การพัฒนาระบบสำรองข้อมูลเว็บไซต์การบริการและฐานข้อมูลของบริษัทตัวอย่าง

โดย
นายณรงค์ฤทธิ์ เอกมงคลชัยกุล

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาการจัดการงานวิศวกรรม แผน ก แบบ ก 2 ปริญญามหาบัณฑิต
ภาควิชาวิศวกรรมอุตสาหการและการจัดการ
บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ปีการศึกษา 2563
ลิขสิทธิ์ของบัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

การพัฒนาระบบสำรองข้อมูลเว็บไซต์การบริการและฐานข้อมูลของบริษัทตัวอย่าง

โดย
นายณรงค์ฤทธิ์ เอกมงคลชัยกุล

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาการจัดการงานวิศวกรรม แผน ก แบบ ก 2 ปริญญามหาบัณฑิต
ภาควิชาวิศวกรรมอุตสาหการและการจัดการ
บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ปีการศึกษา 2563
ลิขสิทธิ์ของบัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

DEVELOP SYSTEM OF DATA BACKUP FOR WEBSITE AND DATABASEOF SAMPLE COMPANY

By

MR. Narongrit EAKMONGKONCHAIKUN

A Thesis Submitted in Partial Fulfillment of the Requirements

for Master of Engineering (ENGINEERING MANAGEMENT)

Department of INDUSTRIAL ENGINEERING AND MANAGEMENT

Graduate School, Silpakorn University

Academic Year 2020

Copyright of Graduate School, Silpakorn University

หัวข้อ	การพัฒนาระบบสำรองข้อมูลเว็บไซต์การบริการและฐานข้อมูลของบริษัทตัวอย่าง
โดย	ณรงค์ฤทธิ์ เอกมงคลชัยกุล
สาขาวิชา	การจัดการงานวิศวกรรม แผน ก แบบ ก 2 ปริญญามหาบัณฑิต
อาจารย์ที่ปรึกษาหลัก	รองศาสตราจารย์ ดร. ประจวบ กล่อมจิตร

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร ได้รับพิจารณาอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต

.....คณบดีบัณฑิตวิทยาลัย
(รองศาสตราจารย์ ดร.จุไรรัตน์ นันทานิช)

พิจารณาเห็นชอบโดย

.....ประธานกรรมการ
(ดร.สิทธิชัย แซ่เหล่ม)

.....อาจารย์ที่ปรึกษาหลัก
(รองศาสตราจารย์ ดร.ประจวบ กล่อมจิตร)

.....ผู้ทรงคุณวุฒิภายนอก
(ผู้ช่วยศาสตราจารย์ ดร.ระพี กาญจนะ)

620920040 : การจัดการงานวิศวกรรม แผน ก แบบ ก 2 ปริญญามหาบัณฑิต
คำสำคัญ : การจัดการความเสี่ยง, การจัดการเทคโนโลยีสารสนเทศ, การสำรองข้อมูล, คำสั่ง DOS

นาย ณรงค์ฤทธิ์ เอกมงคลชัยกุล: การพัฒนาระบบสำรองข้อมูลเว็บไซต์การบริการและฐานข้อมูลของบริษัทตัวอย่าง อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก : รองศาสตราจารย์ ดร. ประจวบ กล่อมจิตร

ความเสี่ยงจากมัลแวร์แรนซัมแวร์ที่มักคุกคามโจมตีระบบสารสนเทศในองค์กรผ่านเครือข่ายอินเตอร์เน็ตนั้นเมื่อเกิดขึ้นย่อมส่งผลทำให้เว็บไซต์การบริการและฐานข้อมูลในองค์กรเสียหายกระทบโดยตรงต่อการดำเนินธุรกิจอันประเมินค่าไม่ได้ วิธีการหนึ่งของการจัดการความเสี่ยงคือการมีระบบสำรองข้อมูลอันช่วยจะลดความเสียหายลงได้ งานวิจัยนี้จึงมีวัตถุประสงค์เพื่อพัฒนาระบบซอฟต์แวร์ประยุกต์สำหรับสำรองข้อมูลเว็บไซต์การบริการและฐานข้อมูลขององค์กร ซึ่งการศึกษาวิจัยนี้ได้นำหลักการจัดการเทคโนโลยีสารสนเทศมาประยุกต์ เพื่อการจัดเก็บข้อมูลที่มีอยู่ให้เป็นระบบในการเรียกใช้ข้อมูลอย่างรวดเร็วในเวลาที่ต้องการดำเนินงานสำรองและกู้คืนข้อมูล โดยงานวิจัยนี้จำนวนมีเครื่องเซิร์ฟเวอร์จะต้องสำรองข้อมูลทั้งหมด 9 เครื่อง จำนวนข้อมูลที่สำรองรวม 858.2 GB ใช้วิธีพัฒนาสำรองข้อมูลด้วยวิธีการเขียนโปรแกรมคำสั่ง DOS ทางคอมพิวเตอร์ระบบปฏิบัติการ Windows ทำเป็น Script และตั้ง Task Scheduler ให้โปรแกรมทำงาน จากผลการศึกษาพบว่าระบบสามารถใช้ได้งานได้จริง โดยพิจารณาจากจำนวนข้อมูลที่สำรองนั้นครบ 858.2 GB มีประสิทธิภาพการสำรองข้อมูลถูกต้อง 100% และผลเปรียบเทียบต้นทุนพบว่าการพัฒนาระบบด้วยการสร้างซอต์ฟแวร์คำสั่ง DOS นั้นในปีแรกทั้งระบบมีต้นทุน 18,090 บาท ถูกว่าต้นทุนค่าแรงใช้พนักงานดำเนินงานด้วยวิธีคัดลอกสำรองข้อมูล 17.47% และถูกกว่าการใช้บริการสำรองข้อมูลจากผู้ให้บริการภายนอก 32.67% จากผลการศึกษานี้ชี้ให้เห็นว่าการพัฒนาระบบดังกล่าวสามารถใช้ได้และเป็นการจัดการลดความเสี่ยงที่ข้อมูลอาจสูญหายได้ รวมทั้งยังประหยัดต้นทุนมากสุดเมื่อเทียบกับการใช้แนวทางอื่น โดยการสำรองข้อมูลนั้นระบบจะทำอย่างเดือนละ 2 ครั้ง และยังสามารถต่อยอดระบบโดยทำระบบสำรองข้อมูลเพิ่มอีกชั้นหนึ่งได้

620920040 : Major (ENGINEERING MANAGEMENT)
Keyword : Risk management, Management Information System, Data Backup, DOS Command

MR. NARONGRIT EAKMONGKONCHAIKUN : DEVELOP SYSTEM OF DATA BACKUP FOR WEBSITE AND DATABASEOF SAMPLE COMPANY THESIS ADVISOR : ASSOCIATE PROFESSOR PRACHUAB KLOMJIT, Ph.D.

The risk of ransomware, which often threatens to attack corporate information systems by the Internet, will result in damage to corporate website service and database directly affect the business operation is priceless. One of the methods of risk management is to have a backup data system that can help reduce damage. This research aims to develop application software systems for backup website services and database of organization. This research has applied principles of information technology management. To systematically store existing data for quick retrieval when required to perform backup and recovery tasks. From this research, there were 9 servers for backup data , and the total number of backups was 858.2 GB. The backup was developed by programming DOS commands on windows computer and made a script and set up a task scheduler to run the program. According to the study results, it was found that The system can be used for real purposes. Considering the number of backups of 858.2 GB, the backup performance is 100% correct and the cost comparison is found in first year total system by creating the DOS command software has cost 18,090 baht, cheaper than labor cost of staff operated by copy backup method 17.47% and 32.67% cheaper than using external backup service.The development of such a system is practical and manages to reduce the risk of data loss as well as the greatest cost savings compared to using other approaches. This backup data system will be done twice a month and can develop backup system by making an additional layer of backup system.

กิตติกรรมประกาศ

งานวิจัยนี้สำเร็จได้ด้วยการสนับสนุนและความกรุณาให้คำปรึกษาในงานวิจัยเล่มนี้อย่างยิ่งของ รองศาสตราจารย์ ดร.ประจวบ กล่อมจิตร ซึ่งเป็นอาจารย์ที่ปรึกษาของการศึกษางานวิจัย ด้วยการแนะนำหลักการวิจัยและให้ความรู้ในดำเนินงานวิจัย ตลอดจนตรวจสอบรายละเอียดของงานวิจัยซึ่งเป็นประโยชน์อย่างมากในการทำวิจัยเล่มนี้ และขอขอบคุณคณะกรรมการที่ให้คำแนะนำในการศึกษางานวิจัยนี้ ซึ่งประกอบไปด้วยอาจารย์ ดร. สิทธิชัย แซ่แหล่ม และ ผู้ช่วยศาสตราจารย์ ดร. ระพี กาญจนะ สำหรับคำแนะนำในการปรับปรุงงานวิจัยให้เสร็จสมบูรณ์ ไว้ ณ ที่นี้ด้วย

ขอขอบคุณผู้บังคับบัญชา เพื่อนร่วมงานของบริษัทกรณีศึกษา ที่ให้ความช่วยเหลือในการดำเนินการพัฒนาระบบงานสำรองข้อมูล เพื่อให้บรรลุวัตถุประสงค์ในการทำวิจัย ให้สำเร็จลุล่วงไปได้ด้วยดี ตลอดจนคณะอาจารย์ ภาควิชาวิศวกรรมอุตสาหการและการจัดการทุกท่านที่ได้อบรมสั่งสอนและให้คำแนะนำเกี่ยวกับการศึกษาด้วยดีมาโดยตลอด

สุดท้ายขอขอบคุณบิดา มารดา และครอบครัวที่สนับสนุนและให้กำลังใจในทุกๆ เรื่องเป็นอย่างดี ผู้วิจัยหวังว่าการศึกษาค้นคว้างานวิจัยนี้จะเป็นประโยชน์แก่ผู้ที่สนใจ และสามารถนำไปประยุกต์ใช้ในการศึกษา หรือเป็นข้อมูลในการอ้างอิงงานวิจัยต่างๆที่เกี่ยวเนื่องต่อไป ส่วนความผิดพลาดและข้อบกพร่องใดๆ ผู้ศึกษากราบขออภัยมา ณ โอกาสนี้ และขอน้อมรับไว้แต่เพียงผู้เดียว

ณรงค์ฤทธิ์ เอกมงคลชัยกุล

มหาวิทยาลัยศิลปากร

สารบัญ

หน้า

มหาวิทยาลัยศิลปากร

สารบัญตาราง

หน้า

สารบัญรูปภาพ

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในช่วง 30 ปีที่ผ่านมาการสื่อสารโทรคมนาคมบนอินเตอร์เน็ตและระบบคอมพิวเตอร์มีความก้าวหน้าอย่างก้าวกระโดด ทำให้เกิดการเปลี่ยนแปลงเข้าสู่ยุคสังคมสารสนเทศอันเป็นผลให้ชีวิตความเป็นอยู่การติดต่อสื่อสารและการทำงานเปลี่ยนแปลงไป ระบบสารสนเทศทางคอมพิวเตอร์จึงเข้ามีบทบาทในองค์กรและเป็นส่วนสำคัญในการขับเคลื่อนธุรกิจขององค์กรอย่างมากในปัจจุบัน เพื่อสนับสนุนและการจัดการงานต่างๆ ครอบคลุมตั้งแต่ งานบุคคล งานเอกสาร งานบัญชี งานการตลาด งานด้านเทคนิค และงานวิเคราะห์ต่างๆล้วนอยู่บนระบบสารสนเทศทางคอมพิวเตอร์ ซึ่งเป็นสิ่งที่สำคัญในการบริหารจัดการงานและข้อมูลขององค์กร ทั้งนี้เพื่อให้เกิดการใช้ข้อมูลร่วมกันอย่างมีประสิทธิภาพทั้งในระดับปฏิบัติงานและระดับบริหาร ด้วยเหตุนี้ฐานข้อมูลที่อยู่ในระบบสารสนเทศทางคอมพิวเตอร์จึงมีความสำคัญเป็นอย่างมากในการดำเนินงานต่างๆของทุกองค์กรในปัจจุบัน

ด้วยความสำคัญของระบบสารสนเทศและฐานข้อมูลขององค์กรที่เป็นส่วนหลักในการดำเนินธุรกิจ ทำให้ปัจจุบันเกิดกลุมผู้ไม่หวังดีทำการโจมตีระบบสารสนเทศในองค์กรต่างๆด้วยการปล่อยไวรัส (Virus) ต่างๆ หรือปล่อยแรนซัมแวร์ (Ransomware) เพื่อเจาะ ทำลาย ขโมย หรือล็อกข้อมูลในองค์กรโดยเรียกค่าไถ่ข้อมูลคืนเป็นเงิน ทำให้ผู้ใช้ในองค์กรไม่สามารถเข้าถึงฐานข้อมูลและระบบเว็บไซต์ไม่สามารถใช้งานได้ส่งผลเสียต่อการดำเนินขับเคลื่อนธุรกิจ เนื่องจากเว็บไซต์และฐานข้อมูลถือเป็นส่วนสำคัญที่สนับสนุนและการจัดการงานต่างๆ ครอบคลุมตั้งแต่งานบุคคล งานเอกสาร งานบัญชี งานการตลาด งานด้านเทคนิค งานวิเคราะห์ผล ดังเช่นที่เห็นข่าวเป็นอย่างมากในปัจจุบัน โดยจากข้อมูลสถิติประเทศที่ถูกแรนซัมแวร์ (Ransomware) โจมตีองค์กรต่างๆนั้น จากข้อมูลในปี 2560 ไทยอยู่อันดับ 8 ของโลกและ ในอาเซียนจากข้อมูลสถิติในปี 2563 ไทยอยู่อันดับ 3 ซึ่งถูกโจมตีกว่า 47,014 ครั้งใน 3 เดือนแรกของปี ดังภาพที่ 1 นั้นแสดงให้เห็นว่า การบริหารความเสี่ยงเทคโนโลยีสารสนเทศจึงมีความสำคัญอย่างมากในการจัดการความเสี่ยงที่อาจจะเกิดขึ้นจากการที่องค์กรอาจถูกโจมตีจากแรนซัมแวร์

ในการที่จะสามารถจัดการความเสี่ยงจากแรนซัมแวร์โจมตีและข้อมูลถูกล็อกได้นั้น หนึ่งในวิธีการแก้ไขปัญหาดังกล่าวคือการมีข้อมูลสำรองของระบบงานต่างๆในองค์กรและทำการกู้คืนได้เมื่อ

ถูกโจมตีภายในระยะเวลาที่รวดเร็ว โดยปัญหาของบริษัทกรณีศึกษาในส่วนพื้นที่ที่รับผิดชอบของผู้วิจัย ในปัจจุบันยังไม่มีการสำรองข้อมูลของระบบงานต่างๆอย่างเป็นระบบ หากถูกแรนซัมแวร์โจมตีย่อมจะส่งผลกระทบต่อระบบงานทั้งหมดที่ไม่สามารถกู้คืนได้ อันจะก่อให้เกิดความเสียหายอันประเมินค่าไม่ได้ สอดคล้องกับปัจจุบันบริษัทกรณีศึกษามีการจัดตั้งหน่วยงานด้านความปลอดภัยของระบบเครือข่ายอินเตอร์เน็ตและข้อมูล (Cyber Security) ขึ้นมาเพื่อกำกับดูแลด้านความปลอดภัยของระบบสารสนเทศในองค์กร โดยผู้วิจัยได้รับมอบหมายให้ดูแลงานในส่วนของความปลอดภัยทางด้านข้อมูล ประกอบด้วยเหตุผลดังที่กล่าวมาจึงมีความจำเป็นที่ต้องมีระบบสำรองข้อมูลเพื่อจัดการความเสี่ยงที่อาจเกิดขึ้นได้ โดยหน่วยงานได้กำหนด 3 แนวทางในการดำเนินการศึกษา 3 กรณี คือ 1) การเช่าพื้นที่สำหรับสำรองข้อมูลของผู้ให้บริการจากภายนอก 2) การใช้พนักงานดำเนินการ 3) การพัฒนาระบบด้วยคำสั่งซอฟต์แวร์

จากความเป็นมาและความสำคัญของงานที่บริษัทต้องการ ผู้วิจัยจึงทำการได้เสนอศึกษาแนวทางจัดการดังกล่าวในรูปแบบของคำสั่งซอฟต์แวร์ โดยการพัฒนาระบบไว้ดังนี้ เริ่มจากเก็บรวบรวมข้อมูลจำนวนเครื่องเซิร์ฟเวอร์ และจำนวนข้อมูลในแต่ละเซิร์ฟเวอร์ที่จะต้องทำการสำรองข้อมูลเพื่อกำหนดจำนวนขนาดพื้นที่ต้องใช้เก็บข้อมูลสำรอง จากนั้นออกแบบระบบสำรองข้อมูลด้วยคำสั่งภาษา DOS สร้างเป็นโปรแกรม Script และทำการตั้งเครื่องเซิร์ฟเวอร์สำหรับสำรองข้อมูล ทำการสร้างไฟล์ข้อมูลร่วมกันภายในเครือข่ายเซิร์ฟเวอร์ (Map Drive) เพื่อให้โปรแกรมสามารถดึงข้อมูลที่จะสำรองมายังเครื่องเซิร์ฟเวอร์สำหรับสำรองข้อมูลได้ ท้ายสุดคือทำการสรุปผลที่ได้รวมถึงต้นทุนงบประมาณที่ใช้งาน เปรียบเทียบกับการใช้วิธีให้พนักงานคัดลอกข้อมูลเอง และการใช้โซลูชั่นจากผู้ให้บริการสำรองข้อมูลจากภายนอก

Country	Q1 2020		Q1 2019	
	Detections	Ranking (globally)	Detections	Ranking (globally)
Indonesia	131944	7	520146	6
Malaysia	4953	35	33868	29
Philippines	7211	26	9550	41
Singapore	145	91	2105	65
Thailand	47014	16	88811	25
Vietnam	77937	14	217750	8

Number of ransomware attempts against SMBs blocked by Kaspersky solutions and the country's ranking based on the share of users almost infected with this malware

ภาพที่ 1 จำนวนการถูกแรนซัมแวร์โจมตีของประเทศในภูมิภาคเอเชียตะวันออกฉียงใต้

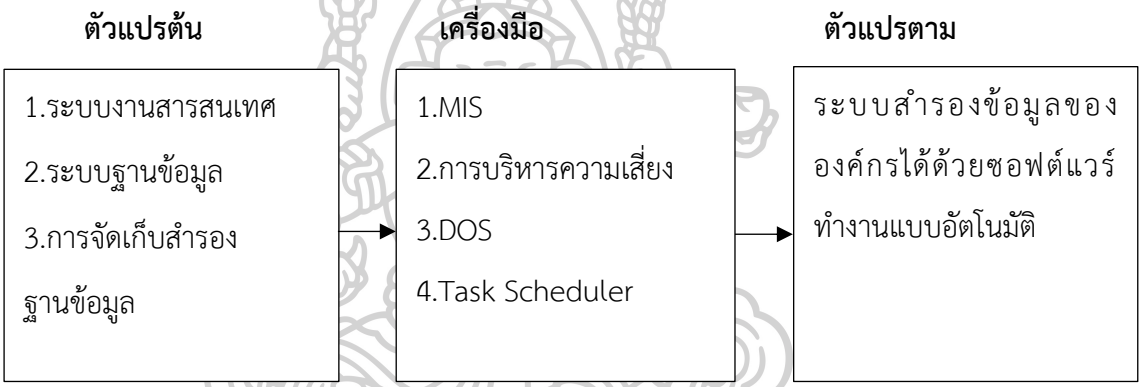
(ที่มา : The Story Thailand , 2563)

1.2 วัตถุประสงค์ของการวิจัย

ศึกษาวิธีการพัฒนาระบบซอฟต์แวร์ประยุกต์สำหรับสำรองข้อมูลเว็บไซต์การบริการและฐานข้อมูลของบริษัทตัวอย่าง เพื่อจัดการลดความเสี่ยงของระบบสารสนเทศจากภัยคุกคามของแรนซัมแวร์ ที่ทำให้ข้อมูลเสียหายกู้คืนไม่ได้ โดยมีต้นทุนการดำเนินการที่ถูกกว่าแนวทางอื่น

1.3 กรอบแนวคิดการวิจัย

งานวิจัยในครั้งนี้เป็นการศึกษาปัจจัยต่างๆ โดยสามารถอธิบายกรอบแนวคิดในลักษณะตัวแปรต้น เครื่องมือที่ใช้ ตัวแปรตาม ได้ดังนี้



ภาพที่ 2 กรอบแนวคิดงานวิจัย

1.4 ขอบเขตของการวิจัย

ในการวิจัยครั้งนี้มุ่งเน้นการพัฒนาระบบซอฟต์แวร์ประยุกต์สำหรับสำรองข้อมูลเว็บไซต์การบริการและฐานข้อมูลของบริษัทตัวอย่าง โดยมีขอบเขตการวิจัยดังนี้

1.4.1 จำนวนเครื่องเซิร์ฟเวอร์ในงานวิจัยมีจำนวน 26 เครื่อง มีเครื่องที่จะต้องสำรองข้อมูล 9 เครื่อง

1.4.2 จำนวนขนาดข้อมูลที่จะต้องสำรองข้อมูลตั้งต้นทั้งหมด 858.2 GB

1.4.3 จำนวนเครื่องเซิร์ฟเวอร์ที่ใช้จัดเก็บข้อมูลที่ทำการสำรองมีจำนวน 1 เครื่อง และมีขนาดพื้นที่ความจุ 4 TB

1.4.4 ชุดโปรแกรมคำสั่ง DOS ที่พัฒนาสำหรับคัดลอกข้อมูลเว็บไซต์การบริการและฐานข้อมูลจากเครื่องเซิร์ฟเวอร์ในเครือข่ายไปยังเครื่องเซิร์ฟเวอร์ที่ใช้จัดเก็บข้อมูลสำรอง

1.4.5 จำนวนต้นทุนของระบบสำรองข้อมูลที่พัฒนาด้วยวิธีการสร้างโปรแกรมคำสั่ง DOS สำหรับคัดลอกข้อมูลไปยังเครื่องเซิร์ฟเวอร์สำหรับจัดเก็บข้อมูลสำรอง เปรียบเทียบกับการใช้พนักงานคัดลอก และ การเช่าผู้ให้บริการสำรองข้อมูลจากภายนอก

1.5 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

1.5.1 จัดการและลดความเสี่ยงจากการถูกแรนซัมแวร์โจมตีและทำให้ข้อมูลสูญหาย

1.5.2 สามารถนำหลักการของระบบสารสนเทศเพื่อการจัดการ (MIS) ในองค์กร

1.5.3 สามารถพัฒนาระบบซอฟต์แวร์เพื่อช่วยในระบบงาน สำรองข้อมูลแบบอัตโนมัติ

1.5.4 สามารถลดต้นทุนในส่วนของการไปซื้อโปรแกรมหรือโซลูชั่นที่จะมีค่าบริการรายเดือนได้

บทที่ 2
ทบทวนทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในบทนี้กล่าวถึงทฤษฎีและแนวคิดที่ผู้วิจัยได้ทำการศึกษาและนำมาใช้ในการช่วยในการดำเนินงานและค้นหาข้อมูลเพื่อวิจัย โดยผู้วิจัยได้ทำการรวบรวมงานวิจัยที่เกี่ยวข้องตามลำดับดังนี้

1. ระบบสารสนเทศเพื่อการจัดการ (MIS : Management Information System)
2. อินเตอร์เน็ต (Internet)
3. แรนซัมแวร์ (Ransomware)
4. หลักการข้อมูลสื่อสาร (Data Communitation)
5. คอมพิวเตอร์เซิร์ฟเวอร์ (Server)
6. ระบบฐานข้อมูล (Database System)
7. ภาษาทางคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบ
8. การบริหารความเสี่ยงเทคโนโลยีสารสนเทศ (IT Risk Management)
9. การสำรองข้อมูล (Backup Data)
10. แผนภาพกระแสข้อมูล (Data Flow Diagram)
11. งานวิจัยที่เกี่ยวข้อง

2.1 ระบบสารสนเทศเพื่อการจัดการ (MIS : Management Information System)

การพัฒนาระบบซอฟต์แวร์สารสนเทศต้องศึกษาหลักการระบบสารสนเทศเพื่อการจัดการ (MIS : Management Information System) ซึ่งระบบสารสนเทศเพื่อการจัดการ คือ ระบบที่รวบรวมและจัดเก็บข้อมูลจากแหล่งต่างๆทั้งภายในและภายนอกองค์กร อย่างมีหลักเกณฑ์เพื่อนำมาประมวลผลและจัดรูปแบบให้ได้สารสนเทศที่ช่วยสนับสนุนในการทำงาน และการตัดสินใจต่างๆ ตามที่ผู้บริหารต้องการทั้งทางด้านสถิติและ Business Management

2.1.1 องค์ประกอบของระบบสารสนเทศ

2.1.1.1 ฮาร์ดแวร์ (Hardware) คือ เครื่องคอมพิวเตอร์ซึ่งเป็นเครื่องมือที่ช่วยในการจัดการสารสนเทศ หรือ อุปกรณ์อื่นๆที่เกี่ยวเนื่อง

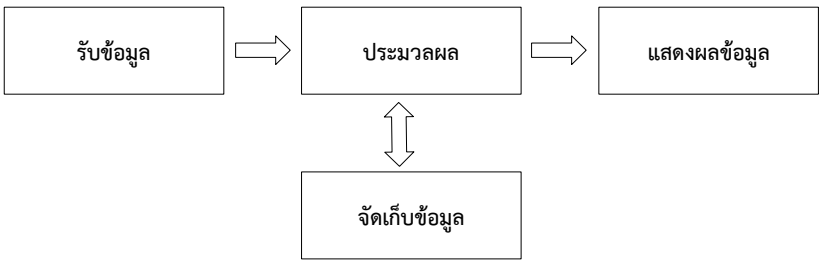
2.1.1.2 ซอฟต์แวร์ (Software) คือลำดับขั้นตอนคำสั่งให้เครื่องคอมพิวเตอร์ ทำงานตามวัตถุประสงค์ที่วางไว้ ซอฟต์แวร์แบ่งเป็น 2 ประเภท

1) ซอฟต์แวร์ระบบ คือ ซอฟต์แวร์ที่ใช้จัดการกับระบบคอมพิวเตอร์ และ อุปกรณ์ต่างๆ ที่มีอยู่ในระบบ เช่น ระบบปฏิบัติการ windows , ระบบปฏิบัติการ DOS ระบบปฏิบัติการ Unix
2) ซอฟต์แวร์ประยุกต์ คือ ซอฟต์แวร์ที่พัฒนาขึ้นเพื่อใช้งานด้านต่างๆ ตามความต้องการของผู้ใช้ เช่น ซอฟต์แวร์กราฟิก ซอฟต์แวร์ประมวลคำ ซอฟต์แวร์ตารางทำงาน

2.1.1.3 ข้อมูล (Data) เป็นวัตถุดิบที่ทำให้เกิดสารสนเทศ ข้อมูลที่เป็นวัตถุดิบจะต่างกันขึ้นกับสารสนเทศที่ต้องการ

2.1.1.4 บุคลากร (Peopleware) เป็นส่วนประกอบที่สำคัญ เพราะบุคลากรที่มีความรู้ความสามารถและเข้าใจวิธีการให้ได้มาซึ่งสารสนเทศจะเป็นผู้ดำเนินการ ในการทำงานทั้งหมด บุคลากรจึงต้องมีความรู้ความเข้าใจในการใช้เทคโนโลยีสารสนเทศ บุคลากรภายในองค์กรเป็นส่วนประกอบที่จะทำให้เกิดระบบสารสนเทศเข้าด้วยกันทุกคน เช่น ร้านขายสินค้าแห่งหนึ่ง บุคลากรที่ดำเนินการในร้านค้าทุกคนตั้งแต่ผู้จัดการถึงพนักงานขาย เป็นส่วนประกอบที่จะทำให้เกิดสารสนเทศได้

2.1.1.5 ขั้นตอนการปฏิบัติงาน (Procedure) ขั้นตอนการปฏิบัติงานเป็นระเบียบวิธีการปฏิบัติงานในการจัดเก็บรักษาข้อมูลให้อยู่ในรูปแบบที่จะทำให้เป็นสารสนเทศได้ เช่น กำหนดให้มีการป้อนข้อมูลทุกวัน ป้อนข้อมูลให้ทันตามกำหนดเวลา มีการแก้ไขข้อมูลให้ถูกต้องอยู่เสมอ กำหนดเวลาในการประมวลผล การทำรายงาน การดำเนินการ ต่างๆ ทั้งนี้สามารถสรุปแผนภาพกระบวนการประมวลผลของข้อมูลได้ตามภาพที่ 3



ภาพที่ 3 กระบวนการประมวลผลของข้อมูลในระบบสารสนเทศ

2.1.2 หน้าที่หลักของระบบสารสนเทศเพื่อการจัดการ

ระบบสารสนเทศเพื่อการจัดการจะประกอบด้วยหน้าที่หลัก 2 ประการ คือ

1) สามารถเก็บรวบรวมข้อมูลจากแหล่งต่างๆ ทั้งจากภายในและภายนอกองค์กรมาไว้ด้วยกันอย่างเป็นระบบ

2) สามารถทำการประมวลผลข้อมูลอย่างมีประสิทธิภาพเพื่อให้ได้สารสนเทศที่ช่วยสนับสนุนการปฏิบัติงานและการบริหารงานของผู้บริหาร

2.1.3 ประเภทของระบบสารสนเทศ

ระบบสารสนเทศสามารถจำแนกได้ตามลักษณะการดำเนินงานได้ดังนี้

1) ระบบสารสนเทศแบบประมวลรายการ (TPS : Transaction Processing Systems) เป็นระบบสารสนเทศที่เกี่ยวกับการบันทึกและประมวลข้อมูลที่เกิดจาก ธุรกรรมหรือการปฏิบัติงานประจำหรืองานขั้นพื้นฐานขององค์กร เช่น การซื้อขายสินค้า การบันทึกจำนวนวัสดุคงคลัง เมื่อใดก็ตามที่มีการทำธุรกรรมหรือปฏิบัติงานในลักษณะดังกล่าวข้อมูลที่เกี่ยวข้องจะเกิดขึ้นทันที เช่น ทุกครั้งที่มีการขายสินค้า ข้อมูลที่เกิดขึ้นก็คือ ชื่อลูกค้า ประเภทของลูกค้า จำนวนและราคาของสินค้าที่ขายไป รวมทั้งวิธีการชำระเงินของลูกค้า

2) ระบบสารสนเทศเพื่อการจัดการ (MIS : Management Information System) คือ ระบบสารสนเทศที่ผู้บริหารต้องการใช้เพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพมากขึ้น โดยรวมระบบสารสนเทศภายในและภายนอกที่เกี่ยวพันกับองค์กรทั้งในอดีตและปัจจุบัน นอกจากนี้ระบบนี้จะต้องสามารถใช้งานช่วงเวลาที่เป็นประโยชน์ เพื่อให้ผู้บริหารสามารถตัดสินใจในการวางแผนการควบคุมและการปฏิบัติการขององค์กรได้อย่างถูกต้อง แม้ว่าผู้บริหารที่จะได้รับประโยชน์จากระบบนี้สูงสุดคือผู้บริหารระดับกลาง แต่โดยพื้นฐานของระบบนี้แล้วจะเป็นระบบที่สามารถสนับสนุนข้อมูลให้ผู้บริหารทั้งสามระดับ คือทั้งผู้บริหารระดับต้น ผู้บริหารระดับกลางและผู้บริหารระดับสูง โดยระบบนี้จะให้รายงานที่สรุปสารสนเทศซึ่งรวบรวมจากฐานข้อมูลทั้งหมดของบริษัท

3) ระบบสนับสนุนการตัดสินใจ (DSS : Decision Support System) เป็นระบบที่พัฒนาขึ้นจากระบบ MIS อีกระดับหนึ่ง เนื่องจาก ถึงแม้ว่าผู้ที่มีหน้าที่ในการตัดสินใจจะสามารถใช้ประสบการณ์หรือใช้ข้อมูลที่มีอยู่แล้วในระบบเอ็มไอเอสของบริษัท สำหรับทำการตัดสินใจได้อย่างมีประสิทธิภาพในงานปกติแต่บ่อยครั้งที่ผู้ตัดสินใจ โดยเฉพาะอย่างยิ่งผู้บริหารในระดับสูงและระดับกลางจะเผชิญกับการตัดสินใจที่ประกอบด้วยปัจจัยที่ซับซ้อนเกินกว่าความสามารถของมนุษย์ที่

จะประมวล เข้าด้วยกันได้อย่างถูกต้อง จึงทำให้เกิดระบบนี้ขึ้นซึ่งเป็นระบบที่สนับสนุนความต้องการเฉพาะของผู้บริหารแต่ละคน (made by order) ในหลายๆสถานการณ์ระบบนี้มีหน้าที่ช่วยให้การตัดสินใจเป็นไปได้อย่างสะดวก

4) ระบบสนับสนุนการตัดสินใจแบบกลุ่ม (GDSS : Group Decision Support System) เป็นระบบย่อยหนึ่งในระบบสารสนเทศเพื่อการจัดการ โดยที่ระบบสนับสนุนการตัดสินใจจะช่วยผู้บริหารในเรื่องการตัดสินใจในเหตุการณ์หรือกิจกรรมทางธุรกิจที่ไม่มีโครงสร้างแน่นอนหรือกึ่งโครงสร้างระบบสนับสนุนการตัดสินใจอาจจะใช้กับบุคคลเดียวหรือช่วยสนับสนุนการตัดสินใจเป็นกลุ่ม นอกจากนั้นยังมีระบบสนับสนุนผู้บริหารเพื่อช่วยผู้บริหารในการตัดสินใจเชิงกลยุทธ์

5) ระบบสารสนเทศภูมิศาสตร์ (GIS : Geographic Information System) ระบบสารสนเทศภูมิศาสตร์ หรือ Geographic Information System : GIS คือกระบวนการทำงานเกี่ยวกับข้อมูลในเชิงพื้นที่ด้วยระบบคอมพิวเตอร์ที่ใช้กำหนดข้อมูลที่มีความสัมพันธ์กับตำแหน่งในเชิงพื้นที่ เช่น ที่อยู่ บ้านเลขที่ สัมพันธ์กับตำแหน่งของแผนที่ตำแหน่ง ของเส้นรุ้ง ของเส้นแวง ข้อมูลและแผนที่ในระบบ GIS เป็นระบบข้อมูลสารสนเทศที่อยู่ในรูปแบบของตารางข้อมูลและฐานข้อมูลที่มีส่วนสัมพันธ์กับข้อมูลเชิงพื้นที่ (Spatial Data) ซึ่งรูปแบบและความสัมพันธ์ของข้อมูลในเชิงพื้นที่ ทั้งนี้จะสามารถนำมาวิเคราะห์ด้วย GIS และทำให้การสื่อความหมายในเรื่องการเปลี่ยนแปลงที่สัมพันธ์กับเวลาได้ เช่น การแพร่ขยายของโรคระบาด การเคลื่อนย้าย ถิ่นฐาน การบุกรุกทำลาย การเปลี่ยนแปลงของการใช้พื้นที่ฯลฯ ข้อมูลเหล่านี้เมื่อปรากฏบนแผนที่ทำให้สามารถแปลและสื่อความหมายใช้งานได้ง่าย

6) ระบบสารสนเทศเพื่อผู้บริหารระดับสูง (EIS : Excutive Information System) เป็นระบบที่สร้างขึ้นเพื่อสนับสนุนระบบสารสนเทศและการตัดสินใจสำหรับผู้บริหารระดับสูงโดยเฉพาะหรือสามารถจะกล่าวได้ว่าระบบนี้คือส่วนหนึ่งของ DSS ที่แยกออกมาเพื่อเน้นการให้สารสนเทศที่สำคัญต่อการบริการแก่ผู้บริหาร

7) ปัญญาประดิษฐ์ (AI : Artificial Intelligence) ระบบที่ทำให้เครื่องคอมพิวเตอร์กลายเป็นผู้ชำนาญการ ในสาขาใดสาขาหนึ่ง คล้ายกับมนุษย์ ระบบผู้เชี่ยวชาญมีส่วนคล้ายคลึงกับระบบอื่นๆ คือเป็นระบบคอมพิวเตอร์ที่ช่วยผู้บริหารแก้ไขปัญหาหรือทำการตัดสินใจได้ดีขึ้น อย่างไรก็ดีระบบผู้เชี่ยวชาญจะแตกต่างกับระบบอื่นอยู่มาก เนื่องจากระบบผู้เชี่ยวชาญจะเกี่ยวข้องกับการจัดการ ความรู้ (Knowledge) มากกว่าระบบสารสนเทศ และถูกออกแบบให้ช่วยในการตัดสินใจโดย

ใช้วิธีเดียวกับผู้เชี่ยวชาญที่มนุษย์โดยใช้หลักการทำงานด้วยระบบ ปัญญาประดิษฐ์ (Artificial Intelligence)

8) ระบบสำนักงานอัตโนมัติ (OAS : Office Automation System) เป็นระบบที่ใช้บุคลากรน้อยที่สุด โดยอาศัยเครื่องมือแบบอัตโนมัติและระบบสื่อสารเชื่องโยงข่าวสารระหว่างเครื่องมือเหล่านั้นเข้าด้วยกัน QAS มีจุดมุ่งหมายให้เป็นระบบที่ไม่ใช้กระดาษ (Paperless System) ส่งข่าว สารถึงกันด้วยข้อมูลอิเล็กทรอนิกส์ (Electronic Data Interchange) แทน ซึ่งมีรูปแบบในการใช้งาน 2 ลักษณะคือ

1. รูปแบบของระบบงานพิมพ์และการประมวลผลทางอิเล็กทรอนิกส์ (Electronic Publishing & Processing System) ได้แก่การสื่อสารด้วยข้อความ รูปภาพ จดหมายอิเล็กทรอนิกส์ (Electronic Mail : E-Mail) โทรสาร (FAX) หรือเสียงอิเล็กทรอนิกส์ (Voice Mail) เป็นต้น

2. รูปแบบการประชุมทางไกลด้วยระบบอิเล็กทรอนิกส์ (Electronic Meeting System) เป็นเทคนิคที่ทำให้กลุ่มคนทั่วโลกสามารถติดต่อสื่อสารกันได้คล้ายการพูดคุยกันโดยตรง เช่น การประชุมทางไกลแบบมีแต่เสียง (Audio Conferencing), การประชุมทางไกลแบบมีทั้งภาพและเสียง (Video Conferencing) หรือ ทั้งจดหมายอิเล็กทรอนิกส์ โทรสาร และ เสียงอิเล็กทรอนิกส์รวมกัน เป็นต้น

2.2 อินเตอร์เน็ต (Internet)

การเชื่อมต่อระบบสารสนเทศระบบงานต่างเชื่อมต่อด้วยเครือข่ายอินเตอร์เน็ต โดยความหมายของอินเตอรเน็ต คือ การเชื่อมต่อของระบบเครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เกิดจากการรวมตัวกันของหลายเครือข่ายย่อยทั้งจากส่วนบุคคลหรือจากองค์กร โดยผู้ใช้หรือผู้เป็นเจ้าของเครือข่ายย่อยจะต้องลงทุนด้านอุปกรณ์เองเพื่อเชื่อมต่อกับเครือข่ายอินเตอร์เน็ต อินเตอร์เน็ตจึงเป็นเครือข่ายที่ไม่มีใครเป็นเจ้าของโดยเบ็ดเสร็จ แต่อย่างไรก็ตามเครือข่ายอินเตอร์เน็ตก็จำเป็นต้องมีองค์กรคอยกำกับดูแลเพื่อให้มีความเป็นระเบียบเรียบร้อยและให้มีมาตรฐานในการใช้งานร่วมกัน

2.2.1 ความเป็นมาเกี่ยวกับอินเตอร์เน็ต

ปี ค.ศ. 1963 Advanced Research Projects Agency (ARPA) ซึ่งเป็นหน่วยงานที่อยู่ภายใต้กระทรวงกลาโหมสหรัฐได้ริเริ่มโครงการวิจัยเพื่อพัฒนาระบบเครือข่ายคอมพิวเตอร์ที่สื่อสารระยะไกล ได้ตั้งโครงการที่ชื่อว่า ARPANET โดยเป็นโครงการวิจัยที่ทำร่วมกับมหาวิทยาลัยต่างๆ เครือข่าย ARPANET ได้ถูกปรับปรุงพัฒนาให้มีความสมบูรณ์ขึ้นเรื่อยๆและได้นำไปใช้ในสถาบันการศึกษา และองค์กรพาณิชย์จนพัฒนาเป็นเครือข่ายอินเตอร์เน็ตในปัจจุบัน

2.2.2 เรื่องพื้นฐานเกี่ยวกับอินเตอร์เน็ต

2.2.2.1 โครงสร้างพื้นฐานระบบเครือข่าย (Network Infrastructure)

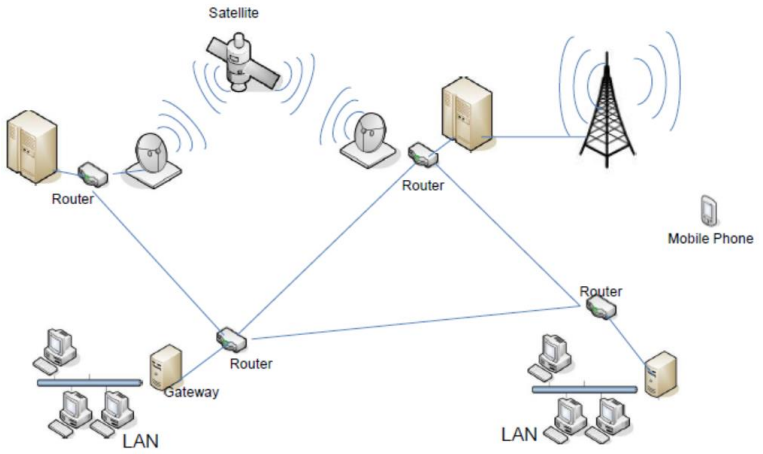
อินเตอร์เน็ต เป็นระบบเครือข่ายคอมพิวเตอร์ขนาดใหญ่ ดังนั้นจึงจำเป็นต้องมีโครงสร้างพื้นฐานของระบบเครือข่าย เพื่อรองรับการสื่อสารระหว่างคอมพิวเตอร์ได้แก่

1) ระบบเครือข่ายย่อย ซึ่งอาจเป็นเครือข่ายส่วนบุคคลหรือขององค์กร ที่ต้องการเชื่อมต่อกับอินเตอร์เน็ต เช่น LAN, MAN หรือ WAN

2) ระบบโครงข่ายการสื่อสาร เช่น โครงข่ายโทรศัพท์ โครงข่าย Fiber Oplics หรือ ระบบดาวเทียมเป็นต้น

3) เราเตอร์ (Router) ซึ่งเป็นอุปกรณ์สำหรับจัดการเส้นทางจราจรของข้อมูลที่ส่งผ่านอินเตอร์เน็ต

ภาพโครงสร้างพื้นฐานระบบเครือข่าย (Network Infrastructure) ดังภาพที่ 4



ภาพที่ 4 โครงสร้างพื้นฐานระบบเครือข่าย

(ที่มา : ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร , 2557)

2.2.2.2 โปโตตอล (Protocol)

โปรโตคอล (Protocol) คือมาตรฐานในการสื่อสารของระบบเครือข่ายอินเตอร์เน็ต เครื่องคอมพิวเตอร์ใดที่ต้องการจะเข้าร่วมเครือข่ายจะต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในโปโตคอลของระบบเครือข่ายนั้น โปรโตคอลของอินเตอร์เน็ตรียกว่า TCP/IP รายละเอียดดังนี้

1) TCP (Tansmission Control Protocol) ใช้สำหรับควบคุมรูปแบบการส่งข้อมูลในอินเตอร์เน็ต

2) IP (nternet Protoco) ใช้สำหรับควบคุมเกี่ยวกับการระบุตำแหน่งของเครื่องที่เชื่อมต่อกับอินเตอร์เน็ต

2.2.2.3 การส่งข้อมูลบนอินเตอร์เน็ต

การรับส่งข้อมูล เป็นแบบ Package Switching มีการแบ่งข้อมูลออกเป็นหน่วยย่อยๆ เรียกว่า Package แต่ละ Package จะมีการระบุส่วนหัว (Header) ซึ่งจะต้องระบุถึงที่หมายเลขที่อยู่ (IP address) ของปลายทางและต้นทาง และข้อมูลอื่นๆ แต่ละ Package จะถูกส่งไปในเครือข่ายซึ่งมีหลายเส้นทางที่จะไปถึงปลายทาง Router จะเป็นตัวจัดเส้นทางในการส่ง Packages ไปยังโหนดถัดไป แต่ละ Package อาจไม่ได้ไปเส้นทางเดียวกันทั้งหมดหรืออาจไม่ไปถึงปลายทางพร้อมกันทั้งหมด เมื่อไปถึงปลายทางเครื่องปลายทางจะรวบรวม Package ทั้งหมดเข้ามาแล้วคืนสภาพกลับมาเป็นข้อมูลเดิม

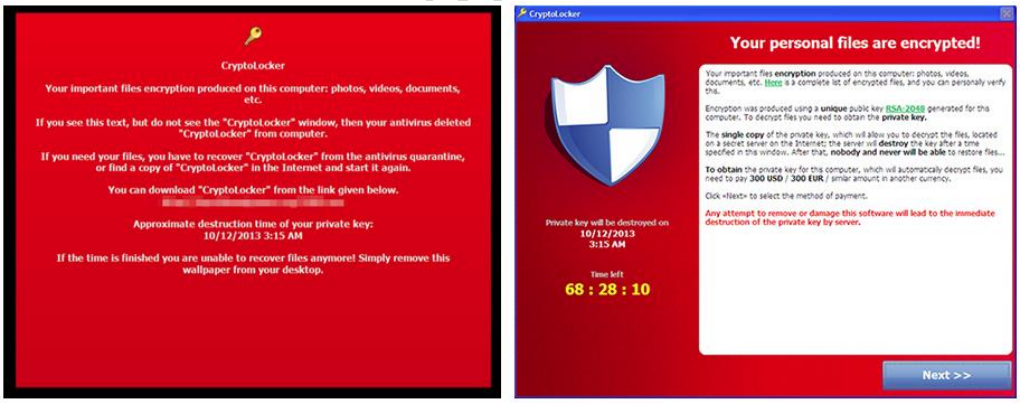
2.2.2.4 ผู้ให้บริการอินเตอร์เน็ต (Internet service provider)

Internet service provider (ISP) หรือ ผู้ให้บริการอินเทอร์เน็ต คือ บริษัทที่ให้ลูกค้าสามารถเข้าถึงอินเทอร์เน็ตได้โดยผู้ให้บริการจะเชื่อมโยงลูกค้าเข้ากับเทคโนโลยีรับและส่งข้อมูลที่เหมาะสมในการส่งผ่านอุปกรณ์บนโพรโทคอลอินเทอร์เน็ต เช่น Dial, DSL, Cable โมเด็มไร้สาย หรือการเชื่อมต่อระบบไฮสปีด เป็นต้น ทั้งนี้ผู้ให้บริการอินเทอร์เน็ตอาจให้บริการสำหรับเปิดบัญชีชื่อผู้ใช้ในอีเมล เพื่อติดต่อสื่อสารกับผู้อื่นโดยการ รับ-ส่ง ผ่านเซิร์ฟเวอร์ของผู้ให้บริการ ในบางครั้งผู้ให้บริการทางอินเทอร์เน็ตอาจให้บริการเก็บไฟล์ข้อมูลระยะไกล รวมถึงเรื่องเฉพาะทางอื่นๆ ด้วย

2.3 แรนซัมแวร์ (Ransomware)

ความเสี่ยงอย่างมากของระบบสารสนเทศขององค์กรต่างๆ คือการถูกแรนซัมแวร์ (Ransomware) โจมตี โดยแรนซัมแวร์ (Ransomware) เป็นมัลแวร์ (Malware) ประเภทหนึ่งที่มีลักษณะการทำงานที่แตกต่างกับมัลแวร์ประเภทอื่นๆ คือไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้ใช้งานแต่อย่างใด แต่มันจะทำการเข้ารหัสหรือล็อกไฟล์ ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ

ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใดๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อกเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ โดยข้อมูลหรือข้อความ “เรียกค่าไถ่” จะแสดงขึ้นหลังไฟล์ถูกเข้ารหัสเรียบร้อยแล้ว ดังภาพที่ 5 จำนวนเงินค่าไถ่ก็จะแตกต่างกันไป โดยเบื้องต้นก็จะมีราคาอยู่ที่ $150–$500 โดยประมาณ และการชำระเงินจะต้องชำระผ่านระบบที่มีความยากต่อการตรวจสอบหรือติดตาม เช่น การโอนเงินผ่านทางอิเล็กทรอนิกส์, Paysafecard หรือ Bitcoin เป็นต้น แต่อย่างไรก็ตาม การชำระเงินก็ไม่ได้หมายความว่าผู้ไม่หวังดีจะส่งคีย์ที่ใช้ในการปลดล็อกไฟล์ให้กับผู้ใช้งาน



ภาพที่ 5 ตัวอย่างข้อความ “เรียกค่าไถ่”

(ที่มา : สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย , ไม่ปรากฏปี)

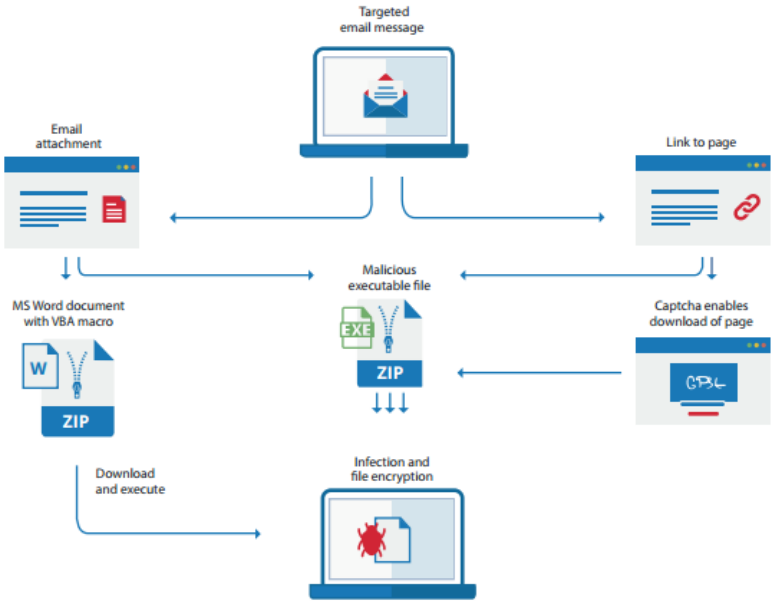
2.3.1 ช่องทางการแพร่กระจายของ Ransomware

แพร่กระจาย Ransomware โดยเบื้องต้นผู้ไม่หวังดีจะใช้วิธีการผ่านช่องทางต่างๆ ดังนี้

2.3.1.1 แฝงมาในรูปแบบเอกสารแนบทางอีเมล

ในกรณีส่วนใหญ่ Ransomware จะมาในรูปแบบเอกสารแนบทางอีเมล โดยอีเมลผู้ส่งก็มักจะเป็นผู้ให้บริการที่เรารู้จักกันดี เช่น ธนาคาร และจะใช้หัวข้อหรือประโยคขึ้นต้นที่ดูน่าเชื่อถืออย่าง “Dear Valued Customer”, “Undelivered Mail Returned to Sender”, “Invitation to connect on LinkedIn.” เป็นต้น ประเภทของไฟล์แนบที่เห็นก็จะเป็น “.doc” หรือ “.xls” ผู้ใช้อาจจะคิดว่าเป็นไฟล์เอกสาร Word หรือ Excel ธรรมดา แต่เมื่อตรวจสอบชื่อไฟล์

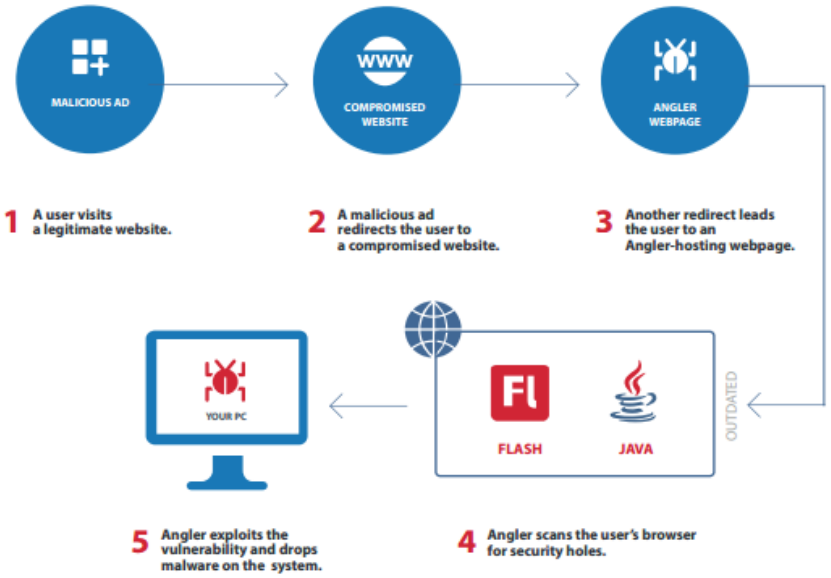
เต็มๆ ก็จะเห็นนามสกุล .exe ซ่อนอยู่ เช่น “Paper.doc.exe” แต่ผู้ใช้จะเห็นเฉพาะ “Paper.doc” และทำให้เข้าใจผิดว่าเป็นไฟล์ที่ไม่เป็นอันตรายแสดงดังภาพที่ 6



ภาพที่ 6 แสดงกระบวนการของ Ransomware ที่ถูกส่งมาทางอีเมล
(ที่มา : สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย , ไม่ปรากฏปี)

2.3.1.2 แฝงตัวมาในรูปแบบของ Malvertising (โฆษณา)

Ransomware นี้อาจจะมาในรูปแบบของโฆษณา ไม่ว่าจะเป็นโฆษณาที่ฝังมากับซอฟต์แวร์หรือตามหน้าเว็บไซต์ต่างๆ เชื่อมโยงไปยังเว็บไซต์อันตรายและอาศัยช่องโหว่ของซอฟต์แวร์ ผู้ใช้ยังสามารถจะกลายเป็นเหยื่อได้โดยไม่ได้ตั้งใจเพียงเข้าเยี่ยมชมหน้าเว็บที่ถูกผู้ไม่หวังดีเข้ามาควบคุม ตัวอย่างเช่น ถูกดาวน์โหลดโค้ด (Code) ที่เป็นอันตรายผ่านทางโฆษณาแบนเนอร์ใน Flash โดย Ransomware มักจะใช้ประโยชน์จากข้อบกพร่องหรือช่องโหว่ด้านความปลอดภัยอื่นๆ ในเบราว์เซอร์, แอปพลิเคชั่น หรือ ระบบปฏิบัติการ บ่อยครั้งก็มักจะเกิดจากช่องโหว่ในเว็บเบราว์เซอร์, Java และ PDF แต่ช่องโหว่ที่พบมากที่สุดก็คือใน Flash ดังภาพที่ 7



ภาพที่ 7 แสดงกระบวนการทำงานของ Ransomware ที่อาศัยช่องโหว่ของซอฟต์แวร์
(ที่มา : สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย , ไม่ปรากฏปี)

2.3.1.3 แฝงตัวมาในรูปแบบของ โปรแกรมเถื่อนจากอินเตอร์เน็ต

Ransomware นี้อาจจะมาในรูปแบบของโปรแกรมเถื่อน ที่ผู้ใช้งาน ทั้งระบบปฏิบัติงาน windows os และ mac os ไปดาวน์โหลดมาจากอินเตอร์เน็ต ที่แหล่งที่มาไม่ปลอดภัย ซึ่งผู้ไม่หวังดีปรับแต่งการทำงานของซอฟต์แวร์นั้น เมื่อผู้ใช้งานทำการติดตั้ง โปรแกรมที่ผู้ไม่หวังดีสามารถแพร่กระจาย Ransomware ไปยังเครื่องของผู้ที่ติดตั้งโปรแกรมเถื่อนนั้น และทำงาน lock เครื่อง หรือ lock ไฟล์ต่างๆให้เปิดไม่ได้ จนกว่าผู้ใช้งานจะยอมจ่ายค่าไถ่กับทางผู้ไม่หวังดี

2.3.2 วิธีป้องกัน Ransomware

2.3.2.1 ทำการสำรองข้อมูล (Backup)

โดยทำเป็นประจำหากผู้ใช้งานติด Ransomware อย่างน้อยถ้ามีการสำรองข้อมูล (Backup) ก็จะสามารถกู้คืนไฟล์ได้ และเพื่อป้องกันข้อมูลที่ Backup ถูกเข้ารหัสไปด้วย ผู้ใช้งานควรสำรองข้อมูลลงบนอุปกรณ์สำหรับจัดเก็บข้อมูลภายนอกเครือข่าย (Cloud Storage, External Hard Drive, USB Flash Drive) ด้วยเหตุนี้เององค์กรต่างๆจึงควร มีระบบการสำรองข้อมูล

2.3.2.2 อัปเดตซอฟต์แวร์ในเครื่องอย่างสม่ำเสมอ

การอัปเดตระบบปฏิบัติการและซอฟต์แวร์จะช่วยป้องกันการโจมตีที่ต้องอาศัยช่องโหว่ของซอฟต์แวร์ได้ โดยเฉพาะอย่างยิ่งใน Adobe Flash, Microsoft Silverlight และเว็บเบราว์เซอร์ ควรติดตามและอัปเดตให้เป็น Version ปัจจุบัน

2.3.2.3 ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware)

ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) ลงบนเครื่องคอมพิวเตอร์เพื่อป้องกันการเข้าถึงเว็บไซต์ที่เป็นอันตรายและตรวจสอบไฟล์ทั้งหมดที่ถูกดาวน์โหลด ควรมีการติดตั้งโปรแกรมป้องกันมัลแวร์ลงบนเครื่องคอมพิวเตอร์ไว้ด้วย ตรวจสอบอีเมลที่เป็นอันตรายเบื้องต้น ผู้ไม่หวังดีมักใช้อีเมลเป็นช่องทางในการหลอกลวงผู้ใช้งานให้หลงเชื่อเปิดหรือดาวน์โหลดเอกสารแนบ ดังนั้น เมื่อเราได้รับอีเมลควรตรวจสอบอีเมลฉบับนั้นให้ดีเสียก่อน

2.3.2.4 ติดตามข่าวสาร

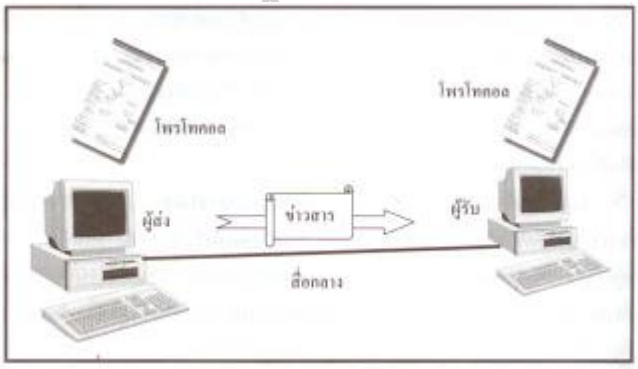
ติดตามข่าวสาร ควรติดตามข่าวสารช่องโหว่หรือภัยคุกคามต่างๆ รวมถึงศึกษาวิธีการป้องกันเพื่อไม่ให้ตกเป็นเหยื่อของเหล่าผู้ไม่หวังดีและเพื่อความปลอดภัยของตัวผู้ใช้งานเอง

2.4 หลักการข้อมูลสื่อสาร (Data Communitation)

หลักการข้อมูลสื่อสาร (Data Communitation) คือ การรับส่ง โอน ย้าย หรือแลกเปลี่ยนข้อมูลและข่าวสาร (Information) จากผู้ส่งไปยังผู้รับข้อมูล โดยการสื่อสารผ่านสื่อซึ่งเป็นตัวกลางในการรับและส่งข้อมูล วัตถุประสงค์ของการสื่อสาร คือ ผู้ส่งต้องการให้ผู้รับสารเข้าใจถึงความหมายของข้อมูลข่าวสารที่ส่งไป ดังภาพที่ 8 ซึ่งจะประกอบด้วยองค์ประกอบของการสื่อสาร 6 ประการ คือ

1) ผู้ส่งข้อมูล (Source) เป็นแหล่งกำเนิดข้อมูล ข่าวสาร อาจเป็นสิ่งมีชีวิต
2) ผู้รับข้อมูล (Destination) เป็นจุดหมายปลายทางของข้อมูลข่าวสาร นำข้อมูลข่าวสารที่ได้รับไปใช้
3) สื่อกลาง (Transmission medium) เป็นสื่อกลางหรือช่องทางที่ใช้สำหรับข้อมูลข่าวสารผ่าน เช่น สายโทรศัพท์ สาย fiber optic อากาศ
4) ตัวแปลงสัญญาณ ได้แก่ Transmitter ทำหน้าที่แปลงข้อมูลให้เป็นสัญญาณและ Receiver ทำหน้าที่แปลงสัญญาณให้เป็นข้อมูล เช่น Modem, โทรศัพท์ เป็นต้น

5) โปรโตคอล (Protocol) คือ กฎเกณฑ์หรือข้อกำหนดที่ควบคุมการสื่อสารให้ผู้ส่งและผู้รับสามารถแลกเปลี่ยนข้อมูลข่าวสารกันได้และสามารถเข้าใจความหมายของข้อมูลข่าวสารตรงกัน เช่น ภาษามือ,ภาษาพูด, Protocol TCP/IP, HTTP, FTP เป็นต้น
6) ข้อมูล (Data) เป็นข้อเท็จจริงที่ใช้แลกเปลี่ยนระหว่างผู้ส่งและผู้รับ มีได้หลายรูปแบบ เช่น ข้อความ ภาพ เสียง การส่งข้อมูลให้ผู้รับนั้นมีทิศทางการส่งข้อมูลที่แตกต่างกัน เช่น การดูโทรทัศน์ หรือฟังวิทยุ



ภาพที่ 8 แผนภาพแสดงการสื่อสารข้อมูล

2.4.1 ทิศทางการสื่อสารข้อมูล (Transmission Mode)

การส่งข้อมูลให้ผู้รับนั้นมีทิศทางการส่งข้อมูลที่แตกต่างกัน เช่น การดูโทรทัศน์ หรือฟังวิทยุเป็นการสื่อสารทิศทางเดียวกัน หรือการคุยโทรศัพท์ การแชทผ่านโปรแกรม Line ระหว่างคอมพิวเตอร์ เป็นการสื่อสารสองทิศทางพร้อมกัน เนื่องจากต้องการผลตอบกลับทันทีทันใด ซึ่งจะทำการสื่อสารแบบใดนั้นขึ้นอยู่กับวัตถุประสงค์ของการสื่อสารข้อมูล ทั้งนี้คุณภาพของการสื่อสารข้อมูลขึ้นอยู่กับปัจจัยหลายประการ เช่น ชนิดของสัญญาณ ข้อมูลที่ถูกส่งไป หรือคุณภาพของ สื่อที่เป็นตัวกลางนำสัญญาณข้อมูลไปยังปลายทาง ทิศทางการสื่อสารข้อมูล (Transmission Mode) สามารถแบ่งได้มี 3 รูปแบบ แสดงภาพที่ 9 รายละเอียดดังนี้

2.4.1.1 Simplex

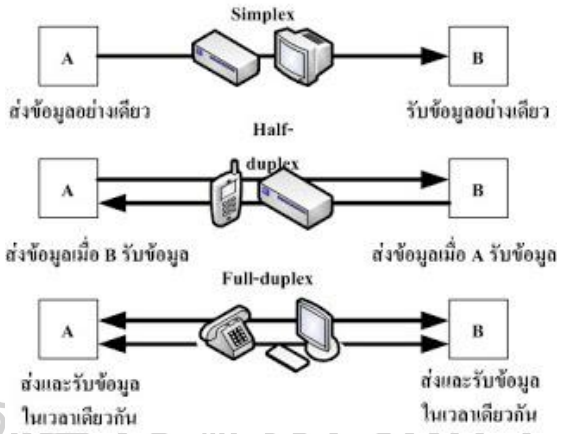
ส่งทางเดียวและรับทางเดียว คือ ขณะที่ผู้ส่งข้อมูลผู้รับจะไม่สามารถส่งข้อมูลกลับมาให้ผู้ส่งได้ในช่องทางเดียวกัน เช่น การแพร่ภาพสัญญาณโทรทัศน์ หรือการแพร่สัญญาณคลื่นวิทยุ

2.4.1.2 Half duplex

สามารถส่งได้ทั้งสองทาง แต่ไม่สามารถส่งพร้อมกันได้ในเวลาเดียวกันในช่องทางเดียวกัน คือเมื่อผู้ส่งส่งข้อมูลให้ผู้รับ ผู้รับสามารถส่งข้อมูลกลับมาให้ผู้ส่งในช่องทางเดียวกันได้แต่ต้องทำคนละเวลา เช่น วิทยุสื่อสารของทหาร

2.4.1.3 Full duplex

สามารถส่งพร้อมๆ กันทั้งสองทางได้ คือ เมื่อผู้ส่งส่งข้อมูลให้ผู้รับ ผู้รับสามารถส่งข้อมูลกลับมาให้ผู้ส่งในช่องทางเดียวกันในเวลาเดียวกันได้ เช่นการสื่อสารทางโทรศัพท์



ภาพที่ 9 รูปแบบทิศทางสื่อสารข้อมูล

2.4.2 ชนิดของสัญญาณข้อมูล (Data signal type)

ข้อมูลที่จะสื่อสารจะต้องถูกแปลงเป็นสัญญาณไฟฟ้าที่เรียกว่า สัญญาณข้อมูล (Data Signal) ทำให้สามารถส่งผ่านสื่อไปในระยะทางไกลด้วยความเร็วสูง ข้อมูลจะถูกแปลงเป็นสัญญาณข้อมูลได้ 2 ประเภท ดังนี้

2.4.2.1 สัญญาณอะนาล็อก (Analog Signal)

คือ สัญญาณข้อมูลแบบต่อเนื่อง (Continuous Data) มีขนาดของสัญญาณไม่คงที่ ข้อมูลอนาล็อกและสัญญาณ อนาล็อกมีลักษณะเป็นคลื่นรูป sine wave ดังภาพที่ 10 สามารถถูกรบกวนได้ง่ายจำแนกสัญญาณรบกวน (Noise) หากมีสัญญาณรบกวนปะปนมากับสัญญาณอนาล็อกแล้ว จะส่งผลให้การส่งข้อมูลช้าลงและทำให้การจำแนกหรือตัดสัญญาณรบกวนออกจากข้อมูลต้นฉบับทำได้ยาก เมื่อสัญญาณอนาล็อกถูกส่งบนระยะทางที่ไกลออกไป ระดับสัญญาณจะถูกลดทอนลง ดังนั้นจึงต้องใช้อุปกรณ์ที่เรียกว่า Amplifier ซึ่งเป็นอุปกรณ์ในการเพิ่มกำลังหรือความเข้ม

ให้สัญญาณ ทำให้สามารถส่งสัญญาณในระยะทางที่ไกลออกไป แต่การเพิ่มกำลังของสัญญาณของ Amplifier จะส่งผลให้สัญญาณรบกวน (Noise) ขยายเพิ่มขึ้นด้วยสัญญาณ Analog โดยทั่วไปจะประกอบด้วยส่วนพื้นฐาน 3 ประการ ดังนี้

1) แอมพลิจูด (Amplitude)

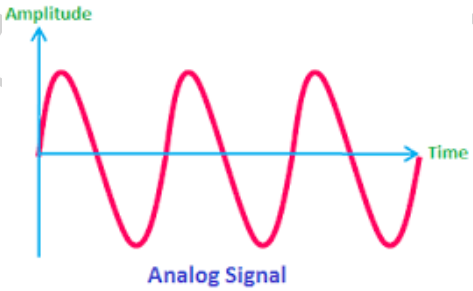
สัญญาณอนาล็อกที่มีการเคลื่อนที่ในลักษณะเป็นรูปคลื่นขึ้นลงสลับกัน และก้าวไปตามเวลาแบบสมบูรณ์นั้น เรียกว่า คลื่นซายน์ (Sine Wave) แอมพลิจูดจะเป็นค่าที่วัดจากแรงดันไฟฟ้า ซึ่งอาจเป็นระดับของคลื่นจุดสูงสุด (High Amplitude) หรือจุดต่ำสุด (Low Amplitude) และแทนด้วยหน่วยวัดเป็นโวลต์ (Volt)

2) ความถี่ (Frequency)

หมายถึง อัตราการขึ้นลงของคลื่น ซึ่งเกิดขึ้นจำนวนรอบใน 1 วินาที โดยความถี่นั้นจะใช้แทนหน่วยวัดเป็นเฮิรตซ์ (Hertz : Hz) คาบ (Period) เป็นระยะเวลาของสัญญาณที่เปลี่ยนแปลงไปจนครบรอบ โดยจะมีรูปแบบซ้ำๆ กันในทุกช่วงเวลา โดยหน่วยวัดของคาบเวลาจะใช้เป็นวินาที และเมื่อคลื่นสัญญาณทำงานครบ 1 รอบ จะเรียกว่า Cycle

3) เฟส (Phase)

เฟส เป็นการเปลี่ยนแปลงของสัญญาณ ซึ่งจะวัดจากตำแหน่งองศาของสัญญาณเมื่อเวลาผ่านไป โดยเฟสสามารถเปลี่ยนแปลงตำแหน่ง (Phase Shift) ในลักษณะเลื่อนไปข้างหน้าหรือข้างหลัง



ภาพที่ 10 รูปแบบสัญญาณ Analog คลื่นรูป sine wave

2.4.2.2 สัญญาณดิจิทัล (Digital Signals)

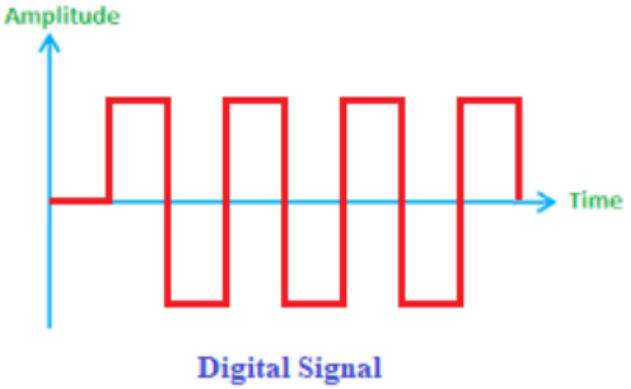
คือ สัญญาณข้อมูลแบบไม่ต่อเนื่อง (Non Continuous Data) เป็นคลื่นแบบไม่ต่อเนื่อง มีรูปแบบของระดับแรงดันไฟฟ้าเป็นคลื่นสี่เหลี่ยม (Square Wave) โดยสัญญาณสามารถเปลี่ยนแปลงจาก 0 เป็น 1 หรือจาก 1 เป็น 0 ซึ่งเป็นการเปลี่ยนสัญญาณในลักษณะก้าวกระโดด

แสดงดังภาพที่ 11 ข้อดีของสัญญาณดิจิทัล คือ สามารถสร้างสัญญาณด้วยต้นทุนที่ต่ำกว่า และทนทานต่อสัญญาณรบกวนได้ดีกว่า และยังสามารถจำแนกระหว่างข้อมูลกับสัญญาณได้ง่ายกว่า หากมีสัญญาณรบกวนไม่มาก ก็ยังสามารถคงรูปสัญญาณเดิมได้ สัญญาณดิจิทัลส่วนใหญ่เป็นสัญญาณชนิดไม่มีคาบ ดังนั้น คาบเวลาและความถี่จึงไม่นำมาใช้งาน โดยมีคำที่เกี่ยวข้อง 2 คาบ คือ

1) Bit Interval ซึ่งมีความหมายเช่นเดียวกับคาบ โดย Bit Interval คือ เวลาที่ส่งข้อมูล 1 บิต

2) Bit Rate คือ จำนวนของ Bit Interval ต่อวินาที โดยมีหน่วยวัดเป็น บิตต่อวินาที (bps)

โดย ไบนารี่ 1 แทนแรงดันบวก ไบนารี 0 แทนแรงดันศูนย์สัญญาณดิจิทัลสามารถมีจำนวนระดับสัญญาณมากกว่า 2 ระดับ โดยในแต่ละระดับสามารถส่งบิตมากกว่าหนึ่งบิต โดยทั่วไปถ้าสัญญาณมีจำนวน L ระดับ ในแต่ละระดับของสัญญาณก็จะสามารถส่งข้อมูลได้จำนวน Log2L บิต



ภาพที่ 11 รูปแบบสัญญาณ Digital

2.4.3 หน่วยวัดความเร็วในการส่งข้อมูล

2.4.3.1 บิต (bit)

บิต คือ binary digit ตัวเลขในระบบฐาน 2 คือ 0 กับ 1 ในการประมวลผลและการเก็บข้อมูล บิต เป็นหน่วยที่เล็กที่สุดของสารสนเทศ (information) ซึ่งคอมพิวเตอร์สามารถจัดการได้

2.4.3.2 ไบต์ (byte)

ไบต์ คือ บิต (bit) จำนวน 8 บิต เรียงต่อกัน ในการประมวลผลของคอมพิวเตอร์นั้นในคลังข้อมูลหน่วยของสารสนเทศได้แก่ อักษร ตัวเลข เครื่องหมายวรรคตอน และอื่นๆ ที่ใช้ในระบบ เพราะว่าไบต์ ใช้แทนปริมาณสารสนเทศได้เพียงเล็กน้อย ดังนั้น ในคลังข้อมูลและใน

หน่วยความจำมักจะใช้ กิโลไบต์ ซึ่งเท่ากับ 1024 ไบต์ หรือ เมกะไบต์ ซึ่งเท่ากับ 1,048,576 ไบต์ เป็นต้นแทน

สามารถสรุปการวัดขนาดข้อมูลได้ดังนี้

1 Byte (ไบต์) = 1 ตัวอักษร

1 KB (กิโลไบต์) = 1024 ตัวอักษร

1 MB (เมกกะไบต์) = 1024 KB

1 GB (กิกะไบต์) = 1024 MB

1 TB (เทราไบต์)= 1024 GB

2.4.3.3 อัตราบิต (Bit Rate/Data Rate)

อัตราบิต คือ จำนวนบิตที่สามารถส่งได้ภายในหนึ่งหน่วยเวลา ซึ่งมีหน่วยเป็นบิตต่อวินาที (bit per second : bps) สามารถเขียนเป็น สมการได้ดังนี้

Bit Rate = baud rate x the number of bit per baud

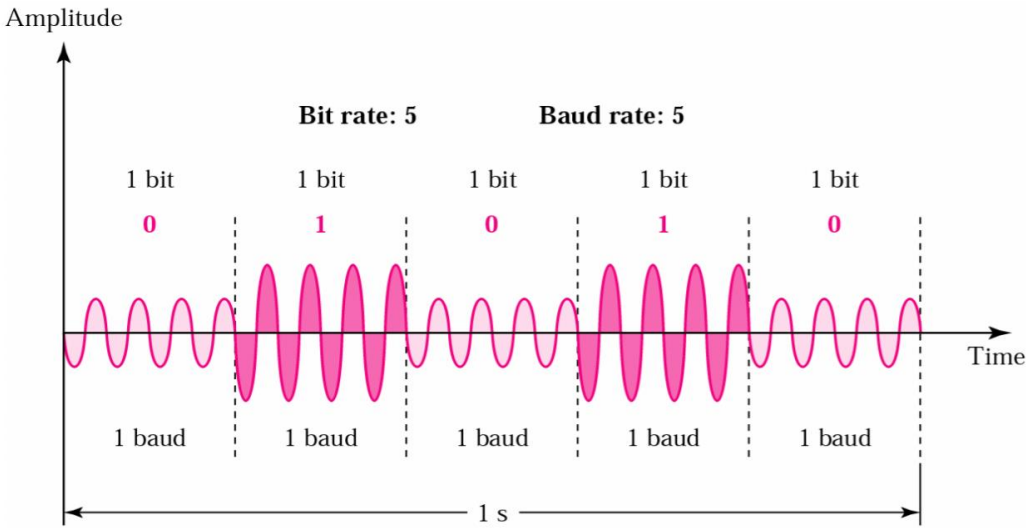
2.4.3.4 อัตราบอด (Baud Rate)

อัตราบอด (Baud Rate) คือ จำนวนของสัญญาณที่สามารถส่งได้ต่อการเปลี่ยนสัญญาณในหนึ่งหน่วยเวลา (baud per second) ปกติอัตราบอดจะมีค่าน้อยกว่าหรือเท่ากับอัตราบิต และแบนด์วิดในระบบสื่อสารนั้นจะขึ้นอยู่กับอัตราบอด สมการได้ดังนี้

Baud Rate = bit rate / the number of bit per baud

สามารถอธิบายเปรียบเทียบกับระบบขนส่งต่อไปนี้ โดย อัตราบอด คือ รถโดยสาร อัตราบิต คือ ผู้โดยสาร

- รถโดยสารสามารถบรรทุกผู้โดยสารได้ครั้งละหนึ่งคนหรือมากกว่า
- หากมีจำนวนรถโดยสาร 1,000 คัน บรรทุกผู้โดยสารคันละหนึ่งคน (1,000 คน)
- หากรถโดยสารแต่ละคันบรรทุกผู้โดยสารได้คันละ 4 คน (4,000 คน) การจราจรที่คล่องตัวย่อมขึ้นอยู่กับจำนวนรถโดยสาร ดังนั้นแบนด์วิดธ์ในระบบสื่อสารจึงขึ้นอยู่กับอัตราบอด



ภาพที่ 12 แสดงรูปแบบของ bit rate และ baud rate

โดยปกติแล้วสัญญาณดิจิทัลจะรับส่งข้อมูลดิจิทัล และสัญญาณอนาล็อกก็จะรับส่งข้อมูลอนาล็อก แต่เราสามารถใช้สัญญาณอนาล็อกเพื่อรับส่งข้อมูลดิจิทัล และใช้สัญญาณดิจิทัลเพื่อรับส่งข้อมูลอนาล็อกได้ การส่งผ่านด้วยสัญญาณอนาล็อกหรือดิจิทัลจะขึ้นอยู่กับสื่อกลางที่ใช้ในระบบสื่อสาร โดยที่สามารถส่งข้อมูลด้วยรูปแบบใดก็ได้ เพียงแต่จำเป็นต้องมีการแปลงรูปหรือเข้ารหัสข้อมูลให้อยู่ในรูปแบบของสัญญาณที่เหมาะสมกับสื่อกลางประเภทนั้นๆ การแปลงข้อมูลระหว่างอนาล็อกและดิจิทัลประกอบไปด้วย

1) การแปลงข้อมูลอนาล็อกเป็นสัญญาณอนาล็อก (Analog Data to Analog Signals)
2) การแปลงข้อมูลดิจิทัลเป็นสัญญาณดิจิทัล (Digital Data to Digital Signals)
3) การแปลงข้อมูลดิจิทัลเป็นสัญญาณอนาล็อก (Digital Data to Analog Signals)
4) การแปลงข้อมูลอนาล็อกเป็นสัญญาณดิจิทัล (Analog Data to Digital Signals)
5) การแปลงข้อมูลอนาล็อกเป็นสัญญาณอนาล็อก (Analog Data to Analog Signals)

ในการแปลงข้อมูลอนาล็อกให้เป็นสัญญาณอนาล็อกเป็นรูปแบบที่ง่าย มีต้นทุนต่ำ โดยจะมีอุปกรณ์ทำหน้าที่แปลงสัญญาณและได้ผลลัพธ์เป็นสัญญาณอนาล็อก เช่น ระบบวิทยุกระจายเสียง

2.4.3.5 การ Tranfers File

การถ่ายโอนข้อมูลระหว่าอุปกรณ์ หรือ เครื่องคอมพิวเตอร์เซิร์ฟเวอร์ (Server) แบ่งออกเป็น 2 ส่วนคือ

1) การดาวน์โหลด (Download) หมายถึง การดึงข้อมูลจากคอมพิวเตอร์อีกเครื่องหนึ่ง ซึ่งเป็นต้นทางมาเก็บไว้ยังเครื่องของเรา โดยผ่านเครือข่ายคอมพิวเตอร์

2) การอัปโหลด (Upload) หมายถึง การนำข้อมูลจากเครื่องคอมพิวเตอร์ที่ใช้อยู่ไปเก็บไว้ยังเครื่องคอมพิวเตอร์ อีกเครื่องที่ปลายทาง โดยผ่านเครือข่ายคอมพิวเตอร์

2.4.3.5.1 อัตราความเร็วในการถ่ายโอนข้อมูล

ตามสมการทางคณิตศาสตร์เราสามารถหาอัตราความเร็วของการถ่ายโอนข้อมูลได้จากสมการ

$$\text{ความเร็วในการถ่ายโอน } (S) = \frac{\text{ขนาดข้อมูล } (A)}{\text{เวลา } (T)}$$

และสามารถหาเวลาที่ใช้ในการถ่ายโอนไฟล์ ได้จาก

$$\text{เวลา } (T) = \frac{\text{ขนาดข้อมูล } (A)}{\text{ความเร็วในการถ่ายโอน } (S)}$$

โดยกำหนดให้

ความเร็วในการถ่ายโอน (S) มีหน่วยลงท้ายเป็น = Byte

ขนาดข้อมูล (A) มีหน่วยลงท้ายเป็น = Byte

เวลา (T) มีหน่วยลงท้ายเป็น = s (วินาที)

2.5 คอมพิวเตอร์เซิร์ฟเวอร์ (Server)

เซิร์ฟเวอร์ (Server) คือเครื่องคอมพิวเตอร์หรือระบบปฏิบัติการหรือโปรแกรมคอมพิวเตอร์ ที่ทำหน้าที่ให้บริการอย่างใดอย่างหนึ่งหรือหลายอย่างแก่เครื่องคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่เป็นลูกข่าย ในระบบเครือข่ายเซิร์ฟเวอร์ ในทาง Computer โดยปกติแล้ว โปรแกรมคอมพิวเตอร์ที่เป็นเซิร์ฟเวอร์ จะทำงานบนระบบปฏิบัติการ อาจจะเป็น Linux หรือ Windows Server จึงไม่ได้หมายถึง คอมพิวเตอร์เพียงอย่างเดียวแต่ยังหมายถึงระบบปฏิบัติการคอมพิวเตอร์หรือโปรแกรม

คอมพิวเตอร์เซิร์ฟเวอร์ซึ่งเป็นอุปกรณ์ที่มีส่วนสำคัญมากในระบบอินเตอร์เน็ตและในระบบเครือข่าย ซึ่งความสามารถของเซิร์ฟเวอร์นั้นเราสามารถประยุกต์ใช้ได้ตามหน้าที่และลักษณะงานให้เข้ากับเซิร์ฟเวอร์ประเภทต่างๆ เพื่อประสิทธิภาพในการทำงานที่ดีที่สุด

2.5.1 หน้าที่ของ เซิร์ฟเวอร์ (Server)

หน้าที่ของเซิร์ฟเวอร์นั้นมีหลากหลายขึ้นอยู่กับลักษณะงานโดยสามารถแบ่งตามประเภทงานได้เป็น 5 หน้าที่หลักๆ ดังต่อไปนี้

1) Web server มีหน้าที่ให้บริการด้านการจัดการเว็บไซต์ โดยส่วนมากโปรแกรมที่นิยมใช้เป็น Web server จะเป็น Apache web server
2) Mail server มีหน้าที่ให้บริการด้าน E-mail โปรแกรมที่ใช้ในด้าน Mail server มีอยู่หลายโปรแกรมด้วยกันแต่ที่นิยมกันจะมีอยู่ 3 โปรแกรมคือ Postfix, qmail, courier
3) DNS server มีหน้าที่ให้บริการด้านโดเมนเนมที่จะค่อยเปลี่ยนชื่อเว็บไซต์ที่เราต้องการให้เป็น IP Address โปรแกรมที่นิยมใช้คือ bind9
4) Database server มีหน้าที่ให้บริการด้านการจัดการดูแลข้อมูลต่างๆ ภายในเว็บไซต์ โปรแกรมที่มีการใช้งานส่วนใหญ่จะเป็น mysql, postgresql, DB2
5) File server มีหน้าที่ให้บริการแชร์ไฟล์เพื่อให้ใช้งานร่วมกัน เช่น Word, Excel, หรือรูปภาพ เป็นต้น

โดยการทำงานของ Server จะทำงานพร้อมกันหลายๆ อย่างได้ในเวลาเดียวกัน เนื่องจากความสามารถของเครื่อง Server ส่วนใหญ่จะมีความสามารถที่สูง โดยการทำงานแต่ละอย่างของระบบเซิร์ฟเวอร์จะทำงานใน Port ที่ต่างกันไป

2.5.2 ระบบปฏิบัติการ เซิร์ฟเวอร์ (Server)

สำหรับระบบปฏิบัติการที่นิยมใช้เป็น server ได้แก่

1) Linux สำหรับ Linux Distribution ที่ได้รับความนิยมได้แก่ Debian Ubuntu Readhat Fedora etc.
2) Windows สำหรับ Windows ที่นิยมใช้เป็น server ได้แก่ อ 2003 , 2008 , 2012 , 2016 , 2019

3) Unix สำหรับ Unix ถือเป็นระบบปฏิบัติการที่เก่าแก่ระบบหนึ่ง ที่ยังใช้งานอยู่จนถึงทุกวันนี้ ได้แก่ BSD

2.6 ระบบฐานข้อมูล (Database System)

ระบบฐานข้อมูล (Database System) คือ ระบบบริหารจัดการฐานข้อมูลคือชุดคำสั่ง หรือโปรแกรม หรือ ซอฟท์แวร์ที่สร้างขึ้นมาเพื่อทำหน้าที่บริหารจัดการฐานข้อมูล เช่น รวบรวมข้อมูลให้เป็นระบบสะดวกและง่ายต่อการจัดการเกี่ยวกับระบบแฟ้มข้อมูลภายในฐานข้อมูล (การเก็บรักษา การเรียกใช้ การแก้ไข การเข้าถึงข้อมูล) รวมถึงการที่จะนำมาปรับปรุงให้ทันสมัย ระบบบริหารจัดการฐานข้อมูลจะทำหน้าที่เป็นเครื่องมือ หรือเป็นตัวกลางระหว่างผู้ใช้ชุดคำสั่งต่างๆ ที่เกี่ยวข้องกับฐานข้อมูล เพื่อจัดการและควบคุมความถูกต้อง ความซ้ำซ้อนและความสัมพันธ์ระหว่างข้อมูลที่อยู่ภายในฐานข้อมูลรวมถึงการรักษาความมั่นคง ความปลอดภัยของข้อมูล การสำรองข้อมูล และการเรียกคืนข้อมูลในกรณีที่ข้อมูลเกิดความเสียหาย โดยที่ผู้ใช้ไม่จำเป็นต้องทราบถึงรายละเอียดภายในโครงสร้างของฐานข้อมูล ตัวอย่างของระบบบริหารจัดการฐานข้อมูลที่นิยมใช้กันอย่างแพร่หลาย เช่น MySQL, PostgreSQL, Microsoft Access, SQL Server, FileMaker, Oracle, Sybase, dBASE, Clipper และ FoxPro เป็นต้น อาจจะสรุปได้ว่าระบบบริหารจัดการฐานข้อมูล คือ กลุ่มของโปรแกรม หรือซอฟต์แวร์ที่ทำหน้าที่เป็นตัวกลางสำหรับดูแลจัดการควบคุมความถูกต้อง ความซ้ำซ้อนและความสัมพันธ์ระหว่างข้อมูลต่างๆ เกี่ยวกับฐานข้อมูล และอำนวยความสะดวกให้กับผู้ใช้ ทั้งในด้านการสร้าง และการปรับปรุงแก้ไขระบบบริหารจัดการฐานข้อมูลที่ดี จะต้องมีความสามารถในการจัดการที่หลากหลายความสามารถพื้นฐานที่ระบบบริหารจัดการฐานข้อมูลทุกตัวจะต้องมี คือความ สามารถใน การจัดเก็บข้อมูล การเรียกค้น การแก้ไขเปลี่ยนแปลง การลบ และการเพิ่มเติม เป็นต้น

2.6.1 ความสำคัญของระบบฐานข้อมูล

ความสำคัญของระบบฐานข้อมูล คือ การจัดข้อมูลให้เป็นระบบฐานข้อมูลทำให้ข้อมูลมีส่วนดีกว่าการเก็บข้อมูลในรูปของแฟ้มข้อมูล เพราะการจัดเก็บข้อมูลในระบบฐานข้อมูล จะมีส่วนที่สำคัญกว่าการจัดเก็บข้อมูลในรูปของแฟ้มข้อมูลดังนี้

1) ลดการเก็บข้อมูลที่ซ้ำซ้อน ข้อมูลบางชุดที่อยู่ในรูปของแฟ้มข้อมูลอาจมีปรากฏอยู่หลายๆ แห่ง เพราะมีผู้ใช้ข้อมูลชุดนี้หลายคนเมื่อใช้ระบบฐานข้อมูลแล้วจะช่วยให้ความซ้ำซ้อนของ

ข้อมูลลดน้อยลง เช่น ข้อมูลอยู่ในแฟ้มข้อมูลของผู้ใช้หลายคน ผู้ใช้แต่ละคนจะมีแฟ้มข้อมูลเป็นของตนเอง ระบบฐานข้อมูลจะลดการซ้ำซ้อนของข้อมูลเหล่านี้ให้มากที่สุดโดยจัดเก็บในฐานข้อมูลไว้ที่เดียวกัน ผู้ใช้ทุกคนที่ต้องการใช้ข้อมูลชุดนี้จะใช้โดยผ่านระบบฐานข้อมูล ทำให้ไม่เปลืองเนื้อที่ในการเก็บข้อมูลและลดความซ้ำซ้อนลงได้

2) รักษาความถูกต้องของข้อมูล เนื่องจากฐานข้อมูลมีเพียงฐานข้อมูลเดียวในกรณีที่มีข้อมูลชุดเดียวกันปรากฏอยู่หลายแห่งในฐานข้อมูล ข้อมูลเหล่านี้จะต้องตรงกัน กรณีถ้ามีการแก้ไขข้อมูลนี้ทุกๆ แห่งที่ข้อมูลปรากฏอยู่จะแก้ไขให้ได้ถูกต้องตามกันหมดโดยอัตโนมัติด้วยระบบจัดการฐานข้อมูล

3) การป้องกันและรักษาความปลอดภัยให้กับข้อมูลทำได้อย่างสะดวก การป้องกันและรักษาความปลอดภัยกับข้อมูลระบบฐานข้อมูลจะให้เฉพาะผู้ที่เกี่ยวข้องเท่านั้นจึงจะมีสิทธิ์เข้าไปใช้ฐานข้อมูลได้เรียกว่ามีสิทธิส่วนบุคคล (privacy) ซึ่งจะก่อให้เกิดความปลอดภัย (security) ของข้อมูลด้วย ฉะนั้นผู้ใดที่จะมีสิทธิ์ที่จะเข้าถึงข้อมูลได้จะต้องมีการกำหนดสิทธิ์กันไว้ก่อนและเมื่อเข้าไปใช้ข้อมูลนั้นๆ ผู้ใช้จะเห็นข้อมูลที่ถูกเก็บไว้ในฐานข้อมูลในรูปแบบที่ผู้ใช้ออกแบบไว้ ตัวอย่างเช่น ผู้ใช้สร้างตารางข้อมูลขึ้นมาและเก็บลงในระบบฐานข้อมูล ระบบจัดการฐานข้อมูลจะเก็บข้อมูลเหล่านี้ลงในอุปกรณ์เก็บข้อมูลในรูปแบบของระบบจัดการฐานข้อมูลซึ่งอาจเก็บข้อมูลเหล่านี้ลงในแผ่นจานบันทึกแม่เหล็กเป็นระเบียนบล็อกหรืออื่นๆ ผู้ใช้ไม่จำเป็นต้องรับรู้ว่าโครงสร้างของแฟ้มข้อมูลนั้นเป็นอย่างไร ปล่อยให้เป็นหน้าที่ของระบบจัดการฐานข้อมูล ดังนั้นถ้าผู้ใช้เปลี่ยนแปลงลักษณะการเก็บข้อมูล เช่น เปลี่ยนแปลงรูปแบบของตารางเสียใหม่ ผู้ใช้ก็ไม่ต้องกังวลว่าข้อมูลของเขาจะถูกเก็บลงในแผ่นจานบันทึกแม่เหล็กในลักษณะใด ระบบการจัดการฐานข้อมูลจะจัดการให้ทั้งหมด ในทำนองเดียวกันถ้าผู้ออกแบบระบบฐานข้อมูลเปลี่ยนวิธีการเก็บข้อมูลลงบนอุปกรณ์จัดเก็บข้อมูล ผู้ใช้ก็ไม่ต้องแก้ไขฐานข้อมูลที่เขาออกแบบไว้แล้ว ระบบการจัดการฐานข้อมูลจะจัดการให้ ลักษณะเช่นนี้เรียกว่า ความไม่เกี่ยวข้องกันของข้อมูล (data independent)

4) สามารถใช้ข้อมูลร่วมกันได้ เนื่องจากในระบบฐานข้อมูลจะเป็นที่เก็บรวบรวมข้อมูลทุกอย่างไว้ ผู้ใช้แต่ละคนจึงสามารถที่จะใช้ข้อมูลในระบบได้ทุกข้อมูล ซึ่งถ้าข้อมูลไม่ได้ถูกจัดให้เป็นระบบฐานข้อมูลแล้ว ผู้ใช้ก็จะใช้ได้เพียงข้อมูลของตนเองเท่านั้น เช่น ข้อมูลของระบบเงินเดือน ข้อมูลของระบบงานบุคคลถูกจัดไว้ในระบบแฟ้มข้อมูลผู้ใช้ที่ใช้ข้อมูลระบบเงินเดือนจะใช้ข้อมูลได้ระบบเดียวแต่ถ้าข้อมูลทั้ง 2 ถูกเก็บไว้เป็นฐานข้อมูลซึ่งถูกเก็บไว้ในที่ที่เดียวกัน ผู้ใช้ทั้ง 2 ระบบก็จะ

สามารถเรียกใช้ฐานข้อมูลเดียวกันได้ ไม่เพียงแต่ข้อมูลเท่านั้นสำหรับโปรแกรมต่างๆ ถ้าเก็บไว้ในฐานข้อมูลก็จะสามารถใช้ร่วมกันได้

5) มีความเป็นอิสระของข้อมูล เมื่อผู้ใช้ต้องการเปลี่ยนแปลงข้อมูลหรือนำข้อมูลมาประยุกต์ใช้ให้เหมาะสมกับโปรแกรมที่เขียนขึ้นมาจะสามารถสร้างข้อมูลนั้นขึ้นมาใช้ใหม่ได้ โดยไม่มีผลกระทบต่อระบบฐานข้อมูล เพราะข้อมูลที่ผู้ใช้นำมาประยุกต์ใช้ใหม่นั้นจะไม่กระทบต่อโครงสร้างที่แท้จริงของการจัดเก็บข้อมูล นั่นคือ การใช้ระบบฐานข้อมูลจะทำให้เกิดความเป็นอิสระระหว่างการจัดเก็บข้อมูลและการประยุกต์ใช้

6) สามารถขยายงานได้ง่าย เมื่อต้องการจัดเพิ่มเติมข้อมูลที่เกี่ยวข้องจะสามารถเพิ่มได้อย่างง่ายไม่ซับซ้อน เนื่องจากมีความเป็นอิสระของข้อมูล จึงไม่มีผลกระทบต่อข้อมูลเดิมที่มีอยู่

7) ทำให้ข้อมูลบูรณะกลับสู่สภาพปกติได้เร็วและมีมาตรฐาน เนื่องจากการจัดพิมพ์ข้อมูลในระบบที่ไม่ได้ใช้ฐานข้อมูล ผู้เขียนโปรแกรมแต่ละคนมีแฟ้มข้อมูลของตนเองเฉพาะ ฉะนั้นแต่ละคนจึงต่างก็สร้างระบบการบูรณะข้อมูลให้กลับสู่สภาพปกติในกรณีที่ข้อมูลเสียหายด้วยตนเองและด้วยวิธีการของตนเอง จึงขาดประสิทธิภาพและมาตรฐาน แต่เมื่อมาเป็นระบบฐานข้อมูลแล้ว การบูรณะข้อมูลให้กลับคืนสู่สภาพปกติจะมีโปรแกรมชุดเดียว และมีผู้ดูแลเพียงคนเดียวที่ดูแลทั้งระบบ ซึ่งย่อมต้องมีประสิทธิภาพและเป็นมาตรฐานเดียวกัน

2.6.2 การบริหารฐานข้อมูล

การบริหารฐานข้อมูล ในระบบฐานข้อมูลนอกจากจะมีระบบการจัดการฐานข้อมูล ซึ่งเป็นซอฟต์แวร์ที่สร้างขึ้นเพื่อจัดการกับข้อมูลให้เป็นระบบ จะได้นำไปเก็บรักษา เรียกใช้ หรือนำมาปรับปรุงให้ทันสมัยได้ง่ายแล้ว ในระบบฐานข้อมูลยังต้องประกอบด้วยบุคคลที่มีหน้าที่ควบคุมดูแลระบบฐานข้อมูล คือผู้บริหารฐานข้อมูลเหตุผลสำหรับประการหนึ่งของการจัดทำระบบจัดการฐานข้อมูล คือ การมีศูนย์กลางควบคุมทั้งข้อมูลและโปรแกรมที่เข้าถึงข้อมูลเหล่านั้น บุคคลที่มีอำนาจหน้าที่ดูแลการควบคุมนี้ เรียกว่า ผู้บริหารฐานข้อมูล หรือ DBA (data base administor) คือ ผู้มีหน้าที่ควบคุมการบริหารงานของฐานข้อมูลทั้งหมด

2.6.2.1 หน้าที่ของผู้บริหารฐานข้อมูล

1) กำหนดโครงสร้างหรือรูปแบบของฐานข้อมูล

โดยทำการวิเคราะห์และตัดสินใจว่าจะรวมข้อมูลใดเข้าไว้ในระบบใดบ้าง ควรจะจัดเก็บข้อมูลด้วยวิธีใด และใช้เทคนิคใดในการเรียกใช้ข้อมูลอย่างไร

2) กำหนดโครงสร้างของอุปกรณ์เก็บข้อมูลและวิธีการเข้าถึงข้อมูล

โดยกำหนดโครงสร้างของอุปกรณ์เก็บข้อมูลและวิธีการเข้าถึงข้อมูล พร้อมทั้งกำหนดแผนการในการสร้างระบบข้อมูลสำรองและการฟื้นสภาพ โดยการจัดเก็บข้อมูลสำรองไว้ทุกระยะ และจะต้องเตรียมการไว้ว่าถ้าเกิดความผิดพลาดขึ้นแล้วจะทำการฟื้นสภาพได้อย่างไร

3) มอบหมายขอบเขตอำนาจหน้าที่ของการเข้าถึงข้อมูลของผู้ใช้

โดยการประสานงานกับผู้ใช้ ให้คำปรึกษา ให้ความช่วยเหลือแก่ผู้ใช้ และตรวจตราความต้องการของผู้ใช้

2.6.3 ระบบการจัดการฐานข้อมูล (data base management system, DBMS)

2.6.3.1 หน้าที่ของระบบการจัดการฐานข้อมูล

ระบบจัดการฐานข้อมูลเป็นซอฟต์แวร์ที่ทำหน้าที่ดังต่อไปนี้

1) ดูแลการใช้งานให้กับผู้ใช้ในการติดต่อกับตัวจัดการระบบแฟ้มข้อมูลได้ในระบบฐานข้อมูลนี้ข้อมูลจะมีขนาดใหญ่ ซึ่งจะถูกจัดเก็บไว้ในหน่วยความจำสำรองเมื่อผู้ใช้ต้องการจะใช้ฐานข้อมูล ระบบการจัดการฐานข้อมูลจะทำหน้าที่ติดต่อกับระบบแฟ้มข้อมูลซึ่งเสมือนเป็นผู้จัดการแฟ้มข้อมูล (file manager) นำข้อมูลจากหน่วยความจำสำรองเข้าสู่หน่วยความจำหลักเฉพาะส่วนที่ต้องการใช้งาน และทำหน้าที่ประสานกับตัวจัดการระบบแฟ้มข้อมูลในการจัดเก็บ เรียกใช้ และแก้ไขข้อมูล

2) ควบคุมระบบความปลอดภัยของข้อมูลโดยป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาเรียกใช้หรือแก้ไขข้อมูลในส่วนป้องกันเอาไว้พร้อมทั้งสร้างฟังก์ชันในการจัดทำข้อมูลสำรอง โดยเมื่อเกิดมีความขัดข้องของระบบแฟ้มข้อมูลหรือของเครื่องคอมพิวเตอร์เกิดการเสียหายนั้น ฟังก์ชันนี้จะสามารถทำการฟื้นสภาพของระบบข้อมูลกลับเข้าสู่สภาพที่ถูกต้องสมบูรณ์ได้

3) ควบคุมการใช้ข้อมูลในสภาพที่มีผู้ใช้พร้อมๆ กันหลายคน โดยจัดการเมื่อมีข้อผิดพลาดของข้อมูลเกิดขึ้น

2.7 ภาษาทางคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบ

2.7.1 คำสั่ง DOS

คำสั่ง DOS คือ ภาษาคำสั่งในระบบปฏิบัติการในรูปแบบของตัวอักษร (Text Mode) ถึงแม้ว่าปัจจุบันระบบคอมพิวเตอร์ส่วนใหญ่จะใช้ Windows (ระบบรูปภาพ หรือ Graphics Mode) แต่อย่างไรก็ตาม การเรียนการใช้งาน DOS ก็ยังถือว่ามีส่วนสำคัญ เช่น การติดตั้ง Windows การแบ่ง harddisk แต่ละ drive (Partition Harddisk) อาจจำเป็นต้องมีการ boot เข้าระบบดอสก่อน และเช่นเดียวกับบางบริษัทที่มีใช้งานในระบบเครือข่าย Novell Netware ก็ยังจำเป็นต้องทำงานในระบบ DOS เช่นกัน ชื่อ DOS หรือ MS DOS หมายถึง Microsoft Disk Operating System (บริษัทไมโครซอฟท์เป็นผู้ผลิต) ความแตกต่างที่เห็นในชัดของชื่อไฟล์ในระบบ DOS กับ Windows คือ ความยาวของชื่อไฟล์ Windows สามารถตั้งชื่อให้ยาวได้มากถึง 255 ตัวอักษร ส่วนในระบบ DOS ชื่อและนามสกุลของไฟล์จะถูกจำกัดได้เพียง ชื่อยาวไม่เกิน 8 ตัวอักษร นามสกุลยาวไม่เกิน 3 ตัวอักษร ตัวอย่าง Readme.TXT (ชื่อไฟล์ Readme หลังจุดคือนามสกุล TXT)

2.7.1.1 คำสั่งระบบ DOS พื้นฐาน

DIR (Directory) - คำสั่งในการแสดงรายชื่อไฟล์ รายชื่อไดเรกทอรี่ (Folder ใน windows ปัจจุบัน) ตัวอย่างการใช้งาน (รวมคำสั่งย่อยๆ)

Dir - แสดงรายชื่อไฟล์ ไดเรกทอรี่ทั้งหมด พร้อมทั้งขนาดไฟล์ + วันเวลาอัปเดทที่ล่าสุด

Dir /p - แสดงรายชื่อไฟล์ ไดเรกทอรี่ในแนวนอน ให้หยุดแสดงทีละหน้า (กรณีที่มีจำนวนไฟล์ยาวมากกว่า 1 หน้าจอ)

Dir /w - แสดงรายชื่อไฟล์ ไดเรกทอรี่ในแนวนอน

Dir /s, - แสดงรายชื่อไฟล์ ไดเรกทอรี่ และไฟล์ที่อยู่ในไดเรกทอรี่ย่อยด้วย

Dir /od - แสดงรายชื่อไฟล์ ให้เรียงตามวันที่อัปเดท Dir /n - แสดงรายชื่อไฟล์ ให้เรียงตามชื่อ

CLS (Clear Screen) - คำสั่งสำหรับลบหน้าจอออก

DEL (Delete) - คำสั่งในการลบชื่อไฟล์ที่ต้องการ เช่น DEL readme.txt หมายถึงให้ลบชื่อไฟล์ README.TXT

Del readme.txt - ลบไฟล์ชื่อ readme.txt

Del *.* - ให้ลบไฟล์ทั้งหมดที่อยู่ในไดเรกทอรี่ปัจจุบัน

Del *. - ให้ลบไฟล์ทั้งหมดที่อยู่ในไดเรกทอรี่ปัจจุบัน เฉพาะไฟล์ที่ไม่มีนามสกุล

MD (Make Directory) - คำสั่งในการสร้างไดเรกทอรี่ เช่น MD Photo จะได้ไดเรกทอรี่ C:Photo

CD (Change Directory) - คำสั่งในการเข้าไปในไดเรกทอรี่ (CD คือคำสั่งในการออกจากห้องไดเรกทอรี่)

RD (Remove Directory) - คำสั่งในการลบไดเรกทอรี่ เช่น RD Photo (เราจะต้องอยู่นอกห้องไดเรอทอรี่ Photo)

REN (Rename) - คำสั่งในการเปลี่ยนชื่อ เช่น REN readme.txt read.me หมายถึงการเปลี่ยนชื่อไฟล์เป็น READ.ME

Robocopy – คำสั่งในการ copy ไฟล์มีความสามารถ copy ไฟล์ได้ทั้ง folder ซึ่งเหมาะจะนำมาพัฒนาระบบสำรองข้อมูล

2.7.1.2 ชนิดคำสั่ง DOS

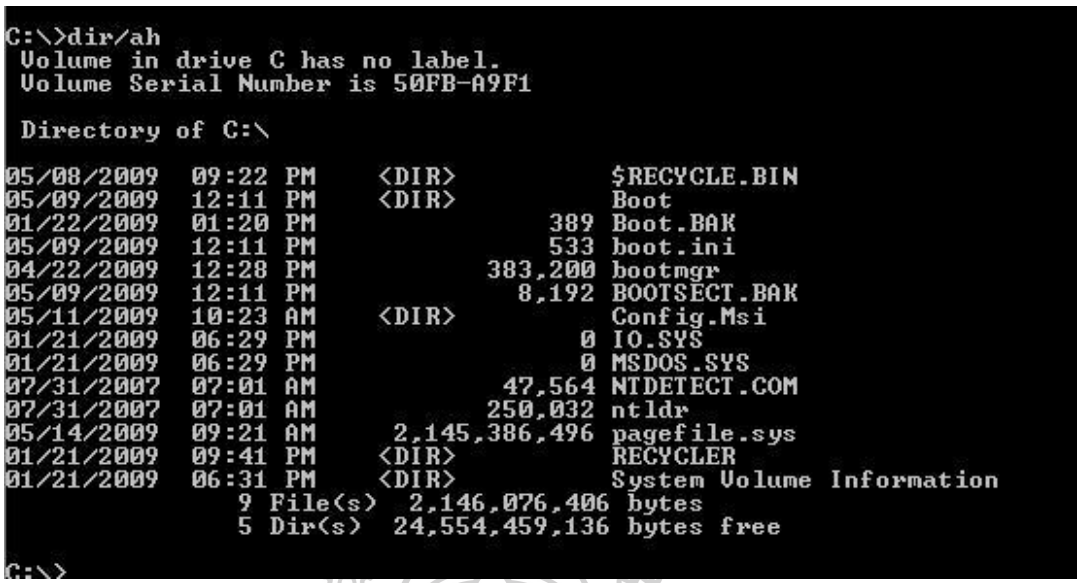
ภาษาคำสั่งที่ใช้พัฒนาซอฟต์แวร์คือคำสั่ง DOS (Disk Operating System) เป็นภาษาคำสั่งในระบบปฏิบัติการ Windows ในรูปแบบของตัวอักษร (Text Mode) การใช้คำสั่งผ่านบรรทัดคำสั่ง (Command Line) ดังตัวอย่างภาพที่ 13 เพื่อจัดการเครื่องคอมพิวเตอร์นั้นๆ สามารถประยุกต์การทำงานต่างๆได้มากมาย

คำสั่งของ DOS มีอยู่ 2 ชนิดคือ

1) คำสั่งภายใน (Internal Command) เป็นคำสั่งที่เรียกใช้ได้ทันทีตลอดเวลาที่เครื่องเปิดใช้งานอยู่ เพราะคำสั่งประเภทนี้ถูกบรรจุลงในหน่วยความจำหลัก (ROM) ตลอดเวลา หลังจากที่ Boot DOS ส่วนมากจะเป็นคำสั่งที่ใช้อยู่เสมอ เช่น CLS, DIR, COPY, REN เป็นต้น

2) คำสั่งภายนอก (External Command) คำสั่งนี้จะถูกเก็บไว้ในดิสก์หรือแผ่น DOS คำสั่งเหล่านี้จะไม่ถูกเก็บไว้ในหน่วยความจำ เมื่อต้องการใช้คำสั่งเหล่านี้คอมพิวเตอร์จะเรียกคำสั่งเข้าสู่หน่วยความจำ ถ้าแผ่นดิสก์หรือฮาร์ดดิสก์ไม่มีคำสั่งที่ต้องการใช้อยู่ก็ไม่สามารถเรียกคำสั่งนั้นๆ ได้ ตัวอย่างเช่น คำสั่ง FORMAT, DISKCOPY, TREE, DELTREE เป็นต้น

จากข้อมูลดังกล่าวคำสั่ง DOS จึงสามารถนำมาประยุกต์ใช้ในการสร้างชุดโปรแกรมพื้นฐานให้คอมพิวเตอร์ในระบบปฏิบัติการพื้นฐาน Windows ได้มาก



ภาพที่ 13 ตัวอย่างหน้าต่างคำสั่ง DOS

2.8 การบริหารความเสี่ยงเทคโนโลยีสารสนเทศ

ผู้ดูแลระบบสารสนเทศและผู้บริหารต้องเข้าใจหลักการและแนวทางของการบริหารความเสี่ยงเทคโนโลยีสารสนเทศ โดยมีรายละเอียดดังนี้

2.8.1 สภาพแวดลอมด้านเทคโนโลยีสารสนเทศ

ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น ฐานข้อมูลด้านการจัดการงานขาย ฐานข้อมูลลูกค้า ฐานข้อมูลบุคลากร ฐานข้อมูลการติดตามผลการดำเนินงานตามแผนยุทธศาสตร์ฐานข้อมูลการเงินงบประมาณ และฐานข้อมูลคุมทะเบียนทรัพย์สิน เป็นต้น ระบบฐานข้อมูลบริหารงานภายใน (Back Office) หรือระบบฐานข้อมูลงานบริหารสำนักงานอัตโนมัติ (e-Office) ได้แก่ ฐานข้อมูลระบบสำนักงานอิเล็กทรอนิกส์ (e-Office) ฐานข้อมูลระบบสารบรรณอิเล็กทรอนิกส์ (e-Document) ฐานข้อมูลสารสนเทศทรัพยากรบุคคล และฐานข้อมูลครุภัณฑ์คอมพิวเตอร์เป็นต้นระบบการให้บริการบนเครือข่ายคอมพิวเตอร์ ได้แก่ โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Anti-Virus) โปรแกรมระบบปฏิบัติการจัดการเครือข่าย (Network Software) และโปรแกรมปฏิบัติการบนหน้าจอเว็บไซต์ (Web Application Program) เป็นต้น อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบเครือข่าย (Network Server)

เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องแม่ข่ายสำหรับให้บริการเว็บไซต์ (Web Server) อุปกรณ์ป้องกันการจู่โจมข้อมูลจากบุคคลภายนอก (Firewall) เครื่องไมโครคอมพิวเตอร์ เครื่องคอมพิวเตอร์ชนิดพกพา (Notebook) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์เลเซอร์ (Laser Printer) เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer) อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching) และอุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access point) เป็นต้น

2.8.2 ความหมายของความเสี่ยง (Risk)

ความเสี่ยง (Risk) หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ซึ่งอาจเกิดขึ้นในอนาคตและมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านกลยุทธ์การปฏิบัติงาน การเงิน และการบริหาร ซึ่งอาจเป็นผลกระทบเชิงบวกด้วยก็ได้ โดยการวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

2.8.3 กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุวิเคราะห์ประเมินและจัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร และการบริหาร/จัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการหลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม 5 ขั้นตอน ดังนี้

ภาพที่ 14 กระบวนการบริหารความเสี่ยง

2.8.4 ความเสี่ยงของระบบสารสนเทศ (Information System risk)

ความเสี่ยงของระบบสารสนเทศ (Information System risk) หมายถึง โอกาสที่จะเกิดข้อผิดพลาด ความเสียหาย การกระทำใดๆที่ก่อให้เกิดการสูญเสียหรือทำลายฮาร์ดแวร์ หรือซอฟต์แวร์ ข้อมูลสารสนเทศหรือความสามารถในการประมวลผลข้อมูลของระบบสารสนเทศ ความเสี่ยงของระบบสารสนเทศแบ่งเป็น

2.8.4.1 ความเสี่ยงที่เกิดจากภายใน

1) การพัฒนาระบบ เช่น ผู้พัฒนาระบบไม่ทราบความต้องการใช้งานอย่างแท้จริง ระบบมีฟังก์ชันงานไม่ครบถ้วน , ผู้พัฒนาระบบไม่มีความรู้เพียงพอ ออกแบบระบบผิดพลาด ไม่ครบถ้วน รวมทั้งอาจมีการฝังโปรแกรมอันตรายเอาไว้เพื่อลักลอบส่งข้อมูลออก
2) การใช้ระบบ เช่น ผู้ใช้ไม่มีอำนาจในการเข้าถึงข้อมูลอาจเข้าได้โดยให้รหัสผ่านกัน , การบันทึกข้อมูลไม่ครบถ้วน ผิดพลาด บกพร่องทั้งคู่มือและรายงานต่างๆ ผู้ใช้ไม่สามารถสืบค้นหรือเรียกข้อมูลที่ต้องการใช้
3) ความเสี่ยงเกี่ยวกับอุปกรณ์ เช่น คอมพิวเตอร์และอุปกรณ์ไม่สามารถทำงานร่วมกันได้ ประสิทธิภาพต่ำ ทำงานช้า อุปกรณ์เกิดความเสียหายเพราะไม่ได้รับการบำรุงรักษาอย่างถูกวิธี การถูกโจรกรรม ถูกทำลายด้วยผู้บุกรุก การนำคอมพิวเตอร์ไปจำหน่าย แต่ไม่ได้ลบข้อมูล ไม่มีการปรับปรุงเครื่องให้ทันสมัยสามารถใช้งานร่วมกับหน่วยงานอื่นได้
4) ความเสี่ยงจากบุคลากรภายใน บุคลากรเจ้าหน้าที่หรือผู้ที่เกี่ยวข้องขององค์กร เช่น เจ้าหน้าที่หรือบุตรหลานอาจจะนำเกมส์จากบ้านมาเล่นกับคอมพิวเตอร์สำนักงาน มีการคัดลอกข้อมูลไปให้บุคคลภายนอกซึ่งอาจจะเป็นความลับ อาจเกิดการไม่พอใจสำนักงานหรือผู้บังคับบัญชาแอบทำงานการใช้โปรแกรมที่ไม่ได้รับการฝึกอบรม หรือเจ้าหน้าที่อาจจะแอบแก้ไขโปรแกรมและข้อมูลระหว่างทำงาน

2.8.4.2 ความเสี่ยงที่เกิดจากภายนอก

ความเสี่ยงด้านข้อมูล ระบบสารสนเทศอาจประสบปัญหาได้หลายเรื่อง เช่น การบุกรุกมาโจรกรรมอุปกรณ์ ในช่วงที่ไม่มีใครดูแล ถูกแรนซัมแวร์ การถูกไวรัสก่อกวนจาก

อินเตอร์เน็ต อีเมล เกม flash drive ไม่ได้ปิดระบบก่อนลุกออกจากโต๊ะทำงาน แฮคเกอร์บุกรุกเข้ามาทางระบบอินเตอร์เน็ตเพื่อทำลาย ซอฟต์แวร์ เว็บหรือข้อมูล

2.8.4.3 ความเสี่ยงจากอุบัติภัย

เกิดขึ้นโดยธรรมชาติหรือโดยฝีมือมนุษย์ เช่น เพลิงไหม้ น้ำท่วม หลังคารั่ว วาตภัย อุบัติเหตุ ระหว่างการขนย้าย

2.8.4.4 แนวการปฏิบัติงานสารสนเทศที่ดี

โดยนำแนวทางปฏิบัติของมาตรฐาน CobiT และ ISO 27001: 2005 มาประยุกต์ใช้ เพื่อให้การปฏิบัติงานสารสนเทศมีระบบการควบคุมภายในที่ดีและมีธรรมาภิบาลด้านเทคโนโลยี IT Governace ดังนี้

1) ผู้บริหารสนใจใช้ระบบไอทีเป็นเครื่องในการบริหารองค์กร
2) ประกาศนโยบายการใช้คอมพิวเตอร์และระบบอย่างเป็นทางการ
3) มีแผนการดำเนินงานประจำปี
4) มีการจัดสรรทรัพยากรให้พอเพียงแก่ความจำเป็นและแผนงาน
5) บุคลากรที่ได้รับมอบหมายให้ปฏิบัติงานกับระบบไอทีได้รับการฝึกอบรมในด้านการใช้อย่างถูกวิธี
6) มีระเบียบการใช้งานไอทีอย่างเหมาะสม เช่น กำหนดสิทธิใช้, การใช้ระบบไอที, การจัดเก็บเอกสารคู่มือ, สำรองข้อมูล
7) การจัดซื้อจัดจ้างจัดหารวมทั้งสัญญาระบบไอทีต้องจัดทำอย่างรัดกุมและรอบคอบ
8) จัดทำระเบียบและขั้นตอนการตรวจรับระบบอย่างรัดกุม
9) จัดเก็บสัญญากับผู้ขายหรือผู้ใช้เช่าเอาไว้อย่างเป็นระบบ และพยายามบริหารให้งานเป็นไปตามสัญญา
10) จัดทำระบบบัญชีฮาร์ดแวร์, ซอฟต์แวร์, และระบบเครือข่าย รวมทั้งจัดทำผังเครือข่ายและการจัดวางระบบคอมพิวเตอร์ (ระบบนี้ไม่ใช่ระบบพัสดุตามปกติ แต่เป็นระบบที่ระบุ Spec ด้านเทคนิคด้วย)
11) จัดวางเซิร์ฟเวอร์และอุปกรณ์ ตลอดจนเดินสายเคเบิลต่างๆ อย่างเป็นระบบเรียบร้อย

12) ดูแลให้ห้องเซิร์ฟเวอร์และอุปกรณ์มีความสะอาด ปราศจากสิ่งของที่ไม่จำเป็น เช่น กระดาษหรือสิ่งของอื่นๆ

13) ดูแลให้ห้องเซิร์ฟเวอร์มีระบบปรับอากาศที่เหมาะสม และเป็นห้องปิดเพื่อไม่ฝุ่นเข้าไป

14) ดูแลการจัดเก็บแผ่นซีดีที่เป็นต้นฉบับของโปรแกรมต่าง ที่จัดหาเอง ได้รับจากกระทรวง หรือได้รับบริจาคเอาไว้อย่างเป็นระบบ และต้องมีสองชุดแยกจากกัน นอกจากนั้นยังไม่อนุญาตให้นำแผ่นซีดีต้นฉบับออกไปใช้นอกสำนักงาน

15) จัดหาอุปกรณ์ไฟฟ้า (UPS) สำหรับเครื่องเซิร์ฟเวอร์และคอมพิวเตอร์ที่ใช้ในงานสำคัญเอาไว้ โดยเลือกใช้อุปกรณ์ที่สามารถสำรองไฟฟ้าได้นานพอสำหรับไฟฟ้าดับในพื้นที่

16) ก่อนปฏิบัติงาน เจ้าหน้าที่จะต้องตรวจสอบความเรียบร้อยของอุปกรณ์ในห้องเซิร์ฟเวอร์ และความพร้อมของอุปกรณ์

17) หากการเริ่มใช้มีปัญหา ให้รีบตรวจสอบปัญหาและแก้ไขตามคู่มือปฏิบัติงาน

18) รวบรวมคู่มือการใช้อุปกรณ์ และคู่มือเกี่ยวกับซอฟต์แวร์ เอาไว้ให้ครบถ้วน (คู่มือซอฟต์แวร์ ได้แก่ คู่มือติดตั้งซอฟต์แวร์ คู่มือการใช้การแก้ปัญหาซอฟต์แวร์, คู่มือการสำรองระบบ)

19) จัดทำหมายเลขโทรศัพท์ของผู้ที่เกี่ยวข้องทุกระดับ (ผู้รับผิดชอบงานไอทีที่กระทรวงและสำนักงานต่างๆ, ผู้บริหาร,ผู้ขาย, ผู้เชี่ยวชาญและที่ปรึกษา, พนักงานและเจ้าหน้าที่ทุกคน)

20) จัดทำหมายเลขโทรศัพท์ของหน่วยงานและบุคคลที่สามารถให้คาปรึกษาได้ในด้านไอที (เนคเทค, บริษัท ทศท, บริษัท กสท., กระทรวงไอซีที, SIPA ,สทอภ., บริษัทผู้ค้าที่เราใช้ HW&SW)

21) จัดทำแผนฉุกเฉิน เพื่อรับมือเมื่อเกิดปัญหาด้านไอซีที

22) สำรองข้อมูลของหน่วยงานเอาไว้ทุกสัปดาห์เป็นอย่างน้อย และให้นำข้อมูลสำรองไปจัดเก็บไว้ในสำนักงานอื่นนอกบริเวณอาคาร

23) ฝึกการนำข้อมูลสำรองกลับเข้ามาใช้งานแทนข้อมูลที่สมมติว่าถูกทำลายไปแล้ว (ควรทำอย่างน้อยปีละ 2 ครั้ง)

24) บันทึกการทำงานรายวัน เช่น เวลาการเปิด-ปิดเซิร์ฟเวอร์ (ในกรณีที่เปิด-ปิดทุกวัน) , การนำซอฟต์แวร์ใหม่เข้าติดตั้ง,การสำรองข้อมูล,การเกิดปัญหาต่างๆ เช่น ไฟฟ้าดับเมื่อใด ดับนานเท่าใด,และนำเครื่องกลับมาทำงานเมื่อใด หรือเครื่องติดไวรัส,พบเมื่อใด,และการจัดด้วยโปรแกรมอะไร ฯลฯ
25) มีการตรวจสอบเว็บของสำนักงานทุกวัน (ตรวจว่าเว็บมีปัญหาหรือไม่,ถูกแฮคเกอร์ป่วนหรือไม่, การเชื่อมโยงต่างๆยังดีอยู่หรือไม่,มีการบันทึกข้อมูลอย่างถูกต้องครบถ้วนหรือไม่
26) มีระบบรับแจ้งและบันทึกปัญหาจากผู้ใช้ภายใน พร้อมกับบริการแก้ไขปัญหาให้ผู้ใช้ภายในขอบเขตที่ทำได้ ในกรณีที่เป็นปัญหายุ่งยากให้เรียกใช้บริการผู้ขาย – หากมีสัญญาบำรุงรักษา การบันทึกให้ระบุชื่อผู้ใช้,ปัญหา,การแก้ปัญหา และระยะเวลาที่ใช้แก้ปัญหา
27) หากเป็นปัญหาเกี่ยวกับซอฟต์แวร์ ต้องบันทึกให้ละเอียดและส่งให้ผู้เกี่ยวข้องแก้ไข
28) จัดฝึกอบรมให้ผู้ปฏิบัติงานใหม่ทราบ (ทั้งผู้ปฏิบัติงานทั่วไปและงานไอที)
29) จัดหาระบบช่วยสอนหรือ Link เชื่อมโยงไปยังแหล่งที่มีระบบช่วยสอนให้ผู้ปฏิบัติงานเข้าไปศึกษา โดยทางฝ่ายไอทีจะต้องจัดเก็บบันทึกว่าผู้ใดผ่านการฝึกอบรมไปแล้ว
30) ร่วมมือกับผู้ตรวจสอบภายใน ในการจัดทำเครื่องมือสำหรับบันทึกข้อมูลการตรวจสอบภายใน (ถ้าผู้ร้องขอ)
31) ให้ความร่วมมือกับผู้ตรวจสอบภายในในการตรวจสอบไอที
32) รวบรวมแหล่งความรู้ใหม่เกี่ยวกับการบริหารงานไอที,เทคนิคเกี่ยวกับการทำงานไอที,การพัฒนาระบบ,การตรวจสอบระบบ,การจัดทำฐานข้อมูล,การสำรองระบบ, โปรแกรมแบบ Open Source ต่างๆ
33) จัดทำรายงานเกี่ยวกับการบริหารและผู้ปฏิบัติไอทีเสนอผู้บริหารระดับสูงให้ทราบเพื่อขอคำแนะนำหรือนโยบายเมื่อเกิดปัญหา

2.8.4.5 แนวการปฏิบัติงานสารสนเทศที่ดี

มาตรฐานความปลอดภัยของข้อมูล ในการประกอบธุรกิจอิเล็กทรอนิกส์ (เวอร์ชั่น 2.5) ประจำปี 2550 มาตรฐาน ISO/IEC 27001 (Information Security

Management System : ISMS) เป็นมาตรฐานที่เกิดจากการรวมกับมาตรฐาน ISO/IEC27001 และ ISO/IEC 17799 ถือเป็นแนวทางปฏิบัติสำหรับผู้ดูแลระบบและเครือข่าย ซึ่งมีสาระสำคัญแบ่งออกเป็น 2 ส่วน คือ

ส่วนที่ 1 กระบวนการการจัดทำระบบหรือการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

ถือเป็นมาตรฐานการจัดการข้อมูลที่มีความสำคัญเพื่อให้ภารกิจขององค์กรดำเนินไปอย่างต่อเนื่อง ซึ่งข้อกำหนดต่างๆถูกกำหนดขึ้นโดยองค์กรที่มีชื่อเสียงและมีความน่าเชื่อถือระหว่างประเทศ คือ ISO (The International organization for Standardization) และ IEC (The International Electrotechnical Commission) การประยุกต์ใช้ ISMS จะช่วยให้กิจกรรมดำเนินการอย่างต่อเนื่องไม่สะดุด รวมทั้งช่วยป้องกันความเสียหายของระบบข้อมูลจากภัยร้ายแรงต่างๆ เช่น แผ่นดินไหว,วาตภัย,อุทกภัย ฯลฯ หลักการของการออกแบบโครงสร้างระบบ ISO/IEC27001:2005 จะใช้ อ้างอิง รูปแบบ PDCA Model (Plan Do Check Action) ซึ่งเป็นโครงสร้างเดียวกับระบบการบริหารที่เป็นสากลที่ใช้กันทั่วโลก เช่น ระบบการจัดการคุณภาพ (ISO 9001:2000) , ระบบการจัดการสิ่งแวดล้อม (ISO14001:2004) ฯลฯ ISMS เป็นระบบการจัดการความปลอดภัยของข้อมูล เพื่อให้มีประสิทธิภาพทั้ง 3 ด้าน ดังนี้

1) เพื่อรักษาความลับ Confidentiality เพื่อให้แน่ใจว่าข้อมูลต่างๆสามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิที่จะเข้าเท่านั้น เช่น การกำหนดสิทธิ์การเข้าถึงข้อมูล เนื่องจากข้อมูลมีความสำคัญและไม่สามารถเปิดเผยให้รับทราบโดยทั่วกัน
2) เพื่อความถูกต้อง Integrity เพื่อให้แน่ใจว่าข้อมูลมีความครบถ้วนถูกต้อง จำเป็นต้องมีการกำหนดมาตรการหรือแนวทางในการป้องกันแก้ไขเปลี่ยนแปลงข้อมูล เพื่อป้องกันความผิดพลาดและการเข้าแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต
3) เพื่อความพร้อมใช้งาน Availability เพื่อให้แน่ใจได้ว่าผู้มีสิทธิ์ในการเข้าถึงข้อมูลในระบบต่างๆของหน่วยงาน ต้องสามารถเข้าใช้ข้อมูลในช่วงเวลาที่ต้องการอย่างต่อเนื่อง โดยไม่เกิดเหตุขัดข้อง หน่วยงานต้องมีการรักษาความปลอดภัยด้านสารสนเทศ ไม่ว่าจะเป็นความปลอดภัยของหน่วยงาน บุคคล สถานที่ทำงานและสภาพแวดล้อม รวมถึงการดูแลรักษาระบบต่างๆอย่างสม่ำเสมอ มีการวางแผนการปฏิบัติที่เป็นแบบแผนชัดเจน เพื่อให้เกิดความปลอดภัยสูงสุด

ISMS เป็นระบบ Dynamic system ที่ใช้โครงสร้าง PDCA ดังนั้น ระบบจะมีการหมุนเพื่อปรับปรุงอย่างต่อเนื่องอยู่ตลอดเวลาไม่มีที่สิ้นสุด โดยโครงสร้างของข้อกำหนด จะถูกแบ่งตาม PDCA ดังนี้

1) Plan คือ ขั้นตอนการกำหนดขอบเขต วัตถุประสงค์ขั้นตอนกระบวนการของ ระบบ ISMS การกำหนดวิธีการประเมินและระดับความเสี่ยงที่ยอมรับได้ การประเมินความเสี่ยง เช่น ทดสอบการเจาะระบบจากภายนอก การตรวจสอบและประเมินช่องโหว่ของระบบที่มีอยู่ รวมทั้ง การแก้ไขความเสี่ยงโดยเลือกว่าจะยอมรับหลีกเลี่ยงหรือโอนความเสี่ยง
2) Do คือ ขั้นตอนในส่วนของการจัดทำแผนการแก้ไขความเสี่ยง โดยนำนโยบาย ขั้นตอนกระบวนการต่างๆ ทางด้านความมั่นคงปลอดภัยมาประยุกต์ใช้งาน รวมทั้ง ดำเนินการทางเทคนิคเพื่อปิดช่องโหว่ต่างๆ ให้กับระบบ เช่น การติดตั้งซอฟต์แวร์ป้องกันความเสี่ยง โดยเฉพาะอย่างยิ่งการฝึกอบรมพนักงาน และผู้บริหาร ตลอดจนผู้ที่เกี่ยวข้องเพื่อให้มีความรู้และสามารถร่วมกันแก้ไขและป้องกัน ความเสี่ยงได้อย่างมีประสิทธิภาพ
3) Check คือ ขั้นตอนในการทบทวนกระบวนการต่างๆ โดยวัดประสิทธิภาพของการแก้ไขความเสี่ยง ทบทวนผลการประเมินความเสี่ยง และการตรวจประเมินภายใน (Internal Audit)
4) Act คือ ขั้นตอนในการแก้ไขปัญหา (Corrective Action) และการป้องกันปัญหา (Preventive Action) รวมถึงการสื่อสารไปยังผู้ที่เกี่ยวข้องเพื่อให้รับทราบถึงผลการแก้ไขความเสี่ยง พร้อมทั้งเรียนรู้ปัญหาที่เกิดขึ้นเพื่อป้องกันไม่ให้ปัญหาเกิดขึ้นอีก

ส่วนที่ 2 มาตรการการจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ

มาตรฐาน ISO/IEC 17799 กล่าวถึงเรื่องของวิธีปฏิบัติที่จะนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัยที่หน่วยจัดทำมาตรการที่กำหนดเป็นไปตามข้อกำหนดในมาตรฐาน ISO/IEC 27001 เป็นกรอบด้านการควบคุมระบบความปลอดภัยข้อมูล ซึ่งแบ่งรายการควบคุม (Controls) ออกเป็น 11 หัวข้อหลัก ดังนี้

1) นโยบายความมั่นคงปลอดภัย (Security policy) ประกอบด้วยนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ ซึ่งมีวัตถุประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

2) การจัดองค์กรในการดูแลความมั่งคงปลอดภัย (Organization Information Security) การบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศองค์กรและหน่วยงานภายนอก
3) การจัดการทรัพย์สิน (Asset Management) ควรมีการกำหนดหน้าที่ความรับผิดชอบต่อทรัพย์สิน และการจัดหมวดหมู่สารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นได้
4) ความมั่นคงปลอดภัยเกี่ยวกับบุคลากร (Physical and environment security) โดยมีการสร้างความมั่นคงปลอดภัยในก่อนการจ้างงาน ระหว่างการจ้างงานจนกระทั่งสิ้นสุดและเปลี่ยนการจ้างงาน เพื่อสร้างความเข้าใจต่อบุคลากร เพื่อลดความเสี่ยงจากการเกิดข้อผิดพลาดในการปฏิบัติหน้าที่ และป้องกันการ ขโมย การฉ้อโกงอีกด้วย
5) ความมั่นปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environment security) โดยต้องมีการรักษาความปลอดภัย เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต และความมั่นคงปลอดภัยของอุปกรณ์ เพื่อป้องกันการสูญหาย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตขององค์กร
6) การบริหารการสื่อสารและการดำเนินการ (Communications and operations management) ควรมีการกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน การบริหารจัดการให้หน่วยงานภายนอก มีการวางแผนและการตรวจรับทรัพยากรสารสนเทศ มีการป้องกันโปรมแกรมที่ไม่พึงประสงค์ การสำรองข้อมูล การจัดการสื่อบันทึกข้อมูล มีการแลกเปลี่ยนสารสนเทศและซอฟต์แวร์กันภายในองค์กรและหน่วยงานภายนอก มีการเฝ้าระวังทางด้านความปลอดภัย เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต
7) การควบคุมการเข้าถึงระบบ (Access Control) มีการกำหนดสำหรับการเข้าถึงสารสนเทศ มีการควบคุมการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาต การควบคุมอุปกรณ์สื่อสารประเภทพกพา และการปฏิบัติงานจากภายนอกเพื่อสร้างความปลอดภัยให้กับอุปกรณ์และการปฏิบัติงานที่เกี่ยวข้อง
8) การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance) ซึ่งได้มีการกำหนดด้านความมั่นคงปลอดภัย เพื่อให้การจัดหาและพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความ

มั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ มีการประมวลผลสารสนเทศใน Application เพื่อป้องกันความผิดพลาดในสารสนเทศ สร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ

9) การจัดการเหตุการที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ (Information security incident management) ผู้ดูแลระบบและพนักงานในด้านต่างๆ ควรมีการรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย รวมทั้งการบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย
10) การบริหารความต่อเนื่องในการดำเนินธุรกิจ (Business continuity management) บทบาทของผู้บริหารสารสนเทศในการกำหนดหัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่อง เพื่อป้องกันการติดขัดหยุดชะงักของกิจกรรมต่างๆ เพื่อป้องกันความล้มเหลวที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม
11) ความสอดคล้องตามข้อกำหนด (Compliance) ต้องปฏิบัติตามข้อกำหนดทางกฎหมาย ระเบียบ ข้อกำหนดในสัญญา รวมทั้งการปฏิบัติตามนโยบาย มาตรฐานความปลอดภัยและข้อกำหนดทางเทคนิค และการตรวจประเมินระบบสารสนเทศ เพื่อตรวจประเมินระบบสารสนเทศให้ได้ประสิทธิภาพสูงสุด

2.8.5 สรุปความเสี่ยงของระบบสารสนเทศ (Information System risk)

ในการจัดการความเสี่ยงระบบสารสนเทศ การจัดการข้อมูลนับมีความสำคัญเป็นอย่างมากระบบการจัดการความปลอดภัยข้อมูล ISO/IEC 27001:2005 หรือ ISMS เป็นระบบ dynamic system ที่มีการประยุกต์หลักการ PDCA Cycle เพื่อให้ระบบข้อมูลขององค์กร มีการรักษาความลับ ความถูกต้องครบถ้วน ความพร้อมใช้งาน โดยระบบ การจัดการ ISMS นั้น จะเป็นระบบการจัดการภายใต้ความเสี่ยงที่ยอมรับได้ ไม่ใช่ให้ระบบไม่มีความเสี่ยงเลยหรือไม่เกิดปัญหาเลย ทำให้เกิดประสิทธิภาพในการใช้ ทรัพยากรในการลงทุนสำหรับการจัดการความปลอดภัยของข้อมูลอย่างมีประสิทธภาพ

2.8.6 การวัดความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์การประเมิน และการจัดระดับความเสี่ยงโดยในเนื้อหานี้พิจารณาความเสี่ยงอันเกิดขึ้นกับระบบสารสนเทศในแง่ของผลกระทบที่เกิดขึ้นจากการที่ระบบเว็บไซต์การบริการและฐานข้อมูลใช้งานไม่ได้ ในเชิงปริมาณ โดยความเสี่ยงคำนวณจาก R = I x P โดยที่ R = ความเสี่ยง , I = ผลกระทบ , P = โอกาสที่จะเกิดขึ้น

เกณฑ์การประเมินผลกระทบ (I) เป็นดังนี้ ระดับการประเมิน (เชิงปริมาณ)

1 คือ น้อย : ผลกระทบตั้งแต่ 11-30 นาที

2 คือ ปานกลาง : ผลกระทบตั้งแต่ 31-60 นาที

3 คือ สูง : ผลกระทบตั้งแต่ 61-180 นาที

4 คือ สูงมาก : ผลกระทบตั้งแต่ 180 นาทีขึ้นไป

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง (R) เป็นดังนี้ ระดับการประเมิน (เชิงปริมาณ)

1 คือ น้อย : 2-4 ปีต่อครั้ง

2 คือ ปานกลาง : 1 ปีต่อครั้ง

3 คือ สูง : 6 เดือนต่อครั้ง

4 คือ สูงมาก : 3 เดือนต่อครั้ง

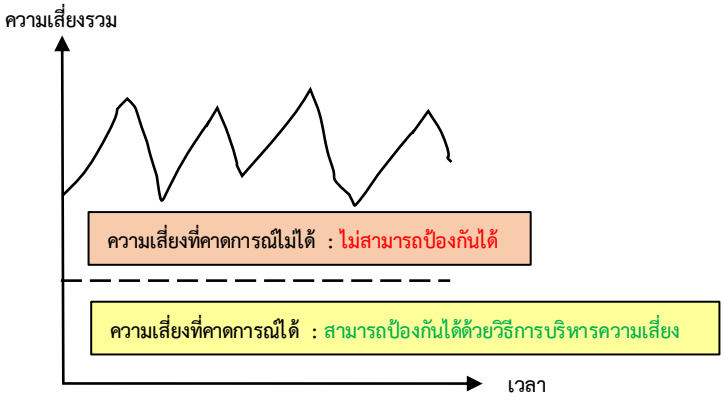
สามารถแสดงรายละเอียดดังอธิบายความหมายของระดับความเสี่ยงได้จากตารางประเมินความเสี่ยง ดังภาพที่ 15 เพื่อให้เข้าใจมากขึ้นสามารถจำแนกระดับความเสี่ยงตามแผนภูมิภาพที่ 16 โดยที่หลักการของการบริหารความเสี่ยงนั้นพบว่าความเสี่ยงหลักจะแบ่งออกเป็นความเสี่ยง ที่คาดการณ์ได้และความเสี่ยงคาดการณ์ไม่ได้ ในระดับที่คาดการณ์ได้นั้นจะสามารถหาแนวทางป้องได้แสดงดังกราฟภาพที่ 17

ระดับความเสี่ยง	ผลลัพธ์ความเสี่ยง	ความหมาย
1	1-2	ความเสี่ยงเล็กน้อย
2	3-6	ความเสี่ยงที่ยอมรับได้ ต้องมีการทบทวนมาตรการควบคุม
3	8-9	ความเสี่ยงสูง ต้องมีการดำเนินการเพื่อลดความเสี่ยง
4	10-16	ความเสี่ยงที่ยอมรับไม่ได้ ต้องมีมาตรการดำเนินการและปรับปรุงแก้ไขเพื่อลดความเสี่ยง ทันที

ภาพที่ 15 ตารางประเมินความเสี่ยง

ภาพที่ 16 แผนภูมิความเสี่ยง (Risk Map)

กราฟระดับความเสี่ยง



ภาพที่ 17 กราฟความเสี่ยง

2.9 การสำรองข้อมูล (Data Backup)

การสำรองข้อมูล (Backup Data) คือการสำรองและป้องกันความเสียหายของข้อมูลเป็นการคัดลอกแฟ้มข้อมูลเพื่อทำสำเนา เพื่อหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหายต่อองค์กรได้โดยสามารถนำข้อมูลที่สำรองไว้มาใช้งานได้ทันที การสำรองข้อมูลโดยหลักมี 2 รูปแบบดังนี้

1) สำรองข้อมูลด้วย ลงไปใน External Drive (ที่เก็บข้อมูลภายนอกแบบฮาร์ดแวร์) คือการสำรองข้อมูลด้วยโปรแกรมหรือคำสั่งซอฟต์แวร์ ไปยังอุปกรณ์ External Drive

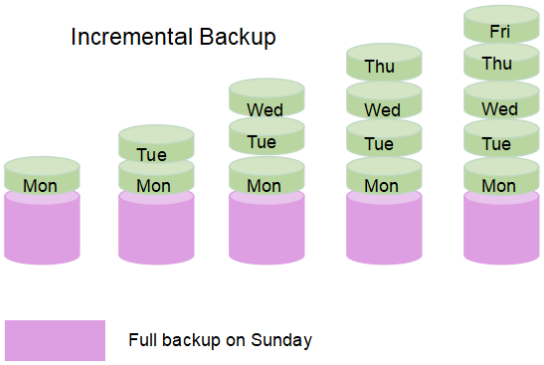
2) สำรองข้อมูลด้วยระบบ Cloud Server (ที่เก็บข้อมูลภายนอกแบบระบบคลาวด์) คือการสำรองข้อมูลด้วยระบบของผู้ให้บริการภายนอกองค์กร

2.9.1 ประเภทการสำรองข้อมูล (Type Backup)

โดยหลักมี 3 รูปแบบ

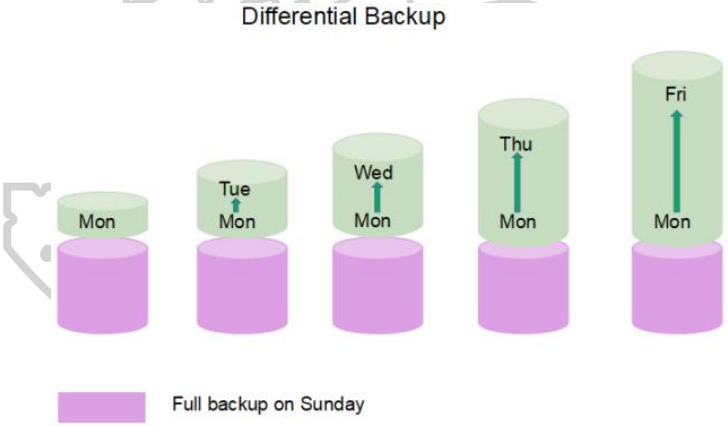
2.9.1.1 Full Backup หรือ Normal Backup คือ การ Backup พื้นฐานที่จะทำการ Backup ข้อมูลทั้งหมดทุกครั้ง โดยไม่สนใจว่าจะเป็นข้อมูลเก่าหรือไม่ กล่าวคือเป็นการ Backup ทุกไฟล์ เช่น Full Backup ของ Windows ก็ทำสำเนาเอาทุกไฟล์ในทุกไดร์ฟอย่าง C:\ , D:\ และอื่นๆ มาทั้งหมด ถ้าใน Unix หรือ Linux ก็ไล่ตั้งแต่ /home, /opt และอื่นๆ ข้อแนะนำคือควรยกเว้นการ Backup เฉพาะไฟล์ที่รู้ว่าไม่จำเป็นจริงๆ เท่านั้น เช่น ไฟล์ Config อย่าง C:\Windows\TEMP หรือ /tmp ใน Linux ทั้งหมดนี้ก็เพื่อหลีกเลี่ยงในกรณีที่คนอื่นๆ อาจนำไฟล์ที่เราไม่รู้ไปวางไว้ที่อื่นและอาจไม่ได้ถูก Backup ไปด้วย

2.9.1.2 Incremetal Backup คือ การ Backup เฉพาะข้อมูลที่มีการเปลี่ยนแปลงหรือเพิ่มเข้ามาใหม่เท่านั้น ไม่ได้เป็นการ Backup ข้อมูลทั้งหมด กล่าวคือ เป็นการ Backup เอาเฉพาะข้อมูลที่มีการเปลี่ยนแปลงจากการ Backup ครั้งล่าสุด ดังภาพที่ 18 ไฟล์ Backup จะมีขนาดเล็กนี่คือข้อดีของการไม่ไปรบกวนประสิทธิภาพของเซิร์ฟเวอร์มากนักเพราะการจะให้ Backup ไฟล์ 10 GB ทั้งๆที่มีการเปลี่ยนแปลงข้อมูลแค่ 1 MB ก็คงเกินความจำเป็นไป แต่หากต้องการได้ข้อมูลของวันศุกร์ก็ต้องเอาข้อมูลจากชุด Backup จากวันจันทร์ ถึง พฤหัส มาประกอบกันถ้าเสียไปอันนึงก็จะมีปัญหา นอกจากนี้ปัจจุบันซอฟต์แวร์ Backup สมัยใหม่ก็มีการใช้งาน Backup แบบ Block-based incremental คือการจัดการในระดับ Block นั่นเอง โดยการใช้ API จาก VMware หรือ Hyper-V



ภาพที่ 18 แผนภาพ Incremetal Backup

2.9.1.3 Synthetic Full Backup คือ การทำ Reversed Incremental โดยปกติจะเป็นการ Backup แบบ Incremental แต่เมื่อถึงระยะเวลาหนึ่งก็จะทำการรวมเอา Incremental ทั้งหมดมาเป็น Full Backup วิธีการนี้เรียกอีกอย่างว่า Differential Backup ดังภาพที่ 19



ภาพที่ 19 แผนภาพ Synthetic Full Backup

2.9.2 นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup Policy)

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

2.9.2.1 แนวทางปฏิบัติในการสำรองข้อมูล

1) จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบเทคโนโลยีสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

2) มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบเทคโนโลยีสารสนเทศแต่ละระบบ

3) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

4) ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

2.9.3 มาตรฐานรอบของการสำรองข้อมูล

จากการศึกษานโยบายด้านความปลอดภัยของทั้งทางภาครัฐและเอกชนพบว่าโดยหลักแล้วในเรื่องการสำรองข้อมูล ผู้ดูแลระบบต้องสำรองข้อมูลและระบบปฏิบัติการอย่างน้อยเดือนละครั้ง และทดสอบการสำรองข้อมูลอย่างน้อยปีละ 2 ครั้งโดยสอดคล้องกับความสำคัญของระบบ

2.9.4 มาตรฐานเครื่องมือและอุปกรณ์ที่ใช้ในการสำรองข้อมูล (Backup Tools)

2.9.4.1 Hardware ได้แก่

1) Hard disk

2) เทป

3) CD

2.9.4.2 Software ได้แก่

1) โปรแกรมซอฟต์แวร์ที่มีจำหน่ายในปัจจุบัน

2.9.5 มาตรฐานกระบวนการหรือระบบในการสำรองและกู้คืนข้อมูล (Backup and Recovery)

2.9.5.1 การสำรองข้อมูลภายในองค์กรแบบ Full backup)

2.9.5.2 มี Agent สำหรับการสำรองฐานข้อมูล ไม่ว่าจะเป็น SQL/Oracle/DB2 หรือฐานข้อมูลอื่นๆ ที่หน่วยงานใช้อยู่

2.9.5.3 สามารถสร้าง Backup Schedule ได้

2.9.5.4 สามารถทำ Restore ได้อย่างมีประสิทธิภาพ

2.9.5.5 กำหนดรายละเอียดเกี่ยวกับกระบวนการ หรือระบบในการสำรองและกู้คืนข้อมูล (Backup and Recovery Procedures)

2.9.5.6 การจัดทำบันทึกการสำรองข้อมูล (Operator logs)

2.9.5.7 การรายงานข้อผิดพลาด (Fault logging)

2.9.5.8 การสำรองข้อมูลภายนอกสำนักงาน (Off-site backup)

2.9.5.9 กำหนดให้ทุกการพัฒนาระบบฐานข้อมูลสารสนเทศ จะต้องจัดให้มีระบบสำรองและกู้คืนข้อมูลที่ได้มาตรฐานสากล

2.9.5.10 มีแนวทางในการสำรองและกู้คืนระบบ เพื่อลดความเสี่ยงจากที่อาจเกิดขึ้นกับข้อมูล และสามารถนำข้อมูลกลับมาใช้งานได้ ในกรณีที่ ฮาร์ดดิสก์เสียหายไวรัสคอมพิวเตอร์ทำลายข้อมูล ผู้บุกรุกทำการลบข้อมูลหรือเปลี่ยนแปลงข้อมูล การเผลอลบข้อมูลหรือเปลี่ยนแปลงข้อมูลโดยผู้ใช้งานเอง

2.10 แผนภาพกระแสขอมูล (Data Flow Diagram)

แผนภาพกระแสข้อมูล (DFD : Data Flow Diagram) เป็นเครื่องมือที่ใช้กันอย่างแพร่หลายในการเขียนแบบระบบงาน หรือในการเขียนแผนภาพจำลองการทำงานของกระบวนการ (Process) ต่างๆ ในระบบ โดยเฉพาะกับระบบที่ "หน้าที่" ของระบบมีความสำคัญและมีความสลับซับซ้อนมากกว่าข้อมูลที่ไหลเข้า จึงเหมาะเป็นเครื่องมือเชิงโครงสร้างที่ใช้บรรยายภาพรวมของระบบโดยแสดงขั้นตอนการทำงานของระบบหรือโพรเซส (process) ระบุแหล่งกำเนิดของข้อมูล การไหลของข้อมูล ปลายทางข้อมูล การเก็บข้อมูลและการประมวลผลข้อมูล กล่าวง่ายๆ คือ Data Flow Diagram จะช่วยแสดงแผนภาพ ว่าข้อมูลมาจากไหน จะไปไหน เก็บข้อมูลไว้ที่ไหน มีอะไรเกิดขึ้นกับ

ข้อมูลระหว่างทางเรียกว่าแผนภาพกระแสข้อมูลหรือ แผนภาพแสดงความเคลื่อนไหวของข้อมูลโดย Data Flow Diagram

2.10.1 วัตถุประสงค์ของการสร้างแผนภาพกระแสข้อมูล

1) เป็นแผนภาพที่สรุปรวมข้อมูลทั้งหมดที่ได้จากการวิเคราะห์ในลักษณะของรูปแบบที่เป็นโครงสร้าง

2) เป็นข้อตกลงร่วมกันระหว่างนักวิเคราะห์ระบบและผู้ใช้งาน

3) เป็นแผนภาพที่ใช้ในการพัฒนาต่อในขั้นตอนของการออกแบบระบบ

4) เป็นแผนภาพที่ใช้ในการอ้างอิง หรือเพื่อใช้ในการพัฒนาต่อในอนาคต

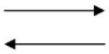
5) ทราบที่มาที่ไปของข้อมูลที่ไหลไปในกระบวนการต่างๆ (Data and Process)

2.10.2 สัญลักษณ์ที่ใช้ในแผนภาพกระแสข้อมูล

สัญลักษณ์ที่ใช้เป็นมาตรฐานในการแสดงแผนภาพกระแสข้อมูลมีหลายชนิด แต่ในที่นี้จะแสดงเพียง 2 ชนิด ได้แก่

- ชุดสัญลักษณ์มาตรฐานที่พัฒนาโดย Gane and Sarson (1979)
- ชุดสัญลักษณ์มาตรฐานที่พัฒนาโดย DeMarco and Yourdon

(DeMarco, 1979; Yourdon and Constantine,1979) โดยมี สัญลักษณ์ดังต่อไปนี้

DeMarco & Yourdon	Gane & Sarson	ความหมาย
		Process : ขั้นตอนการทำงานภายในระบบ
		Data Store : แหล่งข้อมูลสามารถเป็นได้ทั้งไฟล์ข้อมูลและฐานข้อมูล (File or Database)
		External Agent : ปัจจัยหรือสภาพแวดล้อมที่มีผลกระทบต่อระบบ
		Data Flow : เส้นทางการไหลของข้อมูล แสดงทิศทางของข้อมูลจากขั้นตอนการทำงานหนึ่งไปยังอีกขั้นตอนหนึ่ง

ภาพที่ 20 สัญลักษณ์ของแผนภาพกระแสข้อมูล

a. Process – กระบวนการทำงานของระบบ
b. Data Store –แหล่งจัดเก็บข้อมูล
c. Data Flow – เส้นทางการไหลของข้อมูล
d. External Entity – ตัวแทนที่เกี่ยวข้องกับข้อมูล

โดยมีรายละเอียดดังนี้

2.10.2.1 Process หรือ ขั้นตอนการดำเนินงาน คือ งานที่ดำเนินการ/ตอบสนองข้อมูลที่รับเข้าหรือดำเนินการ/ตอบสนองต่อเงื่อนไข/ สภาวะใดๆ ที่เกิดขึ้น ไม่ว่าขั้นตอนการดำเนินงานนั้นจะกระทำโดยบุคคล หน่วยงาน หุ่นยนต์ เครื่องจักร หรือ เครื่องคอมพิวเตอร์ก็ตาม โดยจะเป็นกริยา (Verb)

2.10.2.2 เส้นทางการไหลของข้อมูล (Data Flows) เป็นการสื่อสารระหว่างขั้นตอนการทำงาน (Process) ต่างๆ และสภาพแวดล้อมภายนอกหรือภายในระบบ โดยแสดงถึงข้อมูลที่นำเข้าไปในแต่ละ Process และข้อมูลที่ส่งออกจาก Process ใช้ในการแสดงถึงการบันทึกข้อมูล การลบข้อมูล การแก้ไขข้อมูลต่างๆ สัญลักษณ์ที่ใช้อธิบายเส้นทางการไหลของข้อมูลคือ เส้นตรงที่ประกอบด้วยหัวลูกศรตรงปลายเพื่อบอกทิศทางการเดินทางหรือการไหลของข้อมูล

2.10.2.3 แหล่งจัดเก็บข้อมูล (Data Store) เป็นแหล่งเก็บ/บันทึกข้อมูล เปรียบเสมือนคลังข้อมูล (เทียบเท่ากับไฟล์ข้อมูล และฐานข้อมูล) โดยอธิบายรายละเอียดและคุณสมบัติเฉพาะตัวของสิ่งที่ต้องการเก็บ/บันทึก สัญลักษณ์ที่ใช้อธิบายคือสี่เหลี่ยมเปิดหนึ่งข้าง แบ่งออกเป็นสองส่วน ได้แก่ ส่วนที่ 1 ทางด้านซ้ายใช้แสดงรหัสของ Data Store อาจจะเป็นหมายเลขลำดับหรือตัวอักษรได้ เช่น D1, D2 เป็นต้น สำหรับส่วนที่ 2 ทางด้านขวา ใช้แสดงชื่อ Data Store หรือชื่อไฟล์

2.10.2.4 ตัวแทนข้อมูล (External Agents) หมายถึง บุคคล หน่วยงานในองค์กร องค์กรอื่นๆ หรือระบบงานอื่นๆ ที่อยู่ภายนอกขอบเขตของระบบ แต่มีความสัมพันธ์กับระบบ โดยมีการส่งข้อมูลเข้าสู่ระบบเพื่อดำเนินงาน และรับข้อมูลที่ผ่านการดำเนินงานเรียบร้อยแล้วจากระบบ สัญลักษณ์ที่ใช้อธิบาย คือ สี่เหลี่ยมจตุรัส หรือสี่เหลี่ยมผืนผ้า ภายในจะต้องแสดงชื่อของ External Agent โดยสามารถทำการซ้ำ (Duplicate) ได้ด้วยการใช้เครื่องหมาย \ (back slash) ตรงมุมล่างซ้าย

2.11 งานวิจัยที่เกี่ยวข้อง

(มงคล ลีละปัญญา, 2555) วัตถุประสงค์เพื่อสร้างระบบจัดการไฟล์เซิร์ฟเวอร์ (File Server) เพื่อสำรองข้อมูล และเพื่อลดภาระค่าใช้จ่ายในการลดปริมาณการใช้ทรัพยากรบุคคล โดยการสร้างระบบจัดการไฟล์เซิร์ฟเวอร์ (File Server) ขององค์กร โดยจำลองระบบผ่านระบบปฏิบัติการลินุกซ์ (LINUX) และใช้โปรแกรมแซมบ้า (SAMBA) เพื่อลดภาระงานบุคคลและสำรองข้อมูลเมื่อเกิดความเสียหาย โดยผลสรุปของสร้างระบบจัดการไฟล์เซิร์ฟเวอร์ (File Server) เพื่อสำรองข้อมูล การสร้างซอฟต์แวร์เพื่อควบคุมระบบนั้นสามารถทำให้ลดภาระงาน และทรัพยากรต่างๆลงได้

(อชิรัชญ์ สอนเนียม, 2551) ได้ศึกษาและทำการวิจัยประยุกต์ พัฒนาระบบสำรองข้อมูลของโปรแกรมการตรวจสอบและแจ้งเตือนการสื่อสารภายในเครือข่าย ในกรณีที่การสื่อสารภายในเครือข่ายมีความหนาแน่นมากจนทำให้โปรแกรมไม่สามารถทำงานได้ โดยตรวจสอบจากค่าการใช้ CPU และ RAM ของเครื่อง รวมทั้งสถานะ การสื่อสารภายในเครือข่าย ซึ่งระบบสามารถทำการแลกเปลี่ยนข้อมูลระหว่างเครื่อง ในเครือข่ายได้ โดยเครื่องที่ติดตั้งระบบตรวจสอบอีกเครื่องหนึ่งจะสามารถทำการตรวจสอบได้ในทันที โดยนำหลักการของ RAID มาใช้ในการควบคุมการสำรองข้อมูลสำหรับใช้ในการตรวจสอบและใช้หลักการของ Load Balancing ในการแบ่งภาระงานให้กับระบบสำรองโปรแกรมการตรวจสอบและแจ้งเตือนการสื่อสารภายในเครือข่าย โดยในส่วนของการรับ-ส่งข้อมูลระหว่างระบบ (Sync) จะใช้เทคโนโลยีของ WCF ในการรับ-ส่งข้อมูลผลการประเมินความพึงพอใจในการทดสอบระบบพบว่าคะแนนเฉลี่ยโดยรวมของระบบมีค่าเท่ากับ 4.65 แสดงว่าระบบที่พัฒนาขึ้นมีคุณภาพในระดับดีมาก

(กฤษณา ตีวารี, 2555) ได้ศึกษาและทำการวิจัยประยุกต์ใช้ระบบสารสนเทศ เพื่อลดค่าใช้จ่ายในระบบงานสำรองข้อมูลและป้องกันไวรัส โดยการการออกแบบระบบการสำรองข้อมูลและระบบการจัดการไวรัส ไว้ในระบบเดียวกัน มีความสามารถค้นหาข้อมูลในระบบที่แตกต่างกันได้ด้วย ผลจากการใช้ระบบการจัดการข้อมูลที่มีการออกแบบใหม่ทำให้เกิดความประหยัดต้นทุน ในการจัดเก็บข้อมูลและเกิดระบบป้องกันที่มีประสิทธิภาพสูงขึ้นในการสำรองข้อมูลและการจัดการไวรัส ประหยัดค่าใช้จ่าย 5,000-6,000 บาทต่อเดือน และประสิทธิภาพการใช้งานของผู้ใช้เท่ากับ 4.00 อยู่ในเกณฑ์ดี

(รุ่งโรจน์ กัววัฒนาพันธ์, 2552) ได้ศึกษาและทำการวิจัยประยุกต์ใช้ระบบสารสนเทศเพื่อการจัดการระบบสำรองข้อมูล และจัดการการกู้คืนข้อมูล โดยการออกพัฒนาระบบสำรองข้อมูลและกู้คืนข้อมูลระยะไกล ของเครื่องคอมพิวเตอร์แม่ข่าย ด้วยบริการรับส่งข้อความ ผ่านโทรศัพท์เคลื่อนที่ และอินเทอร์เน็ต ในการทำการสำรองข้อมูลและการกู้คืนข้อมูลของเครื่องคอมพิวเตอร์แม่ข่าย การพัฒนาโปรแกรมใช้ฐานข้อมูล มายเอสคิวแอล เวอร์ชั่น 5 โดยใช้ภาษา พีเอชพี ในการดึงข้อมูลจากฐานข้อมูล และ ใช้ อาร์ปาเช่ ทำหน้าที่เป็นเว็บเซิฟร์เวอร์ ในการแสดงผลทางบราวเซอร์ ใช้ภาษา เซลล์สคริปในการติอต่อ ควบคุมคำสั่งบนเครื่องคอมพิวเตอร์แม่ข่ายใช้โทรศัพท์มือถือพื้นฐานสามารถใช้บริการรับส่งข้อความ เอสเอ็มเอสจากการศึกษา พัฒนา ทดสอบพบว่าระบบสำรองข้อมูลและกู้คืนข้อมูลระยะไกลของเครื่องคอมพิวเตอร์แม่ข่าย ด้วยบริการรับส่งข้อความ ผ่านโทรศัพท์เคลื่อนที่ และอินเทอร์เน็ตสามารถนำมาใช้งานได้จริง ทั้งยังเป็นการนำเอาทรัพยากรและเทคโนโลยีความรู้มาประยุกต์ใช้ในองค์กรให้เกิดประโยชน์

(จารินี ชยาภิรมย์, 2557) ได้ทำการศึกษา วิธีการสำรองข้อมูลแบบเพียร์ทูเพียร์ โดยการวัดจากเวลาที่ใช้ในการสำรองข้อมูลและสภาพพร้อมใช้งานของข้อมูลเป็นปัจจัยหลัก เพื่อนำเสนอแบบจำลองสำหรับการตัดสินใจประสิทธิภาพ (Performance Decisive Mode!, P) เพื่อประเมินประสิทธิภาพในด้านโดยทำการทดลองเปรียบเทียบการสำรองข้อมูลบนระบบสำรองข้อมูลแบบเพียร์ทูเพียซึ่งใช้ขั้นตอนวิธีการแบ่งขึ้นส่วนย่อย 3 รูปแบบได้แห่ การแบ่งสวนย่อยตามจำนวนเครื่องในระบบ, การแบ่งขึ้นส่วนย่อยโดยกำหนดขนาดของสวนย่อยคงที่ และการแบ่งส่วนย่อยโดยใช้อีเรขอร์โค้ด (เลือกใช้ Reed-Solomon และ Luby Transtorm code) ผลการทดลองแสดงให้เห็นว่าการเพิ่มสภาพพร้อมใช้งานของไฟล์ไม่ได้แปรผันตามจำนวนเครื่องภายในระบบเสมอ แบบจำลองดังกล่าวสามารถนำมาใช้เป็นแนวทางสำหรับการตัดสินใจเลือกขั้นนตอนวิธีการถึงการเลือกพารามิเตอร์ที่เหมาะสมสำหรับแต่ละวิธีในการสำรองข้อมูล

(กนกรัตน์ ประสพภักดี, 2546) ได้ศึกษาและทำการวิจัยประยุกต์ใช้ระบบสารสนเทศเพื่อการจัดการระบบสำรองข้อมูล ด้วยการพัฒนาระบบสำรองข้อมูลทางอินเตอร์เน็ตเพื่อใช้ในองค์กร โดยการศึกษารูปแบบทั้งการสำรองข้อมูลและการแชร์ไฟล์ โดยพัฒนาระบบการจัดเก็บและแสดงผลผ่านอินเตอร์เน็ต ด้วยภาษา HTML , ภาษา PHP แสดงผลผ่านหน้าเว็บ และสามารถดึงไฟล์ไปใช้งานต่อ

ได้ ผลการทดสอบโดยการใช้การประเมิน 4 ด้านได้แก่ การติดต่อระหว่างผู้ใช้ การประมวลผล ความปลอดภัย ความตรงตามต้องการ โดยมีผลคะแนนประสิทธิภาพ อยู่ที่ 4.65 ในระดับดี

(ทรงกรด ยอดเจริญ, 2549) ได้ศึกษาและทำการวิจัยประยุกต์ใช้ระบบสารสนเทศเพื่อการจัดการระบบสำรองข้อมูล โดยการวิเคราะห์ เปรียบเทียบถึงเทคโนโลยีการจัดเก็บ และสำรองข้อมูล สำหรับองค์กร โดยเน้นไปที่ระบบ SAN (Storage Area Network) และ NAS (Network Attach Storage) โดยการพัฒนาระบบ DSS โปรแกรมสำหรับช่วยในการตัดสินเลือกใช้ระบบ โดยมีการนำข้อมูลทั้งหมดมาเก็บรวบรวมลงฐานข้อมูลที่ได้ออกแบบไว้ และจัดทำโปรแกรมในลักษณะ Web Application ในรูปแบบสอบถาม เพื่อให้ผู้ที่สนใจต้องการใช้งานระบบจัดเก็บ ข้อมูล ได้เข้ามาใช้ ซึ่งคำตอบที่ได้จากการตอบแบบสอบถาม จะอยู่ในรูปของคำแนะนำในการเลือกใช้งาน ทำให้สามารถช่วยตัดสินใจการเลือกวิธีการจัดเก็บสำรองข้อมูลได้อย่างถูกต้อง

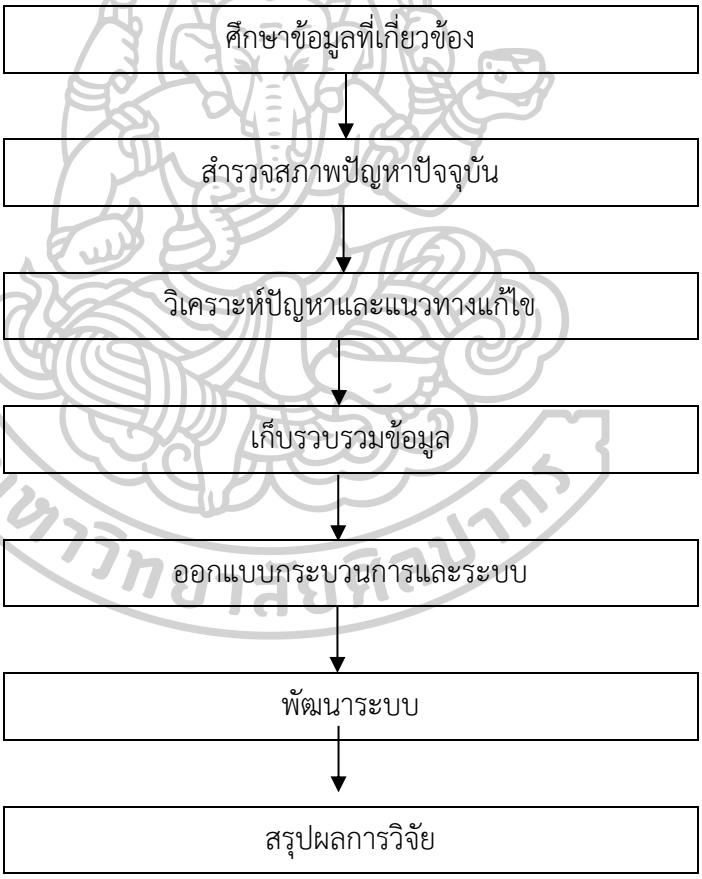
(Lassi Latva-Nirva, 2019) ได้ทำการศึกษาและวิจัยการเปรียบเทียบระบบสำรองข้อมูล แบบ Windows Backup Role และแบบ Veeam Backup Agent โดยวัดค่าและเปรียบเทียบประสิทธิภาพการสำรองข้อมูลทั้ง 2 ระบบ ผลที่ได้พบว่า การใช้ระบบสำรองข้อมูลแบบ Veeam Backup Agent จากผู้ให้บริการให้ผลลัพธ์ด้านความปลอดภัยที่ดีกว่า แต่ก็แลกมาด้วยค่าใช้จ่ายที่มากกว่าการพัฒนาระบบเอง

(Wesley G. Justice, 2008) เสนอแนวทางการพัฒนาและการสำรองข้อมูลที่ครอบคลุมและแผนการกู้คืน แผนสำรองและกู้คืนที่เป็นมาตรฐานโดยเปรียบเทียบพิจารณาฮาร์ดแวร์และซอฟต์แวร์หลายโซลูชัน (ทั้งเชิงพาณิชย์และโอเพ่นซอร์ส) เพื่อลดความเสียหายจากข้อมูลที่อาจจะได้รับผลกระทบ โดยเปรียบเทียบวิธีการสำรองข้อมูล แบบ 1) ใช้โปรแกรม Backup Exec for Windows Servers , 2) ใช้โปรแกรม Retrospect Backup Software , 3) ใช้โปรแกรม Data Protector , 4) ใช้โปรแกรม Tivoli Storage Manager Express , 5) ใช้โปรแกรม BackupPC , 6) ใช้โปรแกรม Duplicity , 7) ใช้โปรแกรม Rsnapshot โดยผลสรุปของโครงการคือการเลือกใช้โปรแกรม ซอฟต์แวร์ Retrospect Backup Software ร่วมกับ ฮาร์ดแวร์ ขององค์กร คือแนวโซลูชั่นที่ให้ประสิทธิภาพดีที่สุด มีค่าใช้จ่ายที่ต่ำที่สุด

บทที่ 3

วิธีดำเนินการวิจัย

การดำเนินงานวิจัยในบทนี้ได้กล่าวถึงข้อมูลทั่วไปของบริษัทกรณีศึกษา รวบรวมข้อมูลจำนวนเครื่องคอมพิวเตอร์เซิร์ฟเวอร์และขนาดไฟล์ที่จะต้องสำรองข้อมูล และทำการสำรวจสภาพปัญหาปัจจุบันและนำข้อมูลมาทำวิเคราะห์เพื่อหาค่าระดับความเสี่ยง จากนั้นทำการออกแบบพัฒนาระบบสำรองข้อมูลทางคอมพิวเตอร์ตามแบบคำสั่งทางคอมพิวเตอร์ เพื่อจัดการลดความเสี่ยงดังกล่าว เพื่อให้สอดคล้องกับวัตถุประสงค์ของงานวิจัย ซึ่งมีรายละเอียดขั้นตอนการดำเนินการดังนี้



ภาพที่ 21 ขั้นตอนการดำเนินงาน

3.1 ศึกษาข้อมูลที่เกี่ยวข้อง

บริษัทที่ทำการศึกษาเป็นการดำเนินธุรกิจเกี่ยวกับด้านโทรคมนาคม ให้บริการบรอดแบนด์ อินเตอร์เน็ต บริการไวไฟ บริการสื่อคอนเทนต์ ต่างๆ โดยเป็นในส่วนของสำนักงานในภูมิภาคตะวันตก มีจำนวนเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ (Server) รวม 26 เครื่อง เพื่อรองรับการทำงานด้านระบบสารสนเทศในด้านของเว็บไซต์การบริการและฐานข้อมูลที่ใช้งานในภูมิภาค โดยเครื่องคอมพิวเตอร์งเซิร์ฟเวอร์ (Server) ทั้งหมดเป็นระบบปฏิบัติการ windows

ภาพที่ 22 เครื่องเซิร์ฟเวอร์ ของบริษัทกรณีศึกษา

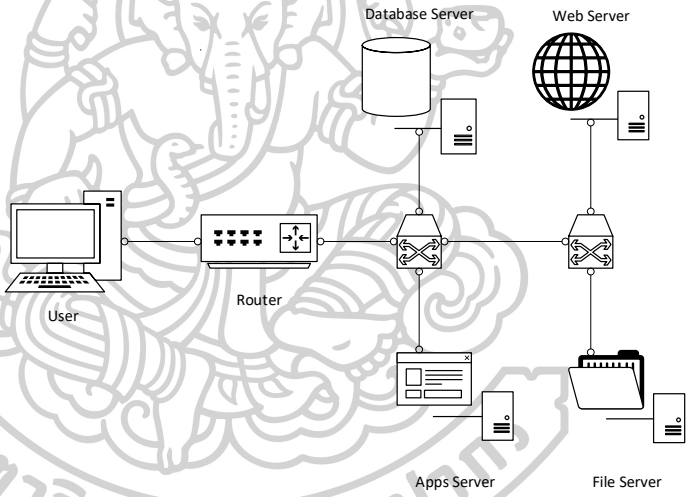
ทั้งนี้จากที่บริษัทกรณีศึกษาได้กำหนดนโยบายด้านความปลอดภัยของข้อมูลของบริษัทเป็นวาระสำคัญ และเพื่อลดความเสี่ยงจากระบบงานสนเทศเสียหายกรณีระบบถูกถูกแรนซัมแวร์โจมตีทำให้ข้อมูลเสียหาย ไม่สามารถเข้าถึงได้จึงต้องมีมาตรการแนวทางดำเนินการในการจัดการเพื่อลดความเสี่ยงดังกล่าว

3.1.1 แผนภาพกระแสข้อมูล (Data Flow Diagram)

ในขั้นตอนนี้ผู้วิจัยได้ทำการศึกษาภาพรวมของระบบเว็บไซต์การบริการและฐานข้อมูลที่มีผู้ใช้งานคือพนักงานในภูมิภาค พบว่าระบบเว็บไซต์การบริการและฐานข้อมูล ของบริษัทกรณีศึกษาประกอบด้วย

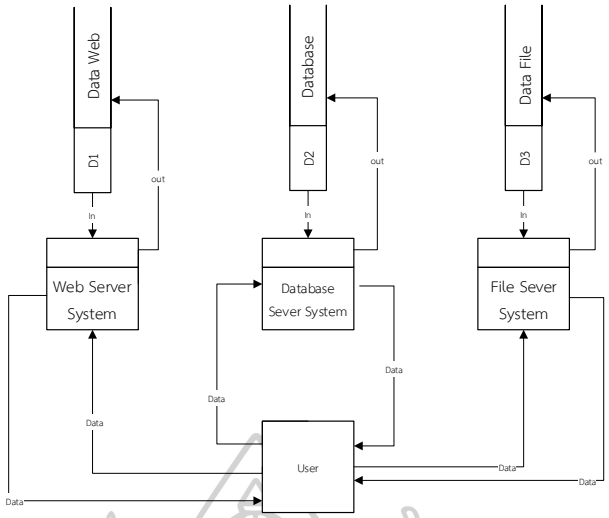
1) Web service (รวม Apps Service ด้วย)
2) Database server
3) File server

จากนั้นทำการศึกษาการเชื่อมต่อของระบบเครือข่ายเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ แสดงการเชื่อมต่อ Diagram ภาพที่ 23



ภาพที่ 23 ผังการเชื่อมต่อระบบคอมพิวเตอร์เซิร์ฟเวอร์

ซึ่งในส่วนของการเข้าถึงข้อมูลของผู้ใช้ ไปยังระบบเว็บไซต์การบริการและฐานข้อมูลภายในต่างๆ สามารถเขียนแสดงการเชื่อมต่อจาก User ไปยัง Server ได้ตามแผนภาพ Data Flow Diagram ภาพที่ 24



ภาพที่ 24 Data Flow Diagram การเข้าถึงระบบเว็บไซต์และฐานข้อมูลของผู้ใช้

3.2 สำรวจสภาพปัญหาปัจจุบัน

จากการที่ผู้วิจัยได้ทำการศึกษาสภาพในปัจจุบันของสำนักงานบริษัทกรณีศึกษานั้น พบ รายละเอียดดังนี้

ปัญหาที่พบ : ระบบเครือข่ายเครื่องเซิร์ฟเวอร์ในปัจจุบันมีไม่มีเครื่องเซิร์ฟเวอร์สำหรับสำรองข้อมูล ดังภาพที่ 23 ที่กล่าวไปแล้วข้างต้น

จากข้อมูลที่ได้มีการศึกษาในสภาพปัจจุบันดังกล่าวเนื่องจากบริษัทกรณีศึกษามีจำนวนเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ (Server) จำนวนมาก แต่ละเครื่องมีการเก็บข้อมูลต่างๆที่สำคัญในส่วนของเว็บไซต์การบริการและฐานข้อมูลไว้ ปัจจุบันมีข่าวองค์กรต่างๆถูกแรนซัมแวร์ โจมตีเป็นจำนวนมาก ซึ่งหากองค์กรของผู้วิจัยถูกโจมตีจะทำให้ข้อมูลในส่วนของเว็บไซต์การบริการและฐานข้อมูลไม่สามารถใช้งานได้ อันจะก่อให้เกิดผลเสียหายต่อระบบงานสารสนเทศและการดำเนินงานต่างๆ ประกอบกับบริษัทนโยบายด้านความปลอดภัยของข้อมูลของบริษัทเป็นวาระสำคัญ จากความเสี่ยงดังกล่าวทำให้ผู้วิจัยต้องมาศึกษาหลักในการจัดการงานสารสนเทศในส่วนนี้

3.2.1 วิเคราะห์ปัญหาและแนวทางแก้ไข

3.2.1.1 วิเคราะห์ปัญหา

ในขั้นตอนการวิเคราะห์ปัญหาของบริษัทกรณีศึกษา ในขั้นแรกผู้วิจัยจะทำการวิเคราะห์ จากสภาพปัจจุบัน และวิเคราะห์ความเสี่ยงตามหลักการของของการวัดความเสี่ยง ในบทที่ 2 หัวข้อที่ 2.8.6

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์การประเมิน และ การจัดระดับความเสี่ยงโดย ความเสี่ยงคำนวณจาก R = I x P

โดยที่ R = ความเสี่ยง , I = ผลกระทบ , P = โอกาสที่จะเกิดขึ้น

โดยเกณฑ์ประเมินความเสี่ยงผลกระทบเกิดขึ้นกับระบบสารสนเทศ อ้างอิงจากเกณฑ์การประเมินในบทที่ 2 หัวข้อที่ 2.8.6 การวัดความเสี่ยง รายละเอียดดังนี้

เกณฑ์การประเมินผลกระทบ (I) เป็นดังนี้ ระดับการประเมิน (เชิงปริมาณ)

1 คือ น้อย : ผลกระทบตั้งแต่ 11-30 นาที

2 คือ ปานกลาง : ผลกระทบตั้งแต่ 31-60 นาที

3 คือ สูง : ผลกระทบตั้งแต่ 61-180 นาที

4 คือ สูงมาก : ผลกระทบตั้งแต่ 180 นาทีขึ้นไป

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง (R) เป็นดังนี้ ระดับการประเมิน (เชิงปริมาณ)

1 คือ น้อย : 2-4 ปีต่อครั้ง

2 คือ ปานกลาง : 1 ปีต่อครั้ง

3 คือ สูง : 6 เดือนต่อครั้ง

4 คือ สูงมาก : 3 เดือนต่อครั้ง

วิเคราะห์ความเสี่ยง : ความเสี่ยงของระบบงานเดิมภาพที่ 24 ในเงื่อนไขที่ผู้วิจัยกำหนดจากข้อมูลของความเป็นจริงโอกาสที่จะเกิดขึ้นตามเกณฑ์การประเมินตามบทที่ 2 หัวข้อที่ 2.8.6 ได้สรุปผลดังตารางที่ 1 ดังนี้

ตารางที่ 1 วิเคราะห์ความเสี่ยงก่อนจัดทำระบบสำรองข้อมูล

ความเสี่ยง	รายการ	ระดับความเสี่ยงขั้นต้น		
		โอกาสของความเสี่ยง	ผลกระทบ	ผลประเมินความเสี่ยง
ก่อนจัดทำระบบ	ถูกแรนซัมแวร์โจมตี	3	4	12
	ข้อมูลถูกเข้ารหัสใช้งานไม่ได้	3	4	12
	ระบบงานไม่สามารถใช้งานได้เป็นระยะเวลานาน	3	4	12

จากข้อมูลดังกล่าวคำนวณตามหลักของ R = I x P จะได้ว่าผลประเมินความเสี่ยงในแต่ละรายการเท่ากับ 12 อ้างอิงจากภาพ 15 ตารางประเมินความเสี่ยง พบว่าระดับของความเสี่ยงอยู่

ที่ระดับ 4 ซึ่งเป็นความเสี่ยงที่ยอมรับไม่ได้ ต้องมีมาตรการดำเนินการและปรับปรุงแก้ไขเพื่อลดความเสี่ยงดังกล่าวทันทีให้อยู่ในระดับที่ยอมรับได้

3.2.1.2 แนวทางแก้ไข

เมื่อทำการวิเคราะห์ค่าระดับความเสี่ยงแล้วต่อมาผู้วิจัยได้ดำเนินการในขั้นต่อไปคือขั้นตอนการดำเนินงานตามระเบียบวิธีวิจัย เพื่อแก้ไขปัญหาดังกล่าว โดยประกอบด้วยขั้นตอนและรายละเอียดดังนี้

1) กำหนดปัญหา : ระบบเครือข่ายเครื่องเซิร์ฟเวอร์ในปัจจุบันมีไม่มีเครื่องเซิร์ฟเวอร์สำหรับสำรองข้อมูล และไม่มีการสำรองข้อมูล
2) ศึกษาความต้องการ : ต้องการระบบสำรองข้อมูลที่ทำงานแบบอัตโนมัติ และมีความปลอดภัย ตลอดจนมีการรายงานผล
3) วิเคราะห์แนวทางแก้ไข : พัฒนาระบบสำรองข้อมูลด้วยคำสั่งซอฟต์แวร์ทางคอมพิวเตอร์ที่ทำงานแบบอัตโนมัติ

3.3 เก็บรวบรวมข้อมูล

จากข้อมูลที่ได้มีการวิเคราะห์และกำหนดแนวทางแก้ไขแล้วทำให้ทราบเป้าหมายของงานวิจัย สิ่งที่จะเป็นองค์ประกอบที่สำคัญในงานวิจัยในขั้นตอนต่อไปคือการเก็บรวบรวมข้อมูลในขั้นตอนนี้ ผู้วิจัยได้กำหนดข้อมูลที่ต้องการเก็บรวบรวมดังนี้

3.3.1 ข้อมูลเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ (Server) และขนาดของไฟล์ที่ต้องสำรองข้อมูล

ผู้วิจัยได้ทำการสำรวจจำนวนเครื่องเซิร์ฟเวอร์ โดยเก็บข้อมูลจากหน้างานจริง ผลการศึกษาเก็บข้อมูลคอมพิวเตอร์เซิร์ฟเวอร์ สามารถสรุปรายการเครื่องเซิร์ฟเวอร์ มีจำนวน 26 เครื่อง โดยลักษณะงานของเครื่องเซิร์ฟเวอร์แบ่งได้ 3 ประเภทตามหน้าที่ หลักดังนี้

1) กลุ่ม Web Service (รวม Apps Service ด้วย) มีหน้าที่เป็น Web server รันโดย Apache web server

2) กลุ่ม Database server มีหน้าที่ให้บริการด้านการจัดการดูแลข้อมูลต่างๆภายในเว็บไซต์ โปรแกรมที่มีการใช้งานส่วนใหญ่จะเป็น My SQL

3) กลุ่ม File server มีหน้าที่ให้บริการแชร์ไฟล์เพื่อให้ใช้งานร่วมกัน เช่น Word, Excel, หรือรูปภาพ เป็นต้น รายละเอียดข้อมูลดังตารางที่ 2

ตารางที่ 2 ตารางข้อมูลเครื่องเซิร์ฟเวอร์ (Server) จำนวน 26 ของบริษัทตัวอย่าง

ลำดับ	เซิร์ฟเวอร์	ไอพี	รายละเอียด	ลักษณะงาน
1	RO01	10.73.161.1	Web Dept	Web Service
2	RO02	10.73.161.2	Web AREA RO6	Web Service
3	RO03	10.73.161.9	Network Storage_1	File Server
4	RO04	10.73.161.11	Database Camera	Database server
5	RO05	10.73.161.12	Network Storage_2	File Server
6	RO06	10.73.161.14	Web Sync Server	Database server
7	RO07	10.73.161.15	Finger Scan	Database server
8	RO08	10.73.161.32	IVR_1	Web Service
9	RO09	10.73.161.33	IVR_2	Web Service
10	RO10	10.73.161.61	Finger Scan U	Database server
11	RO11	10.73.161.64	Auto Report	Database server
12	RO12	10.73.161.65	CACTI	Web Service
13	RO13	10.73.167.17	Client CCS server	Web Service
14	RO14	10.11.15.68	IP Camera Server 1	Web Service
15	RO15	10.11.15.161	IP Camera Server 2	Web Service
16	RO16	10.11.15.162	Web Guardian	Web Service
17	RO17	10.11.15.163	IP Camera Server 3	Web Service
18	RO18	10.11.15.164	Web Apps RO	Web Service
19	RO19	10.73.168.34	IP Camera Server 4	Web Service
20	RO20	10.73.168.35	IP Camera Server 5	Web Service
21	RO21	10.73.168.36	IP Camera Server 6	Web Service
22	RO22	10.73.168.37	IP Camera Server 7	Web Service
23	RO23	10.73.168.38	IP Camera Server 8	Web Service
24	RO24	10.73.168.39	IP Camera Server 9	Web Service
25	RO25	10.73.168.40	IP Camera Server 10	Web Service
26	RO26	10.73.168.41	IP Camera Server 11	Web Service

เมื่อได้ข้อมูลของเครื่องเซิร์ฟเวอร์ จากนั้นทำการสำรวจขนาดของข้อมูลสำคัญของแต่ละเครื่องเซิร์ฟเวอร์ ที่จะต้องการสำรองข้อมูล โดยอ้างอิงเป็นข้อมูลตั้งต้น ได้ข้อมูลดัง ตารางที่ 3

ตารางที่ 3 ตารางข้อมูลขนาดไฟล์สำคัญที่ต้องสำรองของแต่ละเครื่องเซิร์ฟเวอร์ (Server)

ลำดับ	เซิร์ฟเวอร์	ไอพี	รายละเอียด	ลักษณะงาน	ขนาดไฟล์สำคัญ ที่ต้องสำรองข้อมูลรวม (กิกะไบต์)
1	RO01	10.73.161.1	Web Dept	Web Service	51.9
2	RO02	10.73.161.2	Web AREA RO6	Web Service	67.5
3	RO03	10.73.161.9	Network Storage_1	File Server	257.2
4	RO04	10.73.161.11	Database Camera	Database server	0.863
5	RO05	10.73.161.12	Network Storage_2	File Server	409
6	RO06	10.73.161.14	Web Sync Server	Database server	7.51
7	RO07	10.73.161.15	Finger Scan	Database server	10.3
8	RO08	10.73.161.32	IVR_1	Web Service	0
9	RO09	10.73.161.33	IVR_2	Web Service	0
10	RO10	10.73.161.61	Finger Scan U	Database server	0
11	RO11	10.73.161.64	Auto Report	Database server	0.086
12	RO12	10.73.161.65	CACTI	Web Service	0
13	RO13	10.73.167.17	Client CCS server	Web Service	53.8
14	RO14	10.11.15.68	IP Camera Server 1	Web Service	0
15	RO15	10.11.15.161	IP Camera Server 2	Web Service	0
16	RO16	10.11.15.162	Web Guardian	Web Service	0
17	RO17	10.11.15.163	IP Camera Server 3	Web Service	0
18	RO18	10.11.15.164	Web Apps RO	Web Service	0
19	RO19	10.73.168.34	IP Camera Server 4	Web Service	0
20	RO20	10.73.168.35	IP Camera Server 5	Web Service	0
21	RO21	10.73.168.36	IP Camera Server 6	Web Service	0
22	RO22	10.73.168.37	IP Camera Server 7	Web Service	0
23	RO23	10.73.168.38	IP Camera Server 8	Web Service	0
24	RO24	10.73.168.39	IP Camera Server 9	Web Service	0
25	RO25	10.73.168.40	IP Camera Server 10	Web Service	0
26	RO26	10.73.168.41	IP Camera Server 11	Web Service	0
ผลรวม					**858.2**

จากตารางที่ 3 พบว่า จากเครื่องเครื่องเซิร์ฟเวอร์ทั้งหมด 26 เครื่อง มีจำนวนเครื่องที่จะต้องทำการสำรองข้อมูล 9 เครื่องที่มีไฟล์งานสำคัญต้องสำรองข้อมูล มีขนาดข้อมูลที่จะสำรองทั้งหมดโดยอ้างอิงเป็นข้อมูลตั้งต้น ณ วันที่ 1 มีนาคม 2564 คือ 858.2 GB สรุปได้ดังตารางข้อมูลดังตารางที่ 4

ตารางที่ 4 ตารางข้อมูลเครื่องเซิร์ฟเวอร์ (Server) ที่ต้องสำรองข้อมูล

ลำดับ	เซิร์ฟเวอร์	ไอพี	รายละเอียด	ขนาดไฟล์สำคัญ ที่ต้องสำรองข้อมูล รวม (กิกะไบต์)
1	RO01	10.73.161.1	Web Dept	51.9
2	RO02	10.73.161.2	Web AREA RO6	67.5
3	RO03	10.73.161.9	Network Storage_1	257.2
4	RO04	10.73.161.11	Database Camera	0.863
5	RO05	10.73.161.12	Network Storage_2	409
6	RO06	10.73.161.14	Web Sync Server	7.51
7	RO07	10.73.161.15	Finger Scan	10.3
8	RO11	10.73.161.64	Auto Report	0.086
9	RO13	10.73.167.17	Client CCS server	53.8
ผลรวม				**858.2**

จากตารางที่ 4 แสดงสรุปรายการเครื่องเซิร์ฟเวอร์ (Server) ที่จะสำรองข้อมูลทั้งหมด

3.3.2 ประเภทของอุปกรณ์ในห้องเซิร์ฟเวอร์

จากข้อมูลที่ได้ทำการสำรวจในหัวข้อที่ 3.3.1 พบว่าในห้องเซิร์ฟเวอร์มีประเภทของอุปกรณ์ที่เป็นเครือข่ายที่เกี่ยวกับระบบเว็บไซต์การบริการและฐานข้อมูลดังนี้

1) คอมพิวเตอร์เซิร์ฟเวอร์ แบบ PC = 24 เครื่อง
2) เซิร์ฟเวอร์เก็บข้อมูลแบบ NAS Storage = 2 เครื่อง

3.3.3 ความเร็วอินเตอร์เน็ตของระบบเครือข่ายในห้องเซิร์ฟเวอร์

ความเร็วอินเตอร์เน็ตมีผลต่อการถ่ายโอนไฟล์จากเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ไปยังเครื่องที่ทำหน้าที่สำรองข้อมูล โดยจากการเก็บข้อมูลพบว่า ภายเครือข่ายในห้องเซิร์ฟเวอร์เชื่อมต่อกับด้วยสายแลน ที่มีความเร็วในการรับส่งข้อมูลอยู่ที่ 1 Gb ต่อวินาที หรือ 12.5 MB ต่อวินาที จากนั้นทางผู้วิจัยได้ทำการคำนวณประมาณระยะเวลาการถ่ายโอนไฟล์ไว้ ตามหลักการคำนวณ บทที่ 2 เรื่องหลักการข้อมูลสื่อสาร หัวข้อ 2.4.3.5.1 อัตราความเร็วในการถ่ายโอนข้อมูล ได้ข้อมูลระยะเวลาดังตารางที่ 5

ตารางที่ 5 ตารางข้อมูลระยะเวลาการถ่ายโอนไฟล์แต่ละเครื่องเซิร์ฟเวอร์ (Server)

ลำดับ	เซิร์ฟเวอร์	ไอพี	รายละเอียด	ขนาดไฟล์สำคัญ ที่ต้องสำรองข้อมูล รวม (กิกะไบต์)	ความเร็วการถ่ายโอนไฟล์ (เมกกะไบต์)	ระยะเวลาการถ่ายโอนไฟล์ (วินาที)	ระยะเวลาการถ่ายโอนไฟล์ (นาที)	ระยะเวลาการถ่ายโอนไฟล์ (ชั่วโมง)
1	RO01	10.73.161.1	Web Dept	51.9	12.5	4,252	71	1.18
2	RO02	10.73.161.2	Web AREA RO6	67.5	12.5	5,530	92	1.54
3	RO03	10.73.161.9	Network Storage_1	257.2	12.5	21,070	351	5.85
4	RO04	10.73.161.11	Database Camera	0.863	12.5	71	1	0.02
5	RO05	10.73.161.12	Network Storage_2	409	12.5	33,505	558	9.31
6	RO06	10.73.161.14	Web Sync Server	7.51	12.5	615	10	0.17
7	RO07	10.73.161.15	Finger Scan	10.3	12.5	844	14	0.23
8	RO11	10.73.161.64	Auto Report	0.086	12.5	7	0	0.00
9	RO13	10.73.167.17	Client CCS server	53.8	12.5	4,407	73	1.22
ผลรวม				**858.2**	**12.5**	**70,300**	**1,172**	**19.53**

3.4 ออกแบบกระบวนการและระบบ

เนื่องจากเครื่องเซิร์ฟเวอร์ของบริษัทกรณีศึกษาที่จะสำรองข้อมูลนั้นเป็นระบบปฏิบัติการ windows 24 เครื่อง และเป็น Storage เก็บข้อมูล 2 เครื่อง ในขั้นตอนการออกแบบกระบวนการทำงานและระบบสำรองข้อมูลนั้นผู้วิจัยจึงกำหนดเครื่องมือที่ใช้ในการวิจัย ดังนี้

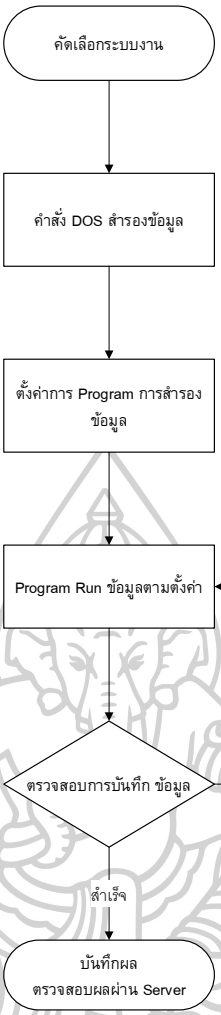
3.4.1 ชุดคำสั่ง DOS สำหรับสร้างคำสั่งคัดลอกข้อมูล

3.4.2 เครื่องคอมพิวเตอร์เซิร์ฟเวอร์สำหรับสำรองข้อมูล

3.4.3 Windows Task Scheduler สำหรับการกำหนดเวลาในการให้โปรแกรมงาน

จากนั้นผู้วิจัยจะทำการศึกษาและทำการเขียนผังภาพรวมทำงานของระบบ โดยกำหนดกรอบของทำงานรายละเอียดดังนี้

1) Flow Chart กระบวนการออกแบบระบบการสำรองข้อมูล ดังภาพที่ 25

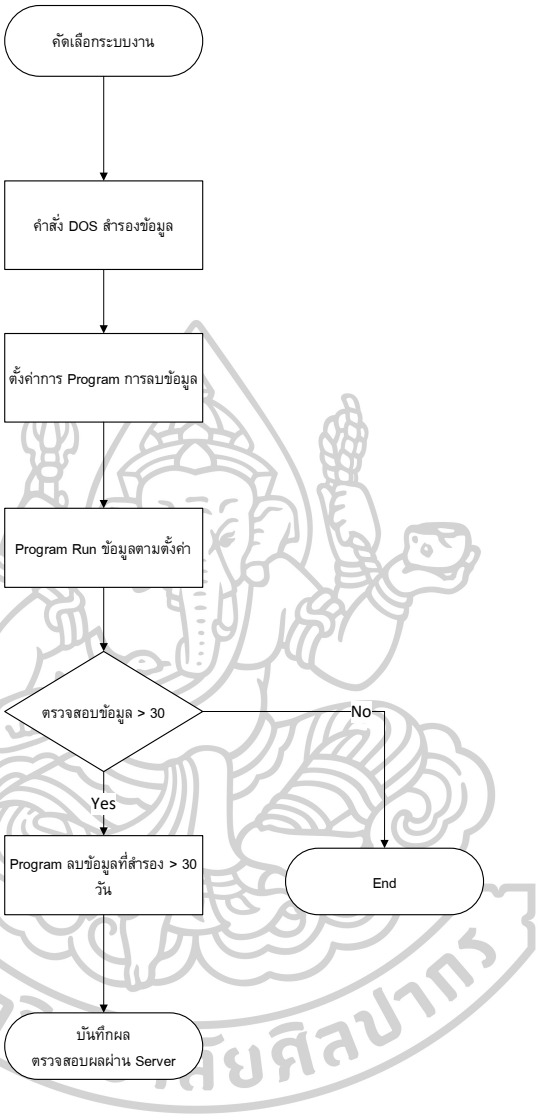


ภาพที่ 25 Flow การออกแบบระบบการสำรองข้อมูล

โดยจาก Flow Cart กระบวนการออกแบบระบบการสำรองข้อมูล สามารถอธิบายได้ดังนี้

- เริ่มแรกผู้วิจัยจะดำเนินการคัดเลือกระบบงานที่จะสำรองข้อมูล
- จากนั้นออกแบบคำสั่ง DOS เพื่อทำโปรแกรมสำรองข้อมูล
- นำโปรแกรมไปตั้งค่าใน Windows Task Scheduler
- โปรแกรทำงานตามวันที่และเวลาที่ตั้ง
- พนักงาน IT ตรวจสอบการสำรองข้อมูลและบันทึกผลรายงาน

2) Flow Chart การออกแบบระบบการลบข้อมูลที่สำรองที่มีอายุมากกว่า 30 วัน ดังภาพที่ 26



ภาพที่ 26 Flow การออกแบบระบบการลบข้อมูลที่สำรองที่มีอายุมากกว่า 30 วัน

โดยจาก Flow Cart การออกแบบระบบการลบข้อมูลที่สำรองที่มีอายุมากกว่า 30 วันสามารถอธิบายได้ดังนี้

- เริ่มแรกผู้วิจัยจะดำเนินการคัดเลือกระบบงานที่จะลบข้อมูล
- จากนั้นออกแบบคำสั่ง DOS เพื่อทำโปรแกรมลบข้อมูลที่สำรองที่มีอายุมากกว่า 30 วัน
- นำโปรแกรมไปตั้งค่าใน Windows Task Scheduler
- โปรแกรทำงานตามวันที่และเวลาที่ตั้ง

- พนักงาน IT ตรวจสอบการสำรองข้อมูลและบันทึกผลรายงาน

3.5 พัฒนาทดสอบระบบ

ในส่วนนี้ผู้วิจัยจะทำการตั้งค่าและทดสอบระบบที่ได้ออกแบบตามกระบวนการที่ได้ศึกษาแนวทางไว้ พร้อมทั้งเปรียบเทียบผลการดำเนินการและค่าใช้จ่ายที่เกิดขึ้น พร้อมเทียบเคียงค่าใช้จ่ายกับการใช้โซลูชั่นจากภายนอก

3.6 สรุปผลการวิจัย

จากนั้นนำเสนอผลงานวิจัย หลังจากประยุกต์ใช้ระบบสารสนเทศเพื่อการจัดการมาพัฒนาระบบสำรองข้อมูลแบบอัตโนมัติ ด้วยคำสั่งทางซอฟต์แวร์ของบริษัทกรณีศึกษา พร้อมข้อเสนอแนะเพื่อให้เกิดประโยชน์ ทั้งผู้ปฏิบัติงานและผู้ที่เกี่ยวข้องสำหรับการพัฒนาในอนาคต จากนั้นจึงจัดทำรูปเล่มรายงานการวิจัย

มหาวิทยาลัยศิลปากร

บทที่ 4

ผลการดำเนินการวิจัย

จากที่มาของปัญหาของบริษัทกรณีศึกษาในระบบสารสนเทศเครือข่ายเครื่องเซิร์ฟเวอร์ (Server) ที่ไม่มีระบบสำรองข้อมูล หากเกิดแรนซัมแวร์โจมตีย่อมก่อให้เกิดความเสียหายอันประเมินค่าไม่ได้ ตามการวิเคราะห์ความเสี่ยงที่อยู่ในระดับ 4 จะต้องเร่งดำเนินการลดความเสี่ยงดังกล่าวซึ่งในการจัดการปัญหาดังกล่าวจะต้องมีระบบสำรองข้อมูลทำงานแบบอัตโนมัติ ตามที่ได้ดำเนินการออกแบบไว้ในบทที่ 3 ในบทนี้จะกล่าวถึงสิ่งที่ผู้วิจัยได้ดำเนินการโดยมีรายละเอียดดังนี้

1) แนวทางในวิเคราะห์ข้อมูล
2) การดำเนินการออกแบบระบบ
3) การดำเนินการติดตั้งระบบ
4) ผลการดำเนินการ
5) สรุปผลที่ได้จากการดำเนินการ

4.1 แนวทางในวิเคราะห์ข้อมูล

การศึกษาวิจัยเรื่อง “การพัฒนาระบบสำรองข้อมูลเว็บไซต์การบริการและฐานข้อมูลของบริษัทตัวอย่าง” ผู้วิจัยได้จากการศึกษางานวิจัย จากสภาพปัญหาและข้อมูลที่ได้มีการศึกษาและเก็บรวบรวมจากบทที่ 3 ที่ ข้อมูลเกี่ยวข้องผู้วิจัยสามารถวิเคราะห์สรุปข้อมูลที่ได้ดังนี้

1) มีจำนวนเครื่องเซิร์ฟเวอร์ (Server) ที่จะต้องสำรองข้อมูลทั้งหมด 9 เครื่อง มีขนาดข้อมูลรวม 858.2 GB ดังนั้น จากตารางที่ 3 นำมาวิเคราะห์ความสำคัญของข้อมูลโดยจัดกลุ่มได้ดังตารางที่ 6

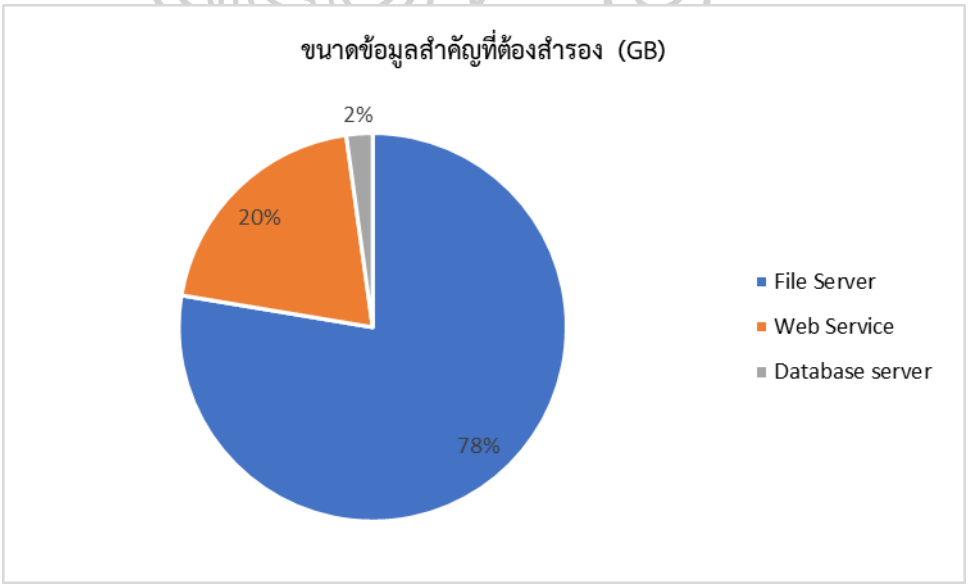
ตารางที่ 6 ตารางข้อมูลจำนวนไฟล์ที่จะต้องสำรองแยก Type Server

ประเภทเซิร์ฟเวอร์	จำนวน (เครื่อง)	% เครื่อง	ขนาดข้อมูลสำคัญที่ต้องสำรอง (กิกะไบต์)	% เครื่อง
File Server	2	22.22%	666.2	77.63%
Web Service	3	33.33%	173.2	20.18%
Database server	4	44.44%	18.8	2.19%
ผลรวม	**9**	**100.00%**	**858.2**	**100.00%**

จากตารางที่ 6 วิเคราะห์โดยการจัดกลุ่มของข้อมูล พบว่าจากเครื่อง 9 เครื่อง มีจำนวนของประเภทไฟล์งานที่ต้องสำรองแบ่งเป็น

- File Server = 666.2 GB
- File Web Service = 173.2 GB
- File Database = 18.8 GB

แสดงข้อมูลได้ดังกราฟภาพที่ 27



ภาพที่ 27 กราฟแสดงจำนวนสัดส่วนข้อมูลที่สำรองแยกตาม Type Server

2) ขนาดพื้นที่ที่ต้องใช้จัดเก็บข้อมูลที่สำรอง จากข้อมูลที่ผู้วิจัยได้ทำการรวบรวมในบทที่ 3 ขนาดข้อมูลที่ต้องสำรองตั้งต้นมีอยู่ที่ 858.2 GB จากหลักการสำรองข้อมูลบทที่ 2 อ้างอิงตามหัวข้อ 2.9.3 มาตรฐานรอบของการสำรองข้อมูล ผู้วิจัยจึงกำหนดให้มีการสำรองข้อมูลเดือนละ 2 ครั้ง ทำให้ 1 เดือน มีขนาดข้อมูลที่สำรองรวมประมาณ 1,716.4 GB ผู้วิจัยจึงกำหนดขนาดของอุปกรณ์จัดเก็บข้อมูลให้มีขนาดที่ 4,000 GB ทั้งนี้เพื่อรองรับการเติบโตของเว็บไซต์การบริการและฐานข้อมูลต่างๆในอนาคตด้วย

4.2 การดำเนินการออกแบบระบบ

จากการศึกษางานวิจัยเชิงประยุกต์ที่เกี่ยวข้อง และข้อมูลที่ได้รวบรวม ในส่วนผลการดำเนินงานมีขั้นตอนและดำเนินการออกแบบไว้ดังนี้

1) ออกแบบภาพรวมระบบการทำงานและอุปกรณ์
2) กำหนดตารางการทำงานของระบบสำรองข้อมูล
3) ออกแบบการทำงานโปรแกรมคำสั่ง DOS

โดยมีรายละเอียดในแต่ละขั้นตอนที่ได้ดำเนินการดังนี้

4.2.1 ออกแบบภาพรวมการทำงานของระบบ

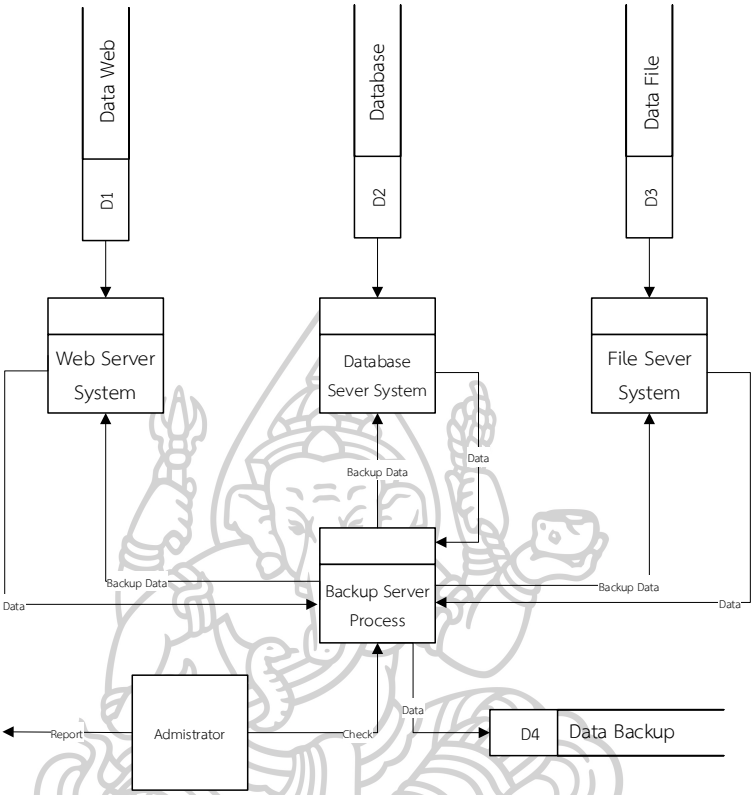
ในส่วนการออกแบบภาพรวมการทำงานของระบบนี้แบ่งเป็น

- ภาพรวมการทำงาน
- ผังการเชื่อมต่อ
- อุปกรณ์และซอฟต์แวร์ที่ใช้

4.2.1.1 ภาพรวมการทำงาน

ภาพรวมการทำงาน ได้กำหนดภาพรวมการทำงานของระบบไว้ โดยสังเขประบบจะทำงานสำรองข้อมูลด้วยคำสั่งภาษา DOS สร้างเป็นโปรแกรม Script ติดตั้งยังเครื่องเซิร์ฟเวอร์ที่ต้องการสำรองข้อมูล เชื่อมต่อถ่ายโอนไฟล์ด้วยวิธีการทำการสร้างไฟล์ข้อมูลร่วมกันภายในเครือข่ายเซิร์ฟเวอร์ (Map Drive) เพื่อให้โปรแกรมสามารถดึงข้อมูลที่จะสำรองมายังเครื่องเซิร์ฟเวอร์สำหรับสำรองข้อมูลได้ โดยทำงานแบบอัตโนมัติ เรียงลำดับจากไฟล์ที่มีความสำคัญมากสุด และมีขนาดน้อยสุดก่อน (อ้างอิงตามทฤษฎีบทที่ 2 หัวข้อ 2.9.2.1 แนวทางปฏิบัติในการสำรองข้อมูล ข้อ 1) และจากนั้นจะลบข้อมูลที่สำรองที่มีอายุมากกว่า 30 วัน แบบอัตโนมัติ โดยจะมีพนักงานในการเข้าไป

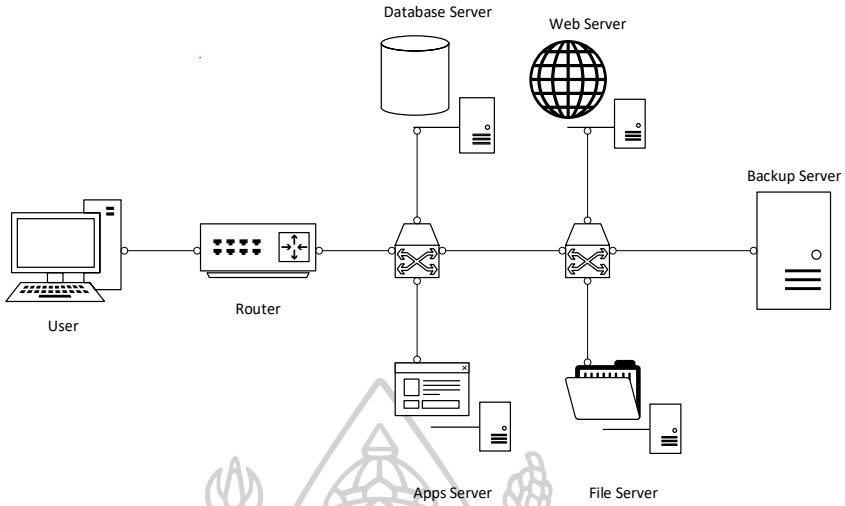
ดำเนินการตรวจเช็คและบันทึกผลลงเอกสารและรายงานผลให้หน่วยงานทราบ ออกแบบระบบดังแผนภาพ Data Flow Diagram ภาพที่ 28



ภาพที่ 28 Data Flow Diagram ภาพรวมของระบบสำรองข้อมูล

4.2.1.2 ผังการเชื่อมต่อ

จากการบทที่ 3 ในส่วนของสำรวจสภาพเครือข่ายเครื่องเซิร์ฟเวอร์ในปัจจุบัน ภาพที่ 23 พบว่า ระบบเครือข่ายไม่มีการสำรองข้อมูลของเว็บไซต์การบริการและฐานข้อมูลที่สำคัญ ทางผู้วิจัยจึงออกแบบเพิ่มเติมเครื่องเซิร์ฟเวอร์สำหรับสำรองข้อมูล โดยสำหรับอุปกรณ์ที่ใช้งานในระบบสำรองข้อมูลจะต้องใช้เครื่องเซิร์ฟเวอร์ที่มีความจุสำหรับจัดเก็บข้อมูล 4 TB (4,000 GB) ดังภาพที่ 29



ภาพที่ 29 ผังการเชื่อมต่อระบบคอมพิวเตอร์เซิร์ฟเวอร์ที่มีเครื่องสำรองข้อมูล

โดยจากรูป เมื่อออกแบบระบบสำรองข้อมูลตามผังภาพที่ 29 แล้วนั้นจะประกอบด้วย 2 ส่วน

1) ส่วนควบคุมกลาง (Main Server) ทำหน้าที่เป็นเครื่องเซิร์ฟเวอร์หลักที่ควบคุมระบบการสำรองข้อมูล และจัดเก็บไฟล์ข้อมูลที่สำรอง หรือเรียกส่วนนี้ว่า Backup Server
2) ส่วนเชื่อมต่อ (Client Server) คือส่วนเครื่องเซิร์ฟเวอร์อื่นๆ ที่อยู่บนเครือข่ายมีไฟล์ข้อมูลต่างๆที่สำคัญต่อระบบงานเว็บไซต์การบริการและฐานข้อมูลอยู่ เพื่อถ่ายโอนคัดลอกไปเก็บยัง Backup Server

4.2.1.3 อุปกรณ์และซอฟต์แวร์

ประกอบด้วย

1) คอมพิวเตอร์เซิร์ฟเวอร์ที่มีความจุสำหรับจัดเก็บข้อมูลแบบแยก OS และ Data

   OS : 250 – 500 GB

   Data : 4,000 GB (4TB)
2) ซอฟต์แวร์สำหรับสำรองข้อมูล : พัฒนาด้วยชุดคำสั่ง DOS (DOS Command)
3) โปรแกรม run ซอฟต์แวร์สำหรับสำรองข้อมูล : windows task scheduler

4.2.2 กำหนดตารางการทำงานของระบบสำรองข้อมูล

4.2.2.1 จัดลำดับการทำงานของการสำรองข้อมูล

จากข้อมูลในบทที่ 3 ตารางที่ 2 และ 3 ที่ได้ทำการเก็บรวบรวมข้อมูลเครื่องเซิร์ฟเวอร์และขนาดข้อมูลที่ต้องสำรองนั้น และจากข้อมูลที่ได้วิเคราะห์ไว้ในตารางที่ 6 ทำให้ผู้วิจัยสามารถกำหนดลำดับการทำงานของการสำรองข้อมูล โดยพิจารณาจากให้ระบบทำงานสำรองข้อมูลจากเครื่องที่มีขนาดไฟล์ที่มีความสำคัญมากสุดที่ต้องสำรองและมีขนาดน้อยที่สุดก่อน ได้ตารางที่ 7

ตารางที่ 7 ตารางข้อมูลจัดลำดับการทำงานของการสำรองข้อมูล

ลำดับ	เซิร์ฟเวอร์	ไอพี	รายละเอียด	ลักษณะงาน	ขนาด File สำคัญที่ต้องสำรองข้อมูลรวม (กิกะไบต์)	ความเร็วการถ่ายโอนไฟล์ (เมกกะไบต์)	ระยะเวลาการถ่ายโอนไฟล์ (วินาที)	ระยะเวลาการถ่ายโอนไฟล์ (นาที)	ระยะเวลาการถ่ายโอนไฟล์ (ชั่วโมง)
1	RO11	10.73.161.64	Auto Report	Database server	0.086	12.5	7	0.1	0.002
2	RO04	10.73.161.11	Database Camera	Database server	0.863	12.5	71	1.2	0.020
3	RO06	10.73.161.14	Web Sync Server	Database server	7.51	12.5	615	10.3	0.171
4	RO07	10.73.161.15	Finger Scan	Database server	10.3	12.5	844	14.1	0.234
5	RO01	10.73.161.1	Web Dept	Web Service	51.9	12.5	4,252	70.9	1.181
6	RO02	10.73.161.2	Web AREA RO6	Web Service	67.5	12.5	5,530	92.2	1.536
7	RO13	10.73.167.17	Client CCS server	Web Service	53.8	12.5	4,407	73.5	1.224
8	RO03	10.73.161.9	Network Storage_1	File Server	257.2	12.5	21,070	351.2	5.853
9	RO05	10.73.161.12	Network Storage_2	File Server	409	12.5	33,505	558.4	9.307

จากข้อมูลตารางที่ 7 พบว่าในการจะตั้งค่าการทำงานของระบบสำหรับ การสำรองข้อมูลนั้นจะต้องทำในส่วนของกลุ่มเครื่องเซิร์ฟเวอร์ที่เป็น Database server , Web server และ File server ตามลำดับ

4.2.2.2 จัดตารางเวลาการทำงานของการสำรองข้อมูลและลบข้อมูล

จากหลักการสำรองข้อมูลในบทที่ 2 หัวข้อ 2.9.3 มาตรฐานรอบของการสำรองข้อมูลคือต้องทำการสำรองข้อมูลอย่างน้อยเดือนละ 1 ครั้ง ทางผู้วิจัยจึงได้กำหนดมาตรฐานการสำรองข้อมูลของบริษัทตัวอย่างไว้ โดยให้สอดคล้องกับนโยบายของบริษัทด้วยดังนี้

1) ตั้งรอบการสำรองข้อมูลเดือนละ 2 ครั้ง ทุกวันที่ 14 , 28 ของทุกเดือน รายละเอียดสรุปดังตารางที่ 8
2) ตั้งรอบเวลาการสำรองข้อมูลในช่วงที่ไม่กระทบต่อระบบการทำงานในช่วงเวลางานปกติ
3) ตั้งรอบการลบข้อมูลที่มีอายุมากกว่า 30 วัน ทุกวันที่ 1 รายละเอียดสรุปดังตารางที่ 9

ตารางที่ 8 ตารางข้อมูลรอบการสำรองข้อมูลของระบบ

ลำดับ	เซิร์ฟเวอร์	ไอพี	รายละเอียด	ลักษณะงาน	ขนาด File สำคัญที่ต้องสำรองข้อมูลรวม (กิกะไบต์)	ระยะเวลาการถ่ายโอนไฟล์ (นาที)	ระยะเวลาการถ่ายโอนไฟล์ (ชั่วโมง)	รอบการสำรองข้อมูล	เวลาที่สำรองข้อมูล
1	RO11	10.73.161.64	Auto Report	Database server	0.086	0.1	0.002	วันที่ 14 , 28	20:00 น.
2	RO04	10.73.161.11	Database Camera	Database server	0.863	1.2	0.020	วันที่ 14 , 28	20:05 น.
3	RO06	10.73.161.14	Web Sync Server	Database server	7.51	10.3	0.171	วันที่ 14 , 28	20:10 น.
4	RO07	10.73.161.15	Finger Scan	Database server	10.3	14.1	0.234	วันที่ 14 , 28	20:20 น.
5	RO01	10.73.161.1	Web Dept	Web Service	51.9	70.9	1.181	วันที่ 14 , 28	20:30 น.
6	RO02	10.73.161.2	Web AREA RO6	Web Service	67.5	92.2	1.536	วันที่ 14 , 28	20:40 น.
7	RO13	10.73.167.17	Client CCS server	Web Service	53.8	73.5	1.224	วันที่ 14 , 28	20:50 น.
8	RO03	10.73.161.9	Network Storage_1	File Server	257.2	351.2	5.853	วันที่ 14 , 28	22:00 น.
9	RO05	10.73.161.12	Network Storage_2	File Server	409	558.4	9.307	วันที่ 14 , 28	22:10 น.

ตารางที่ 9 ตารางข้อมูลรอบการลบข้อมูลของระบบ

ลำดับการลบข้อมูล	เซิร์ฟเวอร์	ไอพี	รายละเอียด	ลักษณะงาน	รอบการลบข้อมูล	เวลาที่ลบข้อมูลสำรอง
1	RO11	10.73.161.64	Auto Report	Database server	วันที่ 1	20:00 น.
2	RO04	10.73.161.11	Database Camera	Database server	วันที่ 1	20:05 น.
3	RO06	10.73.161.14	Web Sync Server	Database server	วันที่ 1	20:10 น.
4	RO07	10.73.161.15	Finger Scan	Database server	วันที่ 1	20:20 น.
5	RO01	10.73.161.1	Web Dept	Web Service	วันที่ 1	20:30 น.
6	RO02	10.73.161.2	Web AREA RO6	Web Service	วันที่ 1	20:40 น.
7	RO13	10.73.167.17	Client CCS server	Web Service	วันที่ 1	20:50 น.
8	RO03	10.73.161.9	Network Storage_1	File Server	วันที่ 1	22:00 น.
9	RO05	10.73.161.12	Network Storage_2	File Server	วันที่ 1	22:10 น.

จากตารางที่ 8 และ 9 เมื่อกำหนดลำดับการทำงานและตารางเวลาสำหรับการสำรองข้อมูลและลบข้อมูลแล้ว ผู้วิจัยจะดำเนินการออกแบบคำสั่งทางคอมพิวเตอร์ด้วยชุดคำสั่ง DOS ในการสำรองข้อมูลเป็นลำดับต่อไป

4.2.3 ออกแบบการทำงานโปรแกรมคำสั่ง DOS และการติดตั้งระบบ

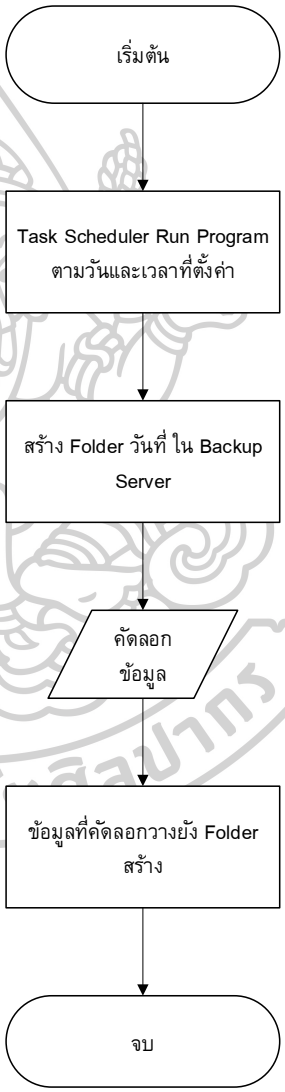
ในส่วนนี้เนื่องจะเป็นการออกแบบโปรแกรมสำรองข้อมูลด้วยคำสั่ง DOS โดยมีรายละเอียดที่ได้ดำเนินการดังนี้

4.2.3.1 ออกแบบ Flow Chart การทำงาน

แบ่งเป็น

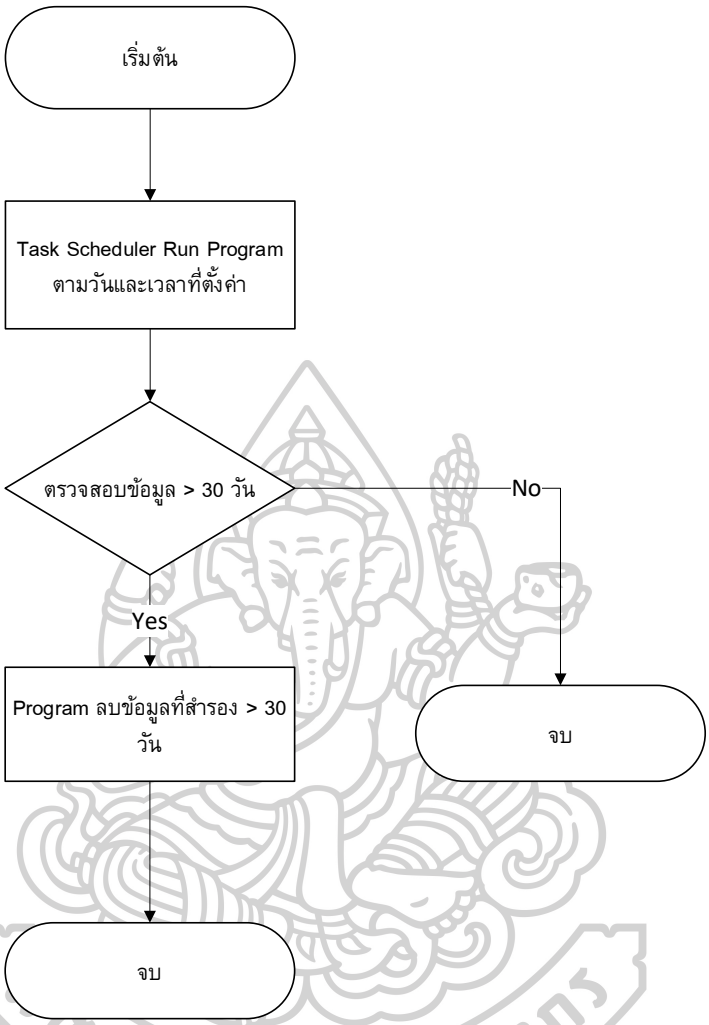
- การสำรองข้อมูล : กำหนดให้ทุกวันที่ 14 , 28 ของทุกเดือน
- การลบข้อมูล : กำหนดให้ทุกวันที่ 1 ของทุกเดือน

4.2.3.1.1 Flow Chart โปรแกรม DOS การสำรองข้อมูล ดังภาพที่ 30



ภาพที่ 30 Flow การทำงานของระบบการสำรองข้อมูลด้วยคำสั่ง DOS

4.2.3.1.2 Flow Chart โปรแกรม DOS การลบข้อมูลที่มากกว่า 30 วัน ดังภาพที่ 31



ภาพที่ 31 Flow การทำงานของระบบการลบข้อมูลที่สำรองที่มีอายุมากกว่า 30 วันด้วยคำสั่ง DOS

4.2.3.2 ชุดคำสั่ง DOS สำหรับสำรองข้อมูลและลบข้อมูล

เมื่อออกแบบ Flow Chart ของโปรแกรมคำสั่ง DOS ส่วนของการสำรองข้อมูล โดยโปรแกรมจะสร้าง Folder หลัก ตามอ้างอิงตามทฤษฎีบทที่ 2 หัวข้อ 2.9.2.1 ข้อ 3 ที่จะสร้างชื่อเป็นวันที่ที่สำรอง และ การลบข้อมูลที่ข้อมูลต่อมาผู้วิจัยดำเนินการเขียนชุดคำสั่ง DOS โดยใช้โปรแกรม Notepad++ ในการเขียน Code โดยมีรายละเอียดดังนี้

1) โปรแกรมคำสั่ง DOS การสำรองข้อมูล

ชุดคำสั่งโปรแกรม DOS สำรองข้อมูลดังตัวอย่าง ภาพที่ 32

```
@echo off


echo ------------------------------------------------------------
echo ------------------------------------------------------------
echo.
echo                    ::  BACKUP RON PROCESSING SERVER_10.73.161.9  ::
echo.
echo ------------------------------------------------------------
echo ------------------------------------------------------------
echo.
echo                    ::  DETIAL PROCESSING  ::
echo.


set DAY="DAY_%date:~7,2%_%date:~4,2%_%date:~10,4%"


robocopy Z:\ D:/DATA_BACKUP_SERVER/SERVER_10.73.161.9/RON/%DAY% /s /e


echo.
echo %DAY%
echo.
echo ------------------------------------------------------------
echo ------------------------------------------------------------
echo.
echo                    ::  Backup RON PROCESSING SERVER_10.73.161.9 COMPLETE ::
echo.
echo ------------------------------------------------------------
echo ------------------------------------------------------------
```

ภาพที่ 32 ตัวอย่าง Code คำสั่ง DOS สำหรับสำรองข้อมูล

รายละเอียดโครงสร้าง Code ชุดคำสั่งสำรองข้อมูลที่ใช้งานเพิ่มเติมในภาคผนวก ก

2) โปรแกรมคำสั่ง DOS ลบข้อมูลที่มากกว่า 30 วัน

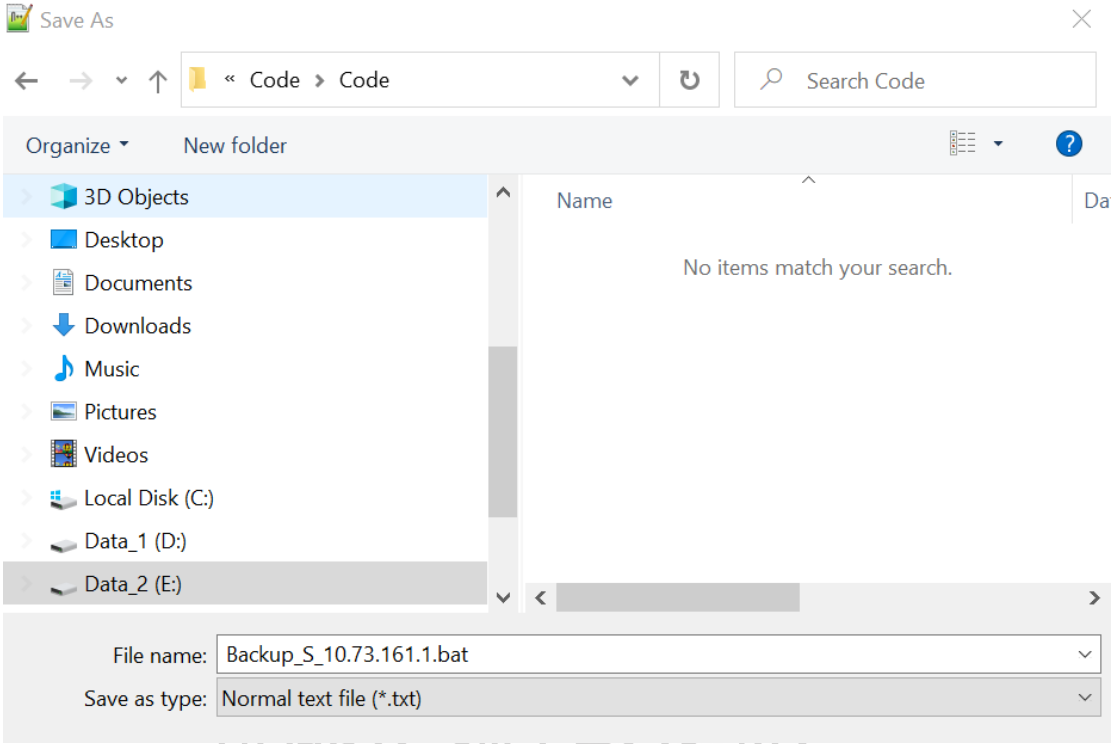
ชุดคำสั่งโปรแกรม DOS ลบข้อมูลที่มีอายุมากกว่า 30 วันดังตัวอย่างภาพที่ 33

```
@echo off

echo ------------------------------------------------------------
echo ------------------------------------------------------------
echo.
echo                    ::  Delete SERVER_10.73.161.1 PROCESSING  ::
echo.
echo ------------------------------------------------------------
echo ------------------------------------------------------------
echo.
echo                    ::  DETIAL SERVER_10.73.161.1 PROCESSING  ::
echo.


@echo off
:: set folder path
set website_database=D:\DATA_BACKUP_SERVER\SERVER_10.73.161.1\website_database

:: set min age of files and folders to delete
set max_days=30

:: remove files from %website_database%

forfiles -p %website_database% -m *.* -d -%max_days% -c "cmd  /c del /q @path"


:: remove sub directories from %website_database%

forfiles -p %website_database% -d -%max_days% -c "cmd /c IF @isdir == TRUE rd /S /Q @path"


echo.
echo %DAY%
echo.
echo ------------------------------------------------------------
echo ------------------------------------------------------------
echo.
echo                    :: Delete SERVER_10.73.161.1 COMPLETE  ::
echo.
echo ------------------------------------------------------------
echo ------------------------------------------------------------

@pause
```

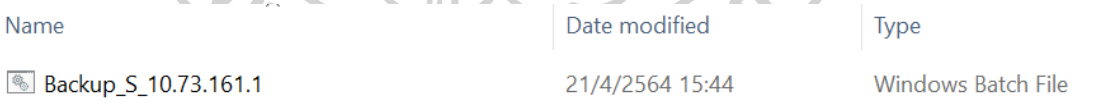
ภาพที่ 33 ตัวอย่าง Code คำสั่ง DOS สำหรับลบข้อมูลที่สำรองที่มีมากกว่า 30 วัน

รายละเอียดโครงสร้าง Code ชุดคำสั่งลบข้อมูลที่ใช้งานเพิ่มเติมในภาคผนวก ข

เมื่อเขียนโปรแกรมชุดคำสั่ง DOS สำหรับสำรองและลบข้อมูลเรียบร้อยแล้ว จากนั้นทำการ Save File Code ที่เขียนเป็นนามสกุล .bat (batch file) เพื่อสำหรับนำไปใช้งานในการ add เข้าโปรแกรม windows task scheduler ดังภาพที่ 34 และจะได้หน้าตาไฟล์ Code ดังภาพที่ 35



ภาพที่ 34 การ Save โปรแกรมคำสั่ง DOS เป็น batch file



ภาพที่ 35 หน้าตาไฟล์โปรแกรมคำสั่ง DOS

โดยผู้วิจัยดำเนินการเขียน Code โปรแกรมคำสั่ง DOS ในส่วนของสำรองข้อมูลและลบข้อมูลให้ครบตามจำนวนงานในแต่ละเครื่องเซิร์ฟเวอร์ที่ต้องจัดเก็บ ตามข้อมูลที่ได้เก็บรวบรวมไว้ในบทที่ 3 ตารางที่ 4

4.3 การดำเนินการติดตั้งระบบ

เมื่อทำการออกแบบระบบและเขียนชุดคำสั่งเรียบร้อยแล้ว ผู้วิจัยดำเนินการติดตั้งระบบโดยมีรายละเอียดดังนี้

- Main Backup Server
- Client Data Server

4.3.1 Main Server

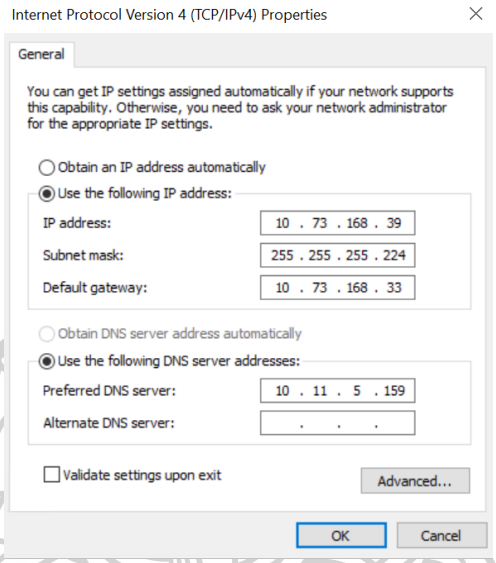
ดำเนินการติดตั้งและตั้งค่าระบบสำรองข้อมูลในส่วนของ Main Backup Server หรือเครื่องคอมพิวเตอร์ Server หลักที่มีหน้าที่จัดเก็บข้อมูลที่สำรอง ดังนี้

1) ติดตั้งเครื่อง Main Backup Server ดังภาพที่ 36

ภาพที่ 36 เครื่องคอมพิวเตอร์เซิร์ฟเวอร์สำหรับระบบสำรองข้อมูล

2) ตั้งค่าพื้นฐานต่างๆ

- IP เครื่อง เพื่อเชื่อมต่อกันบนเครือข่ายอินเตอร์เน็ต โดยพิจารณาอยู่บนเครือข่ายอินเตอร์เน็ตคนละเครือข่ายเพื่อความปลอดภัย ในกรณีเครือข่ายหลักถูกแรนซัมแวร์โจมตี การตั้งค่าดังภาพที่ 37



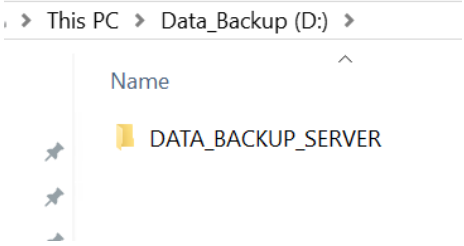
ภาพที่ 37 ตั้งค่า IP เครื่อง

- เปิดการตั้งค่า Share File

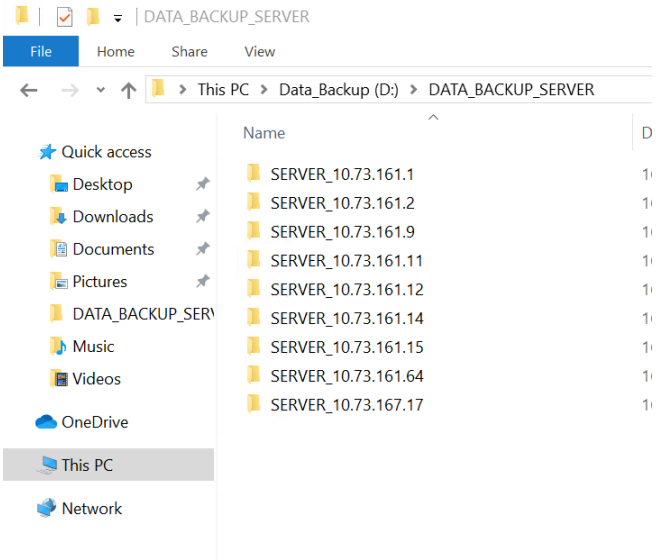
3) สร้าง Folder สำหรับจัดเก็บข้อมูล

ประกอบด้วยขั้นตอนดังนี้

- Folder หลัก : ตั้งชื่อว่า DAT_BACKUP_SERVER ดังภาพที่ 38
- Folder ย่อย : ตามจำนวนเครื่องที่สำรองข้อมูลดังภาพที่ 39

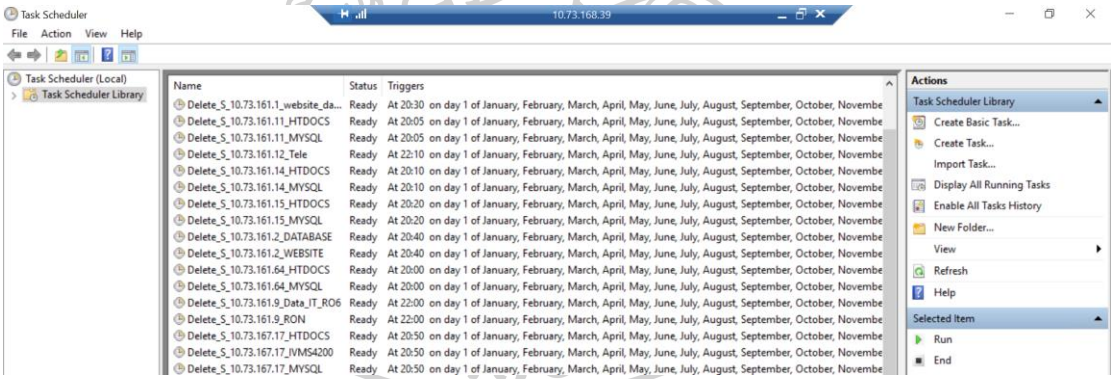


ภาพที่ 38 Folder หลักสำหรับสำรองข้อมูล



ภาพที่ 39 Folder ย่อย แยกตามเครื่องที่สำรองข้อมูล

4) ติดตั้ง Script ลบข้อมูลที่มากกว่า 30 วันลง Windows Task Scheduler ตามตารางที่ 9 ได้มีการออกแบบไว้ จะได้ดังภาพที่ 40

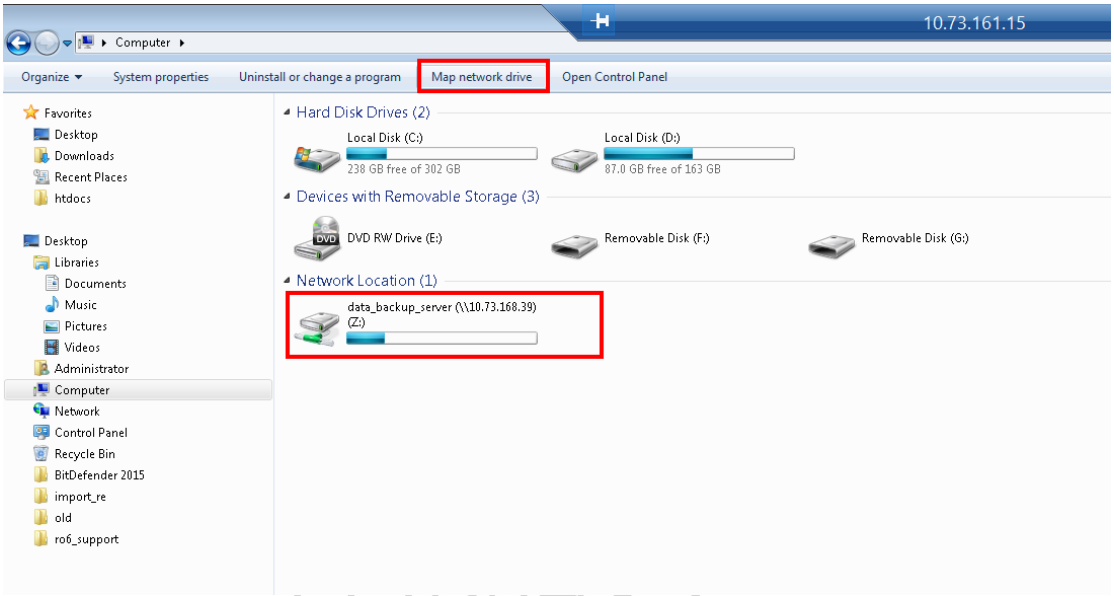


ภาพที่ 40 Add Script โปรแกรมลบข้อมูลที่มากกว่า 30 วันลง Windows Task Scheduler

4.3.2 Client Data Server

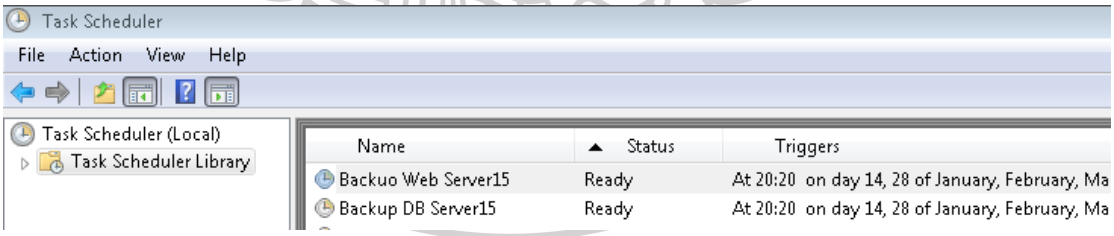
ผู้วิจัยดำเนินการติดตั้งและตั้งค่าในส่วนของ Client Data Server หรือเครื่อง Server ที่เป็นระบบเว็บไซต์การบริการและฐานข้อมูล ต่างๆ สำหรับให้โปรแกรมคัดลอกไปยัง Main Backup Server โดยมีตัวอย่างการดำเนินการดังนี้

1) ทำการสร้าง Map Drive บนเครื่อง Client Data Server เพื่อเชื่อมต่อกับ Folder หลัก ที่ใช้สำรองข้อมูลที่อยู่บน Main Backup Server ชื่อ Drive สร้าง Path ให้สอดคล้องกับโปรแกรมที่เขียนกำหนดไว้ ดังภาพที่ 41



ภาพที่ 41 สร้าง Map Drive บนเครื่อง Client Data Server

2) Add Script และตั้งค่าที่ Windows Task Scheduler ตามตารางที่ 8 ได้มีการออกแบบไว้



ภาพที่ 42 Add Script โปรแกรมคัดลอกข้อมูลที่มากกว่า 30 วันลง Windows Task Scheduler

ในขั้นตอนที่ 4.3.2 ไล่ทำจนครบทุก Server

4.4 ผลการดำเนินการ

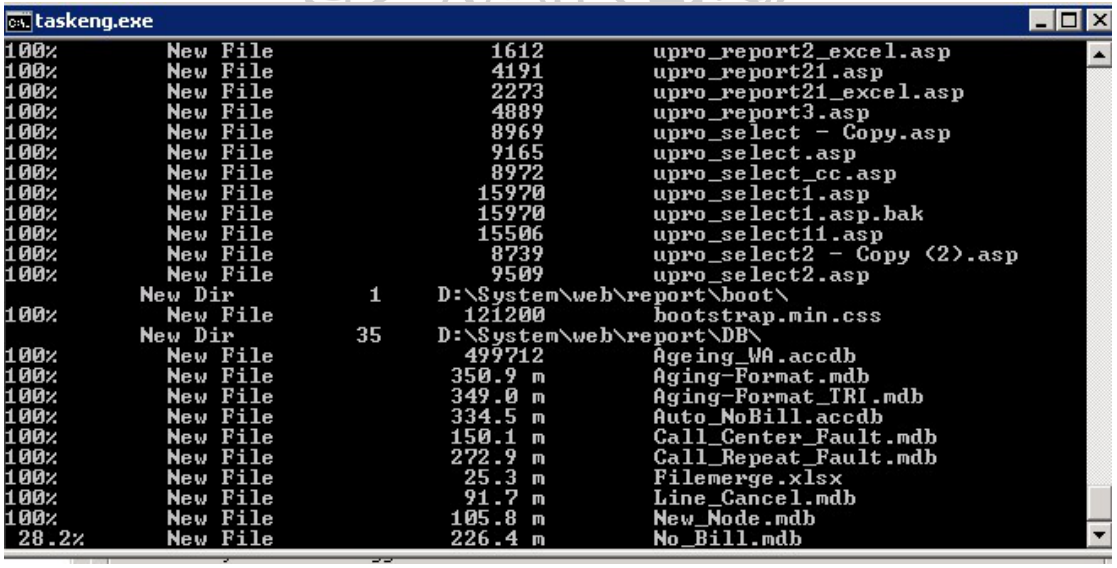
ผู้วิจัยกำหนดมาตรฐานวิธีการทดสอบการทำงานของระบบดังนี้

1) ทดสอบระบบการสำรองข้อมูล คือ การทดสอบให้โปรแกรมที่พัฒนาขึ้นทำงาน เพื่อคัดลอกข้อมูลแบบอัตโนมัติด้วย Windows Task Scheduler

2) ทดสอบระบบการลบข้อมูล คือ การทดสอบให้โปรแกรมที่เขียนทำงานให้ลบข้อมูลที่สำรองที่มีอายุไฟล์มากกว่า 30 วัน แบบอัตโนมัติด้วย Windows Task Schedulerหลังจากที่ได้มีการดำเนินการติดตั้งระบบแล้วทางผู้วิจัยได้ทำการตรวจสอบโดยมีรายละเอียดผลการดำเนินงานดังนี้

4.4.1 ผลการทำงานของ Sofwate สำรองข้อมูล

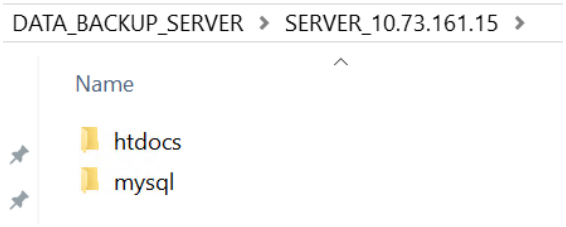
1) หน้าต่าง Commad DOS ขณะ โปรแกรมที่เขียนกำลังทำงานสำรองข้อมูล ดังภาพที่ 43



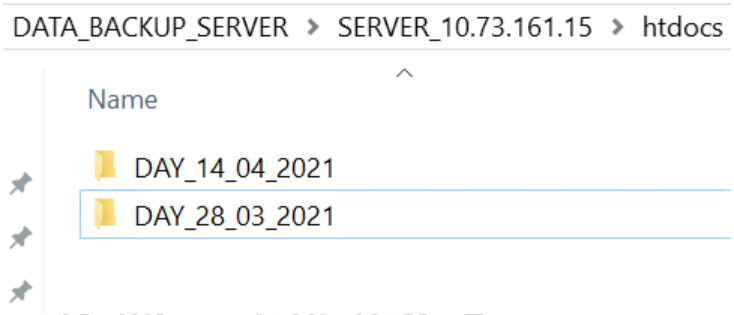
ภาพที่ 43 หน้าต่าง Commad DOS ทำงานคัดลอกข้อมูลไปสำรอง

2) Folder ที่โปรแกรมสร้างหลังจากโปรแกรม run เสร็จจะมีข้อมูลที่คัดลอกมาอยู่ โดยแบ่งเป็น

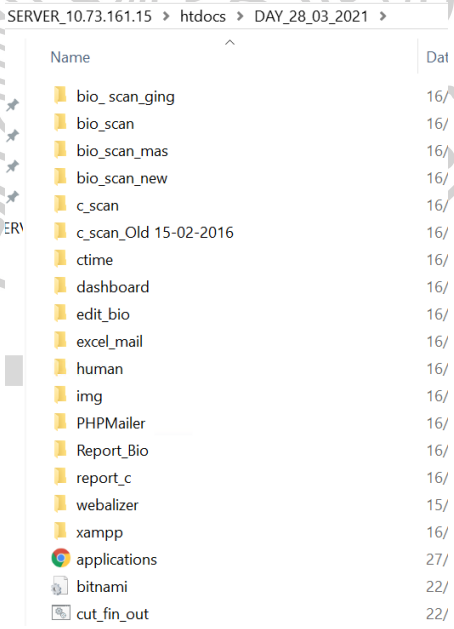
- Folder ย่อยตามประเภทไฟล์ที่โปรแกรมเขียนไว้ ดังภาพที่ 44
- Folder ย่อยที่มีชื่อวันที่นั้นๆของการคัดลอกข้อมูลมาสำรอง ดังภาพที่ 45
- ข้อมูลที่โปรแกรมและงานที่คัดลอกมาสำรองไว้ ดังภาพที่ 46



ภาพที่ 44 Folder ย่อยที่โปรแกรมสร้าง



ภาพที่ 45 Folder ย่อยวันที่ตามวันที่คัดลอกที่โปรแกรมสร้าง



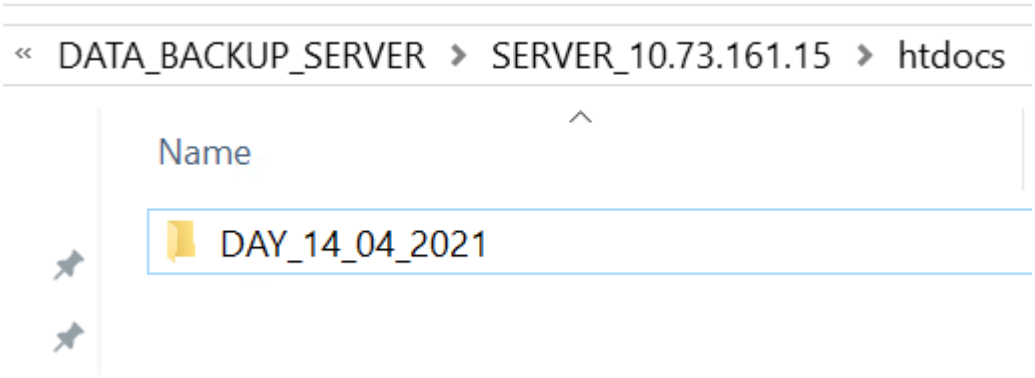
ภาพที่ 46 ข้อมูลและงานที่โปรแกรมคัดลอกมาสำรองไว้

4.4.2 ผลการทำงานของ Sofwate ลบข้อมูล

1) หน้าต่าง Commad DOS ขณะ โปรแกรมที่เขียนกำลังทำงานลบข้อมูล ดังภาพที่ 47

ภาพที่ 47 หน้าต่าง Command DOS ทำงานลบข้อมูลที่สำรองที่มีอายุมากกว่า 30 วัน

เมื่อโปรแกรมทำงานเสร็จจะพบว่า Folder วันที่ ที่มีอายุมากกว่า 30 วัน หายไปดังภาพที่ 48 เมื่อเทียบกับภาพที่ 45 จะพบว่า Folder DAY_28_03_2021 โปรแกรมลบไปแล้ว



ภาพที่ 48 ผลการทำงานของโปรแกรมลบข้อมูล

จากผลการเก็บข้อมูลการทำงานของระบบทางผู้วิจัยพบว่าระบบสำรองข้อมูลที่ออกแบบสามารถทำงานได้จริงและไม่พบ error ของโปรแกรมคำสั่ง DOS ที่พัฒนาขึ้น

4.5 สรุปผลที่ได้ดำเนินการ

4.5.1 สรุปผลด้านประสิทธิภาพของระบบสำรองข้อมูลด้วยคำสั่งทางคอมพิวเตอร์

เมื่อโปรแกรมที่ทำงานตามคำสั่งที่ได้ตั้งไว้ครบทุกเซิร์ฟเวอร์แล้วต่อมาทำการตรวจสอบจำนวนไฟล์ที่ระบบได้สร้างตามโฟลเดอร์ต่างๆและขนาดของข้อมูลที่คัดลอกไปยังเซิร์ฟเวอร์สำรองข้อมูล (Backup Server) ตามกระบวนการที่ได้กล่าวไว้ในบทที่ 3 แสดงดังตารางที่ 10

ตารางที่ 10 เปรียบเทียบผลการสำรองข้อมูลของระบบ

ลำดับการสำรองข้อมูล	เซิร์ฟเวอร์	ไอพี	รายละเอียด	ลักษณะงาน	ขนาดไฟล์สำคัญ ที่ต้องสำรองข้อมูลรวม (กิกะไบต์) (เก็บข้อมูลตั้งต้น 1-3-2020)	ข้อมูลที่สำรองได้		
						14/3/2021	28/3/2021	14/4/2021
1	RO11	10.73.161.64	Auto Report	Database server	0.086	0.086	0.086	0.086
2	RO04	10.73.161.11	Database Camera	Database server	0.863	0.863	0.863	0.863
3	RO06	10.73.161.14	Web Sync Server	Database server	7.51	7.51	7.51	7.51
4	RO07	10.73.161.15	Finger Scan	Database server	10.3	10.3	10.3	10.3
5	RO01	10.73.161.1	Web Dept	Web Service	51.9	51.9	51.9	51.9
6	RO02	10.73.161.2	Web AREA RO6	Web Service	67.5	67.5	67.5	67.5
7	RO13	10.73.167.17	Client CCS server	Web Service	53.8	53.8	53.8	53.8
8	RO03	10.73.161.9	Network Storage_1	File Server	257.2	257.2	260	261.1
9	RO05	10.73.161.12	Network Storage_2	File Server	409	409	410.2	412.7
ผลรวม					858.2	858.2	862.2	865.8

จากผลการดำเนินการวิจัยและข้อมูลขนาดของข้อมูลที่ระบบคัดลอกมาเก็บไว้ โดยที่ได้เก็บผลเพิ่มเติมดังตารางที่ 10 พบว่าระบบทำงานได้อย่างถูกต้องข้อมูลที่สำรองมีขนาดไม่ได้น้อยลงกว่าจำนวนข้อมูลที่ได้มีการสำรวจตั้งต้น ณ วันที่ 1-3-2021 ในส่วนสาเหตุที่ข้อมูลเพิ่มขึ้นเนื่องจาก ระบบไฟล์ในฐานข้อมูลหลักมีขนาดที่โตขึ้นตามการใช้งาน โดยข้อมูลที่สำรองมาทางผู้วิจัยทดสอบแล้วสามารถนำไปให้ได้จริงและครบถ้วน 100%

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

5.1 ผลการวิจัย

จากปัญหาในงานวิจัยและการวิเคราะห์ความเสี่ยงของปัญหาของบริษัทกรณีศึกษาที่ไม่มีระบบสำรองข้อมูลหากถูกแรนซัมแวร์โจมตีอาจก่อให้เกิดการล่มของระบบฐานข้อมูลและเว็บไซต์การบริการได้ ประกอบกับด้วยนโยบายของบริษัทที่มีการจัดตั้งหน่วยงาน Cyber Security โดยผู้วิจัยได้รับมอบหมายให้ดูแลในส่วนความปลอดภัยด้านข้อมูล จึงใช้แนวทางหลักการจัดการเทคโนโลยีสารสนเทศ และการประเมินความเสี่ยงมาใช้ โดยนำมาประยุกต์ในงานวิจัยนี้ซึ่งมุ่งเน้นการพัฒนาระบบซอฟต์แวร์ประยุกต์สำหรับสำรองข้อมูลเว็บไซต์การบริการและฐานข้อมูลของบริษัทกรณีศึกษา เป็นการจัดการลดความเสี่ยงจากข้อมูลที่อาจเสียหาย ถูกล็อก ทำให้ระบบเว็บไซต์การบริการและฐานข้อมูลใช้งานไม่ได้

ผลลัพธ์ที่ได้จากการพัฒนาระบบเองด้วยชุดคำสั่งซอฟต์แวร์ทางคอมพิวเตอร์ หรือชุดคำสั่ง DOS นั้น จะทำให้บริษัทกรณีศึกษาส่วนภูมิภาคตะวันตก มีข้อมูลสำรองของระบบเว็บไซต์การบริการและฐานข้อมูลในกรอบตามมาตรฐานที่ 30 วัน โดยโปรแกรมจะทำงานสำรองข้อมูลทุกๆวันที่ 14 และ 28 ระบบมีการทำงานแบบอัตโนมัติที่ ทั้งในส่วนการคัดลอกและการลบข้อมูลที่มีอายุมากกว่า 30 วันไปแล้ว ต่อมาเมื่อทำการเก็บผลและวิเคราะห์ผลที่ได้มีการบันทึกไว้ในบทที่ 4 พบว่า ระบบนั้นสามารถทำงานได้อย่างถูกต้อง คัดลอกข้อมูลได้ครบถ้วน และจากตารางที่ 10 ในบทที่ 4 มีค่าเปอร์เซ็นต์ความสำเร็จของงานอยู่ที่ 100% ทำให้เมื่อหากเกิดกรณีถูกแรนซัมแวร์โจมตี หรือ เกิดเหตุอื่นๆที่ทำให้ระบบระบบฐานข้อมูลและเว็บไซต์การบริการล่ม จะสามารถกู้คืนระบบขึ้นมาได้ในระยะเวลารวดเร็ว เนื่องจากมีมาตรการระบบสำรองข้อมูลรองรับ

5.2 ต้นทุนระบบ

เปรียบเทียบต้นทุนระบบที่วิจัยพัฒนาขึ้นด้วยคำสั่ง DOS กับการใช้พนักงาน และ การใช้โซลูชั่นจากผู้ให้บริการภายนอก แบ่งเป็นแนวทางที่ 1 , 2 และ 3 ตามลำดับโดยมีรายละเอียดดังนี้

- แนวทางที่ 1 : พัฒนาระบบด้วยภาษา DOS
    - ต้นทุนปีแรก

- ค่าฮาร์ดแวร์ คือ คอมพิวเตอร์ PC = 14,840 บาท , ฮาร์ดดิส 4 TB = 3,250 บาท รวม 18,090 บาท

- ต้นทุนปีต่อไป : -
- ต้นทุนค่าบำรุงรักษา (maintenance cost) คือจะเป็นค่าเปลี่ยนฮาร์ดดิส 4 TB = 3,250 บาท กรณีเสื่อมสภาพ (คิดจากมูลค่าราคา ณ ปี 2564)

- แนวทางที่ 2 : ใช้พนักงานคัดลอกข้อมูลมาเก็บสำรอง
  - ต้นทุนปีแรก
    - ค่าฮาร์ดแวร์ คือ ฮาร์ดดิส 4 TB = 3,250 บาท
    - ค่าแรงคิดจาก จำนวนพนักงานที่ใช้ x ค่าแรงต่อวัน (วันหยุด) x จำนวนวันที่ทำ

    รายละเอียดคือ

    จำนวนพนักงาน = 1 , ค่าแรงที่ต้องทำงานวันหยุด = 500 บาท (เนื่องจากเพื่อไม่ให้กระทบการทำงานของระบบในวันปกติ , จำนวนวันที่ทำการคัดลอกเฉลี่ย เดือนละ 3 วัน จะได้ 1 เดือนใช้ต้นทุนค่าแรงพนักงานในส่วนเดือนละ 1,500 บาท หรือ 18,000 บาท ต่อปี
  - ต้นทุนปีต่อไป : 18,000 บาท ต่อปี
  - ต้นทุนค่าบำรุงรักษา (maintenance cost) คือจะเป็นค่าเปลี่ยนฮาร์ดดิส 4 TB = 3,250 บาท กรณีเสื่อมสภาพ (คิดจากมูลค่าราคา ณ ปี 2564)
- แนวทางที่ 3 : การใช้โซลูชั่นจากผู้ให้บริการภายนอก
  - ต้นทุนปีแรก
    - ค่าบริการเช่าพื้นที่เก็บข้อมูล 2 TB เดือนละ 2,000 บาท ปีละ 24,000 บาท
  - ต้นทุนปีต่อไป : 24,000 บาท ต่อปี
  - ต้นทุนค่าบำรุงรักษา : -

จึงสรุปได้ว่าต้นทุนในปีแรกค่าใช้จ่ายในแนวทางที่ผู้วิจัยพิจารณาศึกษาและดำเนินการวิจัยในงานวิจัยในแนวทางที่ 1 นี้คือ 18,090 บาท ถูกว่าต้นทุนการใช้พนักงานดำเนินงานคัดลอกสำรองข้อมูลในแนวทางที่ 2 อยู่ 3,160 บาท คิดเป็น 17.47% และถูกกว่าการใช้บริการสำรองข้อมูลจากผู้

ให้บริการภายนอกในแนวทางที่ 3 อยู่ 5,910 บาท คิดเป็น 32.67% และในแนวทางแรกนี้ไม่มีต้นทุนค่าใช้จ่ายในปีต่อๆไปแสดงเปรียบเทียบดังตารางที่ 11

ตารางที่ 11 เปรียบเทียบมูลค่าต้นทุนค่าใช้จ่ายของการพัฒนาระบบเองกับแนวทางการใช้พนักงานดำเนินงาน และการใช้บริการสำรองข้อมูลจากผู้ให้บริการภายนอก

แนวทาง	รายการ	รายการ				ระยะเวลาที่สำรองข้อมูลได้	ต้นทุนค่าใช้จ่ายปีแรก	ต้นทุนค่าใช้จ่ายปีต่อๆไป	ต้นทุนค่าบำรุงรักษากรณีฮาร์ดแวร์เสียหาย
		ค่าฮาร์ดแวร์	ค่าซอฟต์แวร์	ค่าแรง	ค่าบริการ				
1	พัฒนาระบบด้วยภาษา DOS	18,090				90	18,090		3,250
2	ใช้พนักงาน	3,250		18,000		90	21,250	18,000	3,250
3	ใช้โซลูชั่นจากผู้ให้บริการภายนอก				24,000	60	24,000	24000	

5.3 ผลการประเมินความเสี่ยง

จากบทที่ 3 ที่ได้มีการวิเคราะห์ความเสี่ยงก่อนมีการจัดทำระบบสำรองข้อมูลดังตารางที่ 1 ดังนั้นหลังจากดำเนินการวิจัยจัดทำระบบสำรองข้อมูลเรียบร้อยแล้ว ผู้วิจัยทำการวิเคราะห์ความเสี่ยงหลังจัดทำระบบในหัวข้อความเสี่ยงเดิมเพื่อเปรียบเทียบผลการประเมินความเสี่ยง และวิเคราะห์เพิ่มเติมในส่วนความเสี่ยงที่ยังคงเหลืออยู่ โดยพิจารณาในด้านโอกาสของความเสียหายจากข้อมูลสูญหายได้ ข้อมูลสรุปดังตารางที่ 12

ตารางที่ 12 สรุปการประเมินความเสี่ยง ก่อนจัดทำระบบ หลังจัดทำระบบ และ ที่คงเหลือ

ความเสี่ยง	รายการ	ระดับความเสี่ยงขั้นต้น		
		โอกาสของความเสี่ยง	ผลกระทบ	ผลประเมินความเสี่ยง
ก่อนจัดทำระบบ	ถูกแรนซัมแวร์โจมตี	3	4	12
	ข้อมูลถูกเข้ารหัสใช้งานไม่ได้	3	4	12
	ระบบงานไม่สามารถใช้งานได้เป็นระยะเวลานาน	3	4	12
หลังจัดทำระบบ	ถูกแรนซัมแวร์โจมตี	3	2	6
	ข้อมูลถูกเข้ารหัสใช้งานไม่ได้	3	2	6
	ระบบงานไม่สามารถใช้งานได้เป็นระยะเวลานาน	3	2	6
ความเสี่ยงคงเหลือหลังจัดทำระบบ	ถูกไวรัสชนิดอื่นๆโจมตี	3	2	6
	อุปกรณ์เก็บข้อมูลสำรองเสียหาย	3	2	6

จากผลการประเมินความเสี่ยงตารางที่ 12 พบว่าก่อนจัดทำระบบมีผลประเมินความเสี่ยงในแต่ละรายการเท่ากับ 12 ซึ่งจัดอยู่ในเกณฑ์ความเสี่ยงระดับที่ 4 ต้องมีมาตรการและแนวทางการในการลดความเสี่ยงดังกล่าวทันที หลังจากที่ดำเนินการวิจัยจัดทำระบบสำรองข้อมูลแล้ว ผู้วิจัยได้ทำการวิเคราะห์ความเสี่ยงในหัวข้อความเสี่ยงเดิมพบว่าผลประเมินความเสี่ยงในแต่ละรายการเท่ากับ 6 จัดอยู่ในเกณฑ์ความเสี่ยงระดับที่ 2 คือยอมรับได้หากมีมาตรการควบคุมและแก้ไขสถานการณ์ จากนั้นผู้วิจัยได้ทำการวิเคราะห์ความเสี่ยงที่เหลืออยู่โดยพิจารณาในด้านโอกาสของความเสี่ยงจากข้อมูลสูญหายได้ในหัวข้อโดนไวรัสอื่นๆโจมตีและอุปกรณ์ที่เก็บข้อมูลเสียหายพบว่า ผลประเมินความเสี่ยงในแต่ละรายการเท่ากับ 6 จัดอยู่ในเกณฑ์ความเสี่ยงระดับที่ 2 คือยอมรับได้และมีมาตรการควบคุมแก้ไขความเสี่ยงดังกล่าว

จากผลการวิเคราะห์ดังกล่าวทำให้สรุปได้ว่าการจัดทำระบบสำรองข้อมูลเว็บไซต์การบริการและฐานข้อมูลนั้นช่วยลดระดับความเสี่ยงจากข้อมูลที่ถูกล็อกไม่สามารถใช้งานได้เมื่อถูกแรนซัมแวร์โจมตี โดยความเสี่ยงลดลงจากระดับที่ 4 มาเหลือระดับที่ 2 คืออยู่ในระดับที่ยอมรับได้

5.4 ข้อเสนอแนะ

งานวิจัยนี้มุ่งเน้นเพื่อแก้ปัญหาของบริษัทกรณีศึกษาที่จะหาแนวทางจัดการลดความเสี่ยงของข้อมูลองค์กรที่อาจเสียหายเมื่อถูกภัยคุกคามทางอินเตอร์จากแรนซัมแวร์โจมตี อันก่อนให้เกิดข้อมูลถูกล็อกเข้ารหัสเสียหายทำให้ไม่สามารถใช้งานระบบฐานข้อมูลและระบบเว็บไซต์การบริการได้ ในส่วนของความเสี่ยงด้านอื่นๆ ผู้วิจัยไม่ได้นำมาพิจารณาในงานวิจัยนี้ โดยการวิจัยนั้นจะเน้นโดยประยุกต์หลักการการจัดสารเทคโนโลยีสารสนเทศมาพัฒนาระบบสำรองข้อมูลขึ้นด้วยวิธีการพัฒนาด้วยซอฟต์แวร์ประยุกต์โปรแกรมคำสั่ง DOS สำหรับสำรองข้อมูลเว็บไซต์การบริการและฐานข้อมูลให้เป็นแบบอัตโนมัติซึ่งระบบนี้ใช้งานได้เฉพาะระบบปฏิบัติ Windows เท่านั้น และทั้งนี้เองก็ยังต้องใช้พนักงานในการเข้าไปตรวจสอบภาพรวมการทำงานของระบบนี้อยู่เสมอ รวมทั้งรูปแบบคำสั่งซอฟต์แวร์ค่อนข้างเฉพาะทางหากต้องการปรับแต่งหรือเพิ่มประสิทธิภาพการทำงานก็ต้องใช้ความระมัดระวังในการแก้ไข

รายการอ้างอิง

สภาพแวดลอมด้านเทคโนโลยีสารสนเทศ. (2557) เข้าถึงได้จาก http://www.otp.go.th/uploads/tiny_uploads/PolicyPlan/8-ICT/PlanITRisk.pdf

การบริหารความปลอดภัยในโรงงานอุตสาหกรรม. (2561). เข้าถึงได้จาก https://drive.google.com/file/d/1LLi7sHUCriiWO9KKivlyztPudnKvNOP/view

มงคล ลีละปัญญา. (2555). ระบบจัดการไฟล์เซิร์ฟเวอร์. วิทยานิพนธ์ระดับวิทยาศาสตร์มหาบัณฑิต , สาขาวิศวกรรมเครือข่ายคณะวิทยาการและเทคโนโลยีสารสนเทศ , มหาวิทยาลัยเทคโนโลยีมหานคร. เข้าถึงได้จาก http://www.msit.mut.ac.th/thesis/Thesis_2555/048 ระบบจัดการไฟล์เซิร์ฟเวอร์.pdf

อชิรัชญ์ สอนเนียม. (2551). การพัฒนาระบบสำรองข้อมูลจากการตรวจสอบและแจ้งเตือนการสื่อสารภายในเครือข่ายกรณีศึกษาบริษัททรูวิชันส์จำกัด. วิทยานิพนธ์ระดับวิทยาศาสตร์มหาบัณฑิต , สาขาวิชาเทคโนโลยีสารสนเทศ , คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ. เข้าถึงได้จาก https://tdc.thailis.or.th/tdc/dccheck.php?Int_code=52&RecId=24708&obj_id=188067

กฤษณา ตีวารี. (2555). การออกแบบระบบการสำรองข้อมูลและระบบการจัดการไวรัส. วิทยานิพนธ์ระดับวิศกรรมศาสตร์มหาบัณฑิต , สาขาวิชาการจัดการงานวิศวกรรม, คณะวิศวกรรมศาสตร์ มหาวิทยาลัยสยาม. เข้าถึงได้จาก https://tdc.thailis.or.th/tdc/browse.php?option=show&browse_type=title&titleid=316736

รุ่งโรจน์ กัววัฒนาพันธ์. (2552). ระบบสำรองข้อมูลและกู้คืนข้อมูลระยะไกล ของเครื่องคอมพิวเตอร์แม่ข่าย ด้วยบริการรับส่งข้อความ ผ่านโทรศัพท์เคลื่อนที่ และอินเทอร์เน็ต. วิทยานิพนธ์ระดับวิทยาศาสตร์มหาบัณฑิต , สาขาวิชาวิทยาการคอมพิวเตอร์ , คณะวิทยาศาสตร์ , มหาวิทยาลัยเชียงใหม่. เข้าถึงได้จาก https://tdc.thailis.or.th/tdc/browse.php?option=show&browse_type=title&titleid=97051

จารินี ชยาภิรมย์. (2557). การวิเคราะห์ประสิทธิภาพของขั้นตอนวิธีการแบ่งชิ้นส่วนไฟล์ของระบบ

สำรองข้อมูลแบบเพียร์ทูเพียร์. วิทยานิพนธ์ระดับวิศกรรมศาสตร์มหาบัณฑิต , สาขาวิชาวิศวกรรมคอมพิวเตอร์, คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. เข้าถึงได้จาก https://tdc.thailis.or.th/tdc/browse.php?option=show&browse_type=title&titleid=367977

กนกรัตน์ ประสพภักดี. (2546). ระบบสำรองข้อมูลทางอินเตอร์เน็ต. วิทยานิพนธ์ระดับวิทยาศาสตร์มหาบัณฑิต , สาขาวิชาเทคโนโลยีสารสนเทศ , คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ. เข้าถึงได้จาก https://tdc.thailis.or.th/tdc/browse.php?option=show&browse_type=title&titleid=33122

ทรงกรด ยอดเจริญ. (2549). การศึกษาเชิงเปรียบเทียบถึงเทคโนโลยีสำรองข้อมูล SAN และ NAS สำหรับองค์กร. วิทยานิพนธ์ระดับวิทยาศาสตร์มหาบัณฑิต , สาขาวิชาเทคโนโลยีสารสนเทศ , คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเกษตรศาสตร์. เข้าถึงได้จาก https://tdc.thailis.or.th/tdc/browse.php?option=show&browse_type=title&titleid=348677

Lassi Latva-Nirva. (2019). BACKUP AND DISASTER RECOVERY IN WINDOWS ENVIRONMENT. Thesis Degree Programme in Information Technology, KARELIA UNIVERSITY

Wesley G.(2008). Designing and Implementing a Backup and Recovery System for Kentucky's Cooperative Extension Service Justice. Thesis Degree Master of Science in Computer Information Technology, Regis University

ภาคผนวก

ภาคผนวก ก

อธิบายโครงสร้าง Code คำสั่ง DOS การสำรองข้อมูล

อธิบายโครงสร้าง Code DOS การสำรองข้อมูล

```
@echo off
echo ------------------------------------------------------------
echo ------------------------------------------------------------
echo.
echo                :: BACKUP DATABASE PROCESSING SERVER_xxxx  ::  // การระบุหัวข้อการทำ Backup
echo.
echo ------------------------------------------------------------
echo ------------------------------------------------------------
echo.
echo                :: DETIAL PROCESSING  ::
echo.
set DAY="DAY_%date:~7,2%_%date:~4,2%_%date:~10,4%" ::  // สร้างวันที่ Folder ที่จะ Backup
robocopy D:\AppServ\MySQL\data Z:/SERVER_xxxx/ชื่อ Folder ย่อย /%DAY%/%DATA_APP% /s /e
// คำสั่ง คัดลอกข้อมูล Drive ที Backup ไปยัง Server Backup
echo.
echo %DAY%
echo.
echo ------------------------------------------------------------
echo ------------------------------------------------------------
echo.
echo                :: Backup DATABASE SERVER_10.73.161.2 COMPLETE  ::
echo.
echo ------------------------------------------------------------
echo ------------------------------------------------------------
```

มหาวิทยาลัยศิลปากร

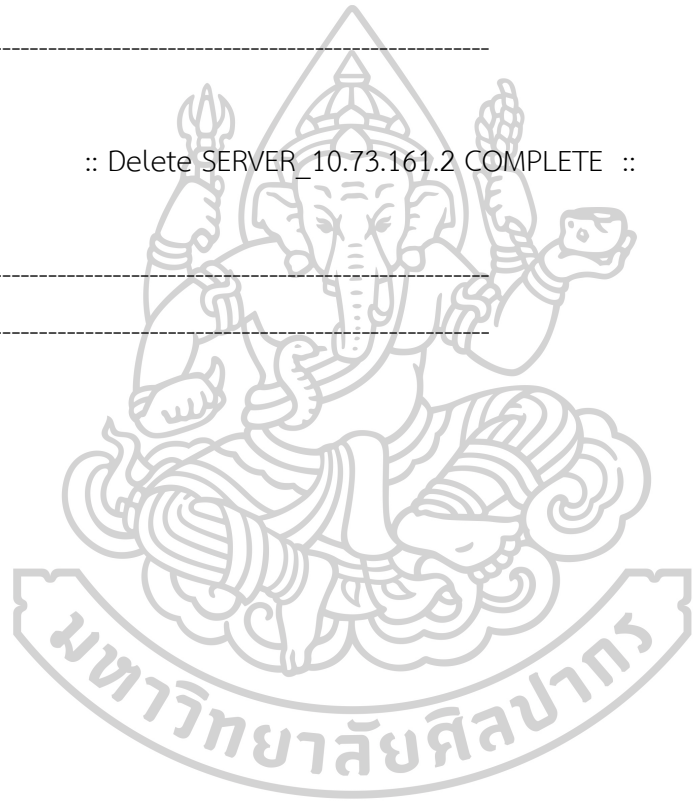
ภาคผนวก ข

อธิบายโครงสร้าง Code คำสั่ง DOS การลบข้อมูลที่สำรอง

อธิบายโครงสร้าง Code DOS การลบข้อมูล

```
@echo off

echo ------------------------------------------------------------
echo ------------------------------------------------------------
echo.
echo                    :: Delete SERVER_xxxx  PROCESSING  ::
echo.
echo ------------------------------------------------------------
echo ------------------------------------------------------------
echo.
echo                    :: DETIAL SERVER_xxxx  PROCESSING  ::
echo.

@echo off
:: set folder path
set database =D:\DATA_BACKUP_SERVER\SERVER_xxxx\database
::  //ไปที่ ชื่อ Folder ย่อย ที่ต้องการลบข้อมูลตาม Path ที่ได้สร้างไว้

:: set min age of files and folders to delete
set max_days=30          //ตั้งค่า Folder มีอายุมากสุดแค่ 30 วัน

:: remove files from %Database%

forfiles -p %database % -m *.* -d -%max_days% -c "cmd  /c del /q @path"
//ตั้งค่า ลบ Folder ย่อย มีอายุมากกว่า 30 วันตาม Path ที่ได้สร้างไว้

:: remove sub directories from %database %
```

```
forfiles -p %database % -d -%max_days% -c "cmd /c IF @isdir == TRUE rd /S /Q
@path"
//ตั้งค่า ลบข้อมูลใน Folder ย่อย ทั้งหมดอายุมากกว่า 30 วัน

echo.
echo %DAY%
echo.
echo ------------------------------------------------------------
echo ------------------------------------------------------------
echo.
echo                    :: Delete SERVER_10.73.161.2 COMPLETE  ::
echo.
echo ------------------------------------------------------------
echo ------------------------------------------------------------
```



ประวัติผู้เขียน

ชื่อ-สกุล	ณรงค์ฤทธิ์ เอกมงคลชัยกุล
วัน เดือน ปี เกิด	4 กันยายน 2534
สถานที่เกิด	นครปฐม
วุฒิการศึกษา	วศ.บ. (วิศวกรรมอิเล็กทรอนิกส์และระบบคอมพิวเตอร์) มหาวิทยาลัยศิลปากร 2557
ที่อยู่ปัจจุบัน	587 ซ.1 ถ.ทางรถไฟตะวันตก ต.นครปฐม อ.เมือง จ.นครปฐม 73000