คู่มือการปฏิบัติงาน

เรื่อง การตรวจสอบและเฝ้าระวังระบบเครือข่ายคอมพิวเตอร์

โดยวิธีปกติ

ของ

นายดาวิชย์ ชานวิทิตกุล

ตำแหน่งนักวิชาการคอมพิวเตอร์ ระดับปฏิบัติการ

(ตำแหน่งเลขที่ พกร. 10085)

ฝ่ายบริการทางการศึกษา คณะพยาบาลศาสตร์เกื้อการุณย์

มหาวิทยาลัยนวมินทราธิราช

ขอประเมินเพื่อแต่งตั้งให้ดำรงตำแหน่ง

นักวิชาการคอมพิวเตอร์ ระดับชำนาญการ

(ตำแหน่งเลขที่ พกร. 10085)

ฝ่ายบริการทางการศึกษา คณะพยาบาลศาสตร์เกื้อการุณย์

มหาวิทยาลัยนวมินทราธิราช

คำนำ

คณะพยาบาลศาสตร์เกื้อการุณย์ มีภารกิจเกี่ยวกับด้านการเรียนการสอน การบริหารจัดการต่างๆ รวมไปถึงหอพักของบุคลากรและนักศึกษา ซึ่งได้มีการนำเครือข่ายคอมพิวเตอร์มารองรับ เพื่อให้บริการทั่วทั้งพื้นที่ ดังนั้นการตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายคอมพิวเตอร์ให้สามารถทำงานได้อย่างมีประสิทธิภาพ จึงมีความสำคัญอย่างยิ่งในการบริหารจัดการและดำเนินการต่างๆ ตามภารกิจของคณะพยาบาลศาสตร์เกื้อการุณย์ ให้มีประสิทธิภาพและเป็นไปด้วยความเรียบร้อย

โดยคู่มือตรวจสอบและเฝ้าระวังระบบเครือข่ายคอมพิวเตอร์ ได้จัดทำขึ้นเพื่อสร้างความเข้าใจในวิธีการและขั้นตอนในการดำเนินการตรวจสอบและเฝ้าระวังระบบเครือข่ายคอมพิวเตอร์ เพื่อให้อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ทำงานได้อย่างเต็มประสิทธิภาพและต่อเนื่อง โดยคู่มือฉบับนี้ใช้เป็นแนวทางเสริมสร้างความเข้าใจในการปฏิบัติงานให้เป็นไปอย่างถูกต้องและมีประสิทธิภาพในการดูแลรักษาอุปกรณ์ที่รองรับการทำงานของระบบเครือข่ายคอมพิวเตอร์ รวมไปถึงการเก็บเป็นข้อมูลเพื่อนำมาเปรียบเทียบ กับข้อมูลของผู้รับจ้างดูแลระบบเครือข่ายฯของคณะฯ เพื่อผลประโยชน์ของคณะพยาบาลศาสตร์เกื้อการุณย์

ผู้จัดทำหวังว่าคู่มือฉบับนี้จะเป็นประโยชน์ต่อผู้ปฏิบัติงานในหน่วยงานและผู้เกี่ยวข้อง สำหรับใช้ในการปฏิบัติงานให้เป็นไปอย่างมีประสิทธิภาพและมีมาตรฐานเดียวกัน คู่มือนี้ยังเป็นเครื่องมือที่จำเป็นในการสร้างความเชื่อมั่นและป้องกันปัญหาที่อาจเกิดขึ้นกับอุปกรณ์ที่รองรับการทำงานของระบบเครือข่ายคอมพิวเตอร์ในอนาคต

นาย ดาวิชย์ ชานวิทิตกุล
นักวิชาการคอมพิวเตอร์ปฏิบัติการ

สารบัญ

สารบัญ (ต่อ)

บทที่ 1

บทนำ

1.1 ประวัติความเป็นมา

ปัจจุบันการใช้งานเครือข่ายคอมพิวเตอร์เป็นที่แพร่หลาย และสำคัญอย่างมากต่อการเรียนการสอน ทำให้การทำงานระบบเครือข่ายคอมพิวเตอร์ มีความสำคัญต่อคณะพยาบาลศาสตร์เกื้อการุณย์ มหาวิทยาลัยนวมินทราธิราช เป็นอย่างมาก เนื่องจากระบบเครือข่ายคอมพิวเตอร์ต้องรองรับการทำงานของโครงสร้างพื้นฐานต่างๆ โดยใช้อุปกรณ์เครือข่ายและอุปกรณ์ที่เกี่ยวข้องในการรองรับระบบเครือข่ายของคณะพยาบาลศาสตร์เกื้อการุณย์

โดยระบบที่อุปกรณ์เครือข่ายต้องรองรับนั้น มีตั้งแต่เครือข่ายคอมพิวเตอร์ไร้สายทั้งหมด ระบบเครือข่ายคอมพิวเตอร์ห้องเรียน-ห้องบรรยาย ระบบงานของส่วนสำนักงาน รวมไปถึงรองรับการใช้งานของนักศึกษา คณาจารย์ และบุคลากร ในส่วนขอหอพัก ทั้งในและนอกเวลาทำการ จึงจำเป็นอย่างมากที่จะต้องมีเฝ้าระวังและตรวจสอบอุปกรณ์ที่ใช้รองรับอย่างต่อเนื่อง รวมถึงให้เกิดข้อผิดพลาดน้อยที่สุดเท่าที่จะเป็นไปได้ และเพื่อให้พร้อมสำหรับการบริการตลอดเวลา ทั้งยังทำให้สามารถแก้ไขปัญหาได้อย่างรวดเร็ว เพื่อให้เกิดผลกระทบต่อผู้ใช้งานให้น้อยที่สุด

ผู้ขอรับการประเมินจึงจัดทำคู่มือตรวจสอบและเฝ้าระวังระบบเครือข่ายคอมพิวเตอร์ เพื่ออำนวยความสะดวก และเพื่อให้ทราบขั้นตอนการปฏิบัติงาน เพื่อจะได้ดำเนินการตรวจสอบและเฝ้าระวังระบบเครือข่ายคอมพิวเตอร์ เพื่อให้อุปกรณ์ที่รองรับการทำงานของระบบเครือข่ายคอมพิวเตอร์ สามารถทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพที่ดีอยู่เสมอ รวมทั้งเพื่อให้สามารถนำข้อมูลที่ได้จากการปฏิบัติงานตามคู่มือนี้ไปเปรียบเทียบกับรายงานของบริษัทที่ทางคณะพยาบาลศาสตร์เกื้อการุณย์ทำการจ้างเหมาบริการดูแลระบบเครือข่าย ว่ามีความถูกต้องและเที่ยงตรงกัน

1.2 วัตถุประสงค์

1.2.1 เพื่อให้งานเทคโนโลยีสารสนเทศ มีการจัดทำคู่มือการปฏิบัติงานที่ชัดเจนอย่างเป็นลายลักษณ์อักษร ที่แสดงถึงรายละเอียด ขั้นตอน ของการปฏิบัติงาน การตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายคอมพิวเตอร์

1.2.2 เพื่อเป็นหลักฐานแสดงวิธีการตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายคอมพิวเตอร์ ที่สามารถถ่ายทอดให้กับผู้เข้ามาปฏิบัติงานใหม่ และใช้ประกอบการประเมินผลการปฏิบัติงานของบุคลากร

1.2.3 เพื่อให้เข้าใจกระบวนการทำงานของการตรวจสอบและเฝ้าระวังอุปกรณ์เครือข่ายคอมพิวเตอร์ และสามารถประเมินการแก้ไขปัญหา รวมถึงแก้ไขปัญหาให้ระบบเครือข่ายสามารถกลับมาใช้งานได้อย่างรวดเร็ว และพร้อมให้บริการอย่างมีประสิทธิภาพ

1.2.4 เพื่อประกอบการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ให้เป็นไปตามประสิทธิภาพสูงสุด ซึ่งจะช่วยให้สามารถประหยัดเวลาและต้นทุนในการใช้งานอุปกรณ์เครือข่ายคอมพิวเตอร์

1.2.5 เพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นกับอุปกรณ์เครือข่ายคอมพิวเตอร์ ซึ่งจะช่วยให้สามารถประหยัดเวลาและต้นทุนในการแก้ไขปัญหานั้น

1.3 ประโยชน์ของคู่มือปฏิบัติงาน

1.3.1 ให้การปฏิบัติงานเป็นไปอย่างราบรื่น ถูกต้อง และทันเวลา

1.3.2 ให้บุคลากรหรือเจ้าหน้าที่ สามารถปฏิบัติงานแทนกันได้

1.3.3 ลดระยะเวลาในการสอนงานและเสริมสร้างความมั่นใจ ในการปฏิบัติงาน

1.3.4 ทำการตรวจสอบและเปรียบเทียบข้อมูลให้ถูกต้องเที่ยงตรง

1.4 ขอบเขตของคู่มือปฏิบัติงาน

การตรวจสอบและเฝ้าระวังระบบเครือข่ายคอมพิวเตอร์ และอุปกรณ์หลักที่เกี่ยวข้อง ที่งานเทคโนโลยีสารสนเทศของคณะฯ ให้บริการกับบุคลากรและนักศึกษาของคณะพยาบาลศาสตร์เกื้อการุณย์ ตั้งแต่อุปกรณ์รักษาความปลอดภัย อุปกรณ์กระจายสัญญาณเครือข่าย และอุปกรณ์จัดเก็บข้อมูล เพื่อนำข้อมูลที่ได้มาเปรียบเทียบกับรายงานในแต่ละเดือนของบริษัทที่ทางคณะฯ จ้างเหมาดูแลระบบเครือข่าย เพื่อให้ข้อมูลถูกต้องและเที่ยงตรง

1.5 นิยามศัพท์

Software	หมายถึง	ชุดคำสั่งหรือโปรแกรมที่ใช้สั่งงานให้คอมพิวเตอร์ทำงาน
Web Browser	หมายถึง	โปรแกรม แอพลิเคชั่น ที่ใช้เอาไว้สำหรับเข้าถึงเว็บไซต์ต่างๆ
URL	หมายถึง	รูปแบบมาตรฐานในเข้าถึงข้อมูลบนอินเทอร์เน็ต
Username	หมายถึง	สิ่งที่ระบุตัวตนของผู้ใช้บริการเว็บไซต์ หรือแอพพลิเคชั่น
Password	หมายถึง	สายอักขระหรือคำที่เป็นความลับ ที่ใช้สำหรับยืนยันตัว พิสูจน์ความเป็นเจ้าของ หรือเข้าถึงแหล่งข้อมูล รหัสผ่านควรจะเก็บเป็นความลับเพื่อไม่ให้คนอื่นเข้าถึงได้
CPU	หมายถึง	หน่วยประมวลผลกลางเป็นส่วนประกอบฮาร์ดแวร์ที่เป็นหน่วยคำนวณหลักในเซิร์ฟเวอร์
Memory	หมายถึง	เป็นหน่วยความจำหลักของคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบสำคัญที่มีผลต่อประสิทธิภาพการทำงานโดยรวม ทั้งยังส่งผลต่อความเร็วในการทำงานของระบบคอมพิวเตอร์ ไม่ว่าอุปกรณ์ชนิดนั้นจะเป็นสมาร์ทโฟน, แท็บเล็ต, คอมพิวเตอร์ หรืออุปกรณ์ใดๆ ที่จำเป็นต้องอ่านและเขียนคำสั่งไปยังหน่วยความจำ
Bandwidth	หมายถึง	ปริมาณข้อมูลที่คุณรับเข้าและส่งออกในช่วงเวลาหนึ่ง
Log	หมายถึง	บันทึกเหตุการณ์
Level	หมายถึง	ระดับ (ระดับของความอันตราย/ความเสี่ยง)

System	หมายถึง	เป็นกลุ่มขององค์ประกอบต่าง ๆ ที่ทำงานร่วมกัน เพื่อจุดประสงค์ในสิ่งเดียวกัน ระบบอาจประกอบด้วยบุคลากร เครื่องมือ วัสดุ วิธีการ การจัดการ ซึ่งทั้งหมดนี้จะต้องมีระบบในการจัดการเพื่อให้บรรลุจุดประสงค์เดียวกัน
Resource	หมายถึง	ทรัพยากรของระบบ/อุปกรณ์
Device	หมายถึง	อุปกรณ์ที่เข้ามาเชื่อมต่อ
Slot	หมายถึง	ช่องเสียบ/ช่องเชื่อมต่ออุปกรณ์
Uptime	หมายถึง	จำนวนระยะเวลา ที่ Server หรือ Host ไม่เคย Restart ไม่เคยดับ ไม่เคยล่ม ไม่เคยเกิดปัญหาการเข้าถึงข้อมูลไม่ได้
Telnet	หมายถึง	การขอเข้าใช้เครื่องคอมพิวเตอร์จากระยะไกล ผู้ใช้นั้นสามารถขอเข้าใช้ได้ขอแค่ติดต่อเครือข่ายที่ได้รับอนุญาต โดยไม่จำเป็นว่าต้องนั่งอยู่หน้าเครื่องคอมพิวเตอร์เครื่องนั้น
SSL	หมายถึง	โปรโตคอลหรือกฎการสื่อสารที่ทำให้ระบบคอมพิวเตอร์สื่อสารกันบนอินเทอร์เน็ตได้อย่างปลอดภัย
Connection Type	หมายถึง	ประเภทการเชื่อมต่อ / ชนิดการเชื่อมต่อ
Storage	หมายถึง	อุปกรณ์เก็บข้อมูล
IP Address	หมายถึง	หมายเลขที่กำหนดให้แก่อุปกรณ์อิเล็กทรอนิกส์แต่ละชนิด
Cursor Mouse	หมายถึง	หัวลูกศรที่อยู่บนหน้าจอคอมพิวเตอร์ ตัวที่บ่งบอกว่าเมาส์เรากำลังชี้อะไรอยู่ และอยู่ตรงไหนของหน้าจอ
Allocated	หมายถึง	พื้นที่ที่มีการจัดสรรแล้ว
Unallocated	หมายถึง	พื้นที่ที่ยังไม่ได้มีการจัดสรรแล้ว
Host Name	หมายถึง	Hosting ซึ่งแปลงมาจาก IP Hosting ให้เป็นชื่อที่เข้าใจง่ายแทนที่จะจดจำเป็นค่าตัวเลข และอาจมีความหมายที่เกี่ยวข้องกับผู้ให้บริการนั้นหรือเป็นที่เข้าใจกันในองค์กร

VPN	หมายถึง	เครือข่ายส่วนตัวเสมือน สร้างการเชื่อมต่อระหว่างอุปกรณ์ ผ่านทางอินเทอร์เน็ต
Backup	หมายถึง	การคัดลอกข้อมูล ไปยังสถานที่เก็บอื่นๆเพื่อการเก็บรักษาในกรณีที่อุปกรณ์ขัดข้องหรือเกิดภัยพิบัติ

บทที่ 2

ภาระหน้าที่ความรับผิดชอบ

2.1 ภาระหน้าที่ความรับผิดชอบ

งานเทคโนโลยีสารสนเทศ คณะพยาบาลศาสตร์เกื้อการุณย์ มหาวิทยาลัยนวมินทราธิราช ให้บริการห้องเรียนคอมพิวเตอร์ บริการด้านการติดตั้งโปรแกรม และอัพเดทเวอร์ชั่นของ Software ซ่อม-บำรุงรักษาอุปกรณ์คอมพิวเตอร์ให้กับอาจารย์และเจ้าหน้าที่ ดูแลระบบเครือข่ายให้สามารถใช้งานได้อย่างต่อเนื่องและมีความรวดเร็วในการใช้งาน ป้องกันและรักษาความปลอดภัยของเครื่องคอมพิวเตอร์และระบบเครือข่าย สำรองข้อมูลเครื่องแม่ข่าย ดูแลรักษาความสะอาดคอมพิวเตอร์และเครือข่าย ดูแลระบบบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) พัฒนาและบริหารเว็บไซต์ของคณะฯ และตอบสนองตามนโยบายภาพรวมของคณะกกรมการเทคโนโลยีสารสนเทศของมหาวิทยาลัยฯ

2.2 ลักษณะงานที่ปฏิบัติ

ผู้ขอรับการประเมิน ปัจจุบันดำรงตำแหน่ง นักวิชาการคอมพิวเตอร์ ปฏิบัติการ งานเทคโนโลยีสารสนเทศ ฝ่ายบริการทางการศึกษา คณะพยาบาลศาสตร์เกื้อการุณย์ มีหน้าที่ความรับผิดชอบตามมาตรฐานตำแหน่งที่มหาวิทยาลัยกำหนด มีภาระในความรับผิดชอบตามคำสั่งฝ่ายบริการทางการศึกษา ลงวันที่ 27 มีนาคม 2563 เรื่อง มอบหมายการปฏิบัติงานฝ่ายบริการทางการศึกษาดังนี้

2.2.1. งานติดตั้ง Hardware & Network

2.2.1.1 ติดตั้งเครื่องคอมพิวเตอร์

2.2.1.2 ติดตั้งเครื่อง Printer, Scanner และอุปกรณ์ต่อพ่วง

2.2.1.3 ติดตั้งเครื่องแม่ข่าย (Server)

2.2.1.4 งานติดตั้งสายสัญญาณ UTP และเข้าหัวสายสัญญาณ (พื้นที่โล่งแนวราบ)

2.2.1.5 งานติดตั้งสายสัญญาณ UTP และเข้าหัวสายสัญญาณ (พื้นที่แขวนยึดห้อยฝ้า / เพดาน)

2.2.1.6 Register & Config Network

2.2.2. งานติดตั้ง Software & Application & Driver

2.2.2.1 ติดตั้งระบบเทคโนโลยีสารสนเทศของหน่วยงานหรือซอฟต์แวร์อุปกรณ์พร้อมทดสอบระบบงาน ติดตั้ง Driver Printer & Scanner ทั่วไป, Ink & Laser

2.2.2.2 ติดตั้งโปรแกรมสำเร็จรูปต่าง ๆ ที่จำเป็นต่อการทำงานในหน่วยงาน

2.2.2.3 ตั้งค่า (Config) ระบบเครื่องแม่ข่าย เช่น Web Server, Application Server, Mail Server, Database Server เป็นต้น

2.2.3. ติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย

2.2.3.1 ติดตั้งระบบปฏิบัติการ Windows 7 8 10 และ Driver Mainbroad

2.2.3.2 ติดตั้งระบบปฏิบัติการ Virtual Machine (VMWare, HyperV, OpenStack)

2.2.4. งานดูแล/บำรุงรักษา

2.2.4.1 ดูแลห้องเรียนคอมพิวเตอร์

2.2.4.2 งานยืมคืนอุปกรณ์ด้านคอมพิวเตอร์

2.2.4.3 ตรวจสอบดูแลระบบเครือข่าย (Monitoring Network, Server, Firewall, Log, Internet)

2.2.5. งานฐานข้อมูล

2.2.5.1 ดูแล เฝ้าระวัง ตรวจสอบ พื้นที่จัดเก็บฐานข้อมูล

2.2.5.2 เพิ่มพื้นที่จัดเก็บฐานข้อมูลให้เพียงพอต่อการใช้งานระบบ

1) ระบบงานขนาดเล็ก

2) ระบบงานขนาดใหญ่

2.2.5.3 สำรองข้อมูล หรือตรวจสอบการสำรองข้อมูลให้สำรองข้อมูลได้ครบถ้วน

2.2.5.4 งานประมวลผลและปรับปรุงแก้ไขแฟ้มข้อมูลเพื่อให้ข้อมูลที่ได้ถูกต้องแม่นยำและทันสมัย

2.2.6. งานด้านการวางแผน

2.2.6.1 วางแผนการทำงานที่รับผิดชอบร่วมดำเนินการวางแผนการทำงานของหน่วยงานหรือส่วนงาน หรือโครงการเพื่อให้การดำเนินงานเป็นไปตามเป้าหมาย

2.2.6.2 ประสานการทำงานร่วมกันทั้งภายในและภายนอกทีมงานหรือหน่วยงานหรือส่วนงานเพื่อให้เกิดความร่วมมือและผลสัมฤทธิ์ตามที่กำหนด

2.2.6.3 ชี้แจงและให้รายละเอียดเกี่ยวกับข้อมูล ข้อเท็จจริงแก่บุคคลหรือหน่วยงานหรือส่วนงานที่เกี่ยวข้องเพื่อสร้างความเข้าใจหรือความร่วมมือในการดำเนินงาน

2.2.6.4 ร่างกำหนดคุณลักษณะเฉพาะขอบเขตของงานด้านเทคโนโลยีสารสนเทศ (Terms of Reference: TOR)

2.2.7. งานด้านการบริการ

2.2.7.1 แก้ไขปัญหาคอมพิวเตอร์และอุปกรณ์ไอทีที่เกี่ยวข้องให้กับนักศึกษาอาจารย์ และบุคลากรภายในองค์กร

2.2.7.2 จัดทำสื่อประชาสัมพันธ์ คู่มือการใช้งานระบบหรือคู่มือที่ให้ความรู้กับบุคลากรในมหาวิทยาลัย เพื่อให้ผู้ใช้สามารถทำความเข้าใจได้ด้วยตนเองอย่างมีประสิทธิภาพ

1) ในรูปแบบเอกสาร หรือไฟล์เอกสาร

2) ปรับปรุงข้อมูลเว็บไซต์

2.2.7.3 ดำเนินการฝึกอบรมหรือถ่ายทอดความรู้สนับสนุนการใช้ระบบงานที่พัฒนาแก่เจ้าหน้าที่ผู้ใช้งานเพื่อสร้างความรู้ความเข้าใจในด้านวิชาการคอมพิวเตอร์รวมไปถึงการเตรียมข้อมูลเพื่อใช้ในการฝึกอบรม

2.2.7.4 ให้คำปรึกษา แนะนำเกี่ยวกับงานด้านเทคโนโลยีสารสนเทศ

2.2.7.5 แก้ไขปัญหา และบริการอื่นๆผู้ใช้งานทุกระบบ

1) แก้ไขปัญหา Hardware & Software ทั่วไป

2.2.8. ภาระงานตามที่ได้รับมอบหมาย

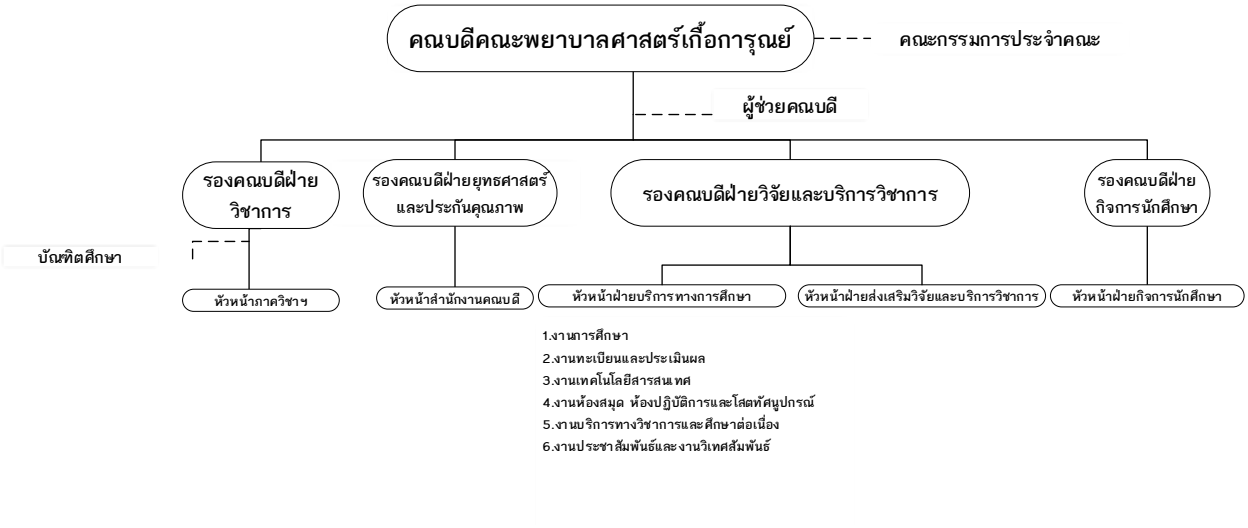
2.2.8.1 เป็นกรรมการ/อนุกรรมการ/คณะทำงานของมหาวิทยาลัย/ส่วนงาน/หน่วยงานและผู้เข้าร่วมประชุม

2.2.8.2 เป็นประธาน/เลขานุการ/ผู้ช่วยเลขานุการในคณะกรรมการ/คณะอนุกรรมการ/คณะทำงานของมหาวิทยาลัย/ส่วนงาน/หน่วยงาน

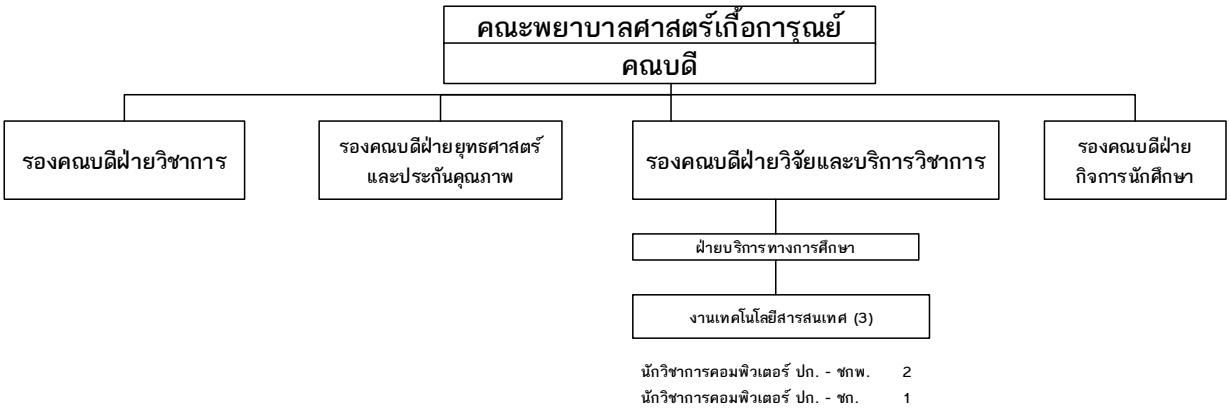
2.2.8.3 ร่างกำหนดคุณลักษณะเฉพาะขอบเขตของส่วนงาน (Terms of Reference: TOR)

2.2.8.4 เข้าร่วมกิจกรรมต่าง ๆ ที่หน่วยงาน/มหาวิทยาลัยกำหนด/หน่วยงานภายนอกการประชุม อบรม เพื่อเพิ่มพูนความรู้

2.3 โครงสร้างคณะพยาบาลศาสตร์เกื้อการุณย์



2.4 โครงสร้างหน่วยงาน



บทที่ 3

แนวทางการปฏิบัติงาน

การตรวจสอบและเฝ้าระวังระบบเครือข่ายคอมพิวเตอร์ ของคณะพยาบาลศาสตร์เกื้อการุณย์มีความจำเป็นจะต้องเข้าถึงอุปกรณ์เครือข่าย เครื่องแม่ข่าย และอุปกรณ์ที่เกี่ยวข้อง ที่กำลังให้บริการอยู่หลากหลายชนิด เพื่อทำการตรวจสอบว่าอุปกรณ์นั้นๆ ทำงานได้อย่างมีประสิทธิภาพ และมีข้อผิดพลาดใดๆหรือไม่ โดยการตรวจสอบดูผ่าน Log ของอุปกรณ์นั้นๆ ด้วยการเข้าถึงด้วยวิธีการต่างๆ ทั้งการใช้ web browser และโปรแกรมที่เกี่ยวข้องในการเข้าถึงอุปกรณ์ โดยอุปกรณ์สามารถแบ่งชนิดได้ดังต่อไปนี้

- อุปกรณ์ป้องกันเครือข่าย (Firewall)
- อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย
- อุปกรณ์กระจายสัญญาณ
- เครื่องคอมพิวเตอร์แม่ข่าย
- อุปกรณ์จัดเก็บข้อมูล

<u>ขั้นตอนและวิธีการปฏิบัติงานการตรวจสอบและเฝ้าระวังระบบเครือข่ายคอมพิวเตอร์</u>

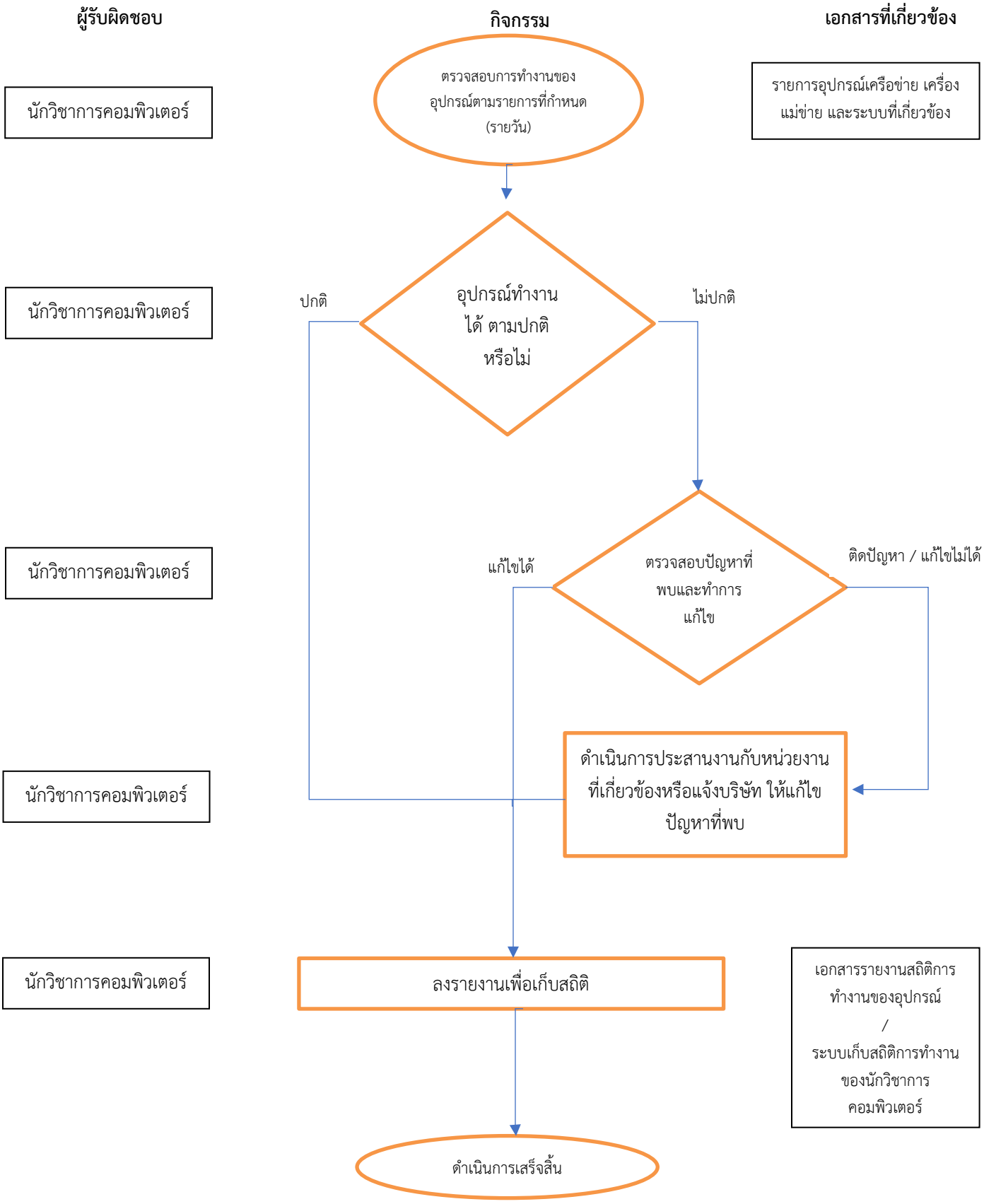
1.ตรวจสอบการทำงานของอุปกรณ์ตามรายการที่กำหนดโดยอ้างอิงจากเอกสาร รายการอุปกรณ์เครือข่ายคอมพิวเตอร์

2.ระหว่างทำการตรวจสอบทีละรายการ หากตรวจพบความไม่ปกติ จากอุปกรณ์ใดก็ตามให้ทำการตรวจสอบปัญหาที่พบและทำการแก้ไขโดยทันที

3.หากไม่สามารถแก้ไขปัญหาที่ตรวจพบโดยทันทีได้ ให้ทำการประสานงานหน่วยงานที่เกี่ยวข้องเข้ามาดำเนินการแก้ไข

4.หลังจากทำการแก้ไขปัญหาแล้ว ให้ทำการลงรายงานเพื่อทำการเก็บสถิติการตรวจสอบ (รายวัน) และบันทึกงานที่ทำลงในระบบเก็บ Work Load ของงานเทคโนโลยีสารสนเทศ คณะพยาบาลศาสตร์เกื้อการุณย์ (Google Form)

Flow Chart กระบวนการขั้นตอนการทำงาน



อุปกรณ์ป้องกันเครือข่าย (Firewall) คืออุปกรณ์ป้องกันการบุกรุก ทำหน้าที่รักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ โดยตรวจสอบข้อมูลที่ผ่านเข้า-ออก ตั้งแต่การเข้าถึงข้อมูลจากภายนอก ไปจนถึงการเข้าถึงเครือข่ายภายใน เช่น เครือข่ายภายในองค์กรหรือคอมพิวเตอร์ส่วนตัวผ่านการกำหนดนโยบาย เพื่อป้องกันว่าข้อมูลที่จะส่งผ่านนั้นมีจะความปลอดภัยในระดับหนึ่ง แต่ก็ขึ้นกับการตัดสินใจของผู้ใช้งานเองด้วย ถ้าหากข้อมูลไม่ปลอดภัยได้แต่รับการอนุญาตจากผู้ใช้งาน Firewall ก็จะอนุญาตให้ผ่านเข้าไปได้ ประโยชน์ของอุปกรณ์ป้องกันเครือข่าย (Firewall) เบื้องต้นมีดังนี้

- ลดช่องโหว่การรักษาความปลอดภัยเครือข่ายขององค์กร

วัตถุประสงค์หลักของ Firewall คือเพื่อป้องกันการโจมตีการรักษาความปลอดภัยเครือข่าย หรือการโจมตีของแฮกเกอร์ สามารถกำหนดนโยบาย (Policy) ที่สามารถจดจำและบล็อคไวรัสและมัลแวร์ได้ และยังสามารถบล็อคการเข้าถึงจากภายนอกที่ไม่ได้รับอนุญาต

- ช่วยปกป้องเครื่องใช้งานจากการเข้าถึงระยะไกลที่ไม่ได้รับอนุญาต

หนึ่งในภัยอันตรายร้ายแรงที่สุดที่อาจเกิดขึ้นกับคอมพิวเตอร์ของผู้ใช้คือ แฮกเกอร์พยายามควบคุมเครื่องจากระยะไกล หากมีอุปกรณ์ firewall ที่ตั้งค่าอย่างถูกต้องแล้ว จะช่วยปิดการใช้งานการเข้าถึงเดสก์ท็อประยะไกล จึงป้องกันไม่ให้แฮกเกอร์เข้ายึดคอมพิวเตอร์ได้

- ช่วยตรวจสอบและควบคุมการใช้อินเตอร์เน็ต

นอกเหนือจากการตรวจสอบการรับส่งข้อมูลขาเข้าแล้ว Firewall ยังสามารถใช้เพื่อตรวจสอบและบล็อคการรับส่งข้อมูลขาออกจากภายในองค์กรได้อีกด้วยโดยการกำหนดนโยบาย ไอทีสามารถบล็อคการเข้าถึง ระบุตัวตน และหยุดการเข้าถึงเว็บไซต์ที่ไม่เหมาะสมได้ รวมถึงยังสามารถจำกัดการใช้งานอินเตอร์เน็ตทั้งในและนอกเวลาทำการอีกด้วย

- เป็นฮาร์ดแวร์หรือซอฟต์แวร์ก็ได้

Firewall ไม่จำเป็นต้องเป็นซอฟต์แวร์เสมอไป สามารถเป็นฮาร์ดแวร์ได้ ส่วนใหญ่จะพบเป็นการใช้ในบ้านโดยจะอยู่ภายในเราเตอร์ ซึ่งการเข้าถึง Firewall แบบฮาร์ดแวร์ จะใช้ข้อมูลประจำตัวของผู้ดูแลระบบสำหรับเราเตอร์ (ที่สำคัญต้องตั้งค่ารหัสผ่านใหม่ อย่าใช้รหัสผ่าน default เด็ดขาด) และเมื่อลงชื่อเข้าใช้แล้ว จะสามารถตรวจสอบตัวเลือกและเปลี่ยนแปลงได้หากจำเป็นบางครั้งจะต้องทำการปรับแต่ง โดยเฉพาะอย่างยิ่งสำหรับการเล่นเกมออนไลน์ด้วยคอนโซลเกม ตัวอย่างเช่น การเปลี่ยนประเภท NAT บน PlayStation 4 เป็นการแก้ไขปัญหาการเชื่อมต่อเกมออนไลน์ทั่วไป ผู้ใช้ควรตรวจสอบเอกสารประกอบสำหรับเราเตอร์ เพื่อทำความคุ้นเคยกับการตั้งค่าก่อนที่จะเริ่มบันทึกการเปลี่ยนแปลงใด ๆ

แต่สิ่งที่ Firewall ยังไม่สามารถทำได้คือการรับมือภัยคุกคามที่ซับซ้อน การจัดการไวรัส มัลแวร์ต่างๆ รวมถึงการเข้าถึงที่ระดับ Application Layer ซึ่ง Firewall โดยทั่วไปยังไม่สามารถทำได้ จึงทำให้เกิด Next Generation Firewall ขึ้น โดยจะมีความแตกต่างกับ Firewall ปกติดังนี้

ตารางข้อแตกต่างระหว่าง Firewall โดยทั่วไป และ Next-generation Firewall (NGFW)		
Parameter	**Firewall**	**Next-generation Firewall (NGFW)**
Working Layer	ทำงานที่ Layer ๑ – Layer ๔	ทำงานที่ Layer ๒ – Layer ๗
Packet Filtering	Firewall โดยทั่วไปจะเป็นตัวช่วยให้ผู้ดูแลระบบไอทีสามารถย่นระยะเวลาในการตรวจสอบแพ็กเกจเข้าและออก	NGFW จะตรวจสอบเนื้อหาเชิงลึก Deep Packet Filtering (DPI) ของแต่ละ แพ็กเกจ รวมไปถึงแหล่งที่มา ซึ่งแตกต่างจากการกรองแพ็กเกจมาตรฐานที่อ่านเฉพาะ Role ที่ตั้งค่าไว้
Stateful หรือ stateless inspection	Firewall จะตรวจสอบแต่ละแพ็กเกจ แยกกันตามข้อมูล เช่น source และ destination ในทางกลับกัน Firewall จะพิจารณาการเชื่อมต่อโดยรวมของระบบ Network ให้มีความปลอดภัยที่มากขึ้น	NGFW ทั้งหมดดำเนินการตรวจสอบแพ็กเกจแบบ stateful packet inspection ในขั้นตอนเดียว
Virtual Private Networks (VPNs)	Firewall จะอนุญาตให้เข้า VPN เพื่อให้มีความปลอดภัยในการใช้งานอินเทอร์เน็ต	NGFW จะอนุญาตให้เข้า VPN เพื่อให้มีความปลอดภัยในการใช้งานอินเทอร์เน็ต
Application Awareness	Firewall ไม่มี Awareness และไม่อนุญาตให้ admin ตั้งค่า role เฉพาะสำหรับแอปพลิเคชันต่าง ๆ	NGFW มี Application Awareness และอนุญาตให้ admin ตั้งค่า role เฉพาะสำหรับแอปพลิเคชันต่าง ๆ
Intrusion Prevention System (IPS)	Firewall ไม่มี IPS	NGFW มี IPS สามารถบล็อก blacklist และการโจมตีต่าง ๆ จากแหล่งที่เป็นอันตราย
Threat Intelligence	Firewall ทำงานบนพื้นฐานของ role ที่กำหนดโดย admin ของระบบ ดังนั้นจึงไม่มี threat intelligence	NGFW สามารถเรียนรู้และ update ฐานข้อมูลของซอฟต์แวร์ที่เป็นอันตรายและภัยคุกคามต่าง ๆ เมื่อมีภัยคุกคามใหม่ๆ NGFW สามารถป้องกันได้ดียิ่งขึ้น
Reporting	Standard Report	สามารถ customise report ได้แบบ real-time

จากตารางจะเห็นได้ว่า Next-generation Firewall จะมีข้อดีที่ถูกพัฒนาขึ้นดังนี้

1. Multi-functional : นอกจากฟังก์ชันเดิม ๆ อย่างการคัดกรองแพ็คเกจ, แปลงที่อยู่และเลขพอร์ตบนเครือข่าย, ตรวจสอบ traffic แบบ Stateful, หรือทำ VPN ได้แล้ว ตัว NGFW จะมี feature ชั้นสูงอย่างระบบตรวจจับและป้องกันการบุกรุกที่วิเคราะห์จาก traffic, signature หรือกิจกรรมที่ต้องสงสัยได้ด้วย ทำให้ครอบคลุมได้มากกว่าลำดับชั้นบน Data Link หรือ Transport Layer ตาม OSI model โดยมักตรวจขึ้นไปได้ถึง Application Layer เลยทีเดียว

2. Application Awareness : การตั้งค่าอนุญาตใช้แอป นอกจากดูผ่านเลขพอร์ตแล้ว เนื่องจากแอปพลิเคชันปัจจุบันเปลี่ยนเลขพอร์ตได้ตามใจ หรือแม้แต่ทำ Tunnel ได้ ดังนั้น NGFW จึงพัฒนาตัวเองให้

สามารถตรวจแพ็คเกจแบบเจาะลึกจนรู้ต้นตอของแอปพลิเคชันได้อย่างละเอียด เช่น อนุญาตให้ user ใช้ facebook แต่ไม่ให้ chat ผ่าน facebook ได้เป็นต้น

3. Streamlined infrastructure : สามารถทำงานต่อเนื่องบนโครงสร้างพื้นฐานทุกแบบ ที่รวม Antivirus, Spam Filtering , deep-packet inspection , และระบบ Application control อยู่ในอุปกรณ์เดียว ไม่สร้างความซับซ้อนเพิ่มขึ้นบนโครงสร้างพื้นฐานที่ใช้งานอยู่

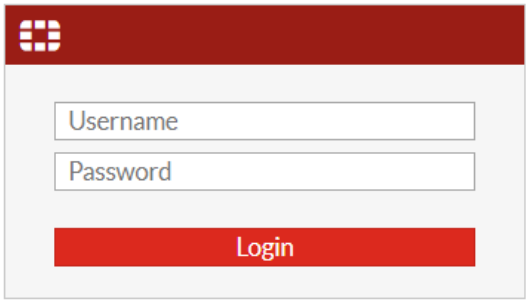
4. Threat protection : ป้องกันอันตรายจากไวรัสและมัลแวร์ที่มีการอัพเกรดตัวเองตลอดเวลา รวมถึงการสแกนหาช่องโหว่บนแอปพลิเคชัน ที่ใช้งานอยู่ ซึ่งนอกจากป้องกันอันตรายแล้ว ยังช่วยลดการใช้ bandwidth ของ traffic ที่ไม่มีประโยชน์ได้ด้วย

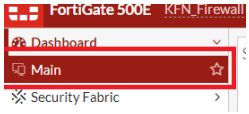
5. Network Speed : รักษาความเร็วของเครือข่ายเดิมได้ เมื่อ Firewall แบบเดิมมักกระทบกับความเร็วบนเครือข่ายอย่างรุนแรง แต่สำหรับ NGFW กลับสามารถรักษา Throughput ได้ใกล้เคียงสถานะปกติได้เป็นอย่างดี

จากที่กล่าวมาข้างต้น จะเห็นได้ว่า อุปกรณ์ป้องกันเครือข่าย (Firewall) มีความสำคัญกับความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์เป็นอย่างมาก ทำให้จำเป็นต้องทำการตรวจสอบการทำงานของอุปกรณ์ และตรวจสอบ Log ของอุปกรณ์ เพื่อลดปัญหาที่อาจจะเกิดขึ้น และสามารถเข้าแก้ไขความเสี่ยงที่อาจจะเกิดขึ้นได้ก่อนที่จะปานปลาย เพื่อให้อุปกรณ์สามารถทำงานได้อย่างมีประสิทธิภาพและต่อเนื่อง โดยอุปกรณ์ป้องกันเครือข่าย ที่ทางคณะพยาบาลศาสตร์เกื้อการุณย์ใช้งานมีวิธีการเข้าถึงและดำเนินงานดังนี้

3.1 อุปกรณ์ป้องกันเครือข่าย (Firewall) ยี่ห้อ Fortigate รุ่น 500E

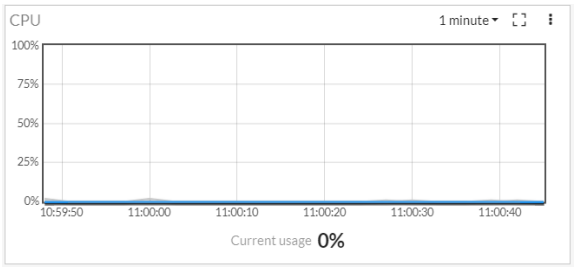
3.1.1 เข้าโปรแกรมเว็บบราวเซอร์ Web Browser แล้วพิมพ์ URL ดังนี้ https://10.1.0.2 จากนั้นกรอก Username และ Password



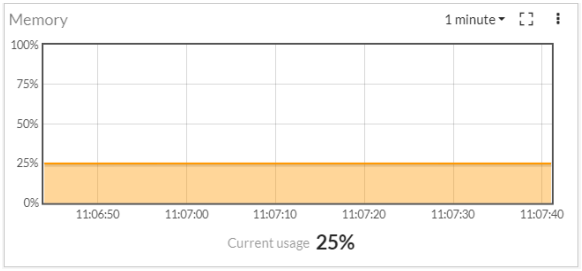


ที่แท็บ Dashboard/Main ตรวจสอบที่ช่องต่างๆ ด้านขวามือดังนี้

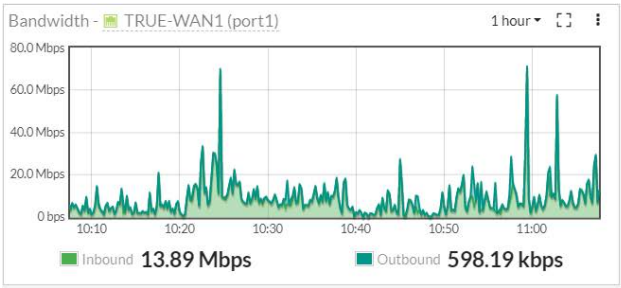
3.1.2 ตรวจสอบ CPU ว่าทำงานอยู่ที่กี่เปอร์เซ็นต์

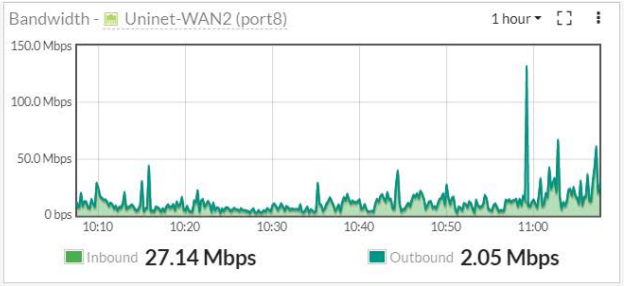


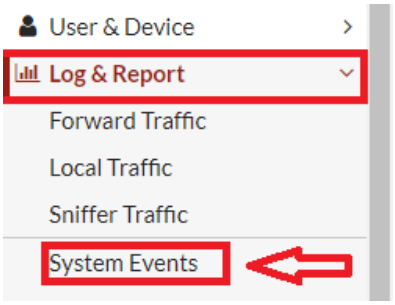
3.1.3 Memory ว่าทำงานอยู่ที่กี่เปอร์เซ็นต์



3.1.4 Bandwidth – TRUE-WAN1 (port1) และ Bandwidth – Uninet-WAN2 (port8) ว่า Internet ทั้ง 2 เส้น ทำงานปกติหรือไม่







3.1.5 จากนั้นไปดูที่แท็บ Log & Report ที่ เมนูย่อย System Events

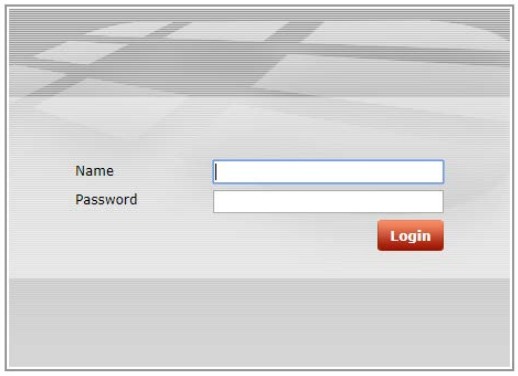
1	2 minutes ago			Performance statistics: average CPU: 0, memory: 26, concurrent sessions: 3710, setup-rate: 0	System performance statistics
2	7 minutes ago			Performance statistics: average CPU: 0, memory: 26, concurrent sessions: 3786, setup-rate: 21	System performance statistics
3	12 minutes ago		davich	Edit system.admin davich	Object attribute configured
4	12 minutes ago			Performance statistics: average CPU: 0, memory: 26, concurrent sessions: 3268, setup-rate: 32	System performance statistics
5	13 minutes ago		davich	Edit system.admin davich	Object attribute configured
6	13 minutes ago		davich	Edit system.admin davich	Object attribute configured
7	13 minutes ago		davich	Edit system.admin davich	Object attribute configured
8	13 minutes ago		davich	Edit system.admin davich	Object attribute configured
9	13 minutes ago		davich	Edit system.admin davich	Object attribute configured
10	13 minutes ago		davich	Edit system.admin davich	Object attribute configured
11	15 minutes ago		davich	Administrator davich logged in successfully from https(10.1.11.3)	Admin login successful
12	17 minutes ago		davich	Administrator davich timed out on https(10.1.11.3)	Admin logout successful
13	17 minutes ago			Performance statistics: average CPU: 0, memory: 26, concurrent sessions: 3348, setup-rate: 0	System performance statistics
14	22 minutes ago			Performance statistics: average CPU: 0, memory: 26, concurrent sessions: 3449, setup-rate: 33	System performance statistics
15	27 minutes ago		davich	Administrator davich logged in successfully from https(10.1.11.3)	Admin login successful
16	27 minutes ago			Performance statistics: average CPU: 0, memory: 26, concurrent sessions: 3682, setup-rate: 31	System performance statistics
17	32 minutes ago			Performance statistics: average CPU: 0, memory: 26, concurrent sessions: 3900, setup-rate: 19	System performance statistics
18	37 minutes ago			Fortigate push update fcni=yes fdni=yes fsci=yes from 209.222.136.8:443	FortiGate update succeeded

*** ดูที่แท็บ Level แท็บยาวหมายถึงมีความเสี่ยงสูง แล้วตรวจสอบว่าเป็นเหตุการณ์ที่เกิดวันไหน เวลาอะไร โดยวันและเวลาจะอยู่ด้านซ้ายมือของ Level และเกิดเหตุการณ์อะไรขึ้น หากสามารถแก้ไขเบื้องต้นได้ ให้ทำการแก้ไขโดยทันที หรือหากแก้ไขเบื้องต้นไม่ได้ ให้ทำการโทรแจ้งบริษัทฯ ***

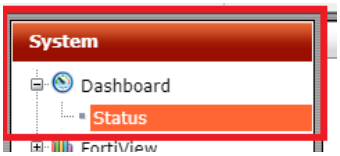
3.1.6 หลังจากการตรวจสอบสถานะ , ดำเนินการแก้ไข หรือประสานงานกับบริษัทที่ดูแล เรียบร้อยแล้ว ให้ทำการบันทึกข้อมูลเพื่อเก็บเป็นรายงานต่อไป

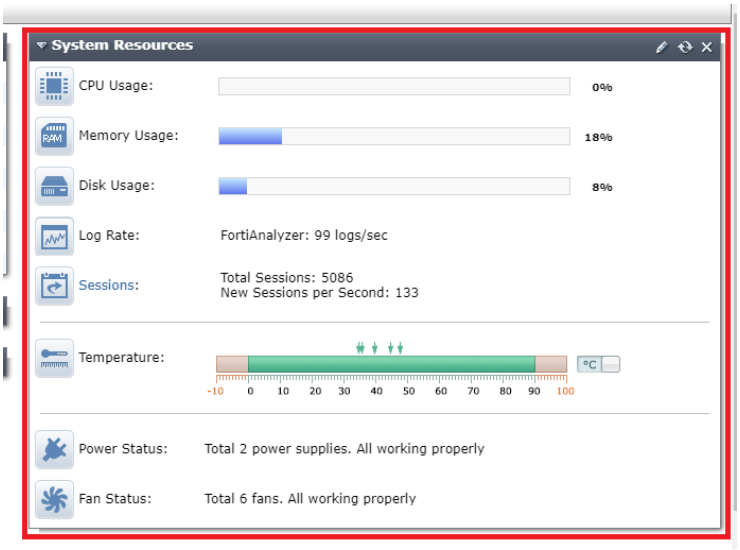
3.2 อุปกรณ์ป้องกันเครือข่าย (Firewall) ยี่ห้อ Fortigate รุ่น 1000C

3.2.1 เข้าโปรแกรมเว็บบราวเซอร์ Web Browser แล้วพิมพ์ URL ดังนี้ https://10.1.0.6 จากนั้นกรอก Username และ Password

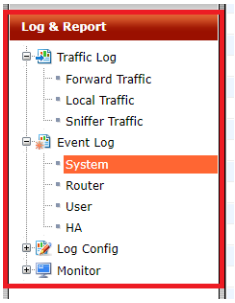


3.2.2 ที่แท็บ System / Dashboard / Status ที่ช่องด้านขวามือ ตรงส่วนของ System Resources ตรวจเช็คการทำงานของ อุปกรณ์ว่าปกติหรือไม่





3.2.3 จากนั้นไปดูที่แท็บ Log & Report / Event Log / System



*** ดูที่แท็บ Level ยิ่งมากยิ่งเสี่ยง แล้วตรวจสอบว่าเป็นเหตุการณ์ที่เกิดวันไหน เวลาอะไร โดยวันและเวลาจะอยู่ด้านซ้ายมือของ Level และเกิดเหตุการณ์อะไรขึ้น หากสามารถแก้ไขเบื้องต้นได้ ให้ทำการแก้ไขโดยทันที หรือหากแก้ไขเบื้องต้นไม่ได้ ให้ทำการโทรแจ้งบริษัทฯ ***

3.2.4 หลังจากการตรวจสอบสถานะ , ดำเนินการแก้ไข หรือประสานงานกับบริษัทที่ดูแล เรียบร้อยแล้ว ให้ทำการบันทึกข้อมูลเพื่อเก็บเป็นรายงานต่อไป

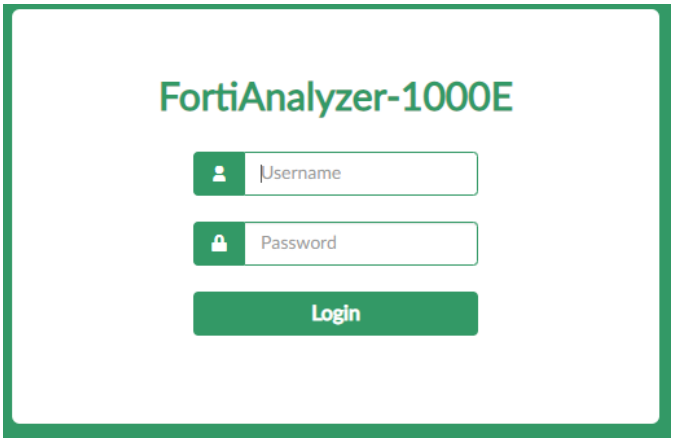
การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) คือ การรวบรวมและบันทึกข้อมูลทุกการเชื่อมต่อของทุก ๆ อุปกรณ์ของผู้รับบริการอินเทอร์เน็ต เป็น Log File เช่น ชนิดของบริการที่ใช้งาน, วันและเวลาที่ใช้งาน, เว็บไซต์ปลายทาง, การรับส่งอีเมล รวมถึงที่อยู่อีเมล (E-mail Address) ไม่ว่าจะเป็นการใช้งานเพื่อติดต่อ สื่อสารใด ๆ การเก็บ Log File ข้อมูลคือสิ่งที่ต้องทำ เพื่อให้เจ้าหน้าที่ตรวจสอบเมื่อเกิดคดีความหรือการกระทำผิด

กระบวนการเก็บ Log File จะทำการผ่านผู้ให้บริการ ซึ่งไม่ได้จำกัดแค่ผู้ให้บริการเครือข่ายอินเทอร์เน็ตหรือโซเชียลมีเดียเท่านั้น แต่รวมถึงกิจการห้างร้านต่าง ๆ ที่ให้บริการอินเทอร์เน็ตแก่ลูกค้าหรือผู้รับบริการ ไม่ว่าอินเทอร์เน็ตจะเป็นส่วนประกอบหลัก สินค้าหลักขององค์กรนั้น ๆ หรือไม่ก็ตาม

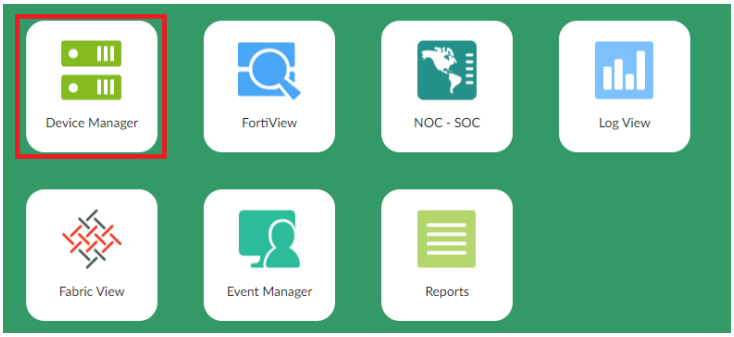
จากที่กล่าวมาข้างต้น จะเห็นได้ว่า อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย มีความสำคัญสำหรับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ทั้งหมดของทางคณะฯ โดยการส่งค่าต่างๆมาจากอุปกรณ์ป้องกันเครือข่าย (Firewall) ข้างต้น มาจัดเก็บในอุปกรณ์นี้ รวมทั้งทำการวิเคราะห์และจัดการข้อมูลให้สามารถออกมาเป็นรายงานให้อ่านและทำความเข้าใจได้ง่าย ทำให้จำเป็นต้องทำการตรวจสอบการทำงานของอุปกรณ์ และตรวจสอบพื้นที่ที่คงเหลือของอุปกรณ์ เพื่อตรวจสอบว่าข้อมูลมีการเติบโตมาแค่ไหน และจะเพียงพอต่อการใช้งานหรือไม่ เพื่อทำการวางแผนในการขยายความจุของอุปกรณ์ต่อไปในอนาคต โดยอุปกรณ์จัดเก็บ Log File ระบบเครือข่ายที่ทางคณะพยาบาลศาสตร์เกื้อการุณย์ใช้งานมีวิธีการเข้าถึงและดำเนินงานดังนี้

3.3 อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย ยี่ห้อ Fortianalyzer รุ่น 1000E

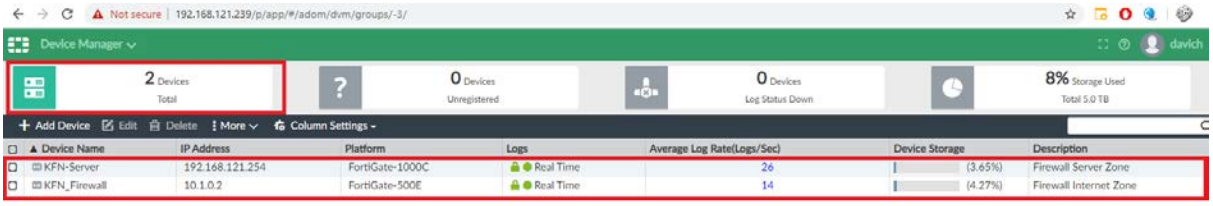
3.3.1 เข้าโปรแกรมเว็บบราวเซอร์ Web Browser แล้วพิมพ์ URL ดังนี้ https://192.168.121.239 จากนั้นกรอก Username และ Password



3.3.2 จากนั้นไปที่ Device Manager



3.3.3 จากนั้นตรวจสอบ ว่าอุปกรณ์เชื่อมต่อกันปกติหรือไม่



*** หากรายการอุปกรณ์ที่เชื่อมต่อหายไป หรือไม่ปกติ ให้ทำการโทรแจ้งบริษัทฯ ***

3.3.4 หลังจากการตรวจสอบสถานะ , ดำเนินการแก้ไข หรือประสานงานกับบริษัทที่ดูแล เรียบร้อยแล้ว ให้ทำการบันทึกข้อมูลเพื่อเก็บเป็นรายงานต่อไป

อุปกรณ์กระจายสัญญาณ (Switch) คือ อุปกรณ์ที่มีลักษณะเป็นกล่อง ประกอบด้วยพอร์ตเชื่อมต่อหลายๆ Port ใช้ในระบบ network เชื่อมต่อกับอุปกรณ์อื่นโดยใช้ผ่านสายแลน (UTP Cable) หรือสายใยแก้วนำแสง (Fiber Optic Cable) เป็นตัวกลางในการส่ง-รับข้อมูล ในรูปแบบIP ซึ่งสวิตช์จะแจกจ่ายสัญญาณให้กับอุปกรณ์ต่างๆ ที่อยู่ในพื้นเครือข่ายอย่างทั่วถึง อีกทั้งช่วยป้องกันการรับส่งข้อมูลระหว่างอุปกรณ์สองเครื่องจากการขัดขวางอุปกรณ์อื่นๆ ในเครือข่ายเดียวกันเพื่อป้องกันข้อมูลส่วนตัวของผู้ใช้รั่วไหลไปในเครือข่ายเน็ตเวิร์คนอก

หน้าที่หลักๆ ของ อุปกรณ์กระจายสัญญาณ (Switch) ประกอบไปด้วย

- การรับและส่งผ่านข้อมูลระหว่างอุปกรณ์ต่างๆ ในระบบเครือข่ายให้สื่อสารกันได้
- เพิ่มจำนวน Port ให้กับระบบเครือข่ายที่มีอยู่แล้ว เพื่อรองรับจำนวนการเชื่อมต่ออุปกรณ์ที่มากขึ้น
- คอยเก็บข้อมูลของอุปกรณ์ที่เชื่อมต่อด้วย เพื่อจัดระเบียบและตรวจสอบข้อมูลในภายหลัง
- สามารถใช้เป็นสะพานเพื่อเชื่อมต่อระบบ Network ตั้งแต่ 2 เครือข่ายขึ้นไปเข้าหากันได้

หลักการทำงานของอุปกรณ์กระจายสัญญาณ (Switch) จะแบ่งการทำงานเป็นชั้นสื่อกลางการส่งข้อมูลในรูปแบบระบบ 2 ชั้น (Data Link Layer 2) โดย switch มีหน้าที่ในการแบ่งแยกการส่งเส้นทางภายในบริเวณของinternet switch แต่ละเครือข่าย และการคัดกรองข้อมูลที่สำคัญที่สุด ให้ถูกจัดหมวดหมู่เป็นลำดับแรก เพื่อส่งให้ส่งข้อมูลไปยังอุปกรณ์รับสัญญาณที่จุดหมายปลายทางได้ไม่ทับซ้อนกัน

Switch เป็นตัวกลางทำให้เส้นทางการส่งข้อมูลแต่ละ Port ที่ทำงานร่วมกับ Router ที่ทำหน้าที่กระจายสัญญาณอินเทอร์เน็ตแต่ละจุดทั่วพื้นที่ แต่ switch เป็นสะพานเชื่อมให้อุปกรณ์ที่อยู่ในเครือข่ายสามารถรองรับสัญญาณได้หลากหลายจำนวน และเข้าถึงสัญญาณทั่วถึง

Network Switch นั้นมีหลากหลายชนิด ซึ่งแต่ละรูปแบบถูกสร้างมาเพื่อรองรับการใช้งานที่ต่างกัน โดยที่ทางคณะใช้งานจะแบ่งเป็นขนิดหลักๆ ดังนี้

- Unmanaged Network Switch เป็น Switch แบบมาตรฐานที่ราคาถูก แต่มีฟังก์ชั่นที่ง่ายต่อการใช้งาน หน้าที่หลักๆ คือ ใช้เพิ่มจำนวน Ethernet Port ให้กับระบบเครือข่าย Unmanaged Switch มักไม่จำเป็นต้องถูกตั้งค่าผ่านอุปกรณ์อื่นๆ อีกทีหนึ่ง เพราะแค่เสียบก็ใช้งานได้เลย เป็นประเภทที่นิยมใช้งานในออฟฟิศขนาดเล็ก หรือพื้นที่ Commercial ที่ไม่ได้ใช้ระบบเครือข่ายมากมาย
- **Managed Network Switch** เป็น Switch ที่ใช้ควบคุม และบริหารจัดการให้มีประสิทธิภาพขึ้น ปรับแต่งการใช้งานได้หลากหลาย อิสระ อีกทั้งมีความสามารถที่มากขึ้น โดยมี Built-in Dashboard หรือ Interface ในตัว ช่วยให้ User ที่เป็น Admin หรือแผนกไอที มีเครื่องมือ

สำหรับใช้ monitor ข้อมูลรับส่งในระบบเครือข่ายทั้งหมด ขณะที่ Traffic กำลังวิ่ง ความสามารถอื่นๆ คือ การกำหนดการเข้าถึง, การทำ Port Mirroring, การทำ Redundancy, การจัดค่าความสำคัญของอุปกรณ์ และอื่นๆ โดย Managed Switch สามารถออกแบบให้ทำงานแบบ Manual ที่มีความยืดหยุ่น หรือ Smart Switch ที่ใช้งานได้ง่ายกว่า ก็ทำได้ ถือว่าเหมาะกับองค์กรระดับใหญ่ ที่ต้องการความ High Availability มั่นคงของระบบ

- **PoE Network Switch** เป็น Switch ที่สามารถส่งผ่านพลังงานให้กับอุปกรณ์ที่เชื่อมต่อกับตนผ่านสาย RJ-45 แทนที่จะส่งได้แต่ข้อมูลเพียงอย่างเดียว ถ้าอุปกรณ์ของคุณส่วนใหญ่เป็นแบบ PoE-enabled แนะนำให้เลือกสวิตช์ประเภทนี้เพื่อการใช้งานที่ยืดหยุ่น และลดจำนวนสายไฟโดยเฉพาะพื้นที่ที่ปลั๊กไฟจำกัด แถมช่วยให้อุปกรณ์ที่เชื่อมต่อมีความเสถียรมากขึ้น
- **Stackable Network Switch** เป็น Switch ที่สามารถทำงานได้ด้วยตัวมันเอง หรือจะทำงานร่วมกับ Stackable Switch ตัวอื่นๆ เพื่อเพิ่มขีดจำกัด และทางเลือกในการเชื่อมต่อให้มีประสิทธิภาพมากขึ้น เมื่อเชื่อมต่อกัน สวิตช์แต่ละตัวจะถูกรวมเข้าทำงานด้วยกันเสมือนเป็น Switch ตัวใหญ่ตัวเดียว ประสิทธิภาพที่ได้จะขึ้นกับว่าเราเชื่อมต่อเข้าด้วยกันกี่ตัว

<u>ประเภทของ Switch</u>

- L1-Switch Switchประเภทชั้นสื่อกลาง การส่งข้อมูลในรูปแบบระบบ 1 ชั้น (Data Link Layer 1) ทำหน้าที่คอยส่งข้อมูลทุกๆ เส้นทางที่มีความเร็วต่ำ
- L2-Switch Switchประเภทชั้นสื่อกลาง การส่งข้อมูลในรูปแบบระบบ 2 ชั้น (Data Link Layer 2) เป็นSwitchตัวเบิกช่องทางการส่งสัญญาณ 2 สายขึ้นไปทำหน้าที่คอยส่งข้อมูลทุกๆ เส้นทางที่มีความเร็วการส่งสัญญาณที่มีประสิทธิภาพสูงกว่า L1-switch
- L3-Switch Switchประเภท network switch layer ที่สามารถส่งสัญญาณให้กับอุปกรณ์ปลายทางหลายๆ เครื่องในรูปแบบหมวดหมู่ และเป็นกลุ่มได้อย่างมีระเบียบ

ความแตกต่างของ Switch แบบ Layer 2 กับ Layer 3

- Layer 2 Switch ทำงานบนเลเยอร์ดาต้าลิงค์ (OSI Layer 2) และใช้ที่อยู่ของ MAC address เพื่อกำหนดเส้นทางผ่านที่เฟรมจะถูกส่งต่อ ใช้เทคนิคการสลับโดยใช้ฮาร์ดแวร์เชื่อมต่อ และส่งข้อมูลในเครือข่าย หากมีการเชื่อมต่อกับเส้นทางจำนวนมาก จำเป็นต้องมี hub คอยแจกจ่ายสัญญาณข้อมูลให้กับจุดหมายปลายทางอีกที
- Layer 3 Switch มีความเร็วในการเปิดเส้นทางของตัว switch ได้อย่างรวดเร็ว และช่วยให้การทำงานใน Network มีประสิทธิภาพสูง โดยรวบรวมเอาฟังก์ชั่นของเราเตอร์มาเสริมการทำงานของตัว Switch อีกทั้งทำให้การเปิดเส้นทางเครือข่ายภายในระบบ Lan ทำได้เร็วขึ้น

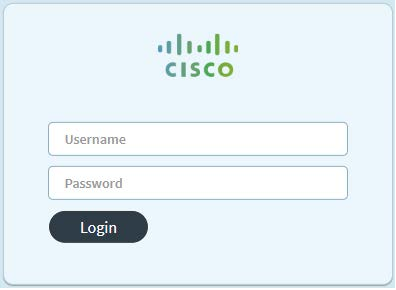
ข้อดีของ Switch

- มีระบบการจัดการด้วยตัวเองแบบมีระเบียบ เพราะตัวระบบมีการจดจำ IP address ของแต่ละอุปกรณ์อิเล็กทรอนิกส์รองรับเครือข่ายอินเทอร์เน็ต ทำให้Switchสามารถจัดส่งข้อมูลได้อย่างแม่นยำ
- เป็นอุปกรณ์ที่ประกอบเทคโนโลยีที่การเชื่อมต่อกับอุปกรณ์ได้ทุกพอร์ต ทำให้Switchสามารถรองรับเชื่อมต่อเครือข่ายเน็ตเวิร์คได้รวดเร็ว
- มีการจัดลำดับการกรองข้อมูลแบบเป็นขั้นเป็นตอน ทำให้เป็นอุปกรณ์ที่สามารถส่งข้อมูลแบบจัดเรียบเรียงได้อย่างเป็นระเบียบ

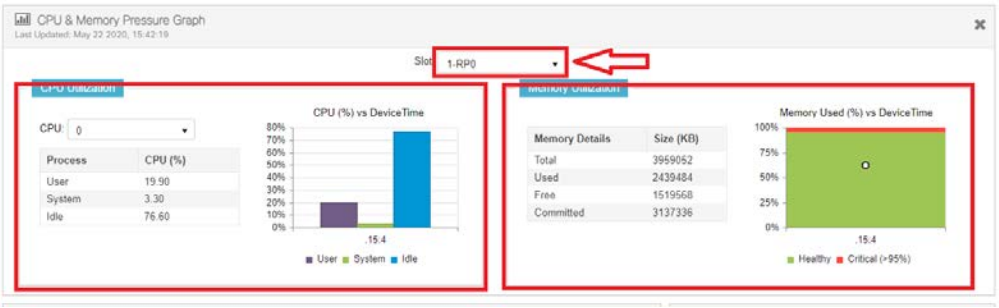
จากข้อมูลข้างต้น จะเห็นได้ว่า อุปกรณ์กระจายสัญญาณ มีความสำคัญสำหรับการจัดการข้อมูลจราจรทางคอมพิวเตอร์ทั้งหมดของทางคณะ จึงมีความจำเป็นอย่างมากที่จะต้องตรวจสอบและเฝ้าระวังให้สามารถทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ โดยอุปกรณ์กระจายสัญญาณที่ทางคณะพยาบาลศาสตร์เกื้อการุณย์ใช้งานจะประกอบไปด้วยอุปกรณ์กระจายสัญญาณทั้งแบบ L3 และ L2 หลากหลายยี่ห้อ มีวิธีการเข้าถึงและดำเนินงานต่างกันตามแต่ละยี่ห้อดังนี้

3.4 อุปกรณ์กระจายสัญญาณ (L3 Switch) ยี่ห้อ Cisco รุ่น Catalyst-3850

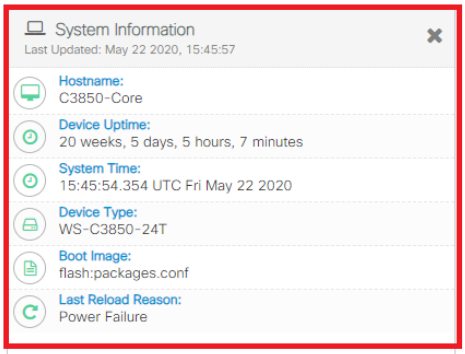
3.4.1 เข้าโปรแกรมเว็บบราวเซอร์ Web Browser แล้วพิมพ์ URL ดังนี้ https://10.1.1.254 จากนั้นกรอก Username และ Password



3.4.2 จากนั้นตรวจสอบ CPU และ Memory ในแต่ละ Slot (เปลี่ยน Slot ที่ลูกศรสีแดง) ว่าสามารถทำงานได้เต็มประสิทธิภาพหรือไม่ สำหรับ CPU แถบสีน้ำเงินมักจะน้อยกว่าสีม่วงเสมอ และสำหรับ Memory ให้ดูที่จุดสีขาว มักจะอยู่ในเขตสีเขียวเสมอ



3.4.3 จากนั้น เลื่อนลงไปด้านล่าง ไปตรวจสอบ System Information ตรงส่วนของ Device Uptime ว่าอุปกรณ์ทำงานมาแล้วเป็นระยะเวลาต่อเนื่องนานเท่าใด



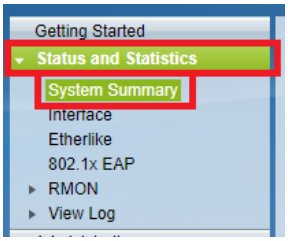
*** หาก Uptime มีเวลาที่น้อย ต้องตรวจสอบว่ามีไฟฟ้าดับไปเมื่อใด (มักจะทำการโทรแจ้งบริษัทฯก่อนดับไฟฟ้าเสมอ) ***

3.4.4 หลังจากการตรวจสอบสถานะ , ดำเนินการแก้ไข หรือประสานงานกับบริษัทที่ดูแล เรียบร้อยแล้ว ให้ทำการบันทึกข้อมูลเพื่อเก็บเป็นรายงานต่อไป

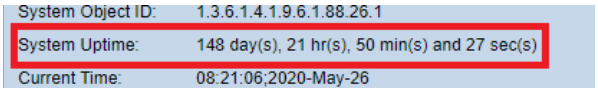
3.5 อุปกรณ์กระจายสัญญาณ (L2 Switch) ยี่ห้อ Cisco รุ่น SG-200 และ SG-220

3.5.1 เข้าโปรแกรมเว็บบราวเซอร์ Web Browser แล้วพิมพ์ URL ที่ต้องการเข้าไปตรวจสอบ โดยเริ่มด้วย https:// เช่น จากนั้นกรอก Username และ Password

3.5.2 จากนั้นไปที่แท็บ Status and Statistics / System Summary



3.5.3 ตรวจสอบที่ System Uptime ว่าอุปกรณ์ออนไลน์มาเป็นเวลาเท่าใดแล้ว



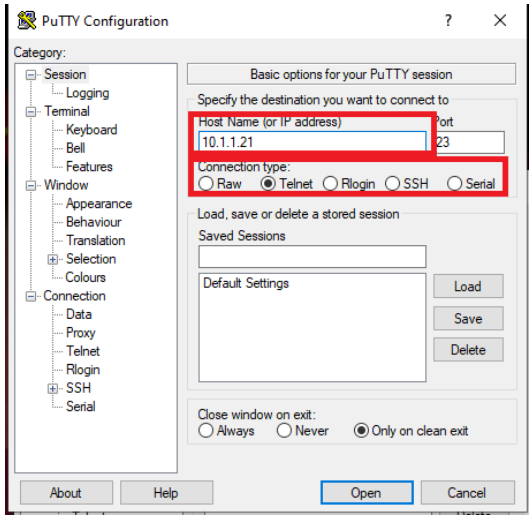
*** หาก Uptime มีเวลาที่น้อย ต้องตรวจสอบว่ามีไฟฟ้าดับไปเมื่อใด (มักจะทำการโทรแจ้งบริษัทฯก่อนดับไฟฟ้าเสมอ) ***

3.5.4 หลังจากการตรวจสอบสถานะ , ดำเนินการแก้ไข หรือประสานงานกับบริษัทที่ดูแล เรียบร้อยแล้ว ให้ทำการบันทึกข้อมูลเพื่อเก็บเป็นรายงานต่อไป

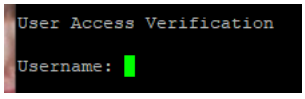
3.6 อุปกรณ์กระจายสัญญาณ (L2 Switch) ยี่ห้อ Cisco รุ่น Catalyst-2960X และ Catalyst-2960S

3.6.1 เข้าโปรแกรม 

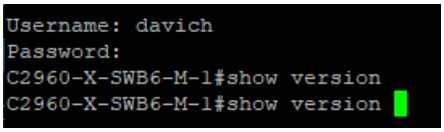
จากนั้นกรอก IP Address ของ Switch ที่ต้องการตรวจสอบในช่อง Host Name (or IP address) เช่น 10.1.1.21 แล้วเลือก Connection type เป็นแบบ Telnet แล้วกด Open



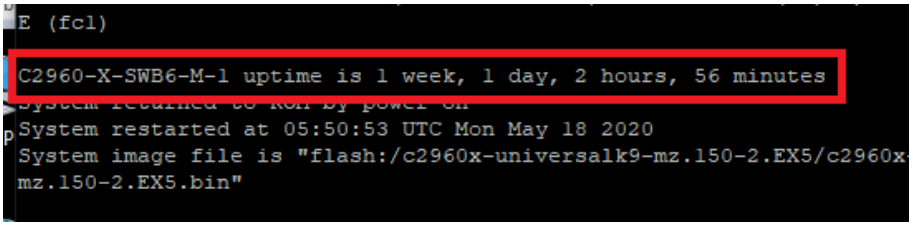
3.6.2 จากนั้นกรอก Username และ Password



3.6.3 แล้วพิมพ์คำสั่ง show version



3.6.4 จากนั้นมองหา uptime ของ switch ว่าอุปกรณ์ออนไลน์มาเป็นเวลาเท่าใดแล้ว



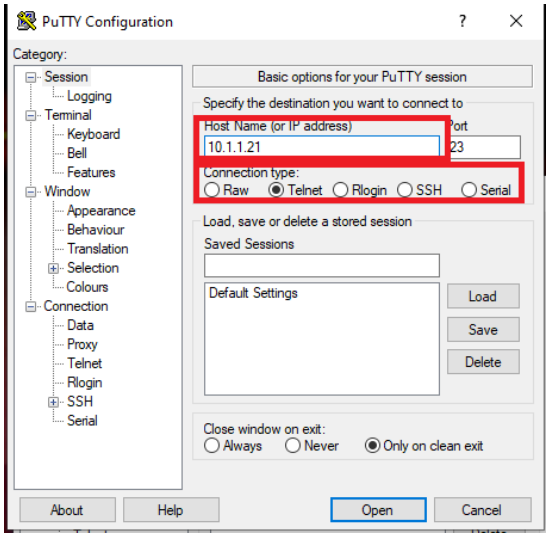
*** หาก Uptime มีเวลาที่น้อย ต้องตรวจสอบว่ามีไฟฟ้าดับไปเมื่อใด (มักจะทำการโทรแจ้งบริษัทฯก่อนดับไฟฟ้าเสมอ) ***

3.6.5 หลังจากการตรวจสอบสถานะ , ดำเนินการแก้ไข หรือประสานงานกับบริษัทที่ดูแล เรียบร้อยแล้ว ให้ทำการบันทึกข้อมูลเพื่อเก็บเป็นรายงานต่อไป

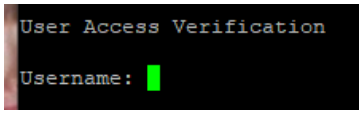
3.7 อุปกรณ์กระจายสัญญาณ (L2 Switch) ยี่ห้อ DCN รุ่น S4200

3.7.1 เข้าโปรแกรม 

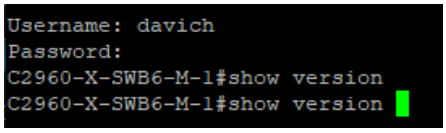
จากนั้นกรอก IP Address ของ Switch ที่ต้องการตรวจสอบในช่อง Host Name (or IP address) เช่น 10.1.1.21 แล้วเลือก Connection type เป็นแบบ Telnet แล้วกด Open



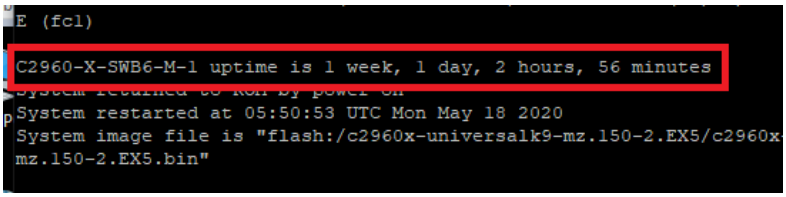
3.7.2 จากนั้นกรอก Username และ Password



3.7.3แล้วพิมพ์คำสั่ง show version



3.7.4 จากนั้นมองหา uptime ของ switch ว่าอุปกรณ์ออนไลน์มาเป็นเวลาเท่าใดแล้ว



*** หาก Uptime มีเวลาที่น้อย ต้องตรวจสอบว่ามีไฟฟ้าดับไปเมื่อใด (มักจะทำการโทรแจ้งบริษัทฯก่อนดับไฟฟ้าเสมอ) ***

3.7.5 หลังจากการตรวจสอบสถานะ , ดำเนินการแก้ไข หรือประสานงานกับบริษัทที่ดูแล เรียบร้อยแล้ว ให้ทำการบันทึกข้อมูลเพื่อเก็บเป็นรายงานต่อไป

เครื่องคอมพิวเตอร์แม่ข่าย (Server) เป็นคอมพิวเตอร์ที่ทำหน้าที่เป็นจุดศูนย์กลางในการให้บริการด้านต่างๆ กับเครื่องคอมพิวเตอร์อื่นๆ ที่อยู่ในเครือข่าย หรือกล่าวได้ว่า Server เป็นแม่ข่ายหลักของเครื่องคอมพิวเตอร์ย่อย ควรจะมีประสิทธิภาพสูง มีความเสถียร และสามารถให้บริการแก่ผู้ใช้ได้เป็นจำนวนมาก โดยสามารถแบ่งตามลักษณะหน้าที่ ได้ดังนี้

1.1 File Server คือเครื่องที่ให้บริการแบ่งปั้นข้อมูล (Share) แก่เครื่องอื่นๆ ให้มีสิทธิ์ การใช้แฟ้มข้อมูล (File) เช่น ฐานข้อมูลบนเครือข่าย (Database)

1.2 Web Server คือเครื่องที่ให้บริการ Web แก่เครื่องที่ร้องขอด้วย Protocol HTTP หมายความว่าเป็นเครื่องที่เก็บเว็บไซต์(Website) สำหรับเก็บโฮมเพจและเว็บเพ็จที่หน่วยงานจัดทำขึ้น

1.3 Proxy Server คือเครื่องที่ให้บริหารเป็นตัวแทนไปรับเว็บแทนลูกข่าย และสะสมข้อมูลของเว็บไซต์นั้นไว้ใน Cache ของตัวเอง สำรองไว้เผื่อลูกข่ายร้องขอเข้าถึงเว็บไซต์เดิมอีกครั้ง จะได้ไม่ต้องออกไปนำข้อมูลมาอีก ทำให้ลูกข่ายเครื่องอื่นๆ สามารถเข้าถึงเว็บที่เคยเปิดมาแล้วเร็วขึ้น และลด Traffic ของ WAN ลงได้

1.4 Mail Server คือเครื่องที่หน้าที่เป็นไปรษณีย์ ทำหน้าที่รับจดหมาย (POP3) เก็บ จดหมาย (Mailbox) และส่งจดหมาย(SMTP) คอยบริการให้กับผู้ใช้ที่ได้รับลงทะเบียนใช้บริการ

1.5 Internet Server คือเครื่องที่ทำหน้าที่ในการเชื่อมต่อระบบอินเทอร์เน็ตและควบคุมการใช้บริการอินเทอร์เน็ตให้กับเครื่องคอมพิวเตอร์ลูกข่าย

1.6 Print Server คือเครื่องที่ให้บริการเกี่ยวกับการพิมพ์โดยทุกเครื่องในเครือข่ายสามารถส่งงานของตนไปพิมพ์ที่เครื่องท าหน้าที่เป็น Print Server

1.7 DNS Server คือเครื่องที่ให้บริการเกี่ยวกับ Domain Name Server ซึ่งเป็นเครื่องที่ใช้สำหรับการอ้างอิงหมายเลข IP กับชื่อที่เราทำการจดทะเบียน

ทั้งนี้ปัจจุบันระบบเหล่านี้มักจะทำงานอยู่บน Virtual Machine อีกชั้นหนึ่ง

Virtual Machine (VM) คือ ซอฟต์แวร์ที่ใช้ทรัพยากรของเครื่องคอมพิวเตอร์ไม่ว่าจะเป็น RAM, Hard disk, CPU ในการจำลองเครื่องคอมพิวเตอร์เสมือน ซึ่งจะเรียกเครื่องที่ถูกใช้ทรัพยากรว่า Host และเรียกเครื่องเสมือนว่า Guest โดยในเครื่อง Guest สามารถติดตั้งและใช้งานระบบปฏิบัติการได้เสมือนกับเป็นซอฟต์แวร์หนึ่งของเครื่องคอมพิวเตอร์ ดังนั้นจึงสามารถติดตั้งระบบปฏิบัติการอื่นที่แตกต่างจากระบบปฏิบัติการหลักของเครื่อง Host ได้ เช่น เครื่อง Host ใช้งาน Microsoft Windows แต่เครื่อง Guest ติดตั้ง Linux เป็นต้น นอกจากนี้ยังสามารถสร้าง Guest ได้มากกว่า 1 Guest ในเครื่อง Host เดียวกันอีกด้วย

Infrastructure ที่ต้องเตรียมก่อนที่จะสร้าง Virtual Machine จะประกอบไปด้วย

- Infrastructure
- Host Operating System
- Hypervisor

บางผู้พัฒนาจะพัฒนา Software ของตัวเองให้รวมเอาทั้ง Host OS และ Hypervisor เข้าด้วยกันเลย เรานิยาม Software แบบนี้ว่า Type -1 Hypervisor ที่นิยมใช้กันในไทยก็มี VMware ESXi, Microsoft Hyper-V , Nutanix AHV และ KVM เป็นต้น

ส่วน Type-2 Hypervisor ก็จะต้องติดตั้งตามโครงสร้างที่ได้กล่าวไปเบื้องต้น ชื่อที่คุ้นเคยกัน ได้แก่ VMware Workstation

Virtual Machine – เปรียบเสมือน Server เสมือนที่สามารถใช้งานได้เทียบเท่ากับ Physical Server แบบเดิม ๆ เลย ส่วนประกอบมีดังนี้

- Guest OS
- Binary/Library
- Application

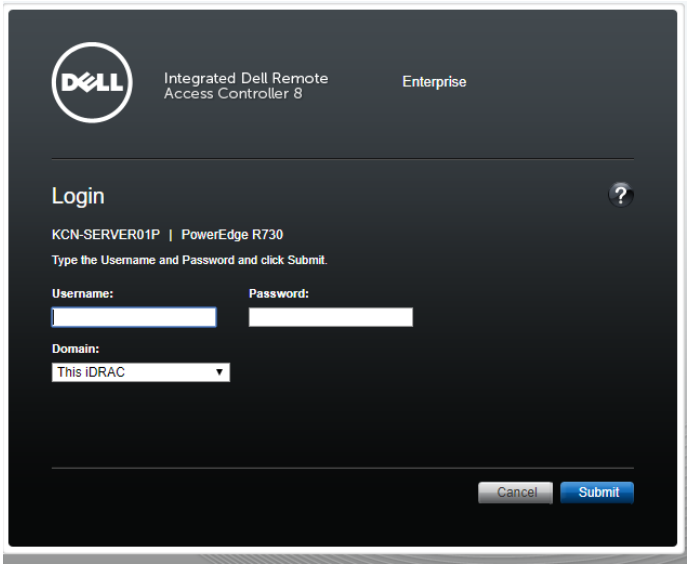
ข้อดีของการใช้ Virtual Machine

- ลดจำนวน Server กรณีที่เป็นองค์กรที่ต้องใช้งานหลายระบบปฏิบัติการในการประมวลผล
- ลดการใช้พลังงาน จากการใช้คอมพิวเตอร์หลายๆเครื่อง
- ช่วยให้การจัดสรรทรัพยากรภายในเครื่องเป็นไปอย่างคุ้มค่า
- อนุญาตให้มีสภาพแวดล้อมระบบปฏิบัติการ (OS) หลายระบบพร้อมกันบนเครื่องเดียวกัน
- การใช้ VM ช่วยให้มั่นใจในการจัดเตรียมแอปพลิเคชันความพร้อมใช้งานที่ดีขึ้น
- บำรุงรักษาและกู้คืนได้ง่าย

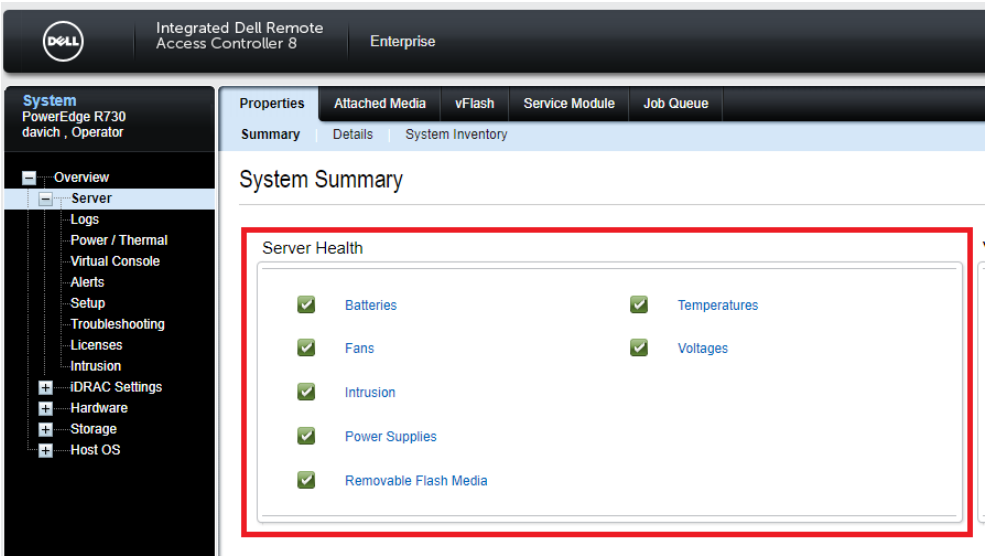
จากข้อมูลข้างต้นจะเห็นได้ว่า เครื่องคอมพิวเตอร์แม่ข่าย 1 หน่วยต้องรองรับการทำงานหลายๆระบบพร้อมกันจึงมีความจำเป็นอย่างมากที่จะต้องทำการตรวจสอบการทำงานของเครื่องแม่ข่ายอย่างสม่ำเสมอ เพื่อให้เครื่องแม่ข่ายทำงานได้อย่างมีประสิทธิภาพ และทำการแก้ไขปัญหาได้อย่างทันท่วงทีหากมีอุปกรณ์ หรือชิ้นส่วนของเครื่องแม่ข่ายชำรุดเสียหาย หรือทำงานผิดพลาด โดยขั้นตอนในการดำเนินงานมีดังนี้

3.8 เครื่องคอมพิวเตอร์แม่ข่าย ยี่ห้อ Dell รุ่น PowerEdge R730

3.8.1 เข้าโปรแกรมเว็บบราวเซอร์ Web Browser แล้วพิมพ์ URL ที่ต้องการเข้าไปตรวจสอบ โดยเริ่มด้วย https:// เช่น https://192.168.120.246 จากนั้นกรอก Username และ Password



3.8.2 ให้สังเกตุตรง Server Health ว่าเป็นปกติตามภาพหรือไม่

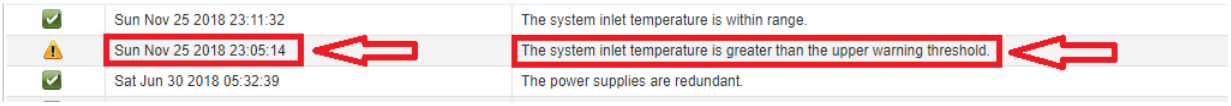


3.8.3 จากนั้นให้เลื่อนลงมาด้านล่าง และไปตรวจสอบ Logged Events มีอะไรแปลกกว่าปกติ หรือเพิ่มจากของเดิมหรือไม่ ถ้าพบปัญหาเบื้องต้นให้ทำการ restart อุปกรณ์ก่อน (แนะนำให้ทำนอกเวลาทำการ และทำประกาศแจ้งล่วงหน้าเพื่อหลีกเลี่ยงผลกระทบกับผู้ใช้งาน)

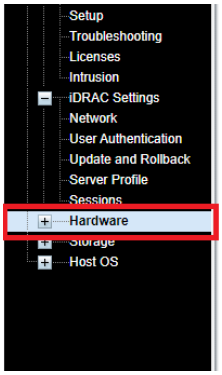

Recent Logged Events

Severity	Date/Time	Description
Options: View Logs		
✓	Sun Nov 25 2018 23:11:32	The system inlet temperature is within range.
⚠	Sun Nov 25 2018 23:05:14	The system inlet temperature is greater than the upper warning threshold.
✓	Sat Jun 30 2018 05:32:39	The power supplies are redundant.
✓	Sat Jun 30 2018 05:32:33	The input power for power supply 1 has been restored.
✗	Sat Jun 30 2018 05:32:24	Power supply redundancy is lost.
✗	Sat Jun 30 2018 05:32:23	The power input for power supply 1 is lost.
✗	Sat May 27 2017 08:05:41	CPU 1 has an internal error (IERR).
✓	Sat May 27 2017 08:05:12	An OEM diagnostic event occurred.
✗	Sat May 27 2017 08:05:12	A fatal error was detected on a component at bus 0 device 1 function 0.
✗	Sat May 27 2017 08:05:12	A fatal error was detected on a component at bus 2 device 0 function 0.

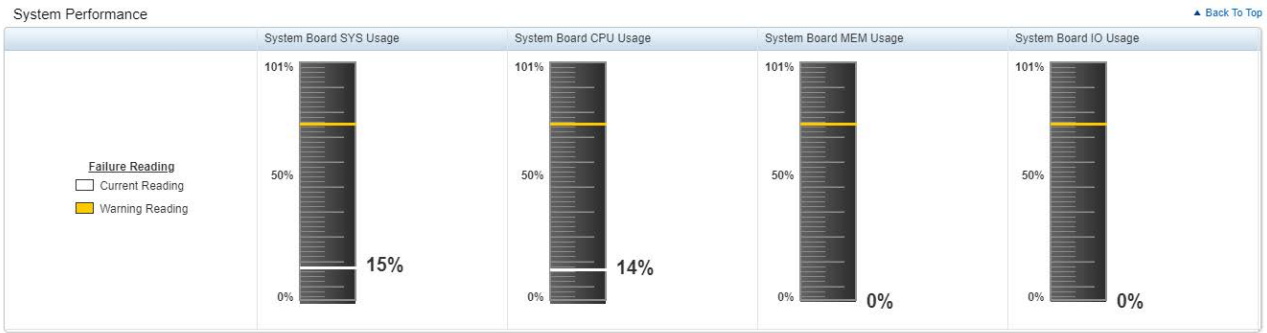
*** ถ้ามีอะไรเพิ่มขึ้นมาเป็นเครื่องหมาย ⚠ หรือ ✗ ให้ไปตรวจสอบว่าเป็นเหตุการณ์ที่เกิดวันไหน เวลาอะไร โดยวันและเวลาจะอยู่ด้านขวามือของเครื่องหมายดังกล่าว และเกิดเหตุการณ์อะไรขึ้น หากสามารถแก้ไขเบื้องต้นได้ ให้ทำการแก้ไขโดยทันที หรือหากแก้ไขเบื้องต้นไม่ได้ ให้ทำการโทรแจ้งบริษัทฯ ***


✓	Sun Nov 25 2018 23:11:32	The system inlet temperature is within range.
⚠	Sun Nov 25 2018 23:05:14	The system inlet temperature is greater than the upper warning threshold.
✓	Sat Jun 30 2018 05:32:39	The power supplies are redundant.

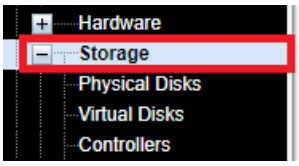
3.8.4 จากนั้น ให้ไปที่แท็บ Hardware ทางซ้ายมือ แล้วเช็คตรง System Performance ดูว่าการทำงานของ Hardware ทำงานหนักแค่ไหนปกติหรือไม่

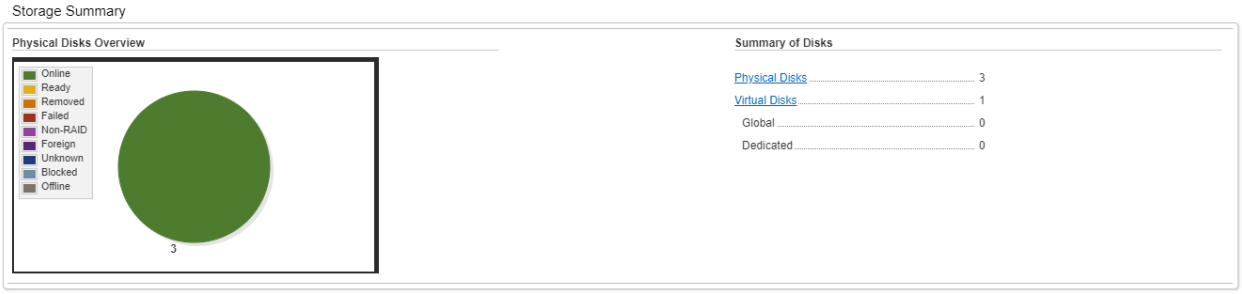


*** หาก Hardware ทำงานหนักกว่าปกติ ให้ทำการตรวจสอบระบบต่างๆ หรือประสานงานบริษัทให้ช่วยตรวจสอบ ***



3.8.5 สุดท้ายให้ไปที่แท็บ Storage ทางซ้ายมือ แล้วเช็คตรง Storage Summery เพื่อตรวจสอบสถานะของ Storage บนเครื่อง Server โดยสถานะต้องเป็น Online ทั้งหมดเสมอ





*** ทำตามขั้นตอนนี้กับเครื่องคอมพิวเตอร์แม่ข่ายทั้ง 3 เครื่อง ทีละ IP Address ***

3.8.6 หลังจากการตรวจสอบสถานะ , ดำเนินการแก้ไข หรือประสานงานกับบริษัทที่ดูแล เรียบร้อยแล้ว ให้ทำการบันทึกข้อมูลเพื่อเก็บเป็นรายงานต่อไป

อุปกรณ์จัดเก็บข้อมูล (Storage) ในสมัยก่อนธุรกิจการค้าไม่ได้แข่งขันกันด้วยข้อมูล จึงทำให้ปริมาณข้อมูลมีไม่มาก แค่ Server เครื่องเดียวก็เอาอยู่ เมื่อนานวันเข้าปริมาณข้อมูลมากขึ้น ก็ใช้วิธีการจัดเก็บง่ายๆ คือ การเพิ่ม Disk จัดเก็บข้อมูลเข้าไป รูปแบบนี้คือการจัดเก็บข้อมูลแบบ DAS ที่ใช้กันในสมัยก่อน ต่อมา ก็เปลี่ยนมาใช้แบบ NAS คือการเชื่อมโยง Server หลายเครื่องให้เข้ากับระบบ Network มีการจัดเก็บข้อมูลบนเครือข่าย แต่เมื่อเวลาผ่านไปก็พบว่า ถ้าองค์กรมีการออนไลน์และทำงานกันบน Network มาก ๆ เพราะจำนวนคนมากขึ้น ก็อาจทำให้การเก็บข้อมูลประสิทธิภาพลดลง เพราะมีการใช้งานพร้อม ๆ กันมาก ทำให้เกิดการดึงสัญญาณกัน นั่นจึงนำไปสู่การพัฒนารูปแบบการจัดเก็บข้อมูลแบบ SAN ซึ่ง SAN Storage คือ การจัดเก็บข้อมูลที่จะทำการแยก Disk ออกมาจากเครือข่ายหลัก มาเชื่อมต่อกับ Server หลายเครื่องแทน โดยมีเทคโนโลยี Fibre Channel ช่วยในการรับส่งข้อมูลระหว่าง Server กับอุปกรณ์จัดเก็บข้อมูลอีกทีทำให้การรับส่งข้อมูลมีความเร็วที่มากขึ้น

หากเป็นบริษัทหรือองค์กรขนาดเล็ก การเลือกจัดเก็บข้อมูลแบบ NAS ก็ถือว่าเพียงพอแล้ว แต่ถ้าเป็นองค์กรขนาดใหญ่มีข้อมูลมากมีจำนวนคนเข้าใช้งานรับส่งข้อมูลต่อวันมาก SAN Storage จะเหมาะสมมากกว่า สำหรับองค์กรขนาดใหญ่ที่ต้องการความเร็วในการจัดเก็บและรับส่งข้อมูล โดยข้อดีของ SAN Storage มีดังนี้

1.ช่วยลดปริมาณการใช้อุปกรณ์การจัดเก็บ ระบบนี้จะช่วยลดการใช้ Disk ลงไปได้มาก ปัญหาส่วนใหญ่ที่จะพบเจอในระบบอื่นก็คือ การที่ต้องเพิ่ม Disk เข้าไปในระบบ ทั้ง ๆ ที่ภายใน Server ยังมี Disk เหลืออยู่แต่จะไม่ได้ใช้เพราะต่อเข้ากับเครื่องไปแล้ว แต่การใช้ระบบ SAN จะเป็นการเชื่อมต่อทุก Disk เข้าหากันให้อยู่ในระบบเดียว ทำให้พื้นที่ทั้งหมดของ Disk ถูกใช้งานอย่างมีประโยชน์ไม่เสียเปล่า จึงไม่ต้องเพิ่ม Disk อีก

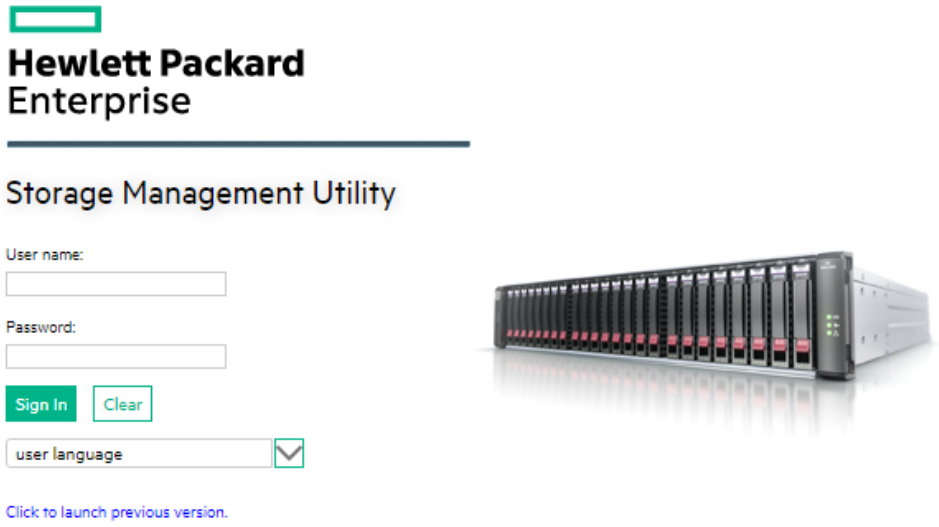
2.ลดปัญหา Traffic ของระบบ Network เมื่อไม่ต้องเชื่อมอุปกรณ์จัดเก็บเข้ากับระบบ Network จึงไม่ต้องมีการแย่งสัญญาณการใช้งาน ระบบ Network ก็จะค่อนข้างเป็นอิสระสามารถทำงานได้เต็มที่ แบบนี้การรับส่งข้อมูลและการทำงานส่วนอื่น ๆ ก็จะไม่เกิดปัญหาล่าช้า

3.มีระบบ Backup ข้อมูลที่สะดวกรวดเร็ว ระบบ SAN จะรวมหลาย ๆ อย่างไว้ในจุดเดียว ทำให้การ Backup ทำได้ง่าย แค่สั่งการครั้งเดียว ทุกระบบก็จะสำรองข้อมูลได้เอง

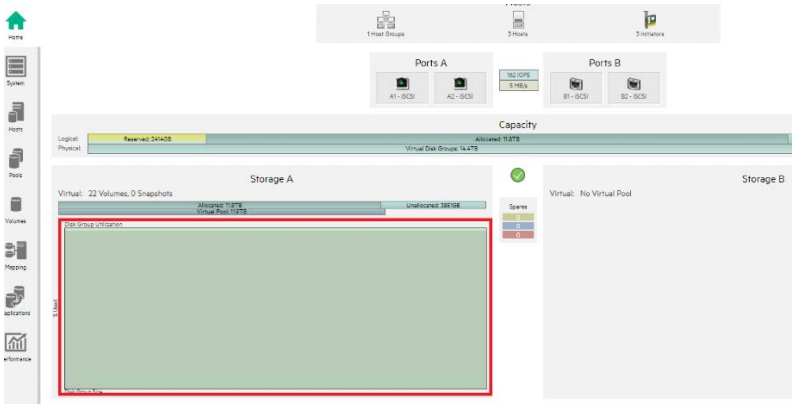
จากข้อมูลข้างต้น จะเห็นว่า SAN Storage มีความสำคัญต่อการเก็บข้อมูลต่างๆของคณะฯ และเก็บข้อมูลที่เกี่ยวข้องกับเครื่องแม่ข่าย รวมไปถึง Backup อีกด้วย ดูแลและตรวจสอบการทำงานอย่างสม่ำเสมอ เพื่อให้การใช้งานพื้นที่เป็นไปอย่างมีประสิทธิภาพ รวมไปถึงติดตามการเติบโตของพื้นที่ที่ใช้งาน เพื่อวางแผนของบประมาณในการขยายพื้นที่เพิ่มเติมในอนาคต โดยมีขั้นตอนในการดำเนินงานดังนี้

3.9 อุปกรณ์จัดเก็บข้อมูลแบบภายนอก ยี่ห้อ HP รุ่น MSA 1040 SAN

3.9.1 เข้าโปรแกรมเว็บบราวเซอร์ Web Browser แล้วพิมพ์ URL ดังนี้ https://192.168.120.213 จากนั้นกรอก Username และ Password



3.9.2 แล้วนำ Cursor Mouse ไปชี้ที่ Disk Group Utilization



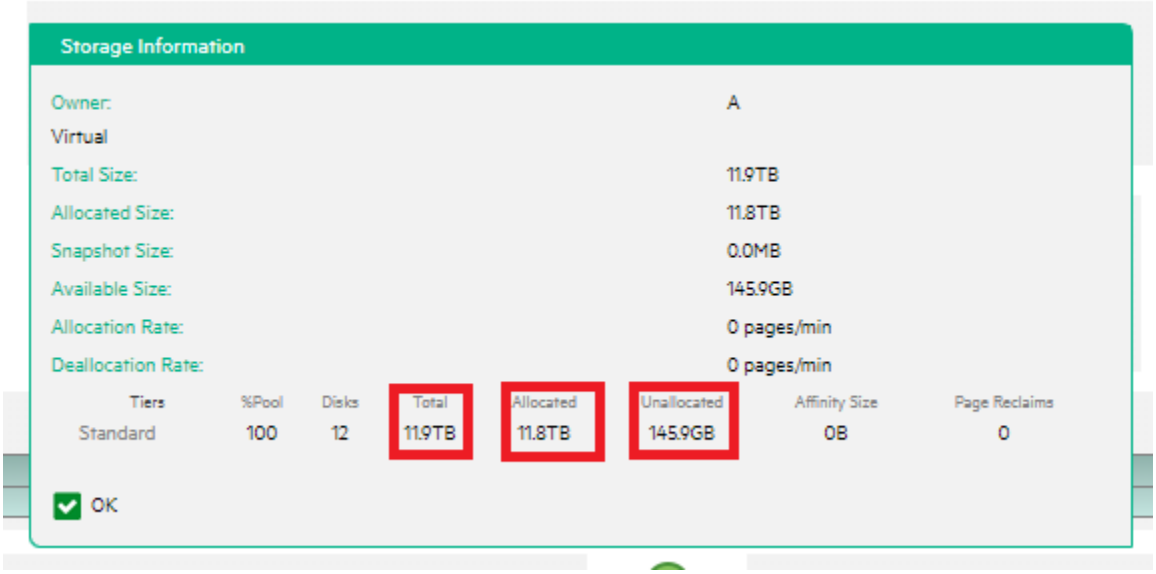
3.9.3 จะขึ้นหน้าต่าง Storage Information ขึ้นมา ตรวจสอบ 3 จุด

3.9.3.1 Total ขนาดของพื้นที่ทั้งหมดของ Storage

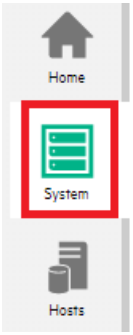
3.9.3.2 Allocated ขนาดของพื้นที่ ที่มีการใช้งานไปแล้ว

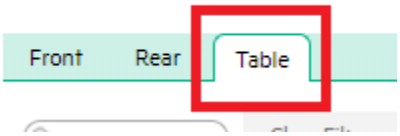
3.9.3.3 Unallocated ขนาดของพื้นที่ ที่เหลือ/ยังไม่ได้มีการใช้งาน

ให้ตรวจสอบว่า มีการเติบโตของข้อมูลมากน้อยแค่ไหน พื้นที่ Unallocated เหลือมากเพียงใด ต้องทำขยายพื้นที่หรือไม่ ? จากนั้นวางแผนทำเรื่องของบประมาณจัดซื้อต่อไป



จากนั้นไปที่แท็บ System ทางด้านซ้ายมือ แล้วคลิ๊กดูที่ Table



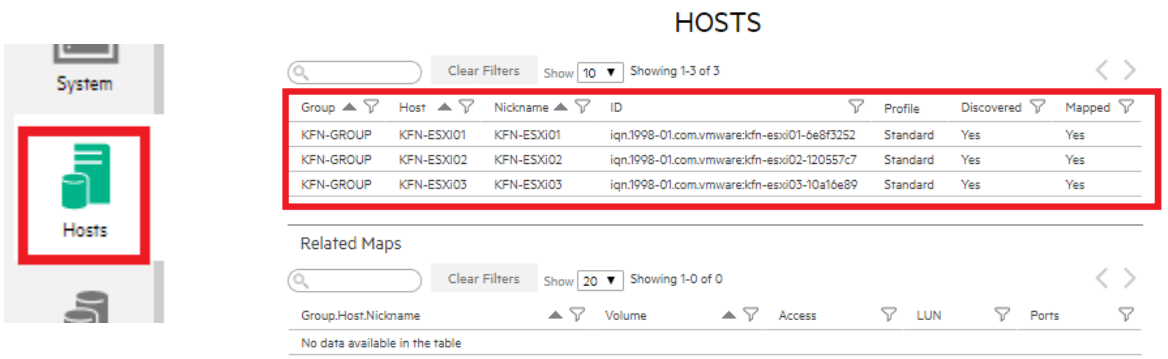


3.9.4 แล้วดูที่ Health ของแต่ละอุปกรณ์

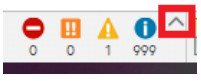
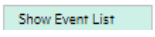
Clear Filters Show 20 Showing 1-20 of 27

Health	Type	Enclosure	Location	Information	Status
N/A	Expansion Port	1	Controller-A	Out Port	Disconnected
N/A	Expansion Port	1	Controller-B	Out Port	Disconnected
OK	CompactFlash	1	Controller-A		Installed
OK	CompactFlash	1	Controller-B		Installed
OK	Controller	1	Bottom	Controller-B	Operational
OK	Controller	1	Top	Controller-A	Operational
OK	Disk	1	1.1	SAS 1.2TB (A:Standard)	Up
OK	Disk	1	1.10	SAS 1.2TB (A:Standard)	Up
OK	Disk	1	1.11	SAS 1.2TB (A:Standard)	Up
OK	Disk	1	1.12	SAS 1.2TB (A:Standard)	Up
OK	Disk	1	1.2	SAS 1.2TB (A:Standard)	Up
OK	Disk	1	1.3	SAS 1.2TB (A:Standard)	Up
OK	Disk	1	1.4	SAS 1.2TB (A:Standard)	Up
OK	Disk	1	1.5	SAS 1.2TB (A:Standard)	Up
OK	Disk	1	1.6	SAS 1.2TB (A:Standard)	Up
OK	Disk	1	1.7	SAS 1.2TB (A:Standard)	Up
OK	Disk	1	1.8	SAS 1.2TB (A:Standard)	Up
OK	Disk	1	1.9	SAS 1.2TB (A:Standard)	Up
OK	Enclosure	1	Rack 0.0	HP SPS-CHASSIS (12 disks)	Up
OK	Host Port	1	A1	iSCSI	Up

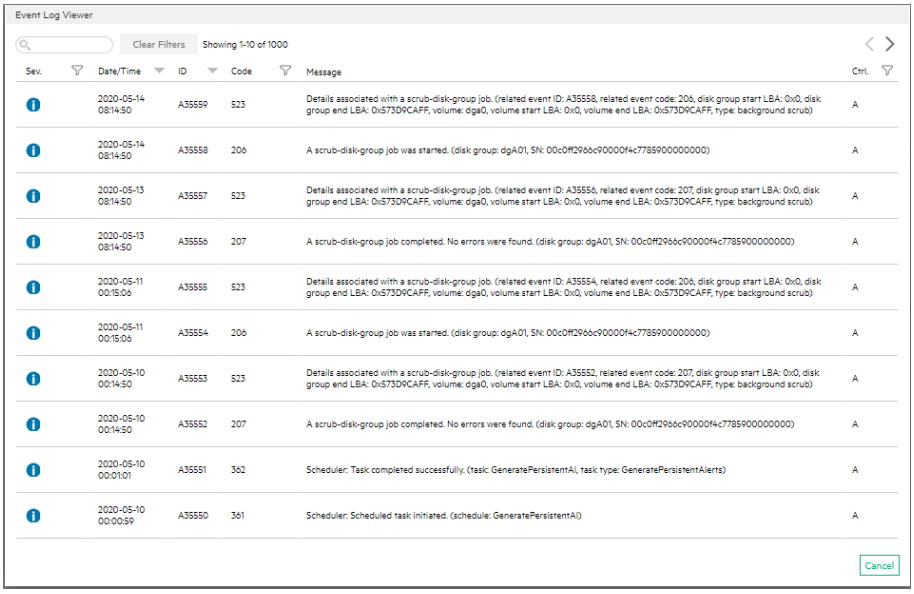
3.9.5 แล้วไปที่แท็บ Hosts แล้วดูว่า การเชื่อมต่อกับ Hosts ปกติหรือไม่



3.9.6 จากนั้นที่ดูที่แท็บด้านล่างสุด 

3.9.7 แล้วกดที่  แล้วเลือก Show Event List  เพื่อแสดง Event Log

3.9.8 จากนั้นตรวจสอบว่ามีอะไรผิดปกติหรือไม่ ถ้าพบปัญหาเบื้องต้นให้ทำการ restart อุปกรณ์ก่อน (แนะนำให้ทำนอกเวลาทำการ และทำประกาศแจ้งล่วงหน้าเพื่อหลีกเลี่ยงผลกระทบกับผู้ใช้งาน)


Event Log Viewer

Clear Filters Showing 1-10 of 1000

Sev.	Date/Time	ID	Code	Message	Ctrl.
	2020-05-14 08:14:50	A35559	523	Details associated with a scrub-disk-group job. (related event ID: A35558, related event code: 206, disk group start LBA: 0x0, disk group end LBA: 0x573D9CAFF, volume: dga0, volume start LBA: 0x0, volume end LBA: 0x573D9CAFF, type: background scrub)	A
	2020-05-14 08:14:50	A35558	206	A scrub-disk-group job was started. (disk group: dgA01, SN: 00c0ff2966c90000f4c7785900000000)	A
	2020-05-13 08:14:50	A35557	523	Details associated with a scrub-disk-group job. (related event ID: A35556, related event code: 207, disk group start LBA: 0x0, disk group end LBA: 0x573D9CAFF, volume: dga0, volume start LBA: 0x0, volume end LBA: 0x573D9CAFF, type: background scrub)	A
	2020-05-13 08:14:50	A35556	207	A scrub-disk-group job completed. No errors were found. (disk group: dgA01, SN: 00c0ff2966c90000f4c7785900000000)	A
	2020-05-11 00:15:06	A35555	523	Details associated with a scrub-disk-group job. (related event ID: A35554, related event code: 206, disk group start LBA: 0x0, disk group end LBA: 0x573D9CAFF, volume: dga0, volume start LBA: 0x0, volume end LBA: 0x573D9CAFF, type: background scrub)	A
	2020-05-11 00:15:06	A35554	206	A scrub-disk-group job was started. (disk group: dgA01, SN: 00c0ff2966c90000f4c7785900000000)	A
	2020-05-10 00:14:50	A35553	523	Details associated with a scrub-disk-group job. (related event ID: A35552, related event code: 207, disk group start LBA: 0x0, disk group end LBA: 0x573D9CAFF, volume: dga0, volume start LBA: 0x0, volume end LBA: 0x573D9CAFF, type: background scrub)	A
	2020-05-10 00:14:50	A35552	207	A scrub-disk-group job completed. No errors were found. (disk group: dgA01, SN: 00c0ff2966c90000f4c7785900000000)	A
	2020-05-10 00:01:01	A35551	362	Scheduler: Task completed successfully. (task: GeneratePersistentAl, task type: GeneratePersistentAlerts)	A
	2020-05-10 00:00:59	A35550	361	Scheduler: Scheduled task initiated. (schedule: GeneratePersistentAl)	A

Cancel

*** ถ้าเครื่องหมายด้านหน้า เป็น 

ให้ไปตรวจสอบว่าเป็นเหตุการณ์ที่เกิดวันไหน เวลาอะไร โดยวันและเวลาจะอยู่ด้านขวามือของเครื่องหมายดังกล่าว และเกิดเหตุการณ์อะไรขึ้น หากสามารถแก้ไขเบื้องต้นได้ ให้ทำการแก้ไขโดยทันที หรือหากแก้ไขเบื้องต้นไม่ได้ ให้ทำการโทรแจ้งบริษัทฯ ***

3.9.9 หลังจากการตรวจสอบสถานะ , ดำเนินการแก้ไข หรือประสานงานกับบริษัทที่ดูแล เรียบร้อยแล้ว ให้ทำการบันทึกข้อมูลเพื่อเก็บเป็นรายงานต่อไป

กรณีศึกษา

1.Switch Uplink ที่อาคารคณะพยาบาลศาสตร์เกื้อการุณย์ ชั้น M Down ทุกสัปดาห์

วันที่ตรวจพบ	ระบบแจ้งเตือน (cacti)
เหตุการณ์	Switch Uplink ที่อาคารคณะพยาบาลศาสตร์เกื้อการุณย์ ชั้น M (ห้อง Data Center ไปยัง ชั้น M) Down ทุกสัปดาห์
สาหตุ.	ไฟฟ้าตก/ไฟกระชาก
ผลกระทบ	อุปกรณ์เสี่ยงต่อการชำรุด และการให้บริการไม่ต่อเนื่อง
วิธีการแก้ไขเบื้องต้น	เปลี่ยน UPS ที่รองรับ switch / เปลี่ยนแบตเตอรี่
แผนแก้ไขระยะยาว	วางแผนตรวจเช็คการทำงานของ UPS ที่รองรับ switch

2.Switch ที่ให้บริการชั้น 5 ไม่ทำงาน

วันที่ตรวจพบ	23 สิงหาคม 2564 เวลา 8.30 น
เหตุการณ์	Switch ที่ให้บริการชั้น 5 อาคารคณะพยาบาลศาสตร์เกื้อการุณย์ down
สาหตุ.	port ที่รองรับ uplink ไปยัง switch ชั้น 5 (ชั้น M ไปยัง ชั้น5) เกิดการชำรุด
ผลกระทบ	เครือข่ายของอาคารคณะพยาบาลศาสตร์เกื้อการุณย์ ชั้น 4-6 ไม่สามารถใช้งานได้
วิธีการแก้ไขเบื้องต้น	ทำการแก้ไข config switch ย้าย port ไปใช้งาน port อื่นแทน
แผนแก้ไขระยะยาว	วางแผนจัดซื้ออุปกรณ์ switch ที่มารองรับ uplink ใหม่เนื่องจากอุปกรณ์เสื่อมสภาพ

3.อุณหภูมิของอุปกรณ์ภายในห้อง server ที่ชั้น 3 อาคารการุณยสภา มีอุณหภูมิสูงกว่าปกติ

วันที่ตรวจพบ	5 กรกฎาคม 2567 เวลา 8.30 น
เหตุการณ์	อุณหภูมิของอุปกรณ์ภายในห้อง server ที่ชั้น 3 อาคารการณยสภา
สาหตุ.	เครื่องปรับอากาศภายในห้องชำรุด
ผลกระทบ	อุปกรณ์มีอุณหภูมิสูงทำให้เสี่ยงต่อการชำรุด
วิธีการแก้ไขเบื้องต้น	ใช้งานแอร์ของอาคาร และเปิดพัดลมภายในห้อง เพื่อช่วยลดอุณหภูมิ
แผนแก้ไขระยะยาว	เขียนโครงการปรับปรุงห้อง Data Center ของคณะฯใหม่ ให้ได้มาตรฐาน

บทที่ 4

ปัญหา อุปสรรคและแนวทางแก้ไข

การจัดทำคู่มือปฏิบัติงานการตรวจสอบและเฝ้าระวังระบบเครือข่ายคอมพิวเตอร์ เพื่อเป็นแนวทางให้ผู้ปฏิบัติงานได้รับความรู้ ความเข้าใจ หลักเกณฑ์ ขั้นตอน และวิธีการปฏิบัติงาน โดยมักพบปัญหาและอุปสรรคในการดำเนินการ ดังรายละเอียดต่อไปนี้

ปัญหาอุปสรรคในการปฏิบัติงาน	แนวทางแก้ไขเบื้องต้น	แนวทางการพัฒนางาน
Port ของ switch มีปัญหา / ชำรุด	ทำการแก้ไข config ของอุปกรณ์ เพื่อเปลี่ยนไปใช้งานบน port ที่ยังสามารถใช้งานได้(กรณี port ยังว่าง)	จัดทำแผนเพื่อของบประมาณจัดซื้อ Switch สำรอง และมีการ Backup Config ของ Switch เดิมไว้ด้วย
มีการดับไฟฟ้าโดยไม่แจ้งล่วงหน้า / ไฟฟ้ากระชากทำให้อุปกรณ์ชำรุด	1.เร่งทำการปิดอุปกรณ์ที่มี UPS รองรับอยู่โดยเร็วก่อนที่ไฟฟ้าสำรองจะหมด 2.ทำการติดต่อประสานงานกับทางสำนักคณบดี/ช่างระบบ เพื่อขอความร่วมมือให้มีการแจ้งล่วงหน้ากรณีที่มีการดับไฟฟ้า	1.จัดทำแผนรับมือกรณีไฟฟ้าดับฉุกเฉิน 2.ทำการของบเพื่อติดตั้ง UPS เพื่อสำรองไฟฟ้าให้อุปกรณ์สำคัญ ทุกจุดเพื่อให้สามารถทำงานได้กรณีไฟฟ้าดับกระทันหัน 3.ทำเรื่องเพื่อเชื่อมต่อ line ไฟฟ้าเข้ากับเครื่องปั่นไฟฟ้าของอาคารเพื่อรองรับกรณีไฟดับ
สายสัญญาณที่เชื่อมต่อระหว่างคณะพยาบาลฯ และมหาวิทยาลัย/คณะแพทย์ฯ โดนตัด ทำให้ใช้งานระบบต่างๆ ของทางมหาวิทยาลัยไม่ได้	1.แก้ไขปัญหาโดยการใช้งาน VPN ของทาง มหาวิทยาลัยเพื่อใช้งานก่อนระหว่างรอเชื่อมสาย fiber (กรณีมี internet backup ปัจจุบันไม่มีแล้วจากนโยบายยกเลิก internet หน่วยงาน)	1.ใช้งานสายสื่อสารใต้ดินเพื่อเชื่อมจากคณะพยาบาลฯ ไปยังมหาวิทยาลัย/คณะแพทย์ แทนการเดินสายแบบเดิม 2.ทำการของบประมาณเพื่อติดตั้ง Internet สำรองสำหรับรองรับในกรณีฉุกเฉิน

ปัญหาอุปสรรคในการปฏิบัติงาน	แนวทางแก้ไขเบื้องต้น	แนวทางการพัฒนางาน
เครื่อง Server มีอุณหภูมิที่สูงเกินกว่าค่ามาตรฐาน เนื่องจาก เครื่องปรับอากาศในห้องชำรุด	1.แจ้งฝ่ายอาคารให้เข้ามาแก้ไขเครื่องปรับอากาศให้สามารถใช้งานได้ 2.เปิดพัดลม เพื่อช่วยให้อากาศถ่ายเทได้ดีขึ้น ช่วยลดอุณหภูมิได้	1.ทำการเขียนโครงการเพื่อปรับปรุงห้อง Data Center ให้ได้มาตรฐาน เพื่อลดปัญหาในระยะยาว และเพิ่มความปลอดภัย
หม้อแปลงไฟฟ้าระเบิด ทำให้ไฟฟ้าดับกระทันหัน	1.เร่งทำการปิดอุปกรณ์ที่มี UPS รองรับอยู่โดยเร็วก่อนที่ไฟฟ้าสำรองจะหมด	1.ทำเรื่องเพื่อเชื่อมต่อ line ไฟฟ้าเข้ากับเครื่องปั่นไฟฟ้าของอาคารเพื่อรองรับกรณีไฟดับ
Traffic เกิดการใช้งานมากเกินกว่าปกติ เนื่องจากเกิด loop ใน unmanaged switch ที่ต่อพ่วงที่หน้างาน เนื่องจากมีการย้ายอุปกรณ์และต่อสายผิด	1.ถอดอุปกรณ์ที่ไม่ได้รับอนุญาตออกจากระบบ 2.เปิด function spanning tree protocol (STP) ของ switch L2 (หาก switch รองรับ)	1.ทำแผนของบประมาณเพื่อเปลี่ยน switch ให้เป็น switch L2 ทั้งหมด เพื่อลดปัญหา 2.แจ้งนโยบายแก่ส่วนงานต่างๆ หากจำเป็นต้องทำการย้ายอุปกรณ์เครือข่ายให้ทำเรื่องแจ้งทางงานเทคโนโลยีสารสนเทศก่อน
ระบบต่างๆรวมไปถึงอุปกรณ์ที่ต่อพ่วงไม่สามารถ Authen กับทาง server ของคณะฯได้ เนื่องจากมีการนำอุปกรณ์ภายนอก (router) เข้ามาต่อพ่วง ทำให้เกิด DHCP ซ้อนทับกัน	1.ทำการกำหนดค่า Port บน switch ทุกตัวให้แจกตาม VLAN ที่กำหนด และหากเป็นอุปกรณ์ของคณะให้ทำการ FIX IP ของอุปกรณ์ปลายทางไว้ด้วยเพื่อห้องกันปัญหาดังกล่าว	1.ทำแผนของบประมาณเพื่อเปลี่ยน switch ให้เป็น switch L2 ทั้งหมด เพื่อลดปัญหา 2.แจ้งนโยบายแก่ส่วนงานต่างๆ ว่าห้ามนำอุปกรณ์ภายนอกเข้ามาต่อพ่วงกับเครือข่ายของคณะฯ

บทที่ 5

ข้อเสนอแนะ

ในการดูแลระบบเครือข่ายจำเป็นต้องมีการดูแลอย่างสม่ำเสมอ รวมไปถึงเฝ้าระวังภัยคุกคามจากภายนอก อีกทั้งยังจำเป็นต้องแก้ไขปัญหาอย่างรวดเร็ว และทันท่วงที เพื่อการให้บริการสารสนเทศเป็นไปอย่างที่ต่อเนื่อง การจัดทำคู่มือปฏิบัติงานการตรวจสอบและเฝ้าระวังระบบเครือข่ายคอมพิวเตอร์จะเป็นประโยชน์ต่อการปฏิบัติงานหรือสำหรับผู้สนใจศึกษาการตรวจสอบและเฝ้าระวังระบบเครือข่ายคอมพิวเตอร์ และสามารถพัฒนางานควบคู่ไปกับการบริหารจัดการของคณะพยาบาลศาสตร์เกื้อการุณย์ต่อไป

จากกรณีศึกษาจะเห็นว่าอุปกรณ์มีการชำรุดเกิดขึ้น เนื่องจากความไม่เสถียรของกระแสไฟฟ้าที่จ่ายให้กับอุปกรณ์ เบื้องต้นแนะนำให้ทำการเปลี่ยน port เพื่อให้สามารถกลับมาทำงานได้ก่อน โดยวิธีแก้ไขในระยะยาว คือการใช้งบประมาณในการซื้ออุปกรณ์สำรองไฟฟ้า (UPS) ขนาดที่เหมาะสม เพื่อทำการต่อพ่วง เพื่อลดการกระชากของกระแสไฟฟ้าที่มาจากตัวอาคาร รวมไปถึงสำรองไฟในกรณีกระแสไฟฟ้าของอาคารดับ ทั้งนี้ควรต้องจัดทำแผนการทดสอบดับไฟฟ้าห้อง Server รวมไปถึงตู้ rack Uplink ทุกๆจุด ที่ติดตั้ง UPS เพื่อทดสอบประสิทธิภาพของ UPS ที่ใช้งาน ว่า Battery มีการชำรุด หรือเสื่อมสภาพไปแค่ไหนแล้ว และทำแผนการดำเนินการจัดซื้อ Battery ทดแทนทุกๆ 2-3 ปี เพื่อให้ UPS สามารถสำรองไฟฟ้าได้อย่างมีประสิทธิภาพ

อีกทั้งปัจจุบันห้อง Server ที่ทำการรองรับอุปกรณ์เครือข่ายของคณะพยาบาลศาสตร์เกื้อการุณย์ยังไม่ได้มาตรฐาน ผู้จัดทำคู่มือนี้มีความเห็นว่าควรที่จะปรับปรุงห้อง Server ของคณะพยาบาลศาสตร์เกื้อการุณย์ให้ได้ตามมาตรฐาน ISO27001 เพื่อให้สอดคล้องกับนโยบายเกี่ยวกับงานเทคโนโลยีสารสนเทศ ของทางมหาวิทยาลัยนวมินทราธิราช และเพื่อความปลอดภัยของข้อมูลและความต่อเนื่องของการให้บริการสารสนเทศของทางคณพยาบาลศาสตร์เกื้อการุณย์

ภาคผนวก

รายการอุปกรณ์เครือข่ายคอมพิวเตอร์

รายการอุปกรณ์	ชื่อ	IP address / URL
อุปกรณ์ป้องกันเครือข่าย (Firewall) ยี่ห้อ Fortigate รุ่น 500E	KCN-Firewall	10.1.0.2
อุปกรณ์ป้องกันเครือข่าย (Firewall) ยี่ห้อ Fortigate รุ่น 1000C	Server Zone-Firewall	10.1.0.6
อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย ยี่ห้อ Fortianalyzer รุ่น 1000E	KCN-LOG	192.168.121.239
อุปกรณ์กระจายสัญญาณ (L3 Switch) ยี่ห้อ Cisco รุ่น Catalyst-3850	C3850-Core	10.1.1.254
อุปกรณ์กระจายสัญญาณ (L2 Switch) ยี่ห้อ Cisco รุ่น SG-200	SG200-SW1-1	10.1.1.1
	SG200-SW1-2	10.1.1.2
	SG200-SW1-3	10.1.1.3
	SG200-SW1-4	10.1.1.4
	SG200-SW2-1	10.1.1.6
	SG200-SW2-2	10.1.1.7
	SG200-SW2-3	10.1.1.8
	SG200-SW2-4	10.1.1.9
	SG200-SW2-5	10.1.1.10
	SG200-SW-Server01	30.30.30.11
	SG200-SW-Server02	30.30.30.12
	SG200-SW3-1	10.1.1.13
	SG200-SW3-1	10.1.1.14
	SG200-SW3-1	10.1.1.15
	SG200-SW12-1	10.1.1.16
	SG200-SW12-2	10.1.1.17
	SG200-SW12-3	10.1.1.18
	SG200-SW20-2	10.1.1.20
	SG200-SWB2-2	10.1.1.25
	SG200 -SW5-1	10.1.1.36

รายการอุปกรณ์	ชื่อ	IP address / URL
อุปกรณ์กระจายสัญญาณ (L2 Switch) ยี่ห้อ Cisco รุ่น SG-220	SG220-SW20-1	10.1.1.19
	SG220-SWB6-5-1	10.1.1.23
	SG220-SWB3-1	10.1.1.26
อุปกรณ์กระจายสัญญาณ (L2 Switch) ยี่ห้อ Cisco รุ่น Catalyst-2960X	C2960-X-SWB6-M-1	10.1.1.21
	C2960-X-SWB2-1	10.1.1.24
อุปกรณ์กระจายสัญญาณ (L2 Switch) ยี่ห้อ Cisco รุ่น Catalyst-2960S	C2960-S-SW1-5	10.1.1.5
อุปกรณ์กระจายสัญญาณ (L2 Switch) ยี่ห้อ DCN รุ่น S4200	DCN01-KarunFL2-SW002	10.1.1.49
	DCN01-KarunFL2-SW003	10.1.1.43
	DCN01-KarunFL2-SW004	10.1.1.44
	DCN01-KarunFL2-SW005	10.1.1.45
	DCN01-KarunFL2-SW006	10.1.1.46
	DCN01-KarunFL2-SW007	10.1.1.47
	DCN01-KarunFL2-SW008	10.1.1.48
เครื่องคอมพิวเตอร์แม่ข่าย ยี่ห้อ Dell รุ่น PowerEdge R730	KCN-Server01P	192.168.120.246
	KCN-Server02P	192.168.120.247
	KCN-Server03P	192.168.120.248
อุปกรณ์จัดเก็บข้อมูลแบบภายนอก ยี่ห้อ HP รุ่น MSA 1040 SAN	KFN-SAN01	192.168.120.213
		192.168.120.214

ตารางรายการตรวจสอบการทำงานของระบบเครือข่ายสารสนเทศ

คณะพยาบาลศาสตร์เกื้อการุณย์ มหาวิทยาลัยนวมินทราธิราช

11 เมษายน 2567

Task List	Start Time	End Time	Pass	Not Pass	Comment
สถานะการทำงานของอุปกรณ์เครื่องแม่ข่าย Dell PowereEdge R730 (KFN-ESXi01)					
- Hardware Status (CPU, Memory, Disk, Fan, Power Supply)	9:00 น.	9:05 น.	✓		
สถานะการทำงานของอุปกรณ์เครื่องแม่ข่าย Dell PowereEdge R730 (KFN-ESXi02)					
- Hardware Status (CPU, Memory, Disk, Fan, Power Supply)	9:05 น.	9:10 น.	✓		
สถานะการทำงานของอุปกรณ์เครื่องแม่ข่าย Dell PowereEdge R730 (KFN-ESXi03)					
- Hardware Status (CPU, Memory, Disk, Fan, Power Supply)	9:10 น.	9:15 น.	✓		
สถานะการทำงานของอุปกรณ์จัดเก็บข้อมูล HP MSA 1040 SAN					
- Hardware Status (Disk, Controller, Fan, Power Supply)	9:15 น.	9:20 น.	✓		
สถานะการทำงานของอุปกรณ์เครือข่าย C3850-Core (Core Network)	9:20 น.	9:25 น.	✓		
สถานะการทำงานของอุปกรณ์เครือข่าย C2960-S-SW1-5 (Uplink DC)	9:25 น.	9:30 น.	✓		
สถานะการทำงานของอุปกรณ์เครือข่าย SG200-SW12-3 (Uplink หอพักชั้น 12)	9:30 น.	9:35 น.	✓		
สถานะการทำงานของอุปกรณ์เครือข่าย SG200-SW20-2 (Uplink หอพักชั้น 16)	9:35 น.	9:40 น.	✓		
สถานะการทำงานของอุปกรณ์เครือข่าย C2960-X-SWB6-M-1 (Uplink อาคาร 6 ชั้น)	9:40 น.	9:45 น.	✓		
สถานะการทำงานของอุปกรณ์เครือข่าย SG200-SWB3-1 (Uplink อาคาร 3)	9:45 น.	9:50 น.	✓		
สถานะการทำงานของอุปกรณ์เครือข่าย C2960-X-SWB2-1 (Uplink อาคาร 2)	9:50 น.	9:55 น.	✓		
สถานะการทำงานของอุปกรณ์เครือข่ายไร้สาย (KCN-WLC5508)	9:55 น.	10:00 น.	✓		
สถานะการทำงานของอุปกรณ์เครือข่าย SG-220-KarunFL2-SW001 (Uplink ชั้น 2)	10:00 น.	10:05 น.	✓		
สถานะการทำงานของอุปกรณ์รักษาความปลอดภัย (KCN-Firewall)					
- Access to Internet	10:05 น.	10:10 น.	✓		
สถานะการทำงานของอุปกรณ์รักษาความปลอดภัย (Server Zone-Firewall)					
- Status Hardware	10:10 น.	10:15 น.	✓		
สถานะการทำงานของอุปกรณ์จัดเก็บ Log (KCN-LOG)					
- Keep Log Realtime	10:15 น.	10:20 น.	✓		
สถานะการทำงานของระบบ www.kcn.ac.th	10:20 น.	10:25 น.	✓		
สถานะการทำงานของระบบ network monitor	10:25 น.	10:30 น.	✓		
สถานะการทำงานของระบบ Intranet	10:30 น.	10:35 น.	✓		
สถานะการทำงานของระบบ Grade	10:35 น.	10:40 น.	✓		
สถานะการทำงานของระบบ RADIUS	10:40 น.	10:45 น.	✓		
สถานะการทำงานของระบบ ห้องสมุด	10:45 น.	10:50 น.	✓		
สถานะการทำงานของระบบ Backup01	10:50 น.	10:55 น.	✓		
สถานะการทำงานของระบบ Backup02	10:55 น.	11:00 น.	✓		
สถานะการทำงานของระบบ Shared File	11:00 น.	11:05 น.	✓		

Switch	Pass	Not Pass	Uptime			Comment
C3850-Core (10.1.1.254)///(Core1+Core2)	✓		0 D	0 H	46 M	**
SG200-SW1-1 (10.1.1.1)	✓		0 D	0 H	51 M	**
SG200-SW1-2 (10.1.1.2)	✓		0 D	0 H	56 M	**
SG200-SW1-3 (10.1.1.3)	✓		0 D	1 H	1 M	**
SG200-SW1-4 (10.1.1.4)	✓		0 D	1 H	6 M	**
C2960-S-SW1-5 (10.1.1.5)	✓		0 D	1 H	11 M	**
SG200-SW2-1 (10.1.1.6)	✓		0 D	1 H	16 M	**
SG200-SW2-2 (10.1.1.7)	✓		0 D	1 H	21 M	**
SG200-SW2-3 (10.1.1.8)	✓		0 D	1 H	26 M	**
SG200-SW2-4 (10.1.1.9)	✓		0 D	1 H	31 M	**
SG200-SW2-5 (10.1.1.10)	✓		0 D	1 H	36 M	**
SG200-SW-Server01 (30.30.30.11)	✓		0 D	1 H	41 M	**
SG200-SW-Server02 (30.30.30.12)	✓		0 D	1 H	46 M	**
SG200-SW3-1 (10.1.1.13)	✓		0 D	1 H	51 M	**
SG200-SW3-2 (10.1.1.14)	✓		0 D	1 H	56 M	**
SG200-SW3-3 (10.1.1.15)	✓		0 D	2 H	1 M	**
SG200-SW12-1 (10.1.1.16)	✓		0 D	0 H	0 M	*** อยู่ระหว่างปรับปรุงหอพัก
SG200-SW12-2 (10.1.1.17)	✓		0 D	0 H	0 M	*** อยู่ระหว่างปรับปรุงหอพัก
SG200-SW12-3 (10.1.1.18)	✓		0 D	2 H	6 M	**
SG200-SW20-2 (10.1.1.20)	✓		0 D	2 H	11 M	**
C2960-X-SWB6-M-1 (10.1.1.21)	✓		0 D	2 H	16 M	**
SG220-SWB6-5-1 (10.1.1.23)	✓		0 D	2 H	21 M	**
C2960-X-SWB2-1 (10.1.1.24)	✓		0 D	2 H	26 M	**
SG200-SWB2-2 (10.1.1.25)	✓		0 D	2 H	31 M	**
SG220-SWB3-1 (10.1.1.26)	✓		0 D	2 H	36 M	**
SG200-SW5-1 (10.1.1.36)	✓		0 D	2 H	41 M	**
SG220-KarunFL2-SW001 (10.1.1.42)	✓		0 D	2 H	46 M	**
DCNS4200-KarunFL2-SW002 (10.1.1.49)	✓		0 D	2 H	51 M	**
DCNS4200-KarunFL2-SW003 (10.1.1.43)	✓		0 D	2 H	56 M	**
DCNS4200-KarunFL2-SW004 (10.1.1.44)	✓		0 D	3 H	1 M	**
DCNS4200-KarunFL2-SW005 (10.1.1.45)	✓		0 D	3 H	6 M	**
DCNS4200-KarunFL2-SW006 (10.1.1.46)	✓		0 D	3 H	11 M	**
DCNS4200-KarunFL2-SW007 (10.1.1.47)	✓		0 D	3 H	16 M	**
DCNS4200-KarunFL2-SW008 (10.1.1.48)	✓		0 D	3 H	21 M	**
						** มีเหตุไฟฟ้ากระชาก 2 รอบวันที่ 14-02-66 เวลาประมาณ 7.30 น.

Checklist	Power		Event Log		Service		Comment
	Pass	Not Pass	Pass	Not Pass	Pass	Not Pass	
Server							
DELL PowerEdge R730 KCN-Server01P (192.168.120.246)	✓		✓		✓		
DELL PowerEdge R730 KCN-Server02P (192.168.120.247)	✓		✓		✓		
DELL PowerEdge R730 KCN-Server03P (192.168.120.248)	✓		✓		✓		
IBM BladeCenter E chassis (192.168.120.125)	✓		✓		✓		
IBM Blade Server Enclosure HS22 (192.168.120.222)	✓		✓		✓		
IBM Blade Server Enclosure HS22 (192.168.120.232)	✓		✓		✓		
Virtual Machine							
VMware vSphere 6 Standard KPN-EXSi01 (192.168.120.241)	✓		✓		✓		
VMware vSphere 6 Standard KPN-EXSi02 (192.168.120.242)	✓		✓		✓		
VMware vSphere 6 Standard KPN-EXSi03 (192.168.120.243)	✓		✓		✓		
VMware vCenter 6 Foundation KPN-VC (192.168.120.240)	✓		✓		✓		
Security and Storage							
HPE MSA1040 KPN-SAN01 (192.168.120.213,192.168.120.214)	✓		✓		✓		Storage A : Allocated 1239.4 GB : Unallocated 1610.5 GB : Total 14.4 TB Storage B : Allocated 5485.9 GB : Unallocated 2706.0 GB : Total 14.4 TB Overall : Reserved 4829.6 GB : Allocated 6725.3 GB : Unallocated 4316.5 GB : Uncommitted 12.9 TB : **Total 28.8 TB**
Fortianalyzer 1000E (192.168.121.239)	✓		✓		✓		**Storage Used 5% : Total 6 TB**
Back-Up System (10.1.2.42:Windows 10 Remote Desktop)	✓		✓		✓		
Fortigate 1000C (10.1.0.6)	✓		✓		✓		
Fortigate 500E (10.1.0.2)	✓		✓		✓		

ลงชื่อเจ้าหน้าที่ผู้ตรวจสอบ

(นาย ศวิชย์ ชานวิทิตกุล)

นักวิชาการคอมพิวเตอร์ปฏิบัติการ

11 เมษายน 2567