กระบวนการในการสำรองและกู้คืนข้อมูล
(Backup and Recovery Procedures)

ศูนย์เทคโนโลยีสารสนเทศ
โรงพยาบาลน่าน

กระบวนการในการสำรองและกู้คืนข้อมูล
(Backup and Recovery Procedures)

ศูนย์เทคโนโลยีสารสนเทศ
โรงพยาบาลน่าน

กระบวนการในการสำรองและกู้คืนข้อมูล
(Backup and Recovery Procedures)
ศูนย์เทคโนโลยีสารสนเทศ

เพื่อให้การดำเนินงานด้านการบำรุงรักษาระบบฐานข้อมูลต่าง ๆ ที่ ศูนย์เทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการพัฒนา หรือการให้การบริการด้านฐานข้อมูลที่เกี่ยวข้องกับหน่วยงานต่าง ๆ เป็นไปอย่างมีประสิทธิภาพและสอดคล้องกับการบริหารจัดการของศูนย์ปฏิบัติการสารสนเทศของโรงพยาบาลน่าน ในประเด็นระบบการบริหารความเสี่ยงของระบบสารสนเทศและเป็นคู่มือในการปฏิบัติตามขั้นตอนต่าง ๆ โดยสรุปในหัวข้อต่าง ๆ ดังนี้

1. **การฟื้นฟูระบบ/ข้อมูลจากความเสียหาย** (Recovery) เพื่อให้การฟื้นฟูระบบ/ข้อมูลจากความเสียหายที่อาจเกิดขึ้นจากการหยุดทำงานของการประมวลผลโปรแกรม (Hang) หรือไฟฟ้าดับตลอดจนเหตุการณ์อื่นใดซึ่งส่งผลต่อเครื่องคอมพิวเตอร์ หรือการประมวลผลของคอมพิวเตอร์หยุดทำงานอย่างกะทันหัน หรือเปลี่ยนการทำงานไปจากเดิม ทำให้ไม่สามารถบันทึกข้อมูลได้ทันเวลา หรือไม่สามารถใช้งานคอมพิวเตอร์ได้ตามปกติ โรงพยาบาลน่านมีมาตรการในการกู้คืนข้อมูล ดังนี้

1. ผู้ใช้งานจะต้องเปิดใช้งานการกู้คืน (Recovery) ของระบบปฏิบัติการตลอดเวลา
2. เจ้าหน้าที่ผู้รับผิดชอบจะต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และการติดตั้งซอฟท์แวร์ใหม่ เพื่อทดแทนของเดิมที่เสียหาย
3. เจ้าหน้าที่ผู้รับผิดชอบจะต้องทำการบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์สนับสนุนเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ

2. **การสำรองข้อมูล** (Back up) เพื่อลดความเสี่ยงจากที่เกิดขึ้นกับข้อมูล และสามารถนำข้อมูลกลับมาใช้งานได้ ในกรณีที่ฮาร์ดดิสก์เสียหาย ไวรัสคอมพิวเตอร์ทำลายข้อมูล ผู้บุกรุกทำการลบข้อมูลหรือเปลี่ยนแปลงข้อมูล การเผลอลบข้อมูลหรือเปลี่ยนแปลงข้อมูลโดยผู้ใช้งานเองโดยมีมาตรการ ดังนี้

1. เจ้าหน้าที่ผู้รับผิดชอบจะต้องตั้งค่าระบบให้มีสำรองข้อมูลโดยอัตโนมัติ หรือทำการสำรองข้อมูลของระบบซึ่งอยู่ในความรับผิดชอบของตนเองตามความเหมาะสมของแต่ละระบบ แต่ไม่ต่ำกว่า 1 ครั้งต่อเดือน
2. เจ้าหน้าที่ผู้รับผิดชอบเครื่องคอมพิวเตอร์แม่ข่ายของเว็บไซต์ (Web server) จะต้องตั้งค่าระบบให้มีสำรองข้อมูลอัตโนมัติ
3. ผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไป จะต้องทำการสำรองข้อมูลในเครื่องคอมพิวเตอร์ของตนเองตามความเหมาะสม แต่ละไม่ตำกว่า 1 ครั้งต่อเดือน
4. เมื่อทางโรงพยาบาลน่านประกาศให้มีการสำรองข้อมูลเนื่องจากจะได้มีการดำเนินการที่อาจส่งผลต่อข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้ ผู้ใช้จะต้องทำการสำรองข้อมูลดังกล่าวภายในระยะเวลาที่กำหนด
5. หากผู้ดูแลระบบหรือผู้ใช้งานเครื่องคอมพิวเตอร์เห็นว่าข้อมูลใดเป็นข้อมูลสำคัญให้พิมพ์ (Print) ออกมาเก็บสำรองไว้ในรูปของเอกสารกระดาษ (Hard Copy)
6. เจ้าหน้าที่ผู้รับผิดชอบเครื่องคอมพิวเตอร์แม่ข่ายและผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไปจะต้องมีการทำสอบความถูกต้องของข้อมูลสำรองและการรายงานผลการตรวจสอบเป็นครั้งคราว ทั้งนี้ขึ้นอยู่กับความสำคัญของข้อมูลในแต่ละระบบฐานข้อมูล หรือของผู้ใช้งานเครื่องคอมพิวเตอร์นั้น ๆ

ขั้นตอนของการทำ backups (Backup Procedures)

ขั้นตอนการทำ backups จะบอกให้ทราบว่า มีสิ่งใดบ้างที่จะต้องทำ backup จะต้องทำเมื่อใดและทำอย่างไร บอกถึงความถี่ของการทำ backups และบอกถึงที่เก็บ copies ของ backups นั้นๆ อย่าง

ที่เราได้กล่าวมาแล้วในตอนต้นว่า คุณลักษณะของ application จะเป็นปัจจัยสำคัญที่มีผลต่อการเลือกกระทำแต่ละอย่างเหล่านี้ เรามาดูกันในรายละเอียดในแต่ละกรณีต่อไปนี้

การกำหนดสถานที่เก็บสำเนาของ backups (Disposition of Backup Copies)

ขั้นตอนของการทำ backups ที่ครอบคลุมจะเป็นหลักประกันให้มั่นใจว่าเราจะมี copies ของ backups จำนวนมากอยู่ในมือพร้อมที่จะใช้งานได้เสมอ และทำให้เรามั่นใจว่ามี copies ที่สมบูรณ์ถูกเก็บรักษาอยู่ในสถานที่ต่างกันอย่างน้อย 2 แห่ง โดยปกติแล้วการแยกเก็บในสถานที่ต่างกันมิได้หมายความว่าอยู่ในห้องติดกัน แต่มันหมายความว่าอยู่ในสื่อเก็บของสถานีอื่น (offsite storage) หรือสถานที่ที่คล้ายกันนี้ ในการติดตั้งบางแห่งจะเก็บ backups ไว้ในห้องใต้ถุนกันไฟ วิธีนี้ไม่ใช่วิธีการเก็บแบบ off-site ที่ให้ผลดีตลอดไปเพราะว่าภัยพิบัติอย่างเช่นการเกิดน้ำท่วมและการระเบิดยังคงสามารถทำความเสียหายให้แก่ backup copies ได้

จุดประสงค์ของการเก็บ backup copies ไว้ที่ site อื่น คือ ช่วยให้สามารถกู้สภาพข้อมูลจากความหายนะได้ ซึ่งเป็นความหายนะที่อาจจะทำลายได้ทั้ง data ของคอมพิวเตอร์และ backup copies ที่เก็บอยู่ ณ ที่สถานีของตนเอง (onsite)

การมี backups จำนวนหลาย copies อาจทำขึ้นด้วยจุดประสงค์อื่นๆ อีก นั่นคือ สื่อ(medium)ที่ใช้เก็บ backup อาจเสื่อมสภาพซึ่งจะส่งผลให้ backup นั้นใช้การไม่ได้ ตัวอย่างเช่นbackups ที่เก็บด้วย magnetic tape อาจเกิดรอยครูด ยืด ฉีกขาด หรือเสียหายเนื่องจากอิทธิพลของสนามแม่เหล็กสภาพแวดล้อมดังกล่าวนี้สามารถทำให้ tape ใช้การไม่ได้ นอกจากนี้ เมื่อเวลาทำ backup ควรจะทำอย่างมีขั้นตอนเพื่อให้มั่นใจว่าสามารถไว้วางใจใน backup นั้นได้ และ software ที่ใช้ทำ backup นั้นอาจต้องมี read-after-write function เพื่อใช้ check ดูว่า data ที่ถูก write ลงไปนั้นสามารถอ่านออกมาได้หรือไม่ การตรวจสอบเพื่อความไว้วางใจอีกประการหนึ่งคือการทำการกู้สภาพเป็นระยะๆ ให้กับ data ที่ถูกทำเป็น backup โดยใช้หน่วยขับสำหรับทดสอบ(test drive) เพื่อตรวจสอบดูความน่าเชื่อถือของสื่อที่ใช้ทำ backup และ hardware ในการกู้สภาพเช่นนี้สิ่งที่ดีที่สุด คือ ทำการกู้สภาพโดยใช้ tape drive ต่างชุดกับ tape drive ที่ใช้ทำbackup นั้น การทำเช่นนี้เป็นการตรวจสอบความสามารถในการทำงานของ drives ทั้งสอง และเป็นการป้องกันไว้เผื่อว่า drive ที่ใช้ทำ backup นั้นเกิดทำงานผิดปกติขึ้นมา การมี backup ของ backup อีกทีจะช่วยให้เรามีทางเลือกสำหรับการทำ recovery อีกทางหนึ่ง การมี backups หลายๆ รุ่นก็ถือว่าเป็นสิ่งสำคัญเช่นกัน มีข้อคิดหนึ่งของการทำ backup ที่กล่าวไว้ว่า“จงอย่านำ backup media ของท่านกลับมาใช้ในทันที” นั่นคือ สมมุติว่าท่านตัดสินใจที่จะใช้ tape เพียงม้วนเดียวในการทำ backup หลายครั้ง สมมุติต่อไปอีกว่า การทำ backup นั้นต้องใช้ความยาว tape ตลอดทั้งม้วนท่านลองคิดดูซิว่าอะไรจะเกิดขึ้นถ้าเกิดความล้มเหลวในระหว่างที่ท่านกำลังทำ backup อยู่ คำตอบก็คือ backup ที่กำลังทำอยู่นั้นจะไม่จบสมบูรณ์ และ backup ก่อนหน้านี้จะถูกเขียนทับโดย backup ที่กำลังทำอยู่นั้น ดังนั้นจึงทำให้ไม่มี backup ที่สมบูรณ์เหลือไว้ให้ท่านใช้งาน

การเก็บรักษาประวัติหรือ backups ไว้หลายๆรุ่นเรียกว่า retention policy บางทีนโยบายการทำ backups (backup policy) ที่ยากที่สุดที่ผู้เป็น LAN administrator จะต้องตัดสินใจคือ จะเก็บรักษา backups นั้นไว้นานสักเท่าใด การทำ backups นั้นจะมีการทำเป็น 3 รุ่นในลักษณะ ปู่-พ่อ-ลูก (grandfather-father-son method) เมื่อมีการสร้าง backup รุ่นหลาน (grandson backup) ขึ้นมาเมื่อใด ตัว grandfather backup ก็จะถูก recycled โดยจะถูกนำออกมาวางเพื่อรอการทำ backup ใหม่ต่อไป ตัว backup ที่เป็น father ก็จะผันตัวเองขึ้นเป็น grandfather แทนและการผันตัวเองเช่นนี้ก็จะตก

ทอดต่อไปสู่ son เช่นกัน ขอให้สังเกตว่าจะต้องมี tapes จำนวน 4 ม้วนในการรักษาลักษณะการทำ backup 3 รุ่น ในการติดตั้งใช้งานบางแห่งการทำเช่นนี้อาจจะเพียงพอ แต่บริษัทส่วนใหญ่ในปัจจุบันจะมีนโยบายในการเก็บรักษาที่ครอบคลุมกว้างขวางกว่านี้การพิจารณาข้อดีข้อเสียในการกำหนดนโยบายการเก็บรักษาจะอาศัยพิจารณาจากสิ่งเหล่านี้เป็นหลักคือสภาพข้อมูลของสถานที่ตั้งแห่งนั้น หรือ ความจำเป็นในการกู้คืนสภาพข้อมูล

ท่านอาจจะมองว่าความสามารถในการครอบคลุมเนื้อหาได้ทุกแง่มุม (comprehensiveness) ของbackup ข้อหนึ่งนั้นคือ ระดับความเป็นจริง (exactness) ของ data ที่ backup นั้นแสดงให้เห็น backup ที่มี comprehensiveness ต่ำ เช่น backup ที่มีความเก่าแก่ถึง 1 ปี จะมีลักษณะความคล้ายคลึงกับสถานะของ data ในปัจจุบันน้อยมาก สำหรับ backup ที่มี comprehensiveness ที่ดี เช่น backup ที่เพิ่งสร้างเสร็จมีอายุเพียงไม่กี่นาที จะมีความใกล้เคียงกับสถานะของ data ในปัจจุบันมาก ลักษณะของ comprehensiveness จะมีมากน้อยเพียงใดนั้น ขึ้นอยู่กับอายุของ backup และขึ้นอยู่กับว่ามันได้มีการเปลี่ยนแปลงไปแล้วมากน้อยเท่าใดนับตั้งแต่ได้มีการทำ backup ครั้งล่าสุดมาแล้ว backup ยิ่งมีความเก่าแก่มากเท่าใด และ data ยิ่งสูญเสียความเป็นปัจจุบันไปมากเท่าใด ก็ยิ่งจะทำให้ลักษณะของ comprehensiveness ต่ำลงไปมากเพียงนั้น แผนการทำ backup ที่ดีจะช่วยให้มีลักษณะของ comprehensiveness ในหลายๆระดับด้วยกัน เหตุผลอันหนึ่งของการมี comprehensiveness หลายระดับคือความจำเป็นที่จะต้องกลับไปค้นหา data อันใดอันหนึ่งเป็นการเฉพาะได้ทันเวลา อย่างเช่น files ของห้องเรียนในมหาวิทยาลัยที่ใช้ประจำปี เป็นต้น อีกเหตุผลหนึ่งก็คือ กาลเวลาอาจจะผ่านไปแล้วชั่วระยะหนึ่งจึงได้รู้ว่ามีปัญหาเกิดขึ้น ยกตัวอย่างเช่น อาจมีโปรแกรมอันหนึ่งที่ได้รับการแก้ไขปรับปรุงมาใหม่ๆหมาดๆ แต่บังเอิญไม่พบว่ามี bugs ซ่อนเร้นอยู่ในระหว่างการ test เสร็จแล้วโปรแกรมอาจจะถูกมาใช้งาน ถ้าไม่พบ bug ที่เป็นตัวทำลาย data นี้สัก 3 วัน backups ทุกอันที่ถูกสร้างขึ้นหลังจากที่ใช้งานโปรแกรมนี้ไปแล้วอาจมี data ที่ได้รับความเสียหายรวมอยู่ด้วย อาจมีการทำ backup ขึ้นหลายอันในช่วงระหว่างเวลาที่ data นั้นได้รับความเสียหายไปจนถึงช่วงเวลาที่สาเหตุแห่งความเสียหายนั้นถูกตรวจพบ การกู้สภาพจึงอาจต้องข้าม backups ย้อนไปหลายรุ่นจนกว่าจะถึง backup ที่ถูกสร้างขึ้นก่อนการเกิดความเสียหายดังกล่าว เมื่อเรานำ backup ที่มีความเก่าแก่มากๆ มาทำการกู้สภาพจะทำให้งานที่ต้องทำมากเพื่อนำ data กลับคืนสู่ความเป็นปัจจุบัน แต่แม้ว่าจะต้องมีงานต้องทำมากก็ตาม ก็ยังมีการนำวิธีนี้มาใช้เหมือนกันถ้าเห็นว่าถ้าใช้วิธีซ่อมแซม data ส่วนที่เสียหายนั้นจะมีราคาแพงกว่าและสิ้นเปลืองเวลามากกว่า

ตัวอย่างนโยบายการเก็บรักษา backup (A Sample Backup Retention Policy)

นโยบายการทำ backup (Backup Policy)

ประจำวัน ทำ backup ให้กับทุก files ที่มีการเปลี่ยนแปลงนับตั้งแต่มี backup ของวันก่อนนี้ทำ copies ขึ้น 2 ชุด แล้วเก็บชุดหนึ่งไว้ที่ site อื่น (off-site)

ประจำสัปดาห์ ทำ backup ให้กับทุก files ทำ copies ขึ้น 2 ชุด แล้วเก็บชุดหนึ่งไว้ที่ site อื่น (off-site)

ปลายปี ทำ backup ให้กับทุก files ของเที่ยงคืนวันที่ 31 ธันวาคมทำ backup ให้กับทุก files ของเที่ยงคืนวันสิ้นงบประมาณ (fiscal year) ทำ copies ขึ้น 2 ชุด แล้วเก็บชุดหนึ่งไว้ที่ siteอื่น (off-site)

นโยบายการเก็บรักษา (Retention Policy)

เก็บรักษา backups ที่ทำประจำสัปดาห์และประจำวันไว้เป็นเวลา 1 เดือน

เก็บรักษา backup อันแรกของแต่ละเดือนไว้เป็นเวลา 1 ปี

เก็บรักษา backup ที่ทำตอนปลายปีไว้เป็นเวลา 5 ปี

การวางแผนรับมือกับภัยพิบัติ (DISASTER PLANNING)

องค์ประกอบอีกอันหนึ่งของขั้นตอนในการทำ recovery และการวางแผนขององค์กรคือแผนรับมือกับภัยพิบัติ (disaster plan) การทำ recovery ที่กล่าวแล้วในเบื้องต้นได้พูดถึงการ fail ของส่วนประกอบเพียงส่วนเดียวของระบบเท่านั้น แต่สำหรับ disaster plan จะมุ่งถึงสถานการณ์ต่างๆ ที่จะทำให้ส่วนประกอบหลักๆของระบบ (เช่น servers, workstations, cabling และอื่นๆ)เกิดความเสียหาย แผนรับมือกับภัยพิบัตินี้จะกล่าวถึงสถานการณ์ต่างๆ ที่เกิดจากไฟไหม้แผ่นดินไหว น้ำท่วม และการกระทำโดยจงใจของผู้ต้องการทำลายระบบ ในแผนรับมือกับภัยพิบัติLAN administrator ควรมองเห็นทุกภาพที่น่าจะเกิดขึ้นแล้วจัดทำแผนเผชิญเหตุ(contingency plans) ซึ่งจะนำไปสู่การแก้ปัญหาสิ่งเหล่านั้นได้อย่างทันที บางครั้งอาจเป็นไปได้ว่า หน่วยงานส่วนใหญ่จะมี backup program ที่ได้กำหนดสิ่งต่างๆ ไว้ใน โปรแกรมเป็นอย่างดี (well-defined)และถูกใช้งานอยู่ในหน่วยของตนแล้ว ส่วนหน่วยงานที่ยังไม่มีสิ่งดังกล่าวอาจจะมีการใช้สักหนึ่งแผนหลังจากการทำ recovery ครั้งแรกไปแล้ว (ถ้ายังคงดำเนินธุรกิจนั้นอยู่) อย่างไรก็ตามมีบริษัทจำนวนน้อยที่มีแผนรับมือกับภัยพิบัติ LAN administrator ที่รอบคอบจะต้องมีบางส่วนของแผนที่ว่านี้ใช้งานอยู่ในขั้นต้น เมื่อปฏิบัติตามขั้นตอนอย่างถูกต้อง LAN administratorสามารถจะทำให้ network ฟื้นกลับคืนมาและสามารถทำงานชนิดได้เกือบสมบูรณ์เหมือนเดิมหลังจากที่ความหายนะนั้นได้จบลง ประเด็นสำคัญของ disaster plan คือ การมี data storage อยู่ ณ ที่อีกแห่งหนึ่ง (off-site storage) และมีการหา hardware ใหม่มาเปลี่ยนทดแทนให้กับ hardware เดิม การเปลี่ยนทดแทน hardware และ cabling อาจสามารถทำได้ในทันทีจากผู้ขายคอมพิวเตอร์ที่อยู่ในท้องถิ่นเดียวกับเรา หรือจากที่ตั้งของบริษัทอื่น แต่สำหรับ data, applications, security settings, command files, common carrier data links, และสิ่งอื่นๆในทำนองนี้ไม่สามารถจะเปลี่ยนทดแทนได้ LAN administrator ทำเพียงแค่จัดเก็บ data สำรองไว้ ณ ที่ตั้งแห่งอื่น (off-site) เป็นประจำเท่านั้น อย่างน้อยที่สุดเขาควรจะได้กำหนดวิธีการหลักๆในการทำ recovery หลังประสบภัยพิบัติไว้ด้วยหลังจากได้วางแผนการทำ recovery ให้กับ software และ data แล้ว LAN administrator ควรจะมีแผนในการสร้างระบบขึ้นใหม่ (rebuilding) ไว้ด้วย ถ้ากล่าวถึง hardware แล้วการทำเช่นนี้อาจได้แก่การมองหาแหล่งของhardware ประเภทcompatible, การมองหาว่ามี hardware ที่อื่นที่ใดบ้างที่เป็นพันธมิตรกันพอจะยืมมาใช้ในช่วงฉุกเฉินได้ การมองหาที่ตั้งสำรองเป็นการชั่วคราวหรือเป็นการถาวรเพื่อติดตั้งระบบใหม่ และการมองหาบริษัทที่เชี่ยวชาญในทุกๆเรื่องเกี่ยวกับระบบ LAN เช่น ด้าน hardware, software, cabling, การติดตั้ง, และการทำ data recovery เป็นต้น การมีรายการไว้ในแผนเพื่อติดต่อประสานงานเช่นนี้เป็นเรื่องสำคัญด้วยเหตุผล 2 ประการ คือประการแรก ความหายนะนั้นเป็นสิ่งที่ทำนายไม่ได้ และ LAN administrator จะไม่รู้ว่าองค์ประกอบใดที่ต้องมีการเปลี่ยนทดแทนหรือซ่อม

ประการที่สองคือ การมีบัญชีรายการต่างๆไว้ในกำมือเกี่ยวกับแหล่งที่จะหาของมาทดแทน แหล่งซ่อม และแหล่งที่จะให้ความช่วยเหลือได้ จะช่วยประหยัดเวลาในช่วงที่ต้องทำการrecovery อย่างฉุกเฉินในกรณีนี้เวลาจึงเป็นสิ่งสำคัญยิ่ง

รายการที่ต้องบรรจุไว้ใน แผนเผชิญภัยพิบัติ (Items Included in Disaster Plan)

การทำประกันภัย จำนวนของประกันภัยที่ต้องทำไว้กับบริษัทประกันภัย เกี่ยวกับsoftware, (Insurance) hardware, และ cabling

ขั้นตอนการปฏิบัติที่จำเป็นเพื่อทำการเปลี่ยนทดแทน/หรือซ่อม อุปกรณ์ที่มีประกันนั้นๆ

- Software สถานที่ตั้งของ storage ที่เก็บ software ไว้ ณ ที่แห่งอื่น (off-site)
- ความเป็นปัจจุบันของ backup ที่เก็บ software ไว้ ณ ที่ตั้งแห่งอื่น (off-site)
- อุปกรณ์ที่จะใช้สร้าง storage ไว้ ณ ที่แห่งอื่น (off-site)
- แหล่งของ software ที่จะนำมาเปลี่ยนทดแทน
- บริษัทที่มีความชำนาญเป็นพิเศษในการทำ recovery ให้กับ data จากสื่อ
- เก็บที่ชำรุดเสียหาย (เช่น backup tapes และ disk drives)
- Data สถานที่ตั้งของ storage ที่ใช้เก็บ data ไว้ ณ ที่ตั้งแห่งอื่น (off-site)
- ความเป็นปัจจุบันของ backup ที่เก็บ data ไว้ ณ ที่ตั้งแห่งอื่น (off-site)
- อุปกรณ์ที่จะใช้สร้าง storage สำหรับเก็บ data ไว้ ณ ที่แห่งอื่น (off-site)
- วิธีการที่จะนำมาใช้เพื่อทำให้ offsite data นั้นกลับคืนสู่สถานะปัจจุบัน
- บริษัทที่มีความชำนาญเป็นพิเศษในการทำ recovery ให้กับ data จากสื่อเก็บที่ชำรุดเสียหาย (เช่น backup tapes และ disk drives)
- Hardware configurations ของ workstations
- Configurations ของ servers
- แผนผัง (diagram) ของ topology / การ wiring ของระบบ LAN
- แหล่งของ hardware ที่จะนำมาเปลี่ยนทดแทน
- แหล่งที่จะบริการการซ่อม hardware ที่ชำรุดเสียหาย
- สถานที่ตั้งของ hardware อะไหล่
- Environment สถานที่ตั้งสำรองที่จะใช้สร้าง network environment ใหม่
- สิ่งจำเป็นที่น้อยที่สุดที่พอเพียงจะสร้าง network environment ใหม่
- ความช่วยเหลือจากภายนอก รายชื่อบริษัทที่มีความชำนาญเป็นพิเศษในการทำ data Recovery,(Outside Help) การ set up ให้กับ network ใหม่, การทำ data entry, การซ่อมสาย,รวมทั้งความชำนาญในการทำสิ่งอื่น

บทสรุป (SUMMARY)

ระบบ LAN ทุกระบบย่อมมีโอกาสจะล้มเหลว (fail) ได้เสมอ แม้ว่าระบบนั้นจะถูกจัดรูปแบบการงาน(configured) ให้มีความสามารถอ่อนตัวในกรณีเกิดความผิดพลาด (fault tolerance) มาเป็นอย่างดีแล้วก็ตาม นอกจากนี้ แม้ว่า hardware และ software ที่ใช้งานจะไม่อ่อนแอจนเกิดความล้มเหลวได้ง่ายก็ตาม แต่ผู้ที่ใช้งานที่ล่อแหลมต่อการทำให้เกิดความล้มเหลวฉะนั้นจึงถือเป็นเรื่องสำคัญอย่างยิ่งที่ LAN administrator จะต้องมีขั้นตอนการปฏิบัติและนโยบายที่ดีที่จะใช้กู้สภาพของระบบหลังจากเกิดความล้มเหลวหนึ่ง ในองค์ประกอบหลักของนโยบายการทำ recovery คือ การทำ data backups นั่นเอง Backups จะถูกนำมาใช้ในการกู้คืนสภาพให้กับdata และ software ให้กลับคืนสู่สถานะที่สามารถใช้งานได้หลังจากระบบเกิดความล้มเหลวซึ่งมีผลให้ data หรือ software เสียหายไปด้วย หนทางที่ data จะเกิดความเสียหายได้นั้นมีมากมายไม่ว่าอะไรจะเป็นสาเหตุที่ทำให้ data เสียหายก็ตาม LAN administrator จะต้องสามารถวินิจฉัยหาสาเหตุให้ได้ แล้วทำการขจัดเหตุแห่งความเสียหายนั้นออกไปถ้าทำได้ แล้วทำการกู้สภาพให้data นั้นกลับคืนสู่สถานะที่สามารถใช้งานได้โดยเร็ว แล้วทำการกู้สภาพให้ network กลับคืนสู่สถานะที่ทำงานได้ตามปกติ นอกจากนี้แล้ว เรายังสามารถนำ backups มาเก็บไว้เป็นประวัติศาสตร์ (data archiving) เก็บไว้เป็นการชั่วคราว และใช้แลกเปลี่ยนข้อมูลกัน (data exchange) ได้อีกด้วย

นโยบายการทำ backup ที่ดีจะช่วยลดงานและเวลาที่จะต้องใช้ไปในการทำ recoveryให้กับ data ที่สูญหายไป นโยบายนี้จะมีรายละเอียดต่างๆ เช่น ความถี่ของการทำ backups การเก็บ backups ไว้ ณ สถานที่อื่น (offsite) การเก็บรักษา backups การจัดการกับ medium ที่ใช้ทำbackup หลังจากที่เราไม่ต้องการใช้อีกแล้ว

บางครั้ง การทำ recovery อาจทำสำเร็จได้โดยไม่ต้องใช้ backups ก็ได้ เพราะจะมี disk editors และ disk utilities สำหรับแก้ปัญหาต่างๆ ที่อาจเกิดขึ้น utilities เหล่านี้จะมีขีดความสามารถหลายอย่าง เช่น การยกเลิกการลบไฟล์(undeleting files) การ write ลงไปโดยตรงลงบนdisk sector การแก้ไข file allocation table การแก้ไข disk directories และแก้ไข volume labelsส่วน utilities อื่นๆ จะมีเน้นหน้าที่ในการนำ files มาต่อกันในรูปแบบอันใดอันหนึ่งโดยเฉพาะ เช่นindex files และ data files ของ database เป็นต้น หนทางปฏิบัติต่างๆ ที่กล่าวมาแล้วนี้ไม่มีอันไหนที่จะทดแทนการทำ backups อย่างสม่ำเสมอได้ การใช้ utilities เหล่านี้อย่างไม่ถูกต้องอาจไปเสริมให้ปัญหาที่กำลังประสบอยู่นั้นสาหัสขึ้นกว่าเดิมได้

นอกเหนือจากการวางแผนในเรื่องการทำ backups และ recovery รวมทั้งการจัดทำขั้นตอนในการปฏิบัติแล้ว LAN administrator ควรจัดทำแผนเผชิญภัยพิบัติ (disaster plan) ไว้อีกด้วย แผนเผชิญภัยพิบัติจะกล่าวถึงวิธีการนำ network กลับคืนสู่สภาพการใช้งานได้ดังเดิมหลังจากเกิดเหตุการณ์ร้ายแรงอย่างเช่น ไฟไหม้ ซึ่งทำให้ส่วนสำคัญของ network เสียหายใช้การไม่ได้ นโยบายหลักที่สำคัญของการทำ backups และ disaster plan คือการเก็บ backups ไว้ ณ สถานที่อื่น (off-site) การเก็บ backups ไว้ ณ สถานที่อื่นจะช่วยป้องกันหน่วยงานนั้นจากความหายนะที่ก่อความเสียหาให้กับ data ที่ต่อ on-line อยู่รวมทั้ง backups ของหน่วยงานนั้น

แผน และ ขั้นตอนการปฏิบัติงาน

- การกำหนด Disaster Recovery Site
- Hot Site ระบบสำรองจะสามารถใช้งานได้เหมือนระบบหลัก รวมทั้งข้อมูลต่าง ๆ จะถูกเก็บทั้งสองแห่ง ลักษณะเหมือนเป็น Mirror Site หากเกิดภัยพิบัติขึ้นระบบสำรองจะสามารถทำงานทดแทนได้เกือบจะในทันทีทันใด ข้อเสียคือ ใช้งบประมาณในการดำเนินการสูง
- Warm Site ระบบสำรองที่สามารถทำงานได้เหมือนระบบหลัก แต่ในส่วนของข้อมูลนั้นจะต้องจำข้อมูลที่ได้สำรอง (Backup) ไว้จากระบบหลักมาทำการติดตั้งใหม่จึงจะดำเนินการต่อได้ ทำให้ต้องมีเวลาในการติดตั้งช่วงเวลาหนึ่งก่อนที่ระบบจะสามารถทำงานต่อไปได้
- Cold Site เป็นการจัดเตรียมโครงสร้างพื้นฐานต่าง ๆ ไว้ก่อนแล้ว อาทิเช่น ระบบเครื่องปรับอากาศ ระบบเครือข่าย ระบบโทรศัพท์ เมื่อเกิดภัยพิบัติขึ้นต้องจัดหาเครื่องคอมพิวเตอร์มาติดตั้งก็สามารถทำงานระบบต่อได้ แต่ข้อเสียคือ ต้องใช้เวลาระยะหนึ่งกว่าระบบจะทำงานได้ตามปกติ
- Standby Site เป็นการจัดหาพื้นที่เตรียมไว้ แต่ไม่ได้ดำเนินการใด ๆ เกี่ยวกับระบบคอมพิวเตอร์
- Nothing คือ การไม่ได้จัดเตรียมสิ่งใดไว้สำหรับภัยพิบัติเลย

กระบวนการในการกู้คืนระบบ

- Recovery Point Objective (RPO) คือ ระยะเวลาที่ยอมให้สูญเสียข้อมูลมากที่สุด
- Recovery Time Objective (RTO) คือ ระยะเวลาตามที่กำหนดไว้เพื่อไม่ให้เกิดความเสียหายต่อองค์กร หรือระยะเวลาเป้าหมายในการกู้คืน
- Maximum Tolerable Downtime (MTD) หมายถึง ระยะเวลาที่นานที่สุดเมื่อเกิดการหยุดชะงักของระบบ และองค์กรยอมรับได้

เวลากู้คืนระบบที่ยอมรับได้ (RTO : Recovery Time Objective)

เป็นระยะเวลาสูงสุดที่ยอมรับได้ในการยอมให้คอมพิวเตอร์ ระบบ เครือข่าย หรือ แอปพลิเคชันหยุดทำงานได้ หลังเกิดเหตุขัดข้อง หรือ เกิดเหตุภัยพิบัติ RTO คือ เครื่องมือกำหนดขอบเขตของเวลาที่เกิดเหตุทำให้การ ดำเนินงานตามปกติสะดุดหยุดลง และการสูญเสียรายได้ โดยเทียบกับหน่วยเวลาอันเนื่องมาจากเหตุภัยพิบัตินั้น ปัจจัยเหล่านี้มีผลต่อเนื่องกัน โดยขึ้นกับอุปกรณ์และแอปพลิเคชันที่ได้รับผลกระทบ RTO วัดได้เป็นวินาที นาที ชั่วโมง หรือวัน และสำคัญต่อการพิจารณาวางแผนการกู้คืนระบบหลังเกิดเหตุภัยพิบัติ

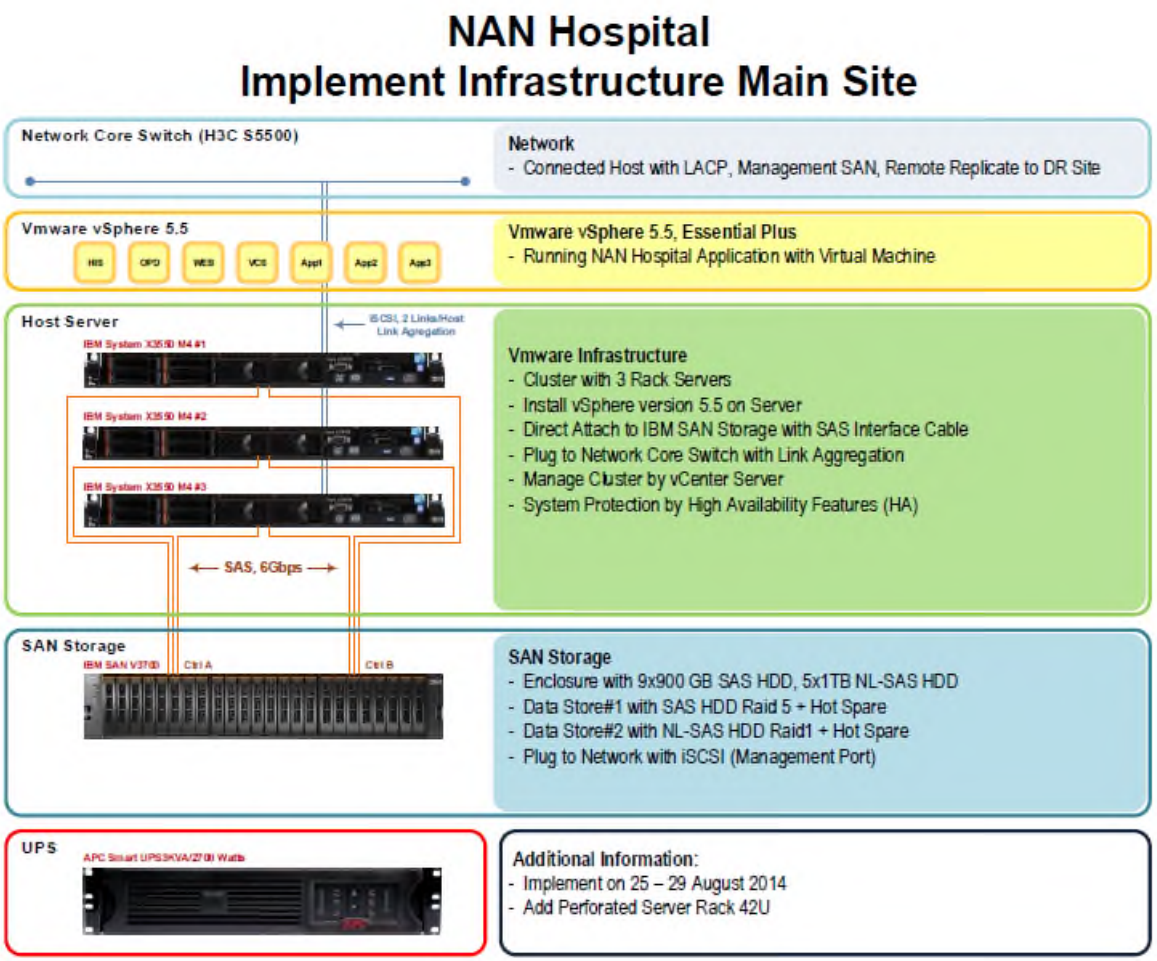
ปริมาณข้อมูลสูญหายในเวลาที่ยอมรับได้ (RPO : Recovery Point Objective)

เป็นกำหนดเวลาที่ไฟล์นั้นต้องได้รับการกู้คืนจากหน่วยจัดเก็บสำรองข้อมูล เพื่อให้กลับสู่การดำเนินงานตาม ปกติ หากคอมพิวเตอร์ ระบบ หรือ เครือข่ายเกิดล่ม อันเนื่องมาจากความขัดข้องของฮาร์ดแวร์ โปรแกรม หรือ ระบบสื่อสาร RPO จะแสดงโดยการย้อนหลังเวลา (กล่าวคือ ย้อนกลับสู่อดีต) จากเวลาปัจจุบันที่เกิดความล้ม เหลว และสามารถระบุได้เป็นวินาที นาที ชั่วโมง หรือ วัน RPO คือ ปัจจัยสำคัญที่ใช้พิจารณาการวางแผนการกู้ คืนระบบหลังเกิดเหตุภัยพิบัติ เมื่อได้ระบุ RPO สำหรับคอมพิวเตอร์ ระบบ หรือ เครือข่ายที่กำหนดแล้ว ค่าดังกล่าวจะเป็นตัวกำหนดความถี่ต่ำสุด ซึ่งต้องมีการสำรองข้อมูลตามความถี่นั้น ปริมาณข้อมูลสูญหายในเวลาที่ยอมรับได้ (RPO) และเวลากู้คืนระบบที่ยอมรับได้ (RTO) จะช่วยให้ผู้ดูแลระบบ สามารถเลือกเทคโนโลยี และกระบวนการที่เหมาะสมที่สุดสำหรับการกู้คืนระบบหลังเกิดเหตุภัยพิบัติ ตัวอย่างเช่น

ถ้า RPO เท่ากับหนึ่งชั่วโมง จะต้องมีการสำรองข้อมูลอย่างน้อยชั่วโมงละครั้ง ในกรณีนี้ ฮาร์ดไดรฟ์เก็บข้อมูลซ้ำซ้อนแบบภายนอกอาจจะถือเป็นโซลูชั่นที่ดีที่สุดในการกู้คืนระบบหลังเกิดเหตุภัยพิบัติ ถ้า RPO เท่ากับ 5 วัน (120 ชั่วโมง) แล้ว จะต้องมีการสำรองข้อมูลในช่วงเวลาเท่ากับ 120 ชั่วโมง หรือน้อยกว่านั้น ในสถานการณ์เช่นนั้น การสำรองข้อมูลด้วยเทปก็น่าจะเพียงพอแล้ว

เทคโนโลยีในการกู้คืนระบบ ๓ ระดับ

- Automation การกู้คืนในช่วงวินาที สามารถสำรองข้อมูลได้ทันที
- Replication เวลาสูงกว่าวินาทีจนถึงชั่วโมง จะสำเนาข้อมูลไปเก็บไว้ที่ปลายทางแล้วใช้ วิธี Manual ทำให้ระบบกลับมาใช้งานได้อีกครั้ง
- Restore เวลาการกู้คืนเป็นวันหรือสัปดาห์ กู้ข้อมูลจาก Tape Backup ซึ่งเทคโนโลยีทั้ง ๓ ระดับมีค่าใช้จ่ายที่ต่างกันหากองค์กรเลือกการกู้คืนในช่วงเวลาต่ำและเทคโนโลยีที่ ทันสมัยจำเป็นต้องเสียค่าใช้จ่ายสูงขึ้น



รูปแสดงโครงสร้างระบบ Vmware Infrastructure Main Site

SAN	Product/ID	S/N	Port	IP
IBM V3700	2072-24C	7848174	A-P1	172.16.2.105
			A-P2	
			B-P1	172.16.2.106
			B-P2	
IBM SystemX 3550M4				
IBM-ESXi-01	7914 AC1	06BVLFX		172.16.2.101
IBM-ESXi-02	7914 AC1	06BVLFP		172.16.2.102
IBM-ESXi-03	7914 AC1	06BVLFV		172.16.2.103
Vsphere Data Protecton				172.16.2.104
VMware vCenter Server Appliance				172.16.2.100
vSphere Management Assistant (UPS)				https://172.16.2.107:5480
				172.16.2.107:6547
APC UPS (Box)		00-C0-B7-B8-27-DC		172.16.2.108

รูปแสดงรายละเอียดระบบ Vmware

3.3.1 ระบบสารสนเทศที่สำคัญ

- ระบบ Database Server
  - § Server_Database_1 : Database หลัก ระบบ His โรงพยาบาล
  - § Server_Database_2 : Replication Database หลัก ระบบ His โรงพยาบาล เพื่อใช้ในการจัดทำรายงาน ผ่านระบบ online
  - § Server_Database_3 : Replication Database หลัก ระบบ His โรงพยาบาล เพื่อใช้ในการจัดทำรายงานโวยการ query
  - § Server_OPD_card : เป็น Server สำหรับเก็บภาพ Scan opd card

- ระบบ Web Intranet และ อินเตอร์เน็ต ประกอบด้วย
  - § Firewall
  - § NameServer
  - § VPN
  - § Virtual_Server
  - § Virtual_database_Web
  - § Virtual_Client
- ระบบ E-office
  - § Windows_Archives_Server ใช้ในการรับส่งหนังสือข้ามหน่วยงาน พัฒนาโปรแกรมโดยสำนักปลัดกระทรวงสาธารณสุข
- ระบบบุคคลากร
  - § Windows_PIS_Server ใช้ในการจัดเก็บข้อมูลบุคลากรโรงพยาบาลน่าน พัฒนาโปรแกรมโดยสำนักปลัดกระทรวงสาธารณสุข

- Windows Server 2008_IIS เครื่องแม่ข่ายสำหรับใช้ติดตั้งระบบที่พัฒนาด้วย ASP
  - § ระบบรายงานความเสียง
  - § ระบบส่งซ่อมพัสดุ
- Windows Server 2008_AppServ เครื่องแม่ข่ายสำหรับใช้ติดตั้งระบบที่พัฒนาด้วย PHP
  - § ระบบสารบรรณภายใน
- ระบบงานอื่น ๆ
  - § Monitor_network

กำหนดลำดับและระยะเวลาเป้าหมาย

ลำดับการกู้คืน	ระบบงาน	รายละเอียดงาน	Hardware/ Softwareที่เกี่ยวข้อง	RPO	RTO	MTD
1.	ระบบ Database Server - Server_Database_1 - Server_Database_2 - Server_Database_3 - Server_OPD_card	Database ระบบ His โรงพยาบาล	- CentOS 3.9 - Samba - MySQL	 1 D 1 W 1 D	 1 H 20 M 20 M	 1 H 2 H 3 H
2.	ระบบ Web Intranet และอินเตอร์เน็ต - Firewall - NameServer - VPN - Virtual_Server - Virtual_Client - Virtual_database_Web	ระบบ Web Intranet และอินเตอร์เน็ต โรงพยาบาล	- CentOS 5.0 - debian-6.0.10 - ZeroShell-3.1.0 - SME Server - Samba - MySQL -FTP - Domain name - open VPN - File Server	 1 W 1 W 1 W 1 W 1 W 1 D	 20 M 20 M 20 M 20 M 20 M 20 M	 1 D 1 D 1 D 1 D 1 D 1 D
3.	ระบบ E-office - Windows_Archives_Server	รับส่งหนังสือข้ามหน่วยงาน	- Windows 7 - AppServ - MySQL - Java 7	1D	1-3 H	3 D
4.	ระบบบุคคลากร - Windows_PIS_Server	ข้อมูลบุคลากร โรงพยาบาล	- Windows 7 - AppServ - PostgreSQL - PG Admin	1D	1-3 H	3 D
5.	Windows Server 2008_IIS - ระบบรายงานความเสียง - ระบบส่งซ่อมพัสดุ	ระบบที่พัฒนาด้วย ASP	- Windows 2008 R2 - IIS 7 - MS SQL -MS Dot net - MS Visual Studio	 1W 1W	 3 D 3 D	 1 W 1 W
6.	Windows Server 2008_ AppServ - ระบบสารบรรณภายใน	ระบบที่พัฒนาด้วย PHP	- Windows 2008 R2 - Appserv - MySQL	 1W 1W	 3 D 3 D	 1 W 1 W

ลำดับการกู้คืน	ระบบงาน	รายละเอียดงาน	Hardware/ Softwareที่เกี่ยวข้อง	RPO	RTO	MTD
7.	ระบบงานอื่น ๆ - Monitor_network		- Windows 7 - Windows 2008 R2 - Windows 7 - debian-6.0.10 - MySQL - Net Framework	1M	1 W	1 M

สถานที่เก็บแผนกู้คืน

- สถานที่ที่ใช้ในการเก็บแผนกู้คืน คือ งานเทคโนโลยีทางการศึกษา คณะแพทยศาสตร์
- โดยทำการจัดเก็บแผนกู้คืนไว้ที่แผนกพัฒนา Software และฐานข้อมูล ผู้รับผิดชอบในการเก็บกุญแจ และรหัสผ่านดังตาราง
- ตารางแสดงรายชื่อผู้รับผิดชอบในการเก็บกุญแจและรหัสผ่านของแผนกู้คืนระบบ

ผู้รับผิดชอบ	ตำแหน่ง	เบอร์โทร	สถานที่	Primary /Secondary
สมบัติ แก้วจันทร์ฉาย	นักวิชาการคอมพิวเตอร์	081-347-1533	ศูนย์เทคโนโลยี ฯ จัดเก็บไว้ในระบบ SAS RAID 10	Primary
สิทธิโชค สุภา	นักวิชาการคอมพิวเตอร์	089-636-1221	ศูนย์เทคโนโลยี ฯ จัดเก็บไว้ในรูปแบบ DVD	Secondary

กำหนด Hardware, Software, data

1. Hardware Database Server (HW1)						
No.	System	OS	CPU Core	Disk Space	Memory	Network
HW1.1	Server_Database_1	Linux Cen 3.9	8	300 GB	16 GB	2
HW1.2	Server_Database_2	Linux Cen 3.9	8	300 GB	16 GB	2
HW1.3	Server_Database_3	Linux Cen 3.9	8	300 GB	16 GB	2
HW1.4	Server_OPD_card	Linux Cen 3.9	4	1 TB	8 GB	1

2. ระบบ Linux Server (HW2)						
No.	System	OS	CPU Core	Disk Space	Memory	Network
HW2.1	Firewall	Pfsense 2.15	4	8 GB	1 GB	3
HW2.2	NameServer	ZeroShell 3.1.0	4	16 GB	1 GB	2
HW2.3	VPN	Pfsense 2.15	4	12 GB	1 GB	2
HW2.4	Virtual_Server	SME Server	4	250 GB	4 GB	1
HW2.5	Virtual_Client	SME Server	2	Boot Cd	1 GB	1
HW2.6	Virtual_database_Web	Turnkey	4	40 GB	4 GB	1
HW2.7	Monitor_network	debian-6.0.10	2	20 GB	512 MB	2

3. Windows Server (HW3)						
No.	System	OS	CPU Core	Disk Space	Memory	Network
HW3.1	Windows_Archives_Server	Win 7	2	250 GB	4 GB	2
HW3.2	Windows_PIS_Server	Win 7	2	250 GB	4 GB	2
HW3.3	Windows Server 2008_IIS	2008 R2	4	250 GB	8 GB	2
HW3.4	Windows Server 2008_Appser	2008 R2	4	250 GB	8 GB	2

4. Software (SW1)				
No.	System	Version	Type	Owner
SW1.1	Linux Cen	3.9	OS	สิทธิโชค สุภา
SW1.2	Linux Cen	5.0	OS	สิทธิโชค สุภา
SW1.3	MySQL	3.2.3.58	APP	สิทธิโชค สุภา
SW1.4	MySQL	5.0	APP	สิทธิโชค สุภา
SW1.5	Samba	3.0.9	APP	สิทธิโชค สุภา
SW1.6	FTP	VSFTP 1.2.1	APP	สิทธิโชค สุภา
SW1.7	HTTP		APP	สิทธิโชค สุภา
SW1.8	Apache	2.2	App	สิทธิโชค สุภา
SW1.9	Windows	Win 2008 R2	OS	สมบัติ แก้วจันทร์ฉาย
SW1.10	Windows	Win 7 Thai edition	OS	สมบัติ แก้วจันทร์ฉาย
SW1.11	phpMyAdmin	5.0.22	APP	สมบัติ แก้วจันทร์ฉาย
SW1.12	AppServer Win32	2.5.10	APP	สมบัติ แก้วจันทร์ฉาย

4. Software (SW1) ต่อ				
No.	System	Version	Type	Owner
SW1.3	MySQL WIN	3.2.3.58	APP	สมบัติ แก้วจันทร์ฉาย
SW1.4	MySQL WIN	5.0	APP	สมบัติ แก้วจันทร์ฉาย
SW1.5	MariaDB	10.0.17	APP	สมบัติ แก้วจันทร์ฉาย
SW1.6	JAVA	Version 8 Update 45		สมบัติ แก้วจันทร์ฉาย

กำหนดแผนการสำรองข้อมูล

No.	ชื่อของระบบ	วัน เวลาที่สำรองข้อมูล	เวลา	ชุดข้อมูล	ระยะเวลาที่ใช้
1	Server_Database_1	ทุกวัน	00.00	7	5 นาที
2	Server_Database_2	ทุกวันศุกร์	20.00	4	10 นาที
3	Server_Database_3	ทุกวัน	12.00	30	3 นาที
4	Server_OPD_card	ทุกวันพุธ	12.00	4	10 นาที
5	Firewall	ทุกวันที 30	01.00	1	3 นาที
6	NameServer	ทุกวันที 30	01.00	1	3 นาที
7	VPN	ทุกวันที 30	01.00	1	3 นาที
8	Virtual_Server	ทุกวันที 30	01.00	1	3 นาที
9	Virtual_Client	ทุกวันที 30	01.00	1	3 นาที
10	Virtual_database_Web	ทุกวันเสาร์	01.00	4	3 นาที
11	Monitor_network	ทุกวันที 30	01.00	1	3 นาที
12	Windows_Archives_Server	ทุกวัน	19.00	7	15 นาที
13	Windows_PIS_Server	ทุกวันเสาร์	08.00	4	15 นาที
14	Windows Server 2008_IIS	ทุกวันที 15	00.00	1	10 นาที
15	Windows Server 2008_Appser	ทุกวันที 15	00.00	1	10 นาที
20	Server_EFORL_EKG	ทุกวัน	18.00	7	60 นาที
21	CentOS_7	ทุกวัน	21.00	15	7 นาที
22	Server_CCTV	สำรองระบบ NAS	-	-	-

ขั้นตอนการปฏิบัติในการสำรองระบบและการกู้คือระบบ