะทำการจ่ายพลังงานไฟฟ้าสำรองได้ไม่นาน หากต้องการระยะเวลาการจ่ายพลังงานไฟฟ้าสำรองที่เพิ่มขึ้น ต้องขยายค่า VA ของ UPS หรือเพิ่มจำนวนแบตเตอรี่ให้มากขึ้น

<u>การคำนวณ Backup Time ของ UPS</u>

เครื่องสำรองไฟฟ้า (UPS) โดยส่วนมากจะมีค่าบอก Backup Time ว่าสามารถสำรองกระแสไฟฟ้าได้กี่นาที ขึ้นอยู่กับ Load โดยการคิดค่า Load เช่น 1000 VA, 600 Watt จะจ่ายกระแสไฟฟ้าได้ ๑๕ นาที เป็นต้น หลักการคำนวณเพื่อบอก Backup Time ได้ ต้องตรวจสอบจาก Spec ของ Battery กับ Efficiency ของเครื่องสำรองไฟฟ้ามีค่าที่ใช้หลัก ๆ มี ๔ ข้อดังนี้

- Battery Capacity มีหน่วยเป็น Ah (Ampere-Hour) คือแปลว่า มันสามารถจ่ายไฟคงที่ที่ x Amps เป็นเวลา 1 ชั่วโมง
- Battery Voltage เช่น 12V
- Efficiency คือค่าประสิทธิภาพของ UPS จะมีค่าเป็น %
- อัตรากินพลังงานของ Load เป็น Watts, VA หรือเป็น Amp

หมายเหตุ : ไฟ AC, Watts ~ = Volt x Ampไฟ DC, Watts = Volt x Amp

ตัวอย่างการคำนวณ

อุปกรณ์กินไฟ 200 วัตต์ คงที่, เครื่องสำรองไฟฟ้ามี Battery ขนาด 10Ah จำนวน ๑ ตัว, Efficiency 90% efficiency 90% แสดงว่า เครื่องสำรองไฟฟ้าสามารถแปลงไฟจาก Battery 100 วัตต์ จะจ่ายได้ 90 วัตต์ Battery จะต้องเสียกำลังไฟฟ้าเพื่อแปลงกระแสไฟฟ้าให้ได้ Output ที่ 200 วัตต์ ดังนั้น วัตต์ที่ใช้จาก Battery = {200/(90/100)} =~ 222.22 Watts จากไฟ DC Watts = Volt x Amp ดังนั้น A = Watts/Volt = 222.22/12 = ~ 18.52A แสดงว่ามันกินไฟจาก Battery เท่ากับ 18.52A สรุปคือนำ Ampere-Hour ของ Battery หารด้วย Ampere-Hour ของอุปกรณ์ที่ใช้งาน Ah_bat/A_use จะมีค่าเท่ากับ 10 Ah/18.52 A = ~ 0.54h คือ ๐.๕๔ ชั่วโมง ค่าที่ได้คือประมาณครึ่งชั่วโมง

จากการคำนวณขนาดของ UPS และ Backup Time จึงนำเครื่องสำรองไฟฟ้าขนาด 40 KVA ที่มี UPS กับ Battery แยกกัน โดย UPS มีความสามารถในการจ่าย Load และมี Battery ที่สามารถสำรองไฟฟ้าให้กับอุปกรณ์เครือข่ายภายในห้อง Server ชั้น ๑๓ ขององค์กรได้อย่างต่อเนื่องและมีประสิทธิภาพเพื่อความปลอดภัยของอุปกรณ์และระบบข้อมูล

ตัวอย่างการคำนวณ ขนาด UPS สำหรับตู้ติดตั้งอุปกรณ์เครือข่าย (ตู้ Rack) ภายในห้อง Server ชั้น ๑๓

รายการ	จำนวน	กระแสไฟฟ้า	การคำนวณ	ขนาด (VA)
HPE 5140	2	100 Vac240 Vac	240V x 1.4 x 2 เครื่อง	720
FortiNet FortiADC 120F	1	100 - 240Vac, 1.5A	240V x 1.5A	360
FortiNet FortiGate 601E	1	100 - 240Vac, 1.5A	240V x 1.5A	360
Softnix Logger SLG-SA 3	1	400Watt	400Watt x 1.4	560
Aruba 6300F	2	110 to 220V AC in	220V x 1.4 x 2 เครื่อง	616
Aruba 7205	2	75.2Watt	75.2Watt x 1.4 x 2 เครื่อง	210.56
Sofnix SDP-LA	1	240 Vac	240V x 1.4	336
HPE MSA2060	1	100 Vac - 240 Vac	240V x 1.4	336
HPE DL360 Gen10	1	200Watt	200Watt x 1.4	280
Trellix Network NS7500	1	300Watt	300Watt x 1.4	420
			Total	**4198.56**

จากการคำนวณขนาดของ UPS ที่สามารถต่อพ่วงกับอุปกรณ์ดังกล่าวได้อย่างปลอดภัย คือ 4200 VA หรือ 4.2 KVA ขึ้นไป และการนำเครื่องสำรองไฟฟ้า ขนาด 40 KVA มาใช้ในองค์กรเพื่อให้เกิมความเสถียรภาพด้านการใช้พลังงานไฟฟ้า และประโยชน์ที่ได้รับจากการดำเนินการ ดังนี้

๒.๑) ช่วยเพิ่มประสิทธิภาพของระบบเครือข่ายที่ต้องใช้พลังงานไฟฟ้าอย่างต่อเนื่อง

๒.๒) เพิ่มความเชื่อถือในการใช้งาน โดยไม่มีการหยุดพัก เนื่องจากมีระบบสำรองไฟฟ้าที่พร้อมจะทำงานในกรณีของภัยพิบัติหรือการขาดแคลน

๒.๓) ป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์จากกระแสไฟฟ้าที่ไม่เสถียร เช่น การกระชากของไฟฟ้าหรือไฟฟ้าตก และช่วยยืดอายุการใช้งานของอุปกรณ์และลดค่าใช้จ่ายในการซ่อมแซมและเปลี่ยนอุปกรณ์

๒.๔) ป้องกันความเสียหายในกระบวนการประมวลผลข้อมูลหรือการเรียกใช้ข้อมูลผ่านระบบเครือข่าย เช่น ระบบ HIS ของหน่วยบริการ ระบบของห้องปฏิบัติการ (LIS) ระบบบันทุกข้อมูลผู้รับวัคซีน เป็นต้น

๒.๕) สามารถรองรับการใช้พลังงานไฟฟ้าให้กับอุปกรณ์เครือข่ายที่ติดตั้งภายในห้อง Server ได้แก่

๒.๔.๑) ตู้ rack ขนาด 27U สำหรับติดตั้งอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) อุปกรณ์กระจายสัญญาณ (L2 Switch) อุปกรณ์กระจายการทำงานสำหรับเครือข่าย (Link Load Balancer) อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย อุปกรณ์กระจายสัญญาณ (L3 Switch) อุปกรณ์ควบคุมเครือข่ายไร้สาย (Access Point Controller) อุปกรณ์วิเคราะห์การจราจรบนเครือข่าย (Log Analyzer) เครื่องสำรองไฟฟ้า(UPS) อุปกรณ์สำหรับจัดเก็บข้อมูลแบบภายนอก (External Storage) เครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System)

๒.๔.๒) อุปกรณ์กองกำจัดความชื้นภายในห้อง Server

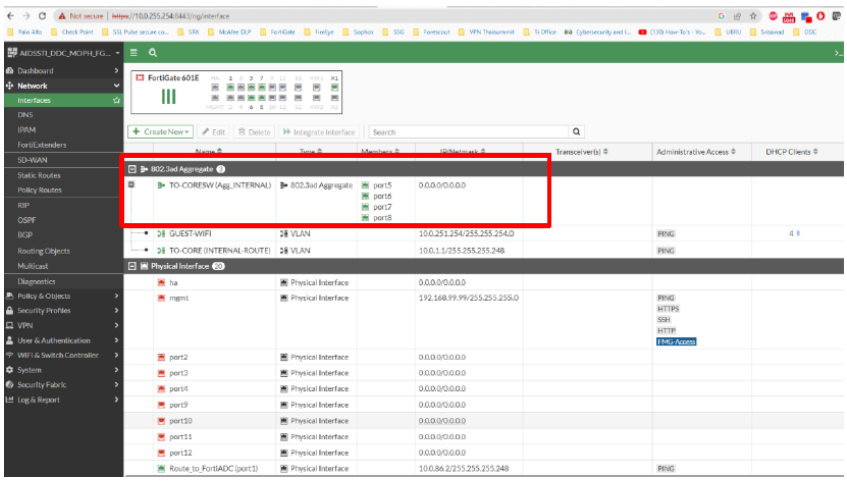
๒.๔.๓) รองรับแผนการย้ายระบบกล้องวงจรปิด (CCTV) รวมถึงรองรับการติดตั้งตู้สำหรับติดตั้งอุปกรณ์เครือข่ายของหน่วยงานอื่น ๆ ที่มีแผนจะเข้าปฏิบัติงานในอาคารศูนย์การแพทย์บางรัก และขอใช้ทรัพยากรร่วมด้วย

๒.๔.๔) รองรับแผนการเชื่อมต่อระบบไฟฟ้าภายในห้อง Server ชั้น ๑๒ โดยมีอุปกรณ์ Core Switch ที่มีการเชื่อมต่อกับอุปกรณ์กระจายสัญญาณแต่ละชั้นภายในอาคาร และระบบโทรศัพท์ IP Phone

๓) มีระบบดูแลความปลอดภัยของเครือข่ายในองค์กร

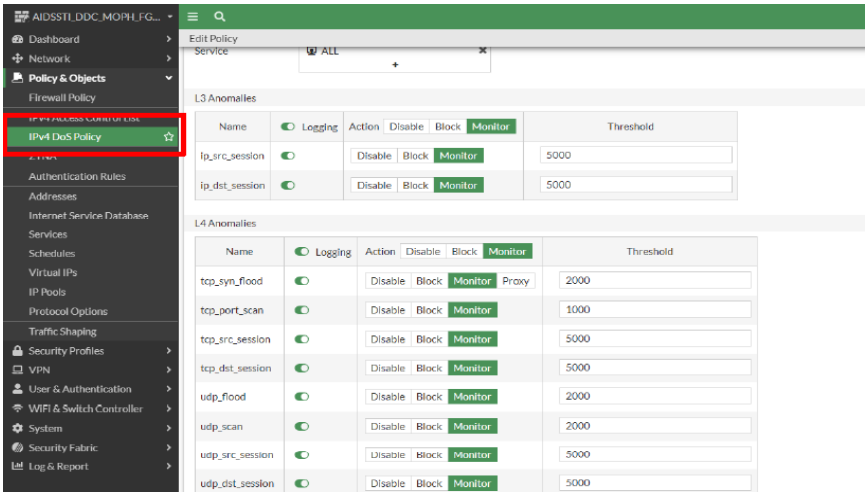
๓.๑) การนำอุปกรณ์ป้องกันเครือข่าย (Firewall) มีความสำคัญช่วยในการป้องกันระบบเครือข่ายขององค์กร มีความสามารถที่สำคัญดังนี้

๓.๑.๑) การตรวจจับและบล็อกการโจมตีที่เกิดขึ้นในเครือข่าย เช่น การตรวจจับแพ็กเก็ตข้อมูลที่มีลักษณะของมัลแวร์ การโจมตีแบบสแปม การโจมตีแบบฝังลึก และการละเมิดข้อมูล เป็นต้น



ภาพที่ ๒๙ : หน้าจอแสดงสถานะ Interfaces ของอุปกรณ์

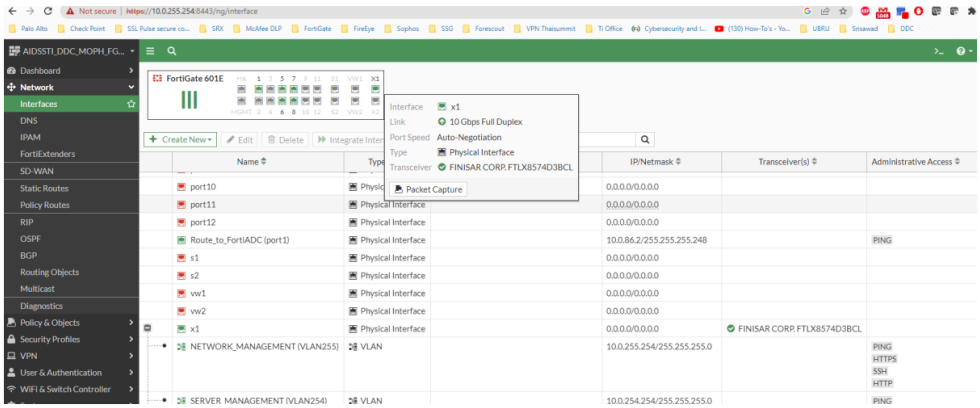
๓.๑.๒) การจัดการนโยบายการเข้าถึงและการใช้งานเครือข่ายได้ตามต้องการ เช่น กำหนดนโยบายการบล็อกการเข้าถึงเว็บไซต์ หรือการควบคุมการเข้าถึง Application



ภาพที่ ๓๐ : การจัดการเกี่ยวกับ Policy การใช้งานระบบเครือข่าย

๓.๑.๓) การวิเคราะห์และการรายงานเกี่ยวกับการใช้งานเครือข่าย ซึ่งช่วยให้ผู้ดูแลระบบสามารถเข้าใจแนวโน้มและรูปแบบการใช้งานเครือข่ายได้

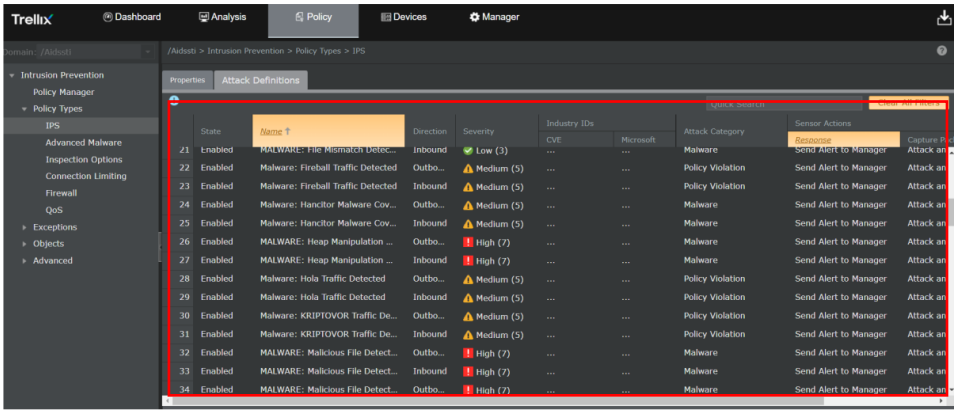
๓.๑.๔) การป้องกันการละเมิดข้อมูล โดยการตรวจสอบและบล็อกการส่งข้อมูลที่มีลักษณะที่คาดเดาได้ว่าเป็นข้อมูลที่ละเมิดความเป็นส่วนตัวหรือความลับขององค์กร



ภาพที่ ๓๑ : การตั้งค่า interface เชื่อมต่อกับ Switch Zone Server

๓.๒) การนำอุปกรณ์ป้องกันและตรวจจับการบุกรุก (IPS) มาใช้ในองค์กรเพื่อช่วยให้องค์กรมีระบบป้องกันการโจมตีและความเสี่ยงต่อข้อมูล ได้อย่างมีประสิทธิภาพ โดยการนำ IPS มาใช้งานในองค์กรมีข้อดีและประโยชน์หลายประการ เช่น

๓.๒.๑) ช่วยป้องกันการโจมตีต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบและข้อมูลขององค์กร เช่น การบุกรุกด้วยการสแกนพอร์ต การโจมตี DDoS และการโจมตีชนิดอื่น ๆ



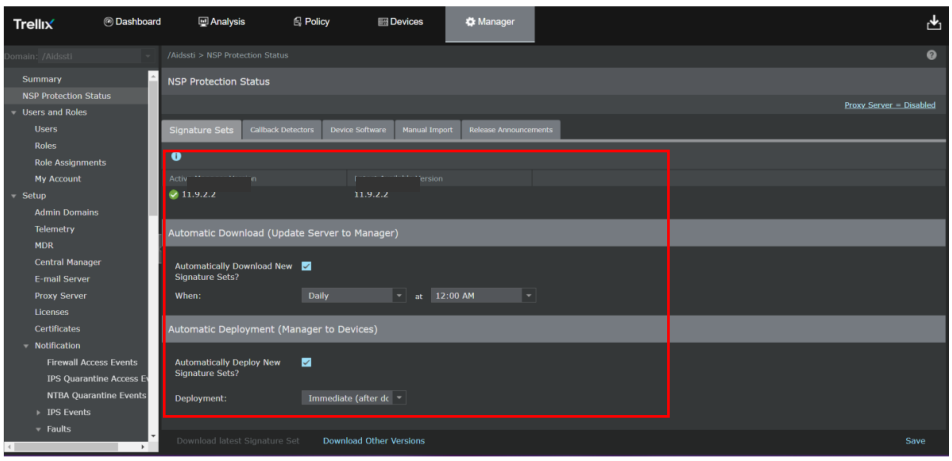
ภาพที่ ๓๒ : การป้องกันการบุกรุก

๓.๒.๒) ช่วยลดการกระทำที่ไม่พึงประสงค์ ทำให้มีประสิทธิภาพในการใช้งานและการเชื่อมต่อของผู้ใช้งานเพิ่มขึ้น

๓.๒.๓) ช่วยป้องกันการลักลอบเข้าถึงข้อมูลที่มีความลับหรือสำคัญขององค์กรและช่วยให้ข้อมูลปลอดภัยจากการถูกเข้าถึงหรือโจมตีโดยไม่ได้รับอนุญาต

๓.๒.๔) ช่วยลดความเสี่ยงทางกฎหมายที่อาจเกิดขึ้นจากการละเมิดความเป็นส่วนตัวหรือการขาดความปลอดภัยของข้อมูล และช่วยลดความเสียหายทางการเงินและภาพลักษณ์ขององค์กร

๓.๒.๕) ช่วยให้องค์กรสามารถตรวจจับและบันทึกการเหตุการณ์ที่เกิดขึ้นในระบบเครือข่ายได้ ซึ่งช่วยในการวิเคราะห์และปรับปรุงนโยบายการรักษาความปลอดภัยในอนาคต



ภาพที่ ๓๓ : การอัพเดท signature set

๓.๒.๖) ช่วยให้สามารถทบทวนและปรับปรุงระบบการป้องกันการโจมตีได้ตามความจำเป็น โดยการวิเคราะห์ผลการใช้งานและการปรับปรุงระบบตามความเหมาะสม

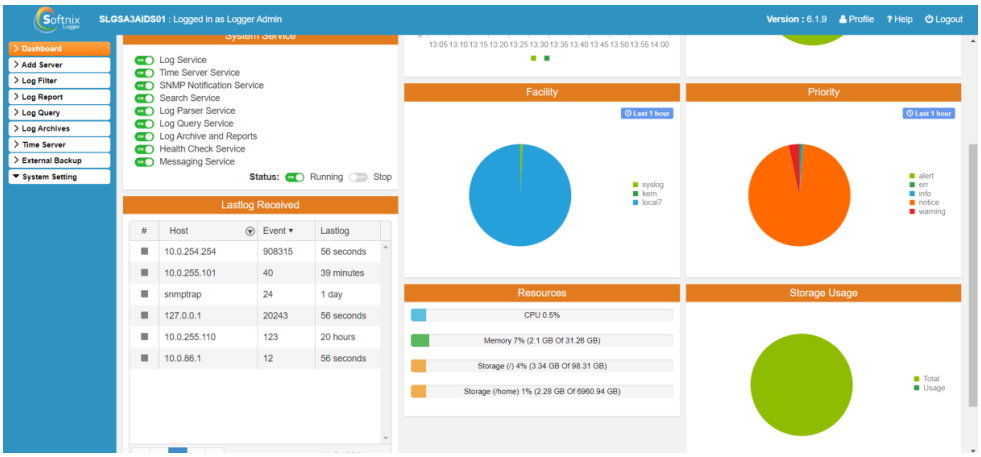
๓.๒.๗) มีระบบรายงานผลการทำงานในการตวจจับการโจมตี

ภาพที่ ๓๔ : จอภาพแสดงผลการตรวจจับการโจมตี

๓.๒.๘) เพิ่มเสถียรภาพของระบบด้วยการป้องกันการโจมตี และการบุกรุกที่อาจทำให้ระบบเกิดความไม่เสถียรมากขึ้น

๓.๓) อุปกรณ์จัดเก็บ Log File ช่วยให้องค์กรมีระบบที่ช่วยดูแลความปลอดภัยเครือข่ายที่มีประสิทธิภาพ สามารถตรวจจับและบันทึกการเหตุการณ์ที่เกิดขึ้นในระบบเครือข่ายเพื่อการแก้ไขปัญหาและป้องกันปัญหาในอนาคตและยังมีองค์ประกอบที่สำคัญ ได้แก่

๓.๓.๑) ช่วยให้สามารถตรวจสอบและวิเคราะห์ปัญหาที่เกิดขึ้นในระบบได้อย่างรวดเร็วและมีประสิทธิภาพ เช่น ตรวจสอบข้อผิดพลาดในระบบ ตรวจสอบการเข้าถึงที่ไม่ได้รับอนุญาต หรือการโจมตีจากภายนอก



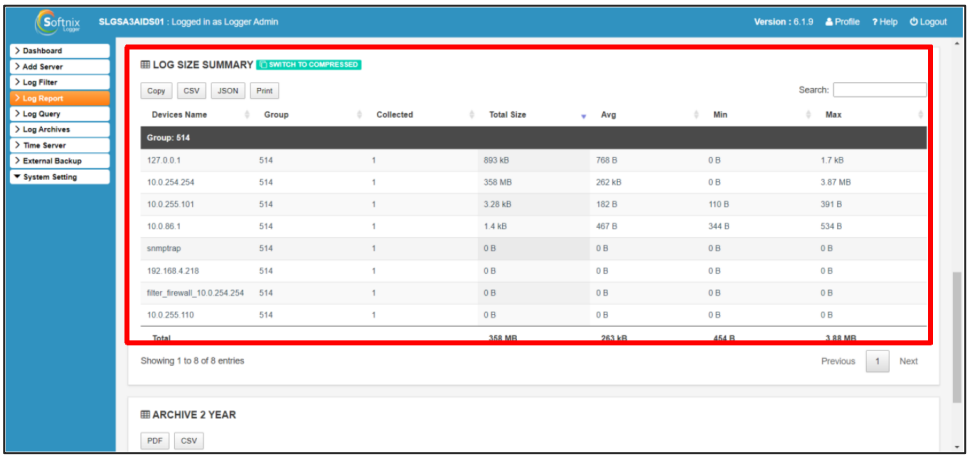
ภาพที่ ๓๕ : Service บนตัวอุปกรณ์ Log File

๓.๓.๒) เพิ่มความปลอดภัยของข้อมูล ช่วยในการตรวจจับการโจมตี สามารถเรียนรู้จากเหตุการณ์ที่เกิดขึ้นเพื่อป้องกันปัญหาที่จะเกิดขึ้นในอนาคต

๓.๓.๓) เพื่อปฏิบัติตามกฎหมายและข้อกำหนด เช่น ข้อกำหนด GDPR (General Data Protection Regulation) หรือ PCI DSS (Payment Card Industry Data Security Standard) ที่กำหนดให้องค์กรต้องเก็บ Log File เพื่อการตรวจสอบและการรายงานเหตุการณ์ที่เกิดขึ้น

๓.๓.๔) สำหรับการวิเคราะห์แนวโน้มของการใช้งานระบบ การจำลองเหตุการณ์เพื่อวางแผนการป้องกัน และการพัฒนาระบบให้มีประสิทธิภาพมากยิ่งขึ้น

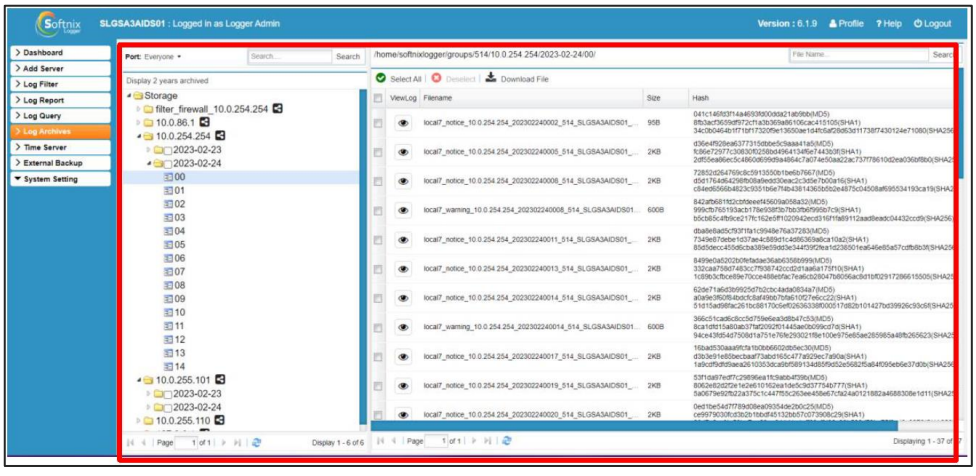
๓.๓.๕) สามารถนำข้อมูลจาก Log File มาวิเคราะห์และตรวจสอบปัญหาที่เกิดขึ้นในอดีต เป็นการศึกษาเรียนรู้ในองค์กรเพื่อการป้องกันปัญหาในอนาคต



ภาพที่ ๓๖ : summary ของ log event per sec

๓.๓.๖) สามารถตรวจสอบและประเมินผลการใช้งานของระบบได้อย่างสม่ำเสมอ และช่วยในการปรับปรุงและปรับปรุงระบบให้มีประสิทธิภาพมากยิ่งขึ้น

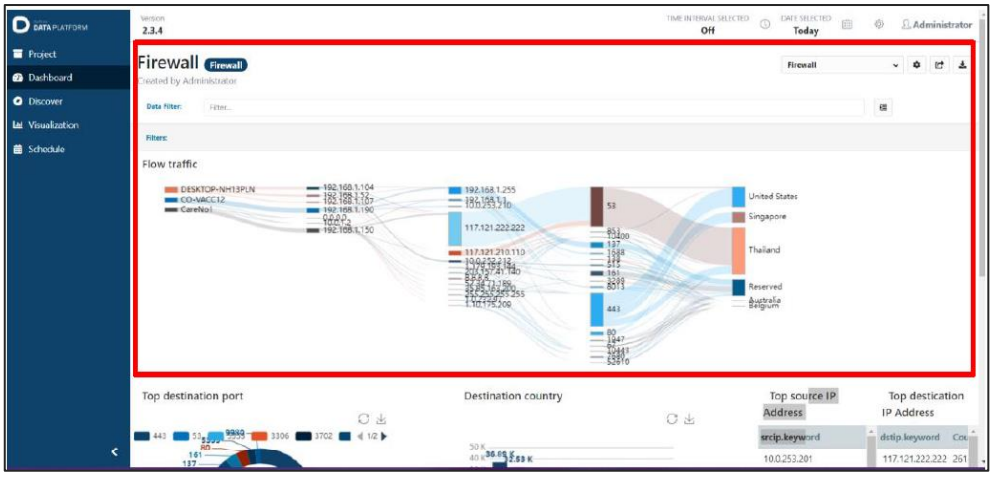
๓.๓.๗) สามารถสร้างสำเนาของ Redo logs และเก็บไว้ในที่เก็บข้อมูลที่แตกต่างจากที่เก็บ Redo logs ปกติ โดยทำการ Archive logs เป็นวิธีการทำ Backup and Recovery ที่มักจะถูกนำมาใช้งานในการกู้ข้อมูลที่สูญหายหรือเสียหาย



ภาพที่ ๓๗ : Backup and Recovery

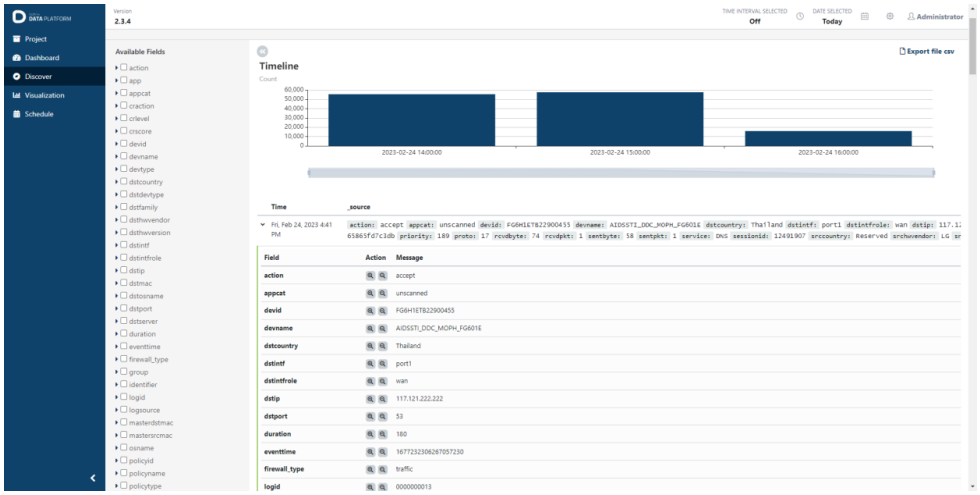
๓.๔) การนำอุปกรณ์วิเคราะห์การจราจรบนเครือข่าย Log Analyzer

๓.๔.๑) ช่วยในการตรวจจับและแก้ไขปัญหาในระบบเครือข่ายอย่างรวดเร็ว โดยทำให้สามารถระบุสาเหตุของปัญหาและพื้นที่ที่มีปัญหาได้ง่ายขึ้น



ภาพที่ ๓๘ : แสดงข้อมูล Log

๓.๔.๒) สำหรับวิเคราะห์ข้อมูลการจราจรบนเครือข่าย โดยองค์กรสามารถระบุพื้นที่ที่มีการใช้งานไม่เหมาะสมหรือมีปัญหา และมีโอกาสปรับปรุงและปรับแต่งระบบเพื่อเพิ่มประสิทธิภาพ

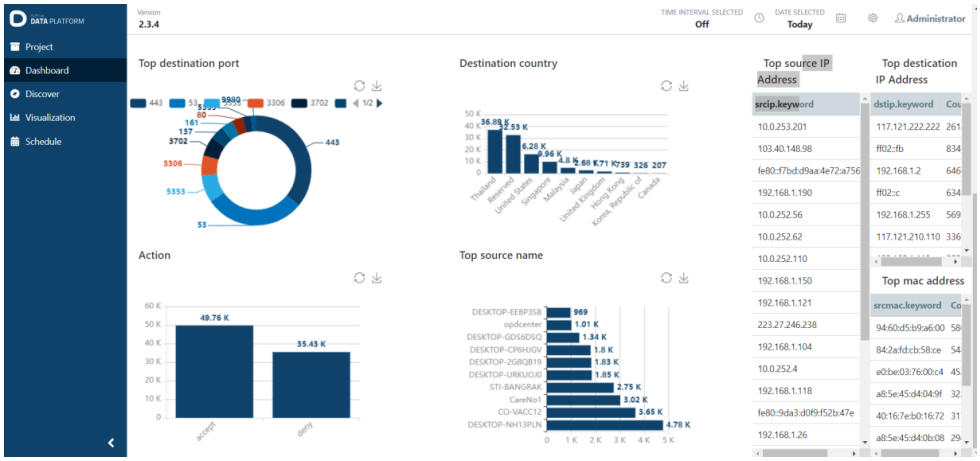


ภาพที่ ๓๙ : การนำ Log มาทำการวิเคราะห์เพื่อแบ่งปัน field ข้อมูล

๓.๔.๓) ช่วยในการตรวจจับกิจกรรมที่เกี่ยวข้องกับความปลอดภัยของระบบ เช่น การตรวจจับการแฮกเกอร์หรือการโจมตีจากภัยคุกคาม

๓.๔.๔) ช่วยในการวิเคราะห์และการคาดการณ์แนวโน้มในการใช้งานและการปฏิบัติต่าง ๆ ของระบบเครือข่าย

๓.๔.๕) ช่วยในการสร้างรายงานและการแจ้งเตือนที่ชัดเจนและแน่นอนเกี่ยวกับสถานะและปัญหาที่เกิดขึ้นในระบบ เพื่อเป็นข้อมูลสนับสนุนให้ผู้บริหารสามารถตัดสินใจและวางแผนได้อย่างมีประสิทธิภาพ



ภาพที่ ๔๐ : การนำ Log มาทำการวิเคราะห์เพื่อแบ่งปัน field ข้อมูล

การนำอุปกรณ์เครือข่ายมาปรับปรุงระบบเครือข่ายของอาคารศูนย์การแพทย์บางรัก กรมควบคุมโรค ทำให้มีการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ที่มีประสิทธิภาพมากขึ้น มีความน่าเชื่อถือในการใช้งานระบบเครือข่าย มีระบบดูแลความปลอดภัยระบบเครือข่ายและระบบข้อมูลที่สำคัญสำหรับใช้ในองค์กร ดังนั้น เพื่อให้ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานมีเสถียรภาพ และสามารถใช้งานได้อย่างต่อเนื่องจำเป็นต้องมีการบำรุงรักษาอุปกรณ์เป็นประจำ เพื่อให้องค์กรสามารถดำเนินงานตามภารกิจขององค์กรต่อไปได้

๔.๓ แผนการดูแลบำรุงรักษาระบบสารสนเทศ

อาคารศูนย์การแพทย์บางรัก ได้ใช้ระบบสารสนเทศในการดำเนินงานตามภารกิจขององค์กร และเพื่อให้บริการกับผู้มารับบริการให้ได้รับความสะดวก อย่างไรก็ตามการใช้ระบบสารสนเทศอาจจะได้รับความเสียหายจากปัจจัยทั้งภายในและภายนอกองค์กร เช่น ภัยจากไวรัสคอมพิวเตอร์ ภัยจากการใช้อินเตอร์เน็ต ภัยจากบุคคลหรือผู้มาติดต่องานภายในองค์กร ฯลฯ ซึ่งอาจจะทำให้ระบบสารสนเทศในองค์กรเกิดความเสียหาย ส่งผลกระทบต่อระบบข้อมูล หรืออุปกรณ์เครือข่ายในองค์กร รวมถึงการปฏิบัติงานของบุคลากรและการให้บริการผู้มารับบริการ

ดังนั้น เพื่อให้ระบบสารสนเทศขององค์กรสามารถใช้งานได้อย่างมั่นคงและต่อเนื่อง การจัดทำแผนการดูแลบำรุงรักษาระบบสารสนเทศ จึงเป็นสิ่งสำคัญเพื่อใช้เป็นแนวทางในการปฏิบัติงานดูแลรักษาด้านสารสนเทศขององค์กร โดยมีวัตถุประสงค์ดังนี้

๑) เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้
๒) เพื่อลดความเสี่ยงและความเสียหายที่จะอาจเกิดกับระบบเทคโนโลยีสารสนเทศ
๓) เพื่อให้ระบบสารสนเทศขององค์กร สามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที
๔) เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

๔.๓.๑ เป้าหมายของการจัดทำแผนดูแลบำรุงรักษาระบบสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศ ของอาคารศูนย์การแพทย์บางรักสามารถดำเนินการได้อย่างต่อเนื่องมีประสิทธิภาพ และสามารถใช้ได้ในกรณีที่มีภาวะฉุกเฉิน เช่น ไฟดับ อินเตอร์เน็ตขัดข้อง ระบบเครือข่ายใช้งานไม่ได้ โดยระบบสารสนเทศ ต้องสามารถกลับมาดำเนินการได้ในระยะเวลา ดังนี้

๑) ระบบสำรองไฟฟ้า สามารถสำรองไฟฟ้า ให้ระบบไม่น้อยกว่า ๓๐ นาที

๒) เครื่องคอมพิวเตอร์แม่ข่าย สามารถใช้พลังไฟฟ้าสำรองได้ ไม่น้อยกว่า ๕๐ นาที

๓) ระบบเครือข่ายในองค์กร สามารถกลับมาใช้งานได้ตามปกติภายในระยะเวลา ๒ ชั่วโมง

๔) ระบบอินเตอร์เน็ต เมื่อมีปัญหาขัดข้อง จะต้องทำให้สามารถใช้งานตามปกติภายในระยะเวลา ๒ ชั่วโมง ทั้งนี้ปัจจัยที่สำคัญขึ้นอยู่กับเครือข่ายผู้ให้บริการ ถ้าแก้ไขไม่ได้ในเวลาที่กำหนด ต้องแก้ไขปัญหาโดยใช้ระบบอินเตอร์เน็ตสำรอง

๔.๓.๒ การประเมินความเสี่ยงกับสถานการณ์

การตรวจสอบความเสี่ยงต่าง ๆ ในระบบสารสนเทศขององค์กรพบว่าสาเหตุของความเสี่ยงที่เกิดขึ้นอาจส่งผลเป็นอันตรายต่อระบบสารสนเทศ สามารถเกิดขึ้นได้จากปัจจัยเสี่ยง ดังนี้

๑) บุคลากรในองค์กรขาดความรู้ความเข้าใจในการใช้เครื่องมือหรืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Harcware และ Software ทำให้ระบบสารสนเทศเสียหายหรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบสารสนเทศได้อย่างเต็มประสิทธิภาพ

๒) ภัยไซเบอร์คุกคาม มัลแวร์ ไวรัสคอมพิวเตอร์ อาจสร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ถึงขั้นใช้งานไม่ได้

๓) ระบบไฟฟ้าขัดข้อง ไม่สามารถใช้งานได้เป็นระยะเวลานาน

๔) ปัจจัยภายนอก เช่น ระบบอินเตอร์เน็ต ไม่สามารถใช้งานได้หรืออาจเกิดจากการบุกรุกโจมตีจากภายนอก

๔.๓.๓ ข้อปฏิบัติในการป้องกัน แก้ไขปัญหาสถานการณ์ความเสี่ยงและภัยพิบัติ

๑) จัดอบรมแนะนำการใช้งานเกี่ยวกับระบบสารสนเทศ เพื่อเสริมสร้างความรู้ความเข้าใจในการใช้งานทั้งด้าน Hardware และ Soffware เพื่อลดความเสี่ยงที่จะเกิดขึ้นให้น้อยที่สุด

๒) การสำรองข้อมูลเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลถูกทำลายโดยไวรัสคอมพิวเตอร์หรือมีผู้บุกรุกทำลายหรือปลี่ยนแปลงข้อมูล การสำรองข้อมูลสามารถนำข้อมูลที่ถูกแก้ไขเปลี่ยนแปลงกลับมาได้ โดยมีแนวทางดำเนินการ ดังนี้

๒.๑) การตั้งค่าระบบสำหรับเครื่องคอมพิวเตอร์แม่ข่าย ให้มีการสำรองข้อมูลโดยอัตโนมัติเป็นประจำทุกวัน (Daily Backup)

๒.๒) การสำรองข้อมูลไว้ใน อุปกรณ์บันทึกหรือคอมพิวเตอร์เครื่องอื่น ๆ เช่น อุปกรณ์สำหรับจัดเก็บข้อมูลแบบภายนอก (External Storage)

๓) การป้องกันไวรัสคอมพิวเตอร์โดยติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยมีวิธีการดังนี้

๓.๑) ติดตั้งโปรแกรมป้องกันไวรัสและปรับปรุง (Update) ข้อมูลไวรัสอยู่เสมอ

๓.๑.๑) ติดตั้งโปรแกรมป้องกันไวรัส

๓.๑.๒) Update ข้อมูลไวรัสเป็นประจำ

๓.๑.๓) ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากสื่อบันทึกข้อมูล ต่าง ๆ เช่น Flash drive/Thumb drive เป็นต้น

๓.๑.๔) สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง

๓.๑.๕) ไม่ควรเปิดไฟล์ที่มีนามสกุลที่ไม่รู้จักหรือน่าสงสัย เช่น .pif, .inf เป็นต้น

๓.๑.๖) ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๓.๒) การเปิด E-Mail

๓.๒.๑) อย่าเปิดไฟล์ E-Mail ถ้าไม่ทราบแหล่งที่มา

๓.๒.๒) ลบ E-Mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๓.๓) การดาวน์โหลดไฟล์ต่าง ๆ จาก Internet

๓.๓.๑) ไม่ควรเปิดไฟล์ที่ไม่รู้จักที่แนบมากับโปรแกรมสนทนาต่าง ๆ เช่น Facebook, Twitter และ Skype เป็นต้น หรือสอบถามผู้ส่งไฟล์ต้นทางก่อนทำการบันทึก

๓.๓.๒) ไม่ดาวน์โหลด ไฟล์จาก Website ที่ไม่น่าเชื่อถือ

๓.๓.๓) หลีกเสี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๔) เครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย Internet ขัดข้อง ดำเนินการดังนี้

๔.๑) ตัดการเชื่อมต่อระบบเครือข่าย และทำการปิดอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

๔.๒) ตรวจสอบแผนผังเครือข่ายอุปกรณ์เพื่อหาสาเหตุการขัดข้อง และดำเนินการแก้ไข หากเกิดจากเครือข่ายอินเทอร์เน็ตต้องดำเนินการแจ้งผู้ให้บริการทันที

๔.๓) กรณีไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับและประสิทธิภาพของเครื่องสำรองไฟฟ้า

๔.๔) กรณีเกิดเหตุไฟไหม้เครื่องคอมพิวเตอร์และเครือข่าย ให้ตัดระบบจ่ายไฟและใช้ถังดับเหลิงฉีดควบคุมเพลิงโดยเร็วรีบขนย้ายเครื่องคอมพิวเตอร์และเครือข่ายไปไว้ในที่ปลอดภัย

๔.๕) กรณีที่อุปกรณ์ด้านฮาร์ดแวร์ชำรุดเสียหาย ต้องรีบดำเนินการหาอุปกรณ์มาสำรองหรือทดแทน และดำเนินการซ่อมแซมให้สามารถใช้งานได้ตามปกติ ถ้าเกินขีดความสามารถในการแก้ไขปัญหาต้องติดต่อผู้เชี่ยวชาญเพื่อขอคำแนะนำหรือช่วยดำเนินการแก้ไขให้สามารถใช้งานได้โดยเร็ว

๕) ซอฟต์แวร์ หรือโปรแกรม เสียหาย ให้ดำเนินการติดตั้งซอฟต์แวร์ หรือโปรแกรมใหม่เพื่อกลับมาใช้งานได้ตามปกติภายใน ๑-๒ วัน

๖) การกู้ระบบคอมพิวเตอร์ให้สามารถนำกลับมาใช้งานได้ตามปกติ

การกู้ระบบเครื่องคอมพิวเตอร์แม่ข่ายคอมพิวเตอร์ และอุปกรณ์กระจายสัญญาณ (Systern recovery) โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์กระจายสัญญาณจะต้องอยู่ในสภาพ

พร้อมใช้งาน รองรับการให้บริการกับเครื่องลูกข่ายต่าง ๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องดำเนินการกู้ระบบคืนให้ได้เร็วที่สุด โดยแผนการกู้ระบบคอมพิวเตอร์นี้เป็นวิธีการที่จะทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและระบบข้อมูลสารสนเทศ กลับมาใช้งานได้ตามปกติ เมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการดังนี้

๖.๑) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๖.๒) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๖.๓) กรณีเครื่องคอมพิวเตอร์แม่ข่ายเสียหาย ใช้คอมพิวเตอร์เครื่องอื่นทดแทนชั่วคราว

๖.๔) นำ Backup ที่ได้สำรองข้อมูลไว้กลับมาดำเนินการ Setup

๖.๕) ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูลสารสนเทศ และความถูกต้องของข้อมูล รวมทั้งระบบเครือข่ายคอมพิวเตอร์อื่น ๆ ที่เกี่ยวข้อง

๗) การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ ได้

๗.๑) ติดตั้งเครื่องสำรองไฟฟ้า เพื่อป้องกันความเสียหายที่จาจเกิดขึ้นกับ อุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งมีระยะเวลาในการสำรองไฟฟ้าได้นาน ประมาณ ๑๕ - ๓๐ นาที

๗.๒) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๗.๓) เมื่อเกิดกระแสไฟฟ้าดับ หากมีเครื่องสำรองไฟฟ้าใช้งานอยู่ให้ผู้ใช้ดำเนินการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ทันทีหลังจากดำเนินบันทึกข้อมูลเสร็จ

๘) ติดตั้งระบบป้องกันไฟไหม้โดยติดตั้งอุปกรณ์ดับเพลิงชนิดสารสะอาดเพื่อป้องการอุปกรณ์เสียหายเพื่อการควบคุมเพลิงในเบื้องต้น

๙) การนำมาตรการความปลอดภัยด้วยรหัสผ่าน เพื่อการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายรหัสผ่านการเข้าโปรแกรม และรหัสผ่านการใช้งานระบบเครือข่ายไร้สาย (Wireless LAN) ภายในบริเวณอาคาร

๔.๔ แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ[๑๐]

เพื่อให้ระบบเทคโนโลยีสารสนเทศของอาคารศูนย์การแพทย์บางรักสามารถให้บริการได้อย่างต่อเนื่องและมีความมั่นคงปลอดภัย รวมถึงป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง หรือจากภัยคุกคามในรูปแบบต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อข้อมูลและทรัพย์สินขององค์กรได้

แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ มีดังนี้

๔.๔.๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานระบบสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์การเข้าถึงหรือการมอบอำนาจ ได้แก่

๑.๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น การอ่านอย่างเดียว สร้างข้อมูล บันทึกข้อมูล แก้ไขข้อมูล ลบข้อมูล อนุมัติ ไม่มีสิทธิ์ เป็นต้น

๑.๒) กำหนดเกณฑ์การระงับสิทธิ์ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งานที่ได้กำหนดไว้

๒) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

๒.๑) จัดแบ่งประเภทของข้อมูล ได้แก่

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านวิทยาศาสตร์การแพทย์ เช่น ข้อมูลผลการตรวจวิเคราะห์ด้านยา ด้านอาหาร ชันสูตรโรค สมุนไพร ชีววัตถุ เป็นต้น

๒.๒) จัดแบ่งระดับความสำคัญของข้อมูล แบ่งออกเป็น ๓ ระบบ ได้แก่

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๒.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๒.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

๔.๔.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๑) ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ โดยตรวจสอบบัญชีผู้ใช้งานเพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

๒) ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ โดยต้องให้สิทธิ์ผู้ใช้งานเฉพาะการปฏิบัติงานในหน้าที่ซึ่งได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษรหรือทางระบบอิเล็กทรอนิกส์ที่สามารถยืนยันตัวบุคคลได้

๓) ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งาน อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

๔) ผู้ดูแลระบบยกเลิกสิทธิ์การใช้งาน ภายหลังจากได้รับการแจ้งจากหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร

๕) การบริหารจัดการรหัสผ่าน ได้แก่

๕.๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือ เกษียณอายุราชการ หรือยกเลิกการใช้งาน ภายหลังจากได้รับการแจ้งจากหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร

๕.๒) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๕.๓) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (Email) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๕.๔) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)

๕.๕) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๕.๖) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

๕.๗) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๔.๔.๓ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๑) การควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย โดยทำการลงข้อมูลในสมุดบันทึกการเข้าออกพื้นที่ทุกครั้ง

๒) กรณีที่เป็นบุคคลภายนอกต้องแลกบัตรที่สามารถระบุตัวตนได้อย่างชัดเจน เช่น บัตรประชาชน ใบอนุญาตขับขี่ และบันทึกข้อมูลการเข้าออกพื้นที่ ให้ชัดเจน

๓) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้บริหารองค์กรก่อนเข้าใช้งาน

๔) การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในองค์กรจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านทุกครั้ง

๕) ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกองค์กรต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall) เพื่อความปลอดภัยของระบบเครือข่ายในองค์กรและป้องกันการกระทำที่ไม่เหมาะสม

๔.๔.๔ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๑) ทำการเปลี่ยนค่าอุปกรณ์เครือข่ายที่มาจากโรงงานให้เป็นค่าที่กำหนดให้ใช้ภายในองค์กรเท่านั้น

๒) กำหนดค่า Wireless Security เป็นแบบ WPA (Wi-Fi Protected Access) หรือ WPA2 (Wi-Fi Protected Access2) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point)

๓) กำหนดชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย

๔) ติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในองค์กร

๕) แยกการใช้งานระหว่างเครือข่ายภายในและภายนอก เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายจากเครือข่ายไร้สาย ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่าย

๖) ไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ขององค์กร

๗) ทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายขององค์กร รวมทั้ง มีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๔.๔.๕ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

๑) ติดตั้งและกำหนดค่าของ Firewall ทั้งหมดและการกำหนดค่าเริ่มต้นของ Firewall ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny) ทุกบริการ (Services) และเส้นทางเชื่อมต่ออินเตอร์เน็ตที่ไม่อนุญาตตาม Policy จะต้องถูกบล็อก (Block) โดย Firewall

๒) ผู้ใช้งานอินเตอร์เน็ตจะต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนการใช้งานทุกครั้ง

๓) การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาต ต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง หากมีการเปลี่ยนแปลงค่าต่าง ๆ ของ Firewall

๔) การเข้าถึงตัวอุปกรณ์ Firewall ต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๕) ตั้งค่าข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ Firewall ให้ส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

๖) กำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

๗) ตั้งค่าการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ Firewall เป็นประจำทุกสัปดาห์หรือทุกครั้งก่อนที่มีการเปลี่ยนแปลงค่า

๘) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศในองค์กร กำหนดให้มีลักษณะการทำงานที่เป็นอินทราเน็ต จะมีการเชื่อมต่อเพื่อใช้งานอินเตอร์เน็ตก็ต่อเมื่อมีความจำเป็น โดยเป็นกรณีไป

๙) ผู้ดูแลระบบเครือข่ายสารามรถระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข ทั้งนี้ผู้ใช้งานที่ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานอินเตอร์เน็ตทันที

๑๐) การเชื่อมต่อเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายภายใน เป็นลักษณะของการ Remote Login จากภายนอก ต้องขออนุญาตพร้อมระบุเหตุผลเป็นลายลักษณ์อักษร โดยต้องได้รับความเห็นชอบจากผู้บริหารองค์กรก่อนดำเนินการ

๔.๔.๖ การควบคุมการใช้อินเตอร์เน็ต (Internet)

๑) กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้ ได้แก่ Proxy, Firewall, IPS-IDS เป็นต้น

๒) การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๓) ไม่ใช้ระบบอินเตอร์เน็ต (Internet) ขององค์กร เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับองค์กร

๔) ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กรที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเตอร์เน็ต (Internet)

๕) การดาวน์โหลด โปรแกรมใช้งานจากระบบอินเตอร์เน็ต (Internet) การอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือดาวน์โหลดจากเว็บไซต์ที่ไม่น่าเชื่อถือ

๖) การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ หรือ Social Network ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับขององค์กร ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่ทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์กร

๗) ไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

๘) หลังจากใช้งานอินเตอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบและให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๙) ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และ พ.ศ.๒๕๖๐ อย่างเคร่งครัด

๔.๔.๗ การตรวจจับการบุกรุก (Intrusion Prevention System: IPS)

๑) ติดตั้งระบบตรวจสอบการบุกรุกและตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากรระบบสารสนเทศและข้อมูลบนเครือข่ายภายในหน่วยงาน ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

๒) ติดตั้งอุปกรณ์ตรวจจับการบุกรุก (IPS) ในระบบเครือข่ายขององค์กรและระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเตอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบ จากระบบ IPS

๓) ระบบเครือข่ายทั้งหมดขององค์กรที่มีการส่งผ่านข้อมูลผ่าน IPS มีการบันทึกผลการตรวจสอบและ Update Patch/Signature เป็นประจำ

๔) การตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำโดยผู้ดูแลระบบ

๕) อุปกรณ์ IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

๖) พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ ต้องมีการรายงานให้ผู้บริหารองค์กรทราบทันทีที่ตรวจพบ

๗) การตรวจสอบการบุกรุกทั้งหมด มีการเก็บบันทึกข้อมูลไว้อย่างน้อย ๙๐ วัน

๘) ระบบ IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคตและดำเนินการตามแผน

๙) องค์กรมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องแจ้งผู้ใช้งานล่วงหน้า

๑๐) ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายขององค์กร เช่นการพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบขององค์กร จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

๔.๔.๘ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

๑) การปรับปรุงระบบปฏิบัติการ (Operating System Update)

๑.๑) ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน

๑.๒) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบและชื่อผู้ใช้งาน (User)

๑.๓) กำหนดชื่อเครื่อง (Computer Name) และตั้งค่า IP Address ตามความจำเป็นของการใช้งาน

๑.๔) ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ

๑.๕) กรณีที่ระบบปฏิบัติการที่มี ServicePatch Update ให้ตรวจสอบหรือปรับปรุงการกำหนดค่าต่างๆ โดยเฉพาะระดับความปลอดภัยของระบบปฏิบัติการ

๒) การบริหารบัญชีผู้ใช้งาน/สิทธิ์การเข้าถึงและการใช้งานระบบ (User Account Management)

๒.๑) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Adminstrator)

๒.๒) กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password)

๒.๓) บันทึกบัญชีผู้ใช้งานและทบทวนสิทธิ์การเข้าใช้ระบบให้เป็นปัจจุบันและสอดคล้องกับหน้าที่ความรับผิดชอบ

๓) ระบบรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการปรับปรุงการป้องกันไวรัส (System Security & Antivirus Update)

๓.๑) ติดตั้งโปรแกรม Antivirus และปรับปรุงฐานข้อมูลไวรัส (virus definition) ให้ทันสมัยอยู่เสมอ และกำหนดค่าการตรวจสอบระบบการสแกนและปรับปรุงโปรแกรม

๓.๒) ดำเนินการ Scan ตรวจหาไวรัสคอมพิวเตอร์เป็นประจำ

๓.๓) ตรวจสอบ เฝ้าระวัง และติดตาม การทำงานของระบบคอมพิวเตอร์

๓.๔) ตรวจสอบประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ จากระบบรักษาความปลอดภัยที่ติดตั้ง

๓.๕) ปรับปรุง / กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปัญหา

๔) การดำเนินการบริหารจัดการฐานข้อมูล (Database Management Operation)

๔.๑) ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการขององค์กร

๔.๒) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูล ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้อง และมีประสิทธิภาพ ตามระบบฐานข้อมูลนั้นกำหนด

๔.๓) สร้างรายชื่อผู้ดูแลระบบฐานข้อมูล (Database Administrator) ชื่อผู้ใช้งาน (User) และกำหนดสิทธิ์การเข้าใช้งาน

๔.๔) ปรับปรุงและกำหนดค่าระบบให้เหมาะสม ทันสมัยอยู่เสมอ เพื่อป้องกันการเกิดปัญหา

๕) ติดตั้งฐานข้อมูลโปรแกรมระบบงานต่าง ๆ กำหนดค่าระบบของโปรแกรมและกำหนดผู้ใช้และสิทธิ์การเข้าใช้บริการหรือเข้าถึงฐานข้อมูล

๕.๑) ติดตั้งโปรแกรมระบบงานตามความต้องการ หรือการพัฒนา

๕.๒) กำหนดค่าโปรแกรม หรือตั้งค่า services ต่าง ๆ ให้ทำงานร่วมกับระบบปฏิบัติการอย่างถูกต้องและมีประสิทธิภาพ

๕.๓) ติดตั้งฐานข้อมูล เชื่อมต่อระบบงาน และทำการทดสอบการให้บริการตามที่ระบบงานกำหนด

๔.๔.๙ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

๑) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความ ครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง

๒) ห้ามแก้ไขข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

๓) กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๔) ป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๔.๔.๑๐ การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบสารสนเทศ

๑) การเปลี่ยนแปลงอุปกรณ์ระบบเครือข่ายและการสื่อสาร ให้ดำเนินการ ดังนี้

๑.๑) ผู้เกี่ยวข้องต้องดำเนินการแจ้งผู้บังคับบัญชาเป็นลายลักษณ์อักษร

๑.๒) ผู้เกี่ยวข้องต้องวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลงนั้น ๆ

๑.๓) ผู้เกี่ยวข้องต้องรายงานผลการเปลี่ยนแปลงและผลกระทบต่อผู้บังคับบัญชาเมื่อสิ้นสุดการดำเนินการ

๒) ประชุมร่วมกับผู้เกี่ยวข้องเพื่อพิจารณาทรัพยากรที่มีอยู่ในปัจจุบัน หากไม่เพียงพอให้ดำเนินการจัดทำคำของบประมาณ ตามแบบฟอร์ม รายงานการจัดหาระบบคอมพิวเตอร์ภาครัฐที่มีมูลค่าไม่เกิน ๕ ล้าน/เกิน ๕ ล้าน

๓) งานสารสนเทศ กลุ่มบริหารงานทั่วไป รวบรวมข้อมูลเสนอคณะกรรมการฯ พิจารณาในรายละเอียดการจัดสรร

การปฏิบัติตามแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ จะช่วยให้องค์กรมีความพร้อมในการรับมือกับความเสี่ยงด้านความปลอดภัยสารสนเทศอย่างมีประสิทธิภาพและมั่นคง และสามารถป้องกันการเกิดเหตุร้ายแรงต่อระบบและข้อมูลขององค์กรได้อย่างมีประสิทธิภาพและเป็นระบบ

บทที่ ๕

บทสรุป ปัญหาอุปสรรค และข้อเสนอแนะ

ในการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ จากผลดำเนินงานที่ผ่านมาทั้งหมด ผู้จัดทำขอสรุปปัญหา และข้อเสนอแนะ เพื่อเป็นประโยชน์สำหรับแนวทางการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ของอาคารศูนย์การแพทย์บางรัก โดยแบ่งเป็นหัวข้อดังนี้

๕.๑ สรุปผลการดำเนินงานการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์

๕.๒ สรุปผลความพึงพอใจด้านระบบสารสนเทศ

๕.๓ การเฝ้าระวังความเสถียรของระบบเครือข่ายคอมพิวเตอร์โดยการคำนวณ SLA

๕.๔ ปัญหาและอุปสรรคในการดำเนินงาน

๕.๕ ข้อเสนอแนะ

๕.๑ สรุปผลการดำเนินงานการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์

การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ที่มีประสิทธิภาพและมีความมั่นคงปลอดภัย การจัดหาอุปกรณ์เครือข่ายจึงเป็นสิ่งจำเป็นสำหรับการดำเนินงาน เพื่อให้ระบบสารสนเทศขององค์กรสามารถให้บริการได้อย่างต่อเนื่องและมีความมั่นคงปลอดภัย ครอบคลุมพื้นที่การให้บริการ อีกทั้งเพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศขององค์กรให้ปลอดภัยจากการเข้าถึงที่ไม่พึงประสงค์และการโจมตีจากภายนอกหรือจากภัยคุกคามในรูปแบบต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อข้อมูลและทรัพย์สินขององค์กรได้ ดังนั้นจึงได้ดำเนินการติดตั้งอุปกรณ์เครือข่ายที่จำเป็น ให้เพียงพอต่อการใช้งาน และติดตั้งเพิ่มเติมในบริเวณที่ไม่มีจุดเชื่อมต่อระบบเครือข่าย ประกอบด้วยอุปกรณ์ดังต่อไปนี้

ตารางที่ ๓ การติดตั้งอุปกรณ์เครือข่ายคอมพิวเตอร์

รายการอุปกรณ์เครือข่าย	จำนวน	สถานที่ติดตั้ง
อุปกรณ์กระจายสัญญาณไร้สาย (Access Point)	๔๐	**ชั้น ๑** บริเวณเคาน์เตอร์ รปภ. **ชั้น ๙** หน้าห้องตรวจ ๒ ห้องเจาะเลือด ศูนย์วัคซีนบางรัก ห้องคลังยา ห้องวิจัย ห้องจุลชีวะ ห้องตรวจชายเวชระเบียน และห้องตรวจชาย **ชั้น ๑๐** ห้องงานปฏิบัติการกลาง ห้องประชุม ห้องปฏิบัติการ ห้องพักเจ้าหน้าที่ และห้องจุลชีวฯ **ชั้น ๑๑** ห้องช่างอาคาร ห้องตรวจโรค ห้องพักเจ้าหน้าที่ **ชั้น ๑๒** งานสารสนเทศ, หัวหน้ากลุ่มบางรักฯ **ชั้น ๑๓** ห้องประชุม, ห้องปฏิบัติการ Server **ชั้น ๑๕** หน้า Reception ห้องประชุม **ชั้น ๑๗** ประชุม ห้องรับรอง ห้องโสต

รายการอุปกรณ์เครือข่าย	จำนวน	สถานที่ติดตั้ง
อุปกรณ์กระจายสัญญาณ (L2 Switch)	๗	ห้องปฏิบัติการ Server ชั้น ๑๒ ห้องปฏิบัติการ Server ชั้น ๑๓ ห้องเซอร์วิส ชั้น ๙ ห้องเซอร์วิส ชั้น ๑๐ ห้องเซอร์วิส ชั้น ๑๑ และสำรอง ๒ เครื่อง
อุปกรณ์กระจายการทำงานสำหรับเครือข่าย (Link Load Balancer)	๑	ห้องปฏิบัติการ Server ชั้น ๑๓
อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall)	๑	ห้องปฏิบัติการ Server ชั้น ๑๓
อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย	๑	ห้องปฏิบัติการ Server ชั้น ๑๓
อุปกรณ์กระจายสัญญาณ (L3 Switch)	๒	ห้องปฏิบัติการ Server ชั้น ๑๓
อุปกรณ์ควบคุมเครือข่ายไร้สาย (Access Point Controller)	๑	ห้องปฏิบัติการ Server ชั้น ๑๓
อุปกรณ์วิเคราะห์การจราจรบนเครือข่าย (Log Analyzer)	๑	ห้องปฏิบัติการ Server ชั้น ๑๓
เครื่องสำรองไฟฟ้าขนาด 40 KVA (UPS)	๑	ห้องปฏิบัติการ Server ชั้น ๑๓
อุปกรณ์สำหรับจัดเก็บข้อมูลแบบภายนอก (External Storage)	๑	ห้องปฏิบัติการ Server ชั้น ๑๓
เครื่องคอมพิวเตอร์แม่ข่าย	๑	ห้องปฏิบัติการ Server ชั้น ๑๓
อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System)	๑	ห้องปฏิบัติการ Server ชั้น ๑๓

การนำอุปกรณ์เครือข่ายดังกล่าวมาปรับปรุงระบบเครือข่ายในองค์กร ช่วยให้การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์มีประสิทธิภาพและครอบคลุมพื้นที่การให้บริการขององค์กรเพิ่มขึ้น เพื่อให้ระบบสารสนเทศขององค์กรสามารถให้บริการได้อย่างต่อเนื่องและมีความมั่นคงปลอดภัย และช่วยเพิ่มประสิทธิภาพของการใช้งานระบบสารสนเทศในองค์กรได้ ดังนี้

๑. เพิ่มประสิทธิภาพในการทำงานของบุคลากร ช่วยให้การทำงานภายในองค์กรเป็นไปอย่างราบรื่นและมีประสิทธิภาพมากขึ้น เช่น การเพิ่มความเร็วในการส่งข้อมูลภายในเครือข่ายภายในองค์กร การลดการขัดข้องและความล่าช้าในการเข้าถึงข้อมูล และการเพิ่มความเสถียรของระบบสารสนเทศในองค์กร
๒. เพิ่มประสิทธิภาพของการบริหารจัดการระบบเครือข่ายได้ เช่น มีระบบแสดงสถานะการทำงานของอุปกรณ์เครือข่ายที่ถูกติดตั้งใช้งานภายในอาคาร และแสดงสถานะใช้งานทรัพยากรได้อย่างแม่นยำ ทำให้สามารถบริการจัดการระบบเครือข่ายได้อย่างสะดวก อีกทั้งสามารถตรวจสอบความบกพร่องการทำงานของระบบเครือข่ายภายในอาคารได้ ทำให้แก้ไขปัญหาได้ทันท่วงที
๓. เพิ่มความเชื่อถือได้ของระบบสารสนเทศ และลดปัญหาเกี่ยวกับการเข้าถึงข้อมูล สามารถใช้งานระบบสารสนเทศได้ตลอดเวลา มีระบบสำรองและจัดเก็บข้อมูลที่มีประสิทธิภาพ และสามารถ

รองรับระบบหรือโปรแกรมที่จะพัฒนาในอนาคต โดยมีการจำกัดสิทธิ์ในการเข้าถึงข้อมูลเพื่อความปลอดภัย

๔. เพิ่มความยืดหยุ่นในการใช้งานของระบบสารสนเทศในองค์กร สามารถใช้งานอินเตอร์เน็ตหรือเข้าถึงข้อมูลจากทุกที่ภายในองค์กร สามารถรองรับการเพิ่มขึ้นของผู้ใช้และอุปกรณ์ในอนาคตได้
๕. เพิ่มความพร้อมใช้ของระบบสารสนเทศในกรณีฉุกเฉิน และการจัดการกับสถานการณ์ที่ไม่คาดคิด เช่น การกู้คืนข้อมูลหลังจากภัยพิบัติ การป้องกันและตอบสนองต่อการบุกรุก และการทดสอบและปรับปรุงการแก้ไขปัญหา
๖. เพิ่มความมั่นคงและความปลอดภัยของข้อมูล มีระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ สามารถตรวจจับและป้องกันการบุกรุกได้ โดยจัดเก็บในรูปแบบ Log File สามารถระบุตัวบุคคลที่เข้าถึงระบบข้อมูล โดยนำมาวิเคราะห์เหตุการณ์ผิดปกติขึ้นในระบบเครือข่ายได้อย่างมีประสิทธิภาพ สามารถบันทึกข้อมูลของการใช้งานระบบเครือข่ายคอมพิวเตอร์ภายในอาคารศูนย์การแพทย์บางรักได้
๗. เพิ่มความมั่นคงและความเสถียรของการใช้พลังงานไฟฟ้าที่สามารถจ่ายกระแสไฟฟ้าได้อย่างต่อเนื่อง ลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นจากการคลาดแคลนพลังงานไฟฟ้า

๕.๒ สรุปผลความพึงพอใจด้านระบบสารสนเทศ

การสำรวจแบบประเมินความพึงพอใจของผู้ใช้บริการด้านระบบสารสนเทศ ใช้แบบสอบถาม สอบถามความคิดเห็นของบุคลากร อาคารศูนย์การแพทย์บางรัก จากการดำเนินงานปรับปรุงระบบเครือข่ายคอมพิวเตอร์เพื่อสนับสนุนการปฏิบัติงานของเจ้าหน้าที่ในการบริการประชาชนด้านการตรวจ ดูแลและรักษา รวมถึงการถ่ายทอดองค์ความรู้ด้านโรคติดต่อทางเพศสัมพันธ์ ให้สอดคล้องกับวัตถุประสงค์และภารกิจขององค์กรที่วางแผนไว้ และเพื่อเป็นแนวทางในการปฏิบัติงานด้านการจัดการระบบเครือข่ายคอมพิวเตอร์ขององค์กรให้มีประสิทธิภาพมากขึ้นต่อไปนั้น ผู้จัดทำได้รวบรวมแบบสอบถามความพึงพอใจในการใช้บริการด้านระบบสารสนเทศหลังจากปรับปรุงระบบดังกล่าวเสร็จสิ้นแล้ว โดยได้รับแบบสอบถามคืนทั้งหมดจำนวน ๖๒ ชุด โดยการรวบรวมข้อมูลแบบสอบถามความพึงพอใจของผู้รับบริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร แบ่งออกเป็น ๓ ส่วน ได้แก่

ส่วนที่ ๑ ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ประกอบด้วย

- เพศ
- ประเภทบุคลากร
- ความถี่ในการใช้อินเตอร์เน็ตต่อวัน
- ความถี่ในการใช้อินเตอร์เน็ตต่อสัปดาห์
- ช่วงระยะเวลาในที่ใช้อินเตอร์เน็ต

ส่วนที่ ๒ ระดับความพึงพอใจของผู้รับบริการด้านระบบสารสนเทศ ประกอบด้วย

- ผลการวิเคราะห์ข้อมูลด้านคุณภาพระบบเครือข่ายคอมพิวเตอร์ (LAN & Wireless)
- ผลการวิเคราะห์ข้อมูลด้านระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ (Network Security)
- ผลการวิเคราะห์ข้อมูลด้านการให้บริการ (Service)

ส่วนที่ ๓ ข้อเสนอแนะเพิ่มเติม กำหนดคะแนนวัดความพึงพอใจแต่ละระดับ ดังนี้

- มีความพึงพอใจมากที่สุด มีค่าเท่ากับ ๕ คะแนน
- มีความพึงพอใจมาก มีค่าเท่ากับ ๔ คะแนน
- มีความพึงพอใจปานกลาง มีค่าเท่ากับ ๓ คะแนน
- มีความพึงพอใจน้อย มีค่าเท่ากับ ๒ คะแนน
- มีความพึงพอใจน้อยที่สุด มีค่าเท่ากับ ๑ คะแนน

การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลเพื่อวิเคราะห์ค่าทางสถิติและนำเสนอในรูปแบบตารางประกอบคำบรรยาย ดังนี้

๑. ข้อมูลเกี่ยวกับข้อมูลทั่วไปของผู้ตอบแบบสอบถามวิเคราะห์ด้วยวิธีหาค่าร้อยละ

๒. ข้อมูลเกี่ยวกับความพึงพอใจของผู้รับบริการด้านระบบสารสนเทศ มีเกณฑ์ในการพิจารณาค่าเฉลี่ย ๕ ระดับ ดังนี้

ค่าเฉลี่ย		ความหมาย
๔.๐๑ – ๕.๐๐	หมายถึง	มีความพึงพอใจในการให้บริการระดับดีมาก
๓.๐๑ – ๔.๐๐	หมายถึง	มีความพึงพอใจในการให้บริการระดับดี
๒.๐๑ – ๓.๐๐	หมายถึง	มีความพึงพอใจในการให้บริการระดับปานกลาง
๑.๐๑ – ๒.๐๐	หมายถึง	มีความพึงพอใจในการให้บริการระดับพอใช้
๐.๐๑ – ๑.๐๐	หมายถึง	มีความพึงพอใจในการให้บริการระดับควรปรับปรุง

สถิติที่ใช้ในการวิเคราะห์ข้อมูล

สถิติที่ใช้ในการวิเคราะห์ข้อมูลประกอบด้วย ร้อยละค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ดังนี้

๑. ร้อยละ

$$P = \frac{f \times 100}{n}$$

P หมายถึง ร้อยละหรือเปอร์เซ็นต์ (Percentage %)

f หมายถึง ความถี่ที่ต้องการเปลี่ยนแปลงให้เป็นร้อยละ

n หมายถึง จำนวนความถี่ทั้งหมดหรือจานวนกลุ่มตัวอย่าง

๒. ค่าเฉลี่ยเลขคณิต (Mean)

$\bar{X}$ หมายถึง ค่าเฉลี่ย

$\sum x_i$ หมายถึง ผลรวมของคะแนน

N หมายถึง จำนวนข้อมูลทั้งหมด

๓. ค่าความเบี่ยงเบนมาตรฐาน (Standard Deviation)

$$S.D. = \sqrt{\frac{n\sum x^2 - (\sum x)^2}{n(n-1)}}$$

S.D.	หมายถึง ค่าความเบี่ยงเบนมาตรฐาน
X	หมายถึง คะแนนแต่ละตัวในกลุ่มตัวอย่าง
n	หมายถึง จำนวนผู้ตอบแบบสอบถาม
$(\sum x)^2$	หมายถึง ผลรวมของคะแนนทั้งหมดยกกำลังสอง
$\sum x^2$	หมายถึง ผลรวมของคะแนนแต่ละตัวยกกำลังสอง
n	หมายถึง ขนาดของกลุ่มตัวอย่าง
n-1	หมายถึง จำนวนตัวแปรอิสระ

ส่วนที่ ๑ ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

เพศ

จากผู้ตอบแบบประเมินความพึงพอใจจำนวน ๖๒ คน พบว่า เป็นเพศชาย จำนวน ๑๘ คน คิดเป็นร้อยละ ๒๙ เป็นเพศหญิง จำนวน ๔๔ คน คิดเป็นร้อยละ ๗๑ รายละเอียดดังตารางที่ ๑

ตารางที่ ๔ แสดงร้อยละของเพศของผู้ตอบแบบประเมิน

ข้อมูลทั่วไป	จำนวน	ร้อยละ
เพศ		
๑. ชาย	๑๘	๒๙
๒. หญิง	๔๔	๗๑
รวม	**๖๒**	**๑๐๐**

ประเภทบุคลากร

จากผู้ตอบแบบประเมินความพึงพอใจจำนวน ๖๒ คน พบว่า ประเภทบุคลากรข้าราชการ มากที่สุด จำนวน ๒๗ คน คิดเป็นร้อยละ ๔๓.๕ รองลงมาคือ ลูกจ้างโครงการ จำนวน ๑๔ คน คิดเป็นร้อยละ ๒๒.๖ พนักงานราชการ จำนวน ๑๐ คน คิดเป็นร้อยละ ๑๖.๑ พนักงานกระทรวงสาธารณสุข จำนวน ๙ คน คิดเป็นร้อยละ ๑๔.๕ และลูกจ้างประจำ จำนวน ๒ คน คิดเป็นร้อยละ ๓.๓ ตามลำดับ รายละเอียดดังตารางที่ ๒

ตารางที่ ๕ แสดงร้อยละของประเภทบุคลากรของผู้ตอบแบบประเมิน

ข้อมูลทั่วไป	จำนวน	ร้อยละ
ประเภทบุคลากร		
๑. ข้าราชการ	๒๗	๔๓.๕
๒. ลูกจ้างประจำ	๒	๓.๓
๓. พนักงานราชการ	๑๐	๑๖.๑
๔. พนักงานกระทรวงสาธารณสุข	๙	๑๔.๕
๕. ลูกจ้างโครงการ	๑๔	๒๒.๖
รวม	**๖๒**	**๑๐๐**

ความถี่ในการใช้อินเตอร์เน็ตต่อวัน

จากผู้ตอบแบบประเมินความพึงพอใจจำนวน ๖๒ คน พบว่า ความถี่ในการใช้อินเตอร์เน็ตต่อวันมากที่สุด คือ ๖ – ๙ ชั่วโมงต่อวัน จำนวน ๒๙ คน คิดเป็นร้อยละ ๔๖.๘ รองลงมาคือ ๓ – ๖ ชั่วโมงต่อวัน จำนวน ๑๕ คน คิดเป็นร้อยละ ๒๔.๒ มากกว่า ๙ ชั่วโมงต่อวัน จำนวน ๑๓ คน คิดเป็นร้อยละ ๒๑ และ ๑ – ๓ ชั่วโมงต่อวัน จำนวน ๕ คน คิดเป็นร้อยละ ๘ ตามลำดับ รายละเอียดดังตารางที่ ๓

ตารางที่ ๖ แสดงร้อยละของความถี่ในการใช้อินเตอร์เน็ต/วันของผู้ตอบแบบประเมิน

ข้อมูลทั่วไป	จำนวน	ร้อยละ
ความถี่ในการใช้อินเตอร์เน็ต/วัน		
๑. ๑ – ๓ ชม./วัน	๕	๘
๒. ๓ – ๖ ชม./วัน	๑๕	๒๔.๒
๓. ๖ – ๙ ชม./วัน	๒๙	๔๖.๘
๔. มากกว่า ๙ ชม./วัน	๑๓	๒๑
รวม	**๖๒**	**๑๐๐**

ความถี่ในการใช้อินเตอร์เน็ตต่อสัปดาห์

จากผู้ตอบแบบประเมินความพึงพอใจจำนวน ๖๒ คน พบว่า ความถี่ในการใช้อินเตอร์เน็ตต่อสัปดาห์มากที่สุด คือ ๕ วันต่อสัปดาห์ จำนวน ๕๘ คน คิดเป็นร้อยละ ๙๓.๖ รองลงมาคือ ๑ วันต่อสัปดาห์ จำนวน ๒ คน คิดเป็นร้อยละ ๓.๒ และมากกว่า ๕ วันต่อสัปดาห์ จำนวน ๒ คน คิดเป็นร้อยละ ๓.๒ รายละเอียดดังตารางที่ ๔

ตารางที่ ๗ แสดงร้อยละของความถี่ในการใช้อินเตอร์เน็ต/สัปดาห์ของผู้ตอบแบบประเมิน

ข้อมูลทั่วไป	จำนวน	ร้อยละ
ความถี่ในการใช้อินเตอร์เน็ต/สัปดาห์		
๑. น้อยกว่า ๑ วัน/สัปดาห์	-	-
๒. ๑ วัน/สัปดาห์	๒	๓.๒
๓. ๒ วัน/สัปดาห์	-	-
๔. ๓ วัน/สัปดาห์	-	-
๕. ๔ วัน/สัปดาห์	-	-
๖. ๕ วัน/สัปดาห์	๕๘	๙๓.๖
๗. มากกว่า ๕ วัน/สัปดาห์	๒	๓.๒
รวม	**๖๒**	**๑๐๐**

ช่วงระยะเวลาในที่ใช้อินเตอร์เน็ต

จากผู้ตอบแบบประเมินความพึงพอใจจำนวน ๖๒ คน พบว่า ช่วงระยะเวลาที่ใช้บริการอินเตอร์เน็ตมากที่สุด คือ ช่วงเวลา ๑๖.๓๐ - ๒๐.๓๐ น. จำนวน ๔๐ คน คิดเป็นร้อยละ ๖๔.๕ รองลงมา คือ ช่วงเวลา ๐๘.๐๐ - ๑๒.๐๐ น. จำนวน ๙ คน คิดเป็นร้อยละ ๑๔.๕ ช่วงเวลา ๑๓.๐๐ - ๑๖.๓๐ น. จำวน ๘ คน คิดเป็นร้อยละ ๑๒.๙ ช่วงเวลา ๑๒.๐๐ - ๑๓.๐๐ น. จำนวน ๓ คน คิดเป็นร้อยละ ๔.๘ และช่วงเวลา ๑๖.๓๐ - ๒๐.๓๐ น. จำนวน ๒ คน คิดป็นร้อยละ ๓.๓ ตามลำดับ รายละเอียดดังตารางที่ ๕

ตารางที่ ๘ แสดงร้อยละของช่วงเวลาที่ใช้อินเตอร์เน็ตของผู้ตอบแบบประเมิน

ข้อมูลทั่วไป	จำนวน	ร้อยละ
ใช้บริการในช่วงใดมากที่สุด		
๑. ๐๘.๐๐ - ๑๒.๐๐ น.	๙	๑๔.๕
๒. ๑๒.๐๐ - ๑๓.๐๐ น.	๓	๔.๘
๓. ๑๓.๐๐ - ๑๖.๓๐ น.	๘	๑๒.๙
๔. ๐๘.๐๐ - ๑๖.๓๐ น.	๔๐	๖๔.๕
๕. ๑๖.๓๐ - ๒๐.๓๐ น.	๒	๓.๓
รวม	**๖๒**	**๑๐๐**

ส่วนที่ ๒ ระดับความพึงพอใจของผู้รับบริการด้านระบบสารสนเทศ

ตารางที่ ๙ ผลสำรวจด้านคุณภาพระบบเครือข่ายคอมพิวเตอร์ (LAN & Wireless)

หัวข้อการประเมิน	ร้อยละระดับความพึงพอใจ					ค่าเฉลี่ย ($\bar{x}$)	ส่วนเบี่ยงเบนมาตรฐาน (S.D)
	ดีมาก จำนวน (ร้อยละ)	ดี จำนวน (ร้อยละ)	ปานกลาง จำนวน (ร้อยละ)	พอใช้ จำนวน (ร้อยละ)	ควรปรับปรุง จำนวน (ร้อยละ)		
๑. ความเร็วการใช้งานอินเตอร์เน็ต (Internet) ผ่านระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน	๒๒ (๓๕.๔๘)	๓๐ (๔๘.๓๙)	๑๐ (๑๖.๑๓)	๐	๐	๔.๑๙	๐.๕๔
๒. ความสะดวกในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน	๒๓ (๓๗.๑๐)	๓๓ (๕๓.๒๓)	๖ (๙.๖๘)	๐	๐	๔.๒๗	๐.๕๕
๓. ความมีสเถียรภาพของระบบเครือข่ายสามารถใช้งานอินเตอร์เน็ต (Internet) ได้อย่างต่อเนื่อง	๒๐ (๓๒.๒๖)	๒๘ (๔๕.๑๖)	๑๒ (๑๙.๓๕)	๒ (๓.๒๓)	๐	๔.๐๖	๐.๕๓
๔. ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน (สาย LAN) สามารถให้บริการได้ ครอบคลุมทั่วถึง	๒๕ (๔๐.๓๒)	๒๗ (๔๓.๕๕)	๘ (๑๒.๙๐)	๒ (๓.๒๓)	๐	๔.๒๑	๐.๕๔
๕. ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานแบบ Wireless สามารถให้บริการได้ ครอบคลุมทั่วถึง	๒๔ (๓๘.๗๑)	๒๗ (๔๓.๕๕)	๙ (๑๔.๕๒)	๑ (๑.๖๑)	๑ (๑.๖๑)	๔.๑๖	๐.๕๔
ภาพรวม	**๓๐.๖๕**	**๓๘.๗๖**	**๑๑.๙๕**	**๑.๔๕**	**๐.๒๙**	**๔.๑๘**	**๐.๕๔**

ผลการสำรวจความพึงพอใจของบุคลากร ณ อาคารศูนย์การแพทย์บางรัก ที่มีต่อการใช้งานระบบสารสนเทศด้านคุณภาพระบบเครือข่ายคอมพิวเตอร์ (LAN & Wireless) โดยภาพรวมอยู่ในระดับดี (ค่าเฉลี่ยความพึงพอใจ ๔.๑๘ ส่วนเบี่ยงเบนมาตรฐาน ๐.๕๔) หัวข้อประเมินด้านคุณภาพระบบเครือข่ายคอมพิวเตอร์ที่บุคลากรมีความพึงพอใจมากที่สุด ได้แก่ หัวความสะดวกในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน (ความพึงพออยู่ในระดับดีมาก ค่าเฉลี่ยความพึงพอใจ ๔.๒๗ ส่วนเบี่ยงเบนมาตรฐาน ๐.๕๕) รองลงมาได้แก่ ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน (สาย LAN) สามารถให้บริการได้ ครอบคลุมทั่วถึง และความเร็วการใช้งานอินเตอร์เน็ต (Internet) ผ่านระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน ตามลำดับ

ตารางที่ ๑๐ ด้านระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ (Network Security)

หัวข้อการประเมิน	ร้อยละระดับความพึงพอใจ					ค่าเฉลี่ย ($\bar{x}$)	ส่วนเบี่ยงเบนมาตรฐาน (S.D)
	ดีมาก	ดี	ปานกลาง	พอใช้	ควรปรับปรุง		
	จำนวน (ร้อยละ)	จำนวน (ร้อยละ)	จำนวน (ร้อยละ)	จำนวน (ร้อยละ)	จำนวน (ร้อยละ)		
๑. ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน มีความปลอดภัยมากน้อยเพียงใด	๒๓ (๓๗.๑๐)	๒๙ (๔๖.๗๗)	๑๐ (๑๖.๑๓)	๐	๐	๔.๒๑	๐.๕๔
๒. การกำหนดสิทธิ์ (Username Account) ในการเข้าใช้งานระบบเครือข่าย คอมพิวเตอร์ มีความปลอดภัย และเป็นประโยชน์ต่อการใช้งาน	๒๙ (๔๖.๗๗)	๒๔ (๓๘.๗๑)	๘ (๑๒.๙๐)	๑ (๑.๖๑)	๐	๔.๓๑	๐.๕๖
๓. ความปลอดภัยของเครื่องคอมพิวเตอร์ที่ท่านใช้งาน ผ่านระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน	๓๐ (๔๘.๓๙)	๒๓ (๓๗.๑๐)	๙ (๑๔.๕๒)	๐	๐	๔.๓๔	๐.๕๖
ภาพรวม	**๓๘.๒๕**	**๓๓.๙๒**	**๑๒.๑๑**	**๐.๕๒**	**๐.๐๐**	**๔.๓๐**	**๐.๕๕**

ผลการสำรวจความพึงพอใจของบุคลากร ณ อาคารศูนย์การแพทย์บางรัก ที่มีต่อการใช้งานระบบสารสนเทศด้านระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ (Network Security) โดยภาพรวมอยู่ในระดับดีมาก (ค่าเฉลี่ยความพึงพอใจ ๔.๓๐ ส่วนเบี่ยงเบนมาตรฐาน ๐.๕๕) หัวข้อประเมินด้านระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ที่บุคลากรมีความพึงพอใจมากที่สุด ได้แก่ ความปลอดภัยของเครื่องคอมพิวเตอร์ที่ท่านใช้งาน ผ่านระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน ความพึงพออยู่ในระดับดีมาก (ค่าเฉลี่ยความพึงพอใจ ๔.๓๔ ส่วนเบี่ยงเบนมาตรฐาน ๐.๕๖) รองลงมาได้แก่ การกำหนดสิทธิ์ (Username Account) ในการเข้าใช้งานระบบเครือข่าย คอมพิวเตอร์ มีความปลอดภัย และเป็นประโยชน์ต่อการใช้งาน และระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน มีความปลอดภัยมากน้อยเพียงใด ตามลำดับ

ตารางที่ ๑๑ ด้านการให้บริการ (Service)

หัวข้อการประเมิน	ร้อยละระดับความพึงพอใจ					ค่าเฉลี่ย ($\bar{x}$)	ส่วนเบี่ยงเบนมาตรฐาน (S.D)
	ดีมาก	ดี	ปานกลาง	พอใช้	ควรปรับปรุง		
	จำนวน (ร้อยละ)	จำนวน (ร้อยละ)	จำนวน (ร้อยละ)	จำนวน (ร้อยละ)	จำนวน (ร้อยละ)		
๑. บริการและดูแลแก้ไขปัญหาผู้ใช้งานระบบเครือข่ายคอมพิวเตอร์ มีความรวดเร็วและทันต่อการใช้งาน	๓๕ (๕๖.๔๕)	๒๑ (๓๓.๘๗)	๖ (๙.๖๘)	๐	๐	๔.๔๗	๐.๕๗
๒. เจ้าหน้าที่สามารถตอบคำถามหรือแก้ไขปัญหาจากการใช้งานได้รวดเร็ว	๓๗ (๕๙.๖๘)	๒๐ (๓๒.๒๖)	๕ (๘.๐๖)	๐	๐	๔.๕๒	๐.๕๘
๓. การนำเทคโนโลยีมาช่วยในการบริการ	๓๑ (๕๐.๐๐)	๒๔ (๓๘.๗๑)	๗ (๑๑.๒๙)	๐	๐	๔.๓๙	๐.๕๖
๔. ติดตาม พัฒนาระบบการทำงานอย่างต่อเนื่อง	๓๑ (๕๐.๐๐)	๒๗ (๔๓.๕๕)	๔ (๖.๔๕)	๐	๐	๔.๔๔	๐.๕๗
๕. ยิ้มแย้มแจ่มใสและกิริยาวาจาสุภาพ	๔๐ (๖๔.๕๒)	๑๗ (๒๗.๔๒)	๔ (๖.๔๕)	๑ (๑.๖๑)	๐	๔.๕๕	๐.๕๘
๖. ความรวดเร็วในการติดต่อและให้บริการ	๓๕ (๕๖.๔๕)	๒๑ (๓๓.๘๗)	๕ (๑.๖๑)	๑ (๑.๖๑)	๐	๔.๔๕	๐.๕๗
ภาพรวม	**๔๖.๔๖**	**๒๘.๙๗**	**๖.๘๒**	**๐.๔๘**	**๐.๐๐**	**๔.๔๗**	**๐.๕๗**

ผลการสำรวจความพึงพอใจของบุคลากร ณ อาคารศูนย์การแพทย์บางรัก ที่มีต่อการใช้งานระบบสารสนเทศด้านการให้บริการ (Service) โดยภาพรวมอยู่ในระดับดีมาก (ค่าเฉลี่ยความพึงพอใจ ๔.๔๗ ส่วนเบี่ยงเบนมาตรฐาน ๐.๕๗) หัวข้อประเมินด้านการให้บริการ (Service) ที่บุคลากรมีความพึงพอใจมากที่สุด ได้แก่ ยิ้มแย้มแจ่มใสและกิริยาวาจาสุภาพ ความพึงพออยู่ในระดับดีมาก (ค่าเฉลี่ยความพึงพอใจ ๔.๕๕ ส่วนเบี่ยงเบนมาตรฐาน ๐.๕๘) รองลงมาได้แก่ เจ้าหน้าที่สามารถตอบคำถาม หรือแก้ไขปัญหาจากการใช้งานได้รวดเร็ว และบริการและดูแลแก้ไขปัญหาผู้ใช้งานระบบเครือข่ายคอมพิวเตอร์ มีความรวดเร็วและทันต่อการใช้งาน ตามลำดับ

ส่วนที่ ๓ ข้อเสนอแนะเพิ่มเติม

ผู้ตอบแบบสอบถามได้ให้ข้อเสนอแนะอื่น ๆ ดังนี้

- เครื่องคอมพิวเตอร์เก่าทำงานช้า พิมพ์เอกสารไม่สามารถพิมพ์เครื่องที่ใช้ไวไฟได้
- ในบางครั้ง เข้าใช้งานรหัส Internet ไม่ได้ โดยที่ยังไม่ครบกำหนดเปลี่ยนรหัส
- บางมุมของตึกสัญญาไม่มี บางวันสัญญานหลุดบ่อย
- ปรับปรุงให้เสถียรมากกว่านี้ แต่อาจจะอยู่ที่งบประมาณก็เป็นได้
- บางครั้งรหัสเข้าใช้งานไม่ได้
- อินเตอร์เน็ตหลุดบ่อย ความสเถียรของสัญญาณ Wi-Fi (บางวันเข้าไม่ได้ แต่เป็นไม่บ่อย)

๕.๓ การเฝ้าระวังความเสถียรของระบบเครือข่ายคอมพิวเตอร์โดยการคำนวณ SLA

การเฝ้าระวังความเสถียรของระบบเครือข่ายคอมพิวเตอร์เป็นกระบวนการที่สำคัญในการตรวจสอบและรักษาความเสถียรของเครือข่ายในองค์กร เพื่อช่วยให้สามารถใช้งานระบบเครือข่ายได้อย่างต่อเนื่องมีประสิทธิภาพ และการคำนวณ SLA (Service Level Agreement) หลังการติดตั้งระบบเครือข่ายเป็นกระบวนการในการประเมินประสิทธิภาพและความเสถียรของบริการเครือข่ายคอมพิวเตอร์

การคำนวณ SLA

การคำนวณ SLA (Service Level Agreement) เป็นกระบวนการที่ใช้ในการวัดและประเมินระดับการบริการที่ผู้ให้บริการต้องรักษาไว้ตามข้อตกลงที่กำหนดร่วมกันกับผู้ใช้งานระบบเครือข่ายในองค์กร ซึ่งโดยทั่วไปจะมุ่งเน้นไปที่การวัดความพร้อมใช้งาน (Uptime) ของระบบ บริการหรือเครือข่าย

๑. กำหนดเมตริกที่ต้องการวัดผล (Define Metrics)
   - ความพร้อมใช้งาน (Availability) เปอร์เซ็นต์ของเวลาที่ระบบพร้อมใช้งาน
   - เวลาในการตอบสนอง (Response Time) เวลาที่ระบบใช้ในการตอบสนองต่อการร้องขอ
   - เวลาในการแก้ไขปัญหา (Resolution Time) เวลาที่ใช้ในการแก้ไขปัญหาหลังจากที่พบ

๒. กำหนดระยะเวลา (Define Time Period) ระบุช่วงเวลาที่จะใช้ในการคำนวณ SLA เช่น รายวัน รายสัปดาห์ รายเดือน หรือรายปี

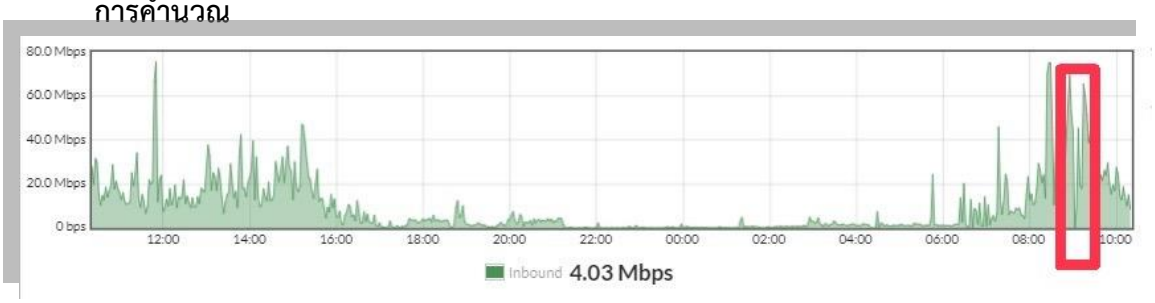
๓. เก็บรวบรวมข้อมูล (Data Collection) โดยใช้เครื่องมือมอนิเตอร์เครือข่ายเพื่อเก็บรวบรวมข้อมูลที่เกี่ยวข้อง เช่น Downtime, Uptime, Response Time, และ Resolution Time

สูตรการคำนวณ SLA

๑. การคำนวณความพร้อมใช้งาน (Availability) ความพร้อมใช้งาน (Availability) สามารถคำนวณได้โดยใช้สูตร

$$\text{Availability (\%)} = \left(\frac{\text{Total Uptime}}{\text{Total Uptime} + \text{Total Downtime}} \right) \times 100$$

การคำนวณ



จากข้อมูลการใช้งานระบบเครือข่ายของอาคารศูนย์การแพทย์บางรักในเดือนมกราคม เฉพาะช่วงเวลาที่หน่วยงานปฏิบัติในเวลาราชการเท่านั้น มีเวลาทั้งหมด ๒๑ วัน หรือ ๕๒๘ ชั่วโมง และระบบมี Downtime รวมทั้งหมด ๔ ชั่วโมง โดย SLA Target = ๙๙.๘%

- การคำนวณ Total Uptime

$$\text{Total Uptime} = 504 \text{ ชั่วโมง} - 4 \text{ ชั่วโมง} = 500 \text{ ชั่วโมง}$$

- การคำนวณ Availability

$$\text{Availability (\%)} = \left(\frac{500}{504}\right)^{\square} \times 100 = 99.2\%$$

- การเปรียบเทียบกับ SLA ที่กำหนด มีการกำหนดความพร้อมใช้งานไว้ที่ ๙๙.๘% และผลคำนวณได้ ๙๙.๒% แสดงว่า Availability ที่คำนวณได้ต่ำกว่าเป้าหมายที่กำหนดไว้

๒. การคำนวณเวลาในการตอบสนอง (Response Time) และเวลาในการแก้ไขปัญหา (Resolution Time)

$$\text{Average Response Time} = \frac{\sum \text{Response Time for Each Incident}}{\text{Number of Incidents}}$$

$$\text{Average Resolution Time} = \frac{\sum \text{Resolution Time for Each Incident}}{\text{Number of Incidents}}$$

ตัวอย่างการคำนวณ

ในเดือนที่ผ่านมามีเหตุการณ์เกิดขึ้น ๑๐ ครั้ง โดยมีเวลาตอบสนองรวมทั้งหมด ๑๐๐ นาที และเวลาแก้ไขปัญหารวมทั้งหมด ๓๐๐ นาที

- **คำนวณ Average Response Time**

$$\text{Average Response Time} = \frac{100 \text{ นาที}}{10} = 10 \text{ นาที/เหตุการณ์}$$

- **คำนวณ Average Resolution Time**

$$\text{Average Resolution Time} = \frac{300 \text{ นาที}}{10} = 30 \text{ นาที/เหตุการณ์}$$

- **เปรียบเทียบกับ SLA ที่กำหนด**

  ในกรณีที่ SLA กำหนดเวลาในการตอบสนองไม่เกิน ๑๕ นาที และเวลาในการแก้ไขปัญหาไม่เกิน ๖๐ นาที ผลคำนวณที่ได้ (๑๐ นาทีสำหรับ Response Time และ ๓๐ นาทีสำหรับ Resolution Time) จะถือว่าเป็นไปตาม SLA ที่กำหนด

การวิเคราะห์และรายงานผล

การคำนวณ SLA เป็นกระบวนการที่สำคัญในการประเมินประสิทธิภาพและความเสถียรของระบบเครือข่ายคอมพิวเตอร์ในองค์กร การเก็บรวบรวมข้อมูลอย่างถูกต้องและการวิเคราะห์ผลลัพธ์จะช่วยให้องค์กรสามารถรักษาความเสถียรของเครือข่ายได้ตามที่กำหนดใน SLA และสามารถตอบสนองต่อปัญหาได้อย่างทันท่วงที มีองค์ประกอบที่สำคัญที่จำเป็นต้องดำเนินงานอย่างต่อเนื่องดังนี้

๑. วิเคราะห์ผลลัพธ์ (Analyze Results)
- ประเมินผลลัพธ์ที่ได้จากการคำนวณ
- ระบุสาเหตุของ Downtime และปัญหาที่เกิดขึ้น

๒. รายงานผล (Reporting)
- สร้างรายงานที่สรุปผลการคำนวณ SLA รวมถึงเหตุการณ์ที่ทำให้เกิด Downtime และการแก้ไขปัญหาที่ดำเนินการ
- รายงานควรประกอบด้วยกราฟหรือแผนภูมิที่แสดงผลลัพธ์เพื่อให้เข้าใจง่าย

๓. ปรับปรุงและพัฒนา (Improvement and Development)
- ใช้ข้อมูลที่ได้จากการวิเคราะห์เพื่อปรับปรุงระบบและกระบวนการต่างๆ เพื่อเพิ่มความเสถียรและประสิทธิภาพของเครือข่าย
- ดำเนินการตามแผนการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) เพื่อป้องกันปัญหาที่อาจเกิดขึ้นในอนาคต
- หาสาเหตุของ Downtime และปรับปรุงระบบเพื่อป้องกันไม่ให้เกิดปัญหาเดิมซ้ำ
- เพิ่มความซ้ำซ้อนในระบบเพื่อเพิ่มความเสถียร
- ปรับปรุงการแจ้งเตือนและตอบสนองเกิดปัญหา
- ศึกษาวิธีเครื่องมือหรืออุปกรณ์ที่ใช้งานในเครือข่ายที่มีประสิทธิภาพ

๕.๔ ปัญหาและอุปสรรคในการดำเนินงาน

การปรับปรุงระบบเครือข่ายคอมพิวเตอร์ของอาคารศูนย์การแพทย์บางรัก ตามขั้นตอนการดำเนินงานที่ได้กำหนดไว้นั้น ผู้จัดทำได้พบปัญหาอุปสรรคในการดำเนินงานดังนี้

ปัญหาและอุปสรรค	การแก้ไขปัญหา
พื้นที่ห้องสารสนเทศบริเวณชั้น ๑๒ คับแคบ ทำให้ไม่สามารถตดตั้งอุปกรณ์เครือข่ายทั้งหมดได้ และเครื่องปรับอากาศมีเพียงเครื่องเดียว ทำให้ต้องเปิดตลอด ๒๔ ชั่วโมง และขาดระบบดับเพลิงชนิดสารสะอาด ไม่เหมาะสมในการติดตั้งอุปกรณ์เครือเพิ่มเติมได้	- สำรวจพื้นที่ภายในอาคารศูนย์การแพทย์รัก - เคลื่อนย้ายอุปกรณ์บางส่วน และอุปกรณ์ที่จัดหาใหม่ไปติดตั้งที่ชั้น ๑๓ เนื่องจากเป็นพื้นที่ที่เหมาะกับการติดตั้งระบบเครือข่าย โดยมีเครื่องปรับอากาศ และระบบดับเพลิงรองรับ

ปัญหาและอุปสรรค	การแก้ไขปัญหา
การเชื่อมต่อระบบเครือข่ายเดิมของอาคารและระบบเครือข่ายที่ปรับปรุงใหม่	- สำรวจจุดเชื่อมต่อเครือข่าย - วางแผนการเดินสายสัญญาณ - ติดตั้งอุปกรณ์กระจายสัญญาณเพิ่มเติมในห้องปฏิบัติการ Server ชั้น ๑๒ - เดินสายสัญญาณ Fiber Optic เพื่อเชื่อมต่ออุปกรณ์เครือข่ายให้สามารถทำงานร่วมกันได้
ห้องปฏิบัติการฯ ชั้น ๑๓ ระบบจ่ายกระไฟฟ้าไม่เพียงพอ ไม่เหมาะกับการติดตั้งอุปกรณ์เครือข่าย	- จัดจ้างติดตั้งระบบไฟฟ้า - เชื่อมต่อระบบไฟฟ้า ๒ ระบบให้กับตู้ติดตั้งอุปกรณ์เครือข่าย ได้แก่ ระบบไฟฟ้าของอาคาร Generator และเครื่องสำรองไฟฟ้าขนาด 40 KVA เพิ่มความมั่นคงในการใช้พลังงานไฟฟ้า
ตู้เก็บแบตเตอรี่ของเครื่องสำรองไฟฟ้ามีขนาดใหญ่และน้ำหนักมาก เป็นอุปสรรคในการติดตั้ง	- ติดตั้งแผ่นกระจายน้ำหนัก สำหรับติดตั้งตู้เก็บแบตเตอรี่
อุปกรณ์เครือข่ายบางตัวไม่สามารถเข้าระบบเพื่อทำการ CONFIGURATION อุปกรณ์ได้	- ติดต่อผู้ที่มีความเชี่ยวชาญเพื่อขอคำปรึกษา

๕.๕ ข้อเสนอแนะ

๕.๕.๑ ในการปรับปรุงอาคารครั้งต่อไป ควรมีการประสานผู้เชี่ยวชาญด้านระบบเครือข่ายคอมพิวเตอร์หรือระบบอื่น ๆ ที่เกี่ยวข้อง เพื่อร่วมกันออกแบบโครงสร้างของระบบและความต้องการของผู้ใช้งานที่ถูกต้องเหมาะสมตั้งแต่ขั้นตอนการเขียนแบบ

๕.๕.๒ เจ้าหน้าที่สารสนเทศหรือผู้ที่ได้รับมอบหมายให้ดูแลระบบเครือข่ายคอมพิวเตอร์ของอาคารควรได้รับการอบรมด้านการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ที่ถูกต้องเหมาะสมและสม่ำเสมอ

๕.๕.๓ เจ้าหน้าที่สารสนเทศหรือผู้ที่ได้รับมอบหมายต้องศึกษาคู่มือ ในการใช้งานอุปกรณ์ และดำเนินการตามแผนการอย่างเคร่งครัดเท่านั้น เนื่องจากอุปกรณ์บางชนิดเป็นอุปกรณ์ไฟฟ้าที่มีความอ่อนไหวต่อการใช้งาน จึงอาจส่งผลเสียหายได้หากไม่ปฏิบัติตาม หรือหากอยู่นอกเหนือจากแผนการดำเนินการต้องมีประชุมเพื่อกำหนดแผนการอีกครั้งร่วมกับผู้เชี่ยวชาญและผู้ผลิตต่อไป

บรรณานุกรม

๑. ธิตินัดดา สิงห์แก้ว. (๒๕๖๒). การพัฒนาระบบดูแลช่วยเหลือนักเรียนโดยใช้วงจร PDCA : กรณีศึกษาโรงเรียนวัดป่าตึงห้วยยาบ อำเภอบ้านธิ จังหวัดลาพูน. สืบค้นจาก http://cmruir.cmru.ac.th/handle/123456789/2163

๒. วีย์รฎา กวิณรวีบริรักษ์. (๒๕๖๔). Services 7 อักษรที่มีความหมาย. สืบค้นจาก https://www.consultthailand.com

๓. น.ส.สุภาพร ศิริยามตย์. (๒๕๖๕). มาตรฐานและเทคโนโลยีของระบบเครือข่าย. สืบค้นจาก https://lo113.blogspot.com/2012/12/3.html

๔. คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ประจำกระทรวงสาธารณสุข. (๒๕๖๕). แนวทางการพิจารณาจัดหาครุภัณฑ์คอมพิวเตอร์. สืบค้นจาก https://ict.moph.go.th/upload_file/files/a442f0c2b0123cfb50e370def535608c.pdf

๕. การรักษาความปลอดภัยในเครือข่าย. (๒๕๕๕). สืบค้นจาก https://aunsana.blogspot.com/2013/01/blog-post.html

๖. ณัฏฐ์ณพัชร์ อ่อนตาม. เทคนิคการบริหารงานแบบ PDCA (Deming Cycle). วารสารสมาคมพัฒนาวิชาชีพการบริหารการศึกษาแห่งประเทศไทย. สืบค้นจาก https://so04.tci-thaijo.org/index.php/JAPDEAT/article/view/250846/170386

๗. สุขสันต์ สุขสงคราม. แนวคิดการบริหารแบบวงจรคุณภาพ (PDCA) กับการบริหารแบบพระพุทธศาสนา. วารสารธรรมวัตร. สืบค้นจาก: https://so09.tci-thaijo.org/index.php/tmwj/article/view/637/233

๘. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข. (๒๕๖๔). เกณฑ์ราคากลางและคุณลักษณะพื้นฐานการจัดหาอุปกรณ์และระบบคอมพิวเตอร์ ฉบับเดือน ธันวาคม ๒๕๖๔. สืบค้นจาก https://ict.moph.go.th/th/extension/803

๙. การคำนวณเบื้องต้นของ UPS. (๒๕๖๔). สืบจาก https://www.pp-ontime.co.th/รายละเอียด/การคำนวณเบื้องต้น_Und_ของ_Und_UPS

๑๐. กรมวิทยาศาสตร์การแพทย์. (๒๕๖๖). นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ. สืบค้นจาก https://rmsc12-1.dmsc.moph.go.th/files/policy2.pdf

ภาคผนวก ก

เกณฑ์ราคากลางและคุณลักษณะพื้นฐานการจัดหาอุปกรณ์และระบบคอมพิวเตอร์

1. เครื่องคอมพิวเตอร์แม่ข่าย แบบที่ 1 ราคา 130,000 บาท

คุณลักษณะพื้นฐาน

- มีหน่วยประมวลผลกลาง (CPU) แบบ 10 แกนหลัก (10 core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2.2 GHz จำนวนไม่น้อยกว่า 1 หน่วย
- หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ 64 bit มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันไม่น้อยกว่า 13 MB
- มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR4 หรือดีกว่า มีขนาดไม่น้อยกว่า 16 GB
- สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID 0, 1, 5
- มีหน่วยจัดเก็บข้อมูล ชนิด SCSI หรือ SAS หรือ SATA ที่มีความเร็วรอบไม่น้อยกว่า 10,000 รอบต่อนาที ขนาดความจุไม่น้อยกว่า 1 TB หรือ ชนิด Solid State Drive หรือดีกว่า ขนาดความจุไม่น้อยกว่า 480 GB จำนวนไม่น้อยกว่า 2 หน่วย
- มี DVD-ROM หรือดีกว่า แบบติดตั้งภายใน (Internal) หรือภายนอก (External) จำนวน 1 หน่วย
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง
- มีจอแสดงภาพขนาดไม่น้อยกว่า 17 นิ้ว จำนวน 1 หน่วย
- มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย

2. เครื่องคอมพิวเตอร์แม่ข่าย แบบที่ 2 ราคา 350,000 บาท

คุณลักษณะพื้นฐาน

- มีหน่วยประมวลผลกลาง (CPU) แบบ 16 แกนหลัก (16 core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2.3 GHz จำนวนไม่น้อยกว่า 2 หน่วย
- หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ 64 bit มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันไม่น้อยกว่า 22 MB
- มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR4 หรือดีกว่า ขนาดไม่น้อยกว่า 32 GB
- สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID 0, 1, 5
- มีหน่วยจัดเก็บข้อมูล ชนิด SCSI หรือ SAS ที่มีความเร็วรอบไม่น้อยกว่า 10,000 รอบ ต่อนาที ขนาดความจุไม่น้อยกว่า 1 TB หรือ ชนิด Solid State Drive หรือดีกว่า ขนาดความจุไม่น้อยกว่า 480 GB จำนวนไม่น้อยกว่า 4 หน่วย
- มี DVD-ROM หรือดีกว่า แบบติดตั้งภายใน (Internal) หรือภายนอก (External) จำนวน 1 หน่วย
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง

13. คอมพิวเตอร์แท็บเล็ต แบบที่ 1 ราคา 10,000 บาท

คุณลักษณะพื้นฐาน

- มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 6 แกนหลัก (6 core)
- มีหน่วยความจำหลัก (RAM) ที่มีขนาดไม่น้อยกว่า 3 GB
- มีหน่วยความจำขนาดไม่น้อยกว่า 32 GB
- มีหน้าจอสัมผัสขนาดไม่น้อยกว่า 10 นิ้ว และมีความละเอียดไม่น้อยกว่า 1,920 x 1,200 Pixel
- สามารถใช้งานได้ไม่น้อยกว่า Wi-Fi (802.11 ac), Bluetooth
- มีกล้องด้านหน้าความละเอียดไม่น้อยกว่า 1.2 Megapixel
- มีกล้องด้านหลังความละเอียดไม่น้อยกว่า 8 Megapixel

14. คอมพิวเตอร์แท็บเล็ต แบบที่ 2 ราคา 20,000 บาท

คุณลักษณะพื้นฐาน

- มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 6 แกนหลัก (6 core)
- มีหน่วยความจำหลัก (RAM) ที่มีขนาดไม่น้อยกว่า 3 GB
- มีหน่วยความจำขนาดไม่น้อยกว่า 32 GB
- มีหน้าจอสัมผัสขนาดไม่น้อยกว่า 10 นิ้ว และมีความละเอียดไม่น้อยกว่า 2,048 x 1,536 Pixel
- สามารถใช้งานได้ไม่น้อยกว่า Wi-Fi (802.11 ac), Bluetooth และ GPS
- มีอุปกรณ์เชื่อมต่อระบบ 4G หรือดีกว่า แบบติดตั้งภายในตัวเครื่อง (built-in)
- มีอุปกรณ์การเขียนที่สามารถใช้งานร่วมกับอุปกรณ์คอมพิวเตอร์แท็บเล็ต
- มีกล้องด้านหน้าความละเอียดไม่น้อยกว่า 1.2 Megapixel
- มีกล้องด้านหลังความละเอียดไม่น้อยกว่า 8 Megapixel

15. อุปกรณ์สำหรับจัดเก็บข้อมูลแบบภายนอก (External Storage) ราคา 570,000 บาท

คุณลักษณะพื้นฐาน

- เป็นอุปกรณ์ที่ทำหน้าที่จัดเก็บข้อมูลแบบภายนอก (External Storage) ซึ่งสามารถทำงานในระบบ SAN (Storage Area Network) ได้
- มีส่วนควบคุมอุปกรณ์ (Controller) แบบ Dual Controller
- มีหน่วยจัดเก็บข้อมูล ชนิด SATA หรือ SAS หรือดีกว่า ขนาดความจุไม่น้อยกว่า 1.2 TB และมีความเร็วรอบไม่น้อยกว่า 10,000 รอบต่อนาที จำนวนไม่น้อยกว่า 12 หน่วย
- สามารถติดตั้ง Hard Disk ได้สูงสุด 24 หน่วย
- สามารถทำงาน แบบ Raid ไม่น้อยกว่า Raid 0, 1, 5

18. ค่าเช่าระบบจัดเก็บ Log File บน Cloud แบบที่ 3 ราคา 18,000 บาทต่อเดือน

คุณลักษณะพื้นฐาน

- สามารถจัดเก็บ Log File บน Cloud ได้
- มีหน่วยประมวลผลกลาง (CPU) จำนวนไม่น้อยกว่า 4 แกนหลัก (Core)
- มีหน่วยความจำหลัก (RAM) ขนาดไม่น้อยกว่า 4 GB
- มีหน่วยจัดเก็บข้อมูล (Storage) เพื่อเก็บ Log file ขนาดความจุไม่น้อยกว่า 3 TB
- สามารถเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตได้
- ติดตั้งระบบปฏิบัติการที่ใช้งานได้ถูกต้องตามกฎหมาย
- มีระบบป้องกันการบุกรุกเครือข่าย (Firewall) พร้อมใช้งาน
- รองรับการใช้งานผ่านระบบเครือข่าย IPv6
- มีการดำเนินการสำรองเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Machine Backup) ที่ให้บริการเช่า
- สามารถจัดเก็บ Log File ได้ไม่น้อยกว่า 90 วัน
- กำหนดเวลา (NTP : Network Time Protocol) ให้กับอุปกรณ์เพื่อไม่ให้เกิดความคลาดเคลื่อนกับเวลามาตรฐาน
- สามารถจัดเก็บ Log File ได้ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ฉบับที่มีผลบังคับใช้

19. อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย แบบที่ 1 ราคา 50,000 บาท

คุณลักษณะพื้นฐาน

- เป็นอุปกรณ์ Appliance หรืออุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์ (logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall, Network Devices ต่างๆ ระบบปฏิบัติการ ระบบ appliances ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น ได้อย่างน้อย 3 อุปกรณ์ต่อระบบ โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (format) เดียวกันได้
- มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน MD5 หรือ SHA-1 หรือดีกว่า
- สามารถเก็บ Log File ในรูปแบบ Syslog ของอุปกรณ์ เช่น Router, Switch, Firewall, VPN, Server เป็นต้น ได้
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH ได้
- สามารถจัดเก็บ log file ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ฉบับที่มีผลบังคับใช้ โดยได้รับรองมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ log file ที่ได้มาตรฐาน เช่น มาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ. 4003.1-2560) เป็นต้น
- สามารถทำการสำรองข้อมูล (Data Backup) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น Tape หรือ DVD หรือ External Storage เป็นต้น ได้
- สามารถจัดเก็บข้อมูลเหตุการณ์ต่อวินาที (Events per Seconds) ได้ไม่น้อยกว่า 1,000 eps

20. อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย แบบที่ 2 ราคา 400,000 บาท

คุณลักษณะพื้นฐาน

- เป็นอุปกรณ์ Appliance หรืออุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์ (logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall, Network Devices ต่าง ๆ ระบบปฏิบัติการ ระบบ appliances ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น ได้อย่างน้อย 10 อุปกรณ์ต่อระบบ โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (format) เดียวกันได้
- มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน MD5 หรือ SHA-1 หรือดีกว่า
- สามารถเก็บ Log File ในรูปแบบ Syslog ของอุปกรณ์ เช่น Router, Switch, Firewall, VPN, Server เป็นต้น ได้
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH ได้
- สามารถจัดเก็บ log file ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่มีผลบังคับใช้ โดยได้รับรองมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ log file ที่ได้มาตรฐาน เช่น มาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ. 4003.1-2560) เป็นต้น
- สามารถทำการสำรองข้อมูล (Data Backup) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น Tape หรือ DVD หรือ External Storage เป็นต้น ได้
- สามารถจัดเก็บข้อมูลเหตุการณ์ต่อวินาที (Events per Seconds) ได้ไม่น้อยกว่า 7,000 eps

21. อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย แบบที่ 3 ราคา 850,000 บาท

คุณลักษณะพื้นฐาน

- เป็นอุปกรณ์ Appliance หรืออุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์ (logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall, Network Devices ต่าง ๆ, ระบบปฏิบัติการ, ระบบ appliances, ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น ได้อย่างน้อย 15 อุปกรณ์ต่อระบบ โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (format) เดียวกันได้
- มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน MD5 หรือ SHA-1 หรือดีกว่า
- สามารถเก็บ Log File ในรูปแบบ Syslog ของอุปกรณ์ เช่น Router, Switch, Firewall, VPN, Server เป็นต้น ได้
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH ได้
- สามารถจัดเก็บ log file ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่มีผลบังคับใช้ โดยได้รับรองมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ log file ที่ได้มาตรฐาน เช่น มาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ. 4003.1-2560) เป็นต้น
- สามารถทำการสำรองข้อมูล (Data Backup) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น Tape หรือ DVD หรือ External Storage เป็นต้น ได้
- สามารถจัดเก็บข้อมูลเหตุการณ์ต่อวินาที (Events per Seconds) ได้ไม่น้อยกว่า 20,000 eps

22. อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) แบบที่ 1 ราคา 240,000 บาท

คุณลักษณะพื้นฐาน

- เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Appliance
- มี Firewall Throughput ไม่น้อยกว่า 2 Gbps
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 5 ช่อง
- มีระบบตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ อย่างน้อย ดังนี้ Syn Flood, UDP Flood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment, ICMP Fragment เป็นต้นได้
- สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้
- สามารถ Routing แบบ Static, Dynamic Routing ได้
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย
- สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้
- สามารถใช้งานตามมาตรฐาน IPv6 ได้

23. อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) แบบที่ 2 ราคา 1,000,000 บาท

คุณลักษณะพื้นฐาน

- เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Appliance
- มี Firewall Throughput ไม่น้อยกว่า 30 Gbps
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 8 ช่อง
- สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ อย่างน้อย ดังนี้ Syn Flood, UDP Flood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment, ICMP Fragment เป็นต้นได้
- สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้
- สามารถทำงานลักษณะ Transparent Mode ได้
- สามารถ Routing แบบ Static, Dynamic Routing ได้
- มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย
- สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้
- สามารถใช้งานตามมาตรฐาน IPv6 ได้

24. อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) แบบที่ 1 ราคา 430,000 บาท

คุณลักษณะพื้นฐาน

- เป็นอุปกรณ์ (Hardware Appliance) ที่ออกแบบมาเพื่อป้องกันการบุกรุกทางเครือข่าย (Intrusion Prevention System)
- สามารถตรวจจับวิธีการบุกรุกและป้องกันเครือข่ายได้อย่างน้อย ดังนี้ Signature matching, Protocol/Packet Anomalies, Statistical anomalies หรือ Application anomalies, Overflow, Worm, Virus, Backdoor Program, Trojan Horse, Port Scanning, Spy ware, Packet Analysis, DOS, DDOS
- สามารถทำงานได้อย่างน้อย 1 Segments ใน IPS mode
- มีความเร็วในการตรวจจับ (IPS Throughput) ไม่น้อยกว่า 600 Mbps
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย
- สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้
- สามารถใช้งานตามมาตรฐาน IPv6 ได้

25. อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) แบบที่ 2 ราคา 1,400,000 บาท

คุณลักษณะพื้นฐาน

- เป็นอุปกรณ์ (Hardware Appliance) ที่ออกแบบมาเพื่อป้องกันการบุกรุกทางเครือข่าย (Intrusion Prevention System)
- สามารถทำงานได้ในโหมด Passive และ In-line หรือ ดีกว่า
- สามารถตรวจจับวิธีการบุกรุกและป้องกันเครือข่ายได้อย่างน้อย ดังนี้ Signature matching, Protocol/Packet Anomalies, Statistical anomalies หรือ Application anomalies, Overflow, Worm, Virus, Backdoor Program, Trojan Horse, Port Scanning, Spy ware, Packet Analysis, DoS, DDoS
- สามารถทำงานได้อย่างน้อย 3 Segments ใน IPS mode
- มีความเร็วในการตรวจจับ (Throughput) ไม่น้อยกว่า 1 Gbps
- เมื่ออุปกรณ์เกิดปัญหาสามารถทำงานได้อย่างต่อเนื่อง (Bypass Traffic) โดยช่องสัญญาณ In-Line Mode สามารถรับส่งข้อมูลได้ตามปกติ
- มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย
- สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้
- สามารถใช้งานตามมาตรฐาน IPv6 ได้

32. อุปกรณ์กระจายสัญญาณ (L2 Switch) ขนาด 24 ช่อง แบบที่ 1 ราคา 4,500 บาท

คุณลักษณะพื้นฐาน

- มีลักษณะการทำงานไม่น้อยกว่า Layer 2 ของ OSI Model
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 24 ช่อง
- มีสัญญาณไฟแสดงสถานะของการทำงานช่องเชื่อมต่อระบบเครือข่ายทุกช่อง

33. อุปกรณ์กระจายสัญญาณ (L2 Switch) ขนาด 24 ช่อง แบบที่ 2 ราคา 18,000 บาท

คุณลักษณะพื้นฐาน

- มีลักษณะการทำงานไม่น้อยกว่า Layer 2 ของ OSI Model
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 24 ช่อง
- มีสัญญาณไฟแสดงสถานะของการทำงานช่องเชื่อมต่อระบบเครือข่ายทุกช่อง
- รองรับ Mac Address ได้ไม่น้อยกว่า 16,000 Mac Address
- สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser ได้

34. อุปกรณ์กระจายสัญญาณ (L3 Switch) ขนาด 24 ช่อง ราคา 110,000 บาท

คุณลักษณะพื้นฐาน

- มีลักษณะการทำงานไม่น้อยกว่า Layer 3 ของ OSI Model
- สามารถค้นหาเส้นทางเครือข่ายโดยใช้โปรโตคอล (Routing Protocol) RIPv2, OSPF ได้เป็นอย่างน้อย
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 24 ช่อง
- มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1/10 Gbps (SFP/SFP+) พร้อม Transceiver Module จำนวนไม่น้อยกว่า 2 ช่อง
- มีสัญญาณไฟแสดงสถานะของการทำงานช่องเชื่อมต่อระบบเครือข่ายทุกช่อง
- รองรับ Mac Address ได้ไม่น้อยกว่า 16,000 Mac Address
- สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser ได้
- สามารถส่งข้อมูล Log File ในรูปแบบ Syslog ได้เป็นอย่างน้อย
- สามารถใช้งานตามมาตรฐาน IPv6 ได้

35. อุปกรณ์กระจายสัญญาณไร้สาย (Access Point) แบบที่ 1 ราคา 5,400 บาท

คุณลักษณะพื้นฐาน

- สามารถใช้งานตามมาตรฐาน (IEEE 802.11b, g, n, ac) ได้เป็นอย่างน้อย
- สามารถทำงานที่คลื่นความถี่ 2.4 GHz และ 5 GHz
- สามารถเข้ารหัสข้อมูลตามมาตรฐาน WPA และ WPA2 ได้เป็นอย่างน้อย

- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 1 ช่อง
- สามารถทำงานได้ตามมาตรฐาน IEEE 802.3af หรือ IEEE 802.3at (Power over Ethernet)
- สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser ได้

36. อุปกรณ์กระจายสัญญาณไร้สาย (Access Point) แบบที่ 2 ราคา 21,000 บาท

คุณลักษณะพื้นฐาน

- สามารถใช้งานตามมาตรฐาน (IEEE 802.11b, g, n, ac) ได้เป็นอย่างน้อย
- สามารถทำงานที่คลื่นความถี่ 2.4 GHz และ 5 GHz ใน SSID เดียวกัน
- สามารถเข้ารหัสข้อมูลตามมาตรฐาน WPA , WPA2 และ WPA3 ได้เป็นอย่างน้อย
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 1 ช่อง
- สามารถทำงานได้ตามมาตรฐาน IEEE 802.3af หรือ IEEE 802.3at (Power over Ethernet)
- สามารถรับสัญญาณขาเข้าไม่น้อยกว่า 3 ช่องสัญญาณ และส่งสัญญาณขาออกไม่น้อยกว่า 3 ช่องสัญญาณ (3x3 MIMO) และสามารถทำงานแบบ Multiuser MIMO (MU-MIMO) ได้เป็นอย่างน้อย
- รองรับการบริหารจัดการผ่านระบบควบคุมเครือข่ายไร้สาย (Wireless Controller)
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTP หรือ HTTPS หรือ SSH ได้เป็นอย่างน้อย

37. อุปกรณ์ค้นหาเส้นทางเครือข่าย (Router) ราคา 44,000 บาท

คุณลักษณะพื้นฐาน

- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง
- มีสัญญาณไฟแสดงสถานะของการทำงานช่องเชื่อมต่อระบบเครือข่ายทุกช่อง
- มีหน่วยความจำแบบ Flash (Flash Memory) ขนาดไม่น้อยกว่า 256 MB
- สามารถค้นหาเส้นทางเครือข่ายโดยใช้โปรโตคอล (Routing Protocol) BGP, OSPFv2, OSPFv3, RIP-1, RIP-2, RIPng, Static IPv4 Routing และ Static IPv6 Routing ได้เป็นอย่างน้อย
- สามารถส่งข้อมูล Log File แบบ Syslog ได้เป็นอย่างน้อย
- สามารถใช้งานตามมาตรฐาน IPv6 ได้

38. อุปกรณ์กระจายการทำงานสำหรับเครือข่าย (Link Load Balancer) ราคา 180,000 บาท

คุณลักษณะพื้นฐาน

- เป็นอุปกรณ์ (Hardware Appliance) ที่ออกแบบมาเพื่อใช้กระจายการทำงานสำหรับเครือข่ายโดยเฉพาะ
- มี Throughput สูงสุดไม่น้อยกว่า 400 Mbps

- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 6 ช่อง
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS ได้เป็นอย่างน้อย
- สามารถใช้งานตามมาตรฐาน IPv6 ได้

39. อุปกรณ์กระจายการทำงานสำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server Load Balancer)
ราคา 210,000 บาท

คุณลักษณะพื้นฐาน

- เป็นอุปกรณ์ (Hardware Appliance) ที่ออกแบบมาเพื่อใช้กระจายการทำงานสำหรับเครื่องคอมพิวเตอร์แม่ข่ายโดยเฉพาะ
- มี Throughput สูงสุดไม่น้อยกว่า 2 Gbps
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 4 ช่อง
- รองรับการทำงานได้อย่างน้อย ดังนี้ Round Robin, High Availability, Layer4 Load Balance และ Layer7 Load Balance
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS ได้เป็นอย่างน้อย
- สามารถใช้งานตามมาตรฐาน IPv6 ได้

40. เครื่องพิมพ์ชนิด Dot Matrix Printer แบบแคร่สั้น ราคา 22,000 บาท

คุณลักษณะพื้นฐาน

- มีจำนวนหัวพิมพ์ไม่น้อยกว่า 24 เข็ม
- มีความกว้างในการพิมพ์ไม่น้อยกว่า 80 คอลัมน์ (Column)
- มีความเร็วขณะพิมพ์ร่างความเร็วสูง ขนาด 10 ตัวอักษรต่อนิ้ว ได้ไม่น้อยกว่า 400 ตัวอักษรต่อวินาที
- มีความละเอียดในการพิมพ์ไม่น้อยกว่า 360x360 dpi
- มีหน่วยความจำแบบ Input Buffer ไม่น้อยกว่า 128 KB
- มีช่องเชื่อมต่อ (Interface) แบบ Parallel หรือ USB 1.1 หรือดีกว่า จำนวนไม่น้อยกว่า 1 ช่อง

41. เครื่องพิมพ์ชนิด Dot Matrix Printer แบบแคร่ยาว ราคา 23,000 บาท

คุณลักษณะพื้นฐาน

- มีจำนวนหัวพิมพ์ไม่น้อยกว่า 24 เข็มพิมพ์
- มีความกว้างในการพิมพ์ไม่น้อยกว่า 136 คอลัมน์ (Column)
- มีความเร็วขณะพิมพ์ร่างความเร็วสูง ขนาด 10 ตัวอักษรต่อนิ้ว ได้ไม่น้อยกว่า 400 ตัวอักษรต่อวินาที
- มีความละเอียดในการพิมพ์ไม่น้อยกว่า 360x360 dpi
- มีหน่วยความจำ แบบ Input Buffer ไม่น้อยกว่า 128 KB
- มีช่องเชื่อมต่อ (Interface) แบบ Parallel หรือ USB 1.1 หรือดีกว่า จำนวนไม่น้อยกว่า 1 ช่อง