องค์ความรู้ที่ได้รับ
จากโครงการฝึกอบรมหลักสูตรประกาศนียบัตรผู้ตรวจสอบภายในภาครัฐ (CGIA)
หลักสูตร Intermediate ด้าน Information Technology
ณ โรงแรมเดอะทวิน ทาวเวอร์ ถนนรองเมือง เขตปทุมวัน กรุงเทพฯ
ระหว่างวันที่ ๒๐ - ๓๐ สิงหาคม ๒๕๖๓

วิชาที่ ๑ การใช้คอมพิวเตอร์ช่วยในการตรวจสอบ โดย อาจารย์มานิต พาณิชย์กุล

เทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ : CAATTs (Computer - Assisted Audit Tools and Techniques) เนื้อหาของวิชา แบ่งออกเป็น ๓ ส่วน คือ

- ก่อนการนำเทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ
- อีกมุมมองของเทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ
- เทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ

- ***<u>ก่อนการนำเทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ</u>***

การควบคุมระบบงานคอมพิวเตอร์ จำแนกได้ ๓ องค์ประกอบ คือ

๑ <u>การควบคุมข้อมูลนำเข้า (Input Control)</u> เป็นการควบคุมที่มีความสำคัญมากเพื่อให้เกิดความแน่ใจว่าข้อมูลของรายการที่ต้องการประมวลผลได้รับการ**บันทึกอย่างถูกต้องครบถ้วน**ในงวดบัญชีที่เกิดรายการและข้อมูลที่ผิดพลาดได้รับการตรวจพบ และแก้ไขให้ถูกต้องก่อนส่งกลับเข้าประมวลผล ประเภทของการการควบคุมข้อมูลนำเข้า มี ๕ ประเภท ได้แก่

๑) ***การควบคุมเอกสารเบื้องต้น*** ต้องมีการใช้เอกสารที่มีเลขที่เอกสารพิมพ์ไว้ล่วงหน้า (Pre-numbered) มีการกำหนดให้ใช้เอกสารเบื้องต้นเรียงตามเลขที่ มีการตรวจเช็คว่าเอกสารทุกใบที่ถูกใช้ไปนั้นมีการบันทึกบัญชีโดยครบถ้วน

๒) ***การควบคุมการแปลงข้อมูล*** เป็นการควบคุมข้อผิดพลาดจากการคีย์ข้อมูลผิด (พิมพ์เพิ่ม พิมพ์ตกหล่น พิมพ์ตัวอื่นแทนที่) การควบคุมข้อผิดพลาดจากการคีย์ข้อมูลสลับตำแหน่ง (สลับตำแหน่งคู่เดียว สลับตำแหน่งมากกว่าคู่เดียว) การควบคุมข้อผิดพลาดจากการเปลี่ยนแปลงข้อมูลด้วยการเพิ่มตัวเลขอีกหนึ่งหลัก **Check Digits ซึ่งควรใช้กับข้อมูลที่สำคัญ ๆ เช่น Primary Key (เช่น เลข ID ๑๓ หลัก) เนื่องจากเปลืองพื้นที่ในการจัดเก็บและสิ้นเปลืองเวลาในการประมวลผล**

๓) ***การควบคุม Batch*** การควบคุม Batch เพื่อให้แน่ใจว่าทุกเอกสารใน Batch ได้มีการประมวลผล ไม่มีเอกสารใดประมวลผลมากกว่า ๑ ครั้ง และมีร่องรอยการตรวจสอบ (Audit Trail) ตลอดการทำงานตั้งแต่ข้อมูลนำเข้าการประมวลผลจนถึงข้อมูลส่งออก การควบคุม Batch ไม่ใช่เป็นเพียงการควบคุมข้อมูลนำเข้าเท่านั้น แต่ยังเป็นการควบคุมข้อมูลจนกระทั่งประมวลผลด้วย เมื่อมีเอกสารใบส่ง Batch จากผู้ใช้ฝ่ายต่าง ๆ ให้หน่วยงานคีย์ข้อมูล ซึ่งเรียกว่า “Batch transmittal sheet” ซึ่งประกอบด้วยเลขที่ Batch ในแบบ Running number วันที่ Batch เลขที่รหัสรายการ และที่สำคัญมากขาดไม่ได้ ๓ สิ่ง คือ **จำนวนของเอกสารใน Batch (Record count) ยอดรวมจำนวนตัวเลขที่เป็นตัวเงิน (Amount control total)** และ **ยอดรวมจำนวนตัวเลขที่ไม่ใช่ตัวเงิน (Hash total)**

กระบวนการควบคุม Batch ๔ ขั้นตอน คือ

(๑) **Users** จัดเตรียมเอกสารรายการที่เกิดขึ้นแล้วจัดส่งให้ Data control clerk

(๒) **Data control clerk** จัดเตรียม Batch transmittal sheet รวบรวมเอกสารเป็น Batch และบันทึกข้อมูลใน Batch control log

(๓) **Data entry group** ทำการคีย์ข้อมูลทั้งหมดจาก Transmittal sheet เพื่อประเมินความสมบูรณ์ในการประมวลผลของ Batch

(๔) **Data control clerk** ทำการกระทบยอดและ Update ข้อมูลใน Batch control log

ภายหลังจากบันทึกข้อมูลนำเข้าแล้วต้องมีการทำ

➢ **Record count check** เป็นการควบคุมโดยกำหนดให้โปรแกรมเปรียบเทียบจำนวน Record ที่มีการนำเข้าสู่ระบบกับจำนวน Record ที่ตรวจนับไว้ก่อนการนำเข้า เพื่อให้ทราบว่าทุกรายการผ่านการนำเข้าหรือไม่

➢ **Amount control total check** เป็นการควบคุมโดยกำหนดให้โปรแกรมเปรียบเทียบยอดรวมจำนวนเงิน (Amount Control Total) ที่ได้จากการรวมจำนวนเงินของรายการทั้งหมดในชุดเอกสารรายการหรือแฟ้มข้อมูลที่นำเข้ากับยอดรวมจำนวนค่าที่คำนวณไว้ใน Batch transmittal sheet ว่าตรงกันหรือไม่

➢ **Hash total check** เป็นการควบคุมโดยกำหนดให้โปรแกรมเปรียบเทียบยอดรวมตัวเลขที่ไม่ใช่จำนวนเงิน (Hash Total) ของ Field ที่มีการนำเข้ากับยอดรวมเลขที่ไม่ใช่จำนวนเงินของ Field นั้นที่คำนวณไว้ใน Batch transmittal sheet ว่าตรงกันหรือไม่ ตัวอย่าง hash total เช่น รหัสสินค้า และ จำนวนหน่วยสินค้า

๔) การควบคุมความถูกต้องของข้อมูลนำเข้า มี ๓ ระดับคือ

➢ **การควบคุมระดับ Field** การทำงานของโปรแกรมที่ตรวจสอบความถูกต้องของข้อมูลนำเข้าใน field ต่าง ๆ เช่น การตรวจสอบต่อไปนี้ :

❖ *Validity check* เป็นการควบคุมโดยใช้โปรแกรมตรวจสอบข้อมูลที่นำเข้าในรูปรหัสหรือตัวอักษรย่อหรือ คำต่าง ๆ ว่ามีอยู่จริงในระบบ ซึ่งได้รับการบันทึกเก็บไว้ในระบบงานคอมพิวเตอร์ ให้เป็นรหัสที่ใช้ทำรายการต่างๆ กับระบบงานนั้นได้ เช่น รหัสลูกค้า

❖ *Filed check* หรือ Type check เป็นการควบคุมโดยใช้โปรแกรมตรวจสอบฟิลด์ (Field) ว่าข้อมูลที่นำเข้าอยู่ในรูปแบบที่ถูกต้องเหมาะสมหรือไม่ เช่น ฟิลด์จำนวนเงิน ข้อมูลที่นำเข้าต้องเป็นตัวเลขเท่านั้น

❖ *Limit check* เป็นการควบคุมโดยโปรแกรมใช้ค่าของข้อมูลนำเข้า หรือค่าของข้อมูลที่ได้จากการคำนวณโดยโปรแกรม เปรียบเทียบกับหลักเกณฑ์หรือข้อจำกัดเกี่ยวกับค่าของข้อมูลที่กำหนดไว้ โดยหลักเกณฑ์หรือข้อจำกัดค่าสูงสุดที่กำหนดไว้ เช่น การตรวจว่าค่าขายเชื่อต้องไม่เกินวงเงินสินเชื่อ ข้อจำกัด คือ จำนวนวงเงินสินเชื่อ ถ้าใส่จำนวนเงินเกินระบบจะส่งข้อความเตือน

❖ *Range check* เป็นการควบคุมโดยโปรแกรมใช้ค่าของข้อมูลนำเข้า เปรียบเทียบกับช่วงของค่าที่ควรจะเป็นที่ได้กำหนดไว้ล่วงหน้า เช่น อายุของพนักงานควรอยู่ในช่วง ๒๐ - ๖๐ ปี

➢ ***การควบคุมระดับ Record*** การทำงานของโปรแกรมที่ตรวจสอบความถูกต้องของข้อมูลนำเข้าใน Field มากกว่า ๑ Field (๒ Field = การควบคุมระดับ Record) โดยลักษณะการตรวจสอบ :

❖ การตรวจสอบความสมเหตุสมผลของข้อมูล (Reasonableness checks) เป็นการควบคุมโดยใช้โปรแกรมตรวจสอบ ว่าข้อมูลรายการที่นำเข้ามีความสัมพันธ์กับฟิลด์อื่นที่เก็บอยู่ในระบบงานอย่างเหมาะสม เช่น อัตราค่าแรงสัมพันธ์กับรหัสตำแหน่งงาน

❖ การตรวจสอบเครื่องหมายของข้อมูลในระดับ Record (Sign checks) การตรวจสอบเครื่องหมาย + หรือเครื่องหมาย –

❖ การตรวจสอบความถูกต้องของการเรียงลำดับข้อมูลใน Transaction file กับ Master file (Sequence checks)

➢ ***การควบคุมระดับ File*** เพื่อให้มั่นใจว่าได้มีการนำ File ที่ถูกต้องมาทำการประมวลผล :

❖ การตรวจสอบฉลากภายใน (Internal label checks) ซึ่งต้องอ่านด้วยเครื่องว่าเป็นแฟ้มข้อมูลเวอร์ชั่นที่ถูกต้อง (Version checks)

❖ การตรวจสอบวันหมดอายุของแฟ้มข้อมูล (Expiration date check)

๕) การแก้ไขข้อผิดพลาด จะทำการแก้ไขทันทีทันใด หรือจำแนกข้อมูลที่ผิดพลาดไว้ต่างหากเพื่อทำการแก้ไข แล้วนำแต่ข้อมูลที่ถูกต้องไปประมวลผล ในกรณีที่ยอดรวม Batch ไม่ตรงกันกับใน Batch transmittal sheet ก็จะต้อง Reject ทั้ง Batch

๒ <u>การควบคุมการประมวลผล (Processing Control)</u> เพื่อให้แน่ใจว่ารายการต่าง ๆ ไม่สูญหายไปในระหว่างที่ทำการประมวลผล

๑) การใช้ยอดรวมของค่า Batchต่าง ๆ มาทำการกระทบยอดในแต่ละการประมวลผล (Run-to-Run Controls)

๒) การแทรกแซงการทำงานของระบบด้วยบุคคล (Operator Intervention Controls) ต้องลดให้น้อยที่สุดเพื่อลดโอกาสที่จะเกิดข้อผิดพลาดในระบบ

๓) การเก็บร่องรอยการตรวจสอบต่าง ๆ (Log)ไว้ เพื่อเป็นประโยชน์สำหรับการตรวจสอบ

๓ <u>การควบคุมข้อมูลส่งออก (Output Control)</u> เพื่อป้องกันไม่ให้เกิดการสูญหายของข้อมูลส่งออก

๑) การควบคุมข้อมูลส่งออกแบบ Batch การสั่งพิมพ์ข้อมูลพร้อม ๆ กันกับผู้อื่นโดยใช้เครื่องพิมพ์เดียวกันต้องระวัง

- การแก้ไขแฟ้มที่เก็บข้อมูลรอพิมพ์ (Spool file)
- การป้องกันไม่ให้ผู้อื่นเห็นข้อมูลที่เป็นความลับที่พิมพ์โดยการที่ User ไปรอหยิบรายงานที่เครื่องพิมพ์เอง
- การสั่งพิมพ์ข้อมูลที่เป็นความลับด้วยกระดาษต่อเนื่อง User ทำการแยกแผ่นและจัดเรียงรายงานที่เครื่องพิมพ์เอง
- การกำจัดรายงานที่ไม่ใช้แล้วอย่างถูกต้องโดยใช้เครื่องย่อย (Shredder)
- Data control ทำการกรองข้อมูลให้มีความถูกต้องชัดเจนเหมาะสมก่อนการส่งให้ End user
- การจัดส่งข้อมูลให้กับบุคคลที่ถูกต้องควรส่งตามรายชื่อผู้ที่มีสิทธิ์รับรายงาน
- End user เป็นผู้รับผิดชอบต่อความถูกต้องของข้อมูลในรายงานต่าง ๆ

๒) การควบคุมข้อมูลส่งออกแบบ Real-time การแสดงผลทางหน้าจอสามารถควบคุมได้โดยใช้ User ID และ Password และ ตารางสิทธิ (Access control matrix) เป็นต้น

การตรวจสอบการควบคุมระบบงานคอมพิวเตอร์ ประกอบด้วย

- การตรวจสอบนอกระบบ (Audit around the computer หรือ Black Box Approach) ผู้ตรวจสอบไม่สนใจว่าระบบคอมพิวเตอร์จะทำการประมวลผลเช่นใด โดยจะนำเอกสารเบื้องต้นมาประมวลผลด้วยมือแล้วนำมาเปรียบเทียบกับผลที่ได้จากระบบคอมพิวเตอร์ และเป็นการตรวจสอบรายการที่ไม่ซับซ้อน
- การตรวจสอบผ่านระบบ (Audit through the computer หรือ White Box Approach) ต้องมีการใช้เทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ (Information technology-based audit techniques or Computer Assisted Audit Techniques: CAATs) ทำการตรวจสอบสิทธิ์ในการทำงาน การตรวจสอบ Application Controls ความถูกต้องสมบูรณ์ของรายการ มีการนำข้อมูลมาประมวลผลซ้ำหรือไม่ การเข้าถึงระบบ ระบบมีการเก็บร่องรอยการตรวจสอบครบถ้วนหรือไม่

- <u>*อีกมุมมองของเทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ*</u>

๑ *Historical Data Techniques* วิธีการตรวจสอบ (เครื่องมือที่ตรวจสอบข้อมูลในอดีต) โดยนำข้อมูลชุดที่ผ่านการปฏิบัติจริงมาทำงาน ด้วยชุดโปรแกรมคอมพิวเตอร์ที่เขียนขึ้นเพื่อการทดสอบ ได้แก่ เทคนิค Parallel Simulation เทคนิค Extended Record เทคนิค Transaction Selection <u>*เทคนิค Generalized Audit Software*</u>

๒ *Concurrent Data Techniques* วิธีการตรวจสอบการทำงานของชุดโปรแกรมคอมพิวเตอร์พร้อมๆ กับการทำงานของระบบงานที่เป็น Production Run สามารถตรวจสอบได้ทันทีที่เกิดรายการ ได้แก่ ***เทคนิค Integrated Test Facilities*** เทคนิค Embedded Module (SCARF) เทคนิค Logging เทคนิค Tagging เทคนิค Monitoring

๓ *Programmed Analysis Techniques* วิธีการตรวจสอบการทำงานของโปรแกรมบางส่วนหรือทั้งหมดว่า Function เหล่านั้นเป็นไปตามที่กำหนดหรือไม่ ได้แก่ ***วิธี Test Data Method*** วิธี Base Case System Evaluation วิธี Snap Shot วิธี Mapping วิธี Tracing

- ***เทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ*** (Computer Assisted Audit Techniques: CAATs)

เทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ เทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ หมายถึง การนำเทคโนโลยีทางคอมพิวเตอร์ เช่น ฮาร์ดแวร์ ซอฟต์แวร์และระบบการจัดการฐานข้อมูลมาช่วยในการตรวจสอบ ที่นิยมอย่างแพร่หลาย ได้แก่ การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบทั่วไป และ การใช้ข้อมูลทดสอบ

การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบทั่วไป (Generalized Audit Software: GAS)

GAS เป็นโปรแกรมสำเร็จรูปที่พัฒนาขึ้นเพื่อใช้ในการตรวจสอบทั่วไปที่นิยมใช้มี ๒ โปรแกรม คือ ๑) IDEA (Interactive Data Extraction and Analysis) และ ๒) ACL (Audit Command Language) ทั้งนี้ GAS ช่วยให้ผู้ตรวจสอบสามารถหาหลักฐานเกี่ยวกับคุณภาพของ record ข้อมูลต่างๆ ได้โดยตรง ซึ่งมีส่วนในการตัดสินใจเกี่ยวกับคุณภาพและการควบคุมภายในของโปรแกรมประยุกต์ว่ามีความน่าเชื่อถือเพียงใด

สาเหตุที่ทำให้เกิดมีการพัฒนา GAS เกิดจากการนำระบบคอมพิวเตอร์มาใช้มากขึ้น ผู้ตรวจสอบประสบกับปัญหาความหลากหลายของชนิดซอฟต์แวร์ และ ฮาร์ดแวร์ที่ผู้รับการตรวจใช้ซึ่งผู้ตรวจสอบจำเป็นต้องดึงข้อมูลที่จัดเก็บมาตรวจสอบ

ประโยชน์ที่จะได้รับจากการใช้ GAS คือ ช่วยประหยัดเวลาที่ใช้ในการเขียนโปรแกรมเพื่อการตรวจสอบระบบได้ สามารถทำได้อย่างรวดเร็ว ในกรณีที่มีการเปลี่ยนวัตถุประสงค์ในการตรวจสอบ (audit objectives) ***ผู้ตรวจสอบที่ไม่มีความชำนาญในเรื่องการเขียนโปรแกรมก็สามารถใช้ GAS ได้*** งานตรวจสอบที่สามารถนำ GAS มาใช้ได้มี ๔ ด้าน ได้แก่ ๑) คุณภาพและการควบคุมภายในของระบบข้อมูล ๒) คุณภาพและการควบคุมภายในของระบบประมวลผล ๓) ความมีอยู่จริงของทรัพย์สิน และ ๔) การวิเคราะห์เปรียบเทียบ

ข้อจำกัดของ GAS ที่สำคัญ ได้แก่ ๑) สามารถตรวจสอบได้เฉพาะหลังจากเกิดรายการแล้ว (ex post auditing) เท่านั้น ๒) สามารถตรวจสอบ processing logic ได้ในกรณีที่ logic ไม่สลับซับซ้อนมากนัก แต่ในกรณีที่ logic มีความสลับซับซ้อนอาจจะไม่คุ้ม ๓) ไม่สามารถบอกถึงแนวโน้มที่ระบบอาจมีข้อผิดพลาด และ ๔) จำเป็นต้องใช้ข้อมูลจากระบบโดยให้ความเชื่อถือว่าข้อมูลที่ได้มามีความครบถ้วนและสมบูรณ์ (ต้องยืนยันยอดกับ GL)

การใช้ข้อมูลทดสอบ

การใช้ข้อมูลทดสอบที่สำคัญ มี ๒ ประเภท คือ การใช้ข้อมูลทดสอบแบบเทสท์ดาต้า (Test Data) และการใช้ข้อมูลทดสอบแบบอินทีเกรเต็ดเทสท์ฟาซิลิตี้ (Integrated Test Facility)

๑. การใช้ข้อมูลทดสอบแบบเทสท์ดาต้า (Test Data) เป็นวิธีที่ออกแบบขึ้นมาเพื่อใช้กับการประมวลผลแบบกลุ่ม (การประมวลผลแบบกลุ่ม (Batch processing) ซึ่งมีขั้นตอนในการทำเทสท์ดาต้า ดังนี้

- สอบทานเอกสารประกอบระบบของลูกค้า เพื่อดูว่าจุดควบคุมมีอะไรบ้าง
- สร้างข้อมูลทดสอบหรือรายการจำลอง (Simulated transactions)
- บันทึกรายการลงในกระดาษทำการของผู้ตรวจสอบ พร้อมที่คำนวณผลการประมวลผลที่คาดว่าจะได้รับ (Predetermined computer results) ด้วยมือ แล้วบันทึกลงในกระดาษทำการ

- ทำการประมวลผลโดยใช้โปรแกรมคอมพิวเตอร์ของลูกค้าโดยทำบนเครื่องคอมพิวเตอร์ของผู้ตรวจสอบ แล้วนำผลการประมวลที่ได้ไปเทียบกับที่คำนวณไว้ล่วงหน้า

ข้อดี คือ ผู้ตรวจสอบมีความมั่นใจมากขึ้นในความเชื่อถือได้ของโปรแกรมที่ผู้รับการตรวจใช้ปฏิบัติงาน

ข้อเสีย คือ ไม่สามารถทำให้แน่ใจว่าการควบคุมภายในมีประสิทธิผล โปรแกรมที่ผู้ตรวจสอบตรวจสามารถทำงานตามที่ควรเฉพาะที่อยู่ในขอบเขตของ Test data เท่านั้น สามารถทดสอบจำกัดเพียงฟังก์ชันที่มีอยู่ในโปรแกรมของลูกค้า เหมาะสำหรับการประมวลผลแบบกลุ่ม (Batch processing) เท่านั้นการพัฒนา Test Data ต้องใช้เวลามากและต้องปรับให้เข้ากับแอปพลิเคชั่น (Application) แต่ละอัน

๒. การใช้ข้อมูลทดสอบแบบอินทีเกรเต็ดเทสท์ฟาซิลิตี้ (Integrated Text Facility = ITF) เป็นเทคนิคซึ่งผู้ตรวจสอบสร้างข้อมูลจำลองขึ้น (Simulated transaction) แล้วนำไปประมวลผลร่วมกับข้อมูลจริงของลูกค้าโดยใช้ โปรแกรมประยุกต์ (Application program) ซึ่งลูกค้าใช้ในการประมวลผลข้อมูลตามปกติบนเครื่องคอมพิวเตอร์ที่ลูกค้าใช้งานอยู่จริง หลังจากการประมวลผลจะนำผลที่ได้มาวิเคราะห์ แต่มีข้อเสีย คือ โปรแกรมประยุกต์ (Application program) ของลูกค้าอาจถูกแก้ไขให้ทำการประมวลผลข้อมูลที่เป็นข้อมูลจำลอง Dummy (ซึ่งมีรหัสพิเศษ) ต่างจากการประมวลผลข้อมูลจริง และระหว่างทดสอบหากการใส่ และลบข้อมูลจำลองอาจทำให้เกิดข้อผิดพลาดขึ้นในข้อมูลจริงได้โดยไม่ได้ตั้งใจ

เทคนิคสำคัญอื่นๆ ยังสามารถแบ่งออกได้อีก ๖ ประเภท ได้แก่

- การใช้โปรแกรมอรรถประโยชน์ หรือยูทิลิตี้ซอฟต์แวร์
- การใช้โปรแกรมที่เขียนขึ้นมาเฉพาะเพื่อการตรวจสอบที่มีลักษณะพิเศษ
- การใช้ภาษาระดับสูง
- การตรวจสอบโปรแกรม
- การใช้โปรแกรมที่พัฒนาขึ้นเพื่อใช้ทำงานในสำนักงานช่วยในการตรวจสอบ
- ระบบผู้เชี่ยวชาญ

การประยุกต์ใช้คอมพิวเตอร์เพื่อช่วยในการตรวจสอบ หรือ ประโยชน์ของการใช้ CAATs คือ

- ทำให้เห็นภาพรวมของระบบและการเคลื่อนไหวของรายการ
- ช่วยในการจัดการกับข้อมูลเหล่านั้น ได้แก่ - การจัดประเภท - การแยกประเภท - การวิเคราะห์ทางสถิติ และคณิตศาสตร์
- ช่วยในการวิเคราะห์รายการที่ผิดปกติง่ายยิ่งขึ้น
- ผู้ตรวจสอบจำเป็นต้องใช้ CAATs ในการตรวจสอบระบบที่ใช้เทคโนโลยีสารสนเทศเพื่อการประมวลผล
- ช่วยลดระดับความเสี่ยงซึ่งเกิดจากการตรวจสอบ
- ช่วยเพิ่มความเป็นอิสระจากผู้รับการตรวจสอบ
- สามารถเพิ่มขอบเขตการตรวจสอบให้ครอบคลุมมากยิ่งขึ้น
- ช่วยเพิ่มโอกาสในการประเมินและวิเคราะห์เชิงปริมาณเพื่อค้นหาจุดอ่อนของการควบคุม
- ช่วยเพิ่มประสิทธิภาพในการสุ่มตัวอย่าง
- เพิ่มประสิทธิผลในการตรวจสอบในกรณีการตรวจสอบสิ่งผิดปกติ/รายการทุจริต
- ลดค่าใช้จ่ายและระยะเวลาในการตรวจสอบ

วิชาที่ ๒ การตรวจสอบวงจรรายได้ (Auditing the Revenue Cycle) โดย อาจารย์สุรพงษ์ ชูรังสฤษฎ์

หน้าที่ผู้ตรวจสอบภายในกับการตรวจสอบรายได้ ต่างกับผู้ตรวจสอบบัญชี คือ ไม่ใช่ตรวจสอบว่า รับมาถูกต้องตามเกณฑ์ และบันทึกรายการเข้าบัญชีรายได้ถูกต้องและครบถ้วนหรือไม่? แต่เป็นการตรวจสอบว่า มีวิธีการควบคุมความถูกต้องและครบถ้วนหรือไม่? มีการปฏิบัติตามการควบคุมหรือไม่? การควบคุมได้ผลหรือไม่? ตรวจสอบความถูกต้องและครบถ้วนของการบันทึกรายการ และหัวหน้างาน ได้ตรวจสอบความถูกต้องครบถ้วนหรือไม่? (Monitoring Control)

ความรู้พื้นฐานที่จำเป็นของ "ผู้ตรวจสอบภายใน"

- ความเสี่ยง (Risk) เพราะใช้ Risk-based Approach
- การควบคุม (Internal Control) เพราะ ต้องประเมินประสิทธิผลเพื่อให้ความเชื่อมั่น
- วัตถุประสงค์การควบคุม (Control Objective) เพราะ ต้องประเมินว่าการควบคุม "ได้ผล" หรือไม่ ซึ่งเป็นที่มาของการตั้งประเด็นการตรวจสอบ
- ความเสี่ยงของการควบคุม (Control Risk) เพราะ เป็นที่มาของการตั้งประเด็น

หน้าที่ของผู้ตรวจสอบ

๑) ให้ความเชื่อมั่นว่า การควบคุมที่มีอยู่ ได้ผลคือ "เรียกเก็บรายได้ ครบถ้วนและถูกต้องตามที่อัตราที่กำหนด"

๒) วิธีการทดสอบการควบคุมว่ามีขั้นตอน และวิธีการที่ทำให้เชื่อได้ว่า จัดเก็บถูกต้อง ครบถ้วน และทดสอบผลว่าที่เรียกเก็บมานั้นว่า ถูกต้องและครบถ้วน

๓) การทดสอบ คือ การพิสูจน์หลักฐาน

๔) ผู้ตรวจสอบต้องเข้าใจการควบคุม วัตถุประสงค์การควบคุม และความเสี่ยงของการควบคุม

๕) การตรวจสอบจะมีความแตกต่างกัน แล้วแต่ระบบการควบคุมของแต่ละแห่ง

Internal Control การควบคุมแตกต่างเพราะ Input – Process ต่างกัน

- **Input Control** ควบคุมด้วย -ใบรับ/หลักฐานการรับเงิน -Running คุมจำนวน -การสอบทาน Bank Statement
- **Processing Control** ควบคุมด้วยPassword Control, Daily Report และSupervisor Review
- **Output Control** ควบคุมด้วย การสอบทาน บัญชี–สำเนาใบรับ–รายงาน และการกระทบยอดกับ Stock Report (กรณีขายสินค้า)

หลักฐานที่ดีจะต้องสามารถ สะท้อนข้อเท็จจริง ที่ผู้เกี่ยวข้องยอมรับ หรือให้ข้อสรุปตรงกัน / ไม่ยุ่งยากในการรวบรวม / เป็นปัจจุบันมากที่สุด และมีปริมาณเพียงพอ ที่แสดงให้เห็นถึงปกติปฏิบัติ หลักฐานการตรวจสอบ (Audit Evidence) ประกอบด้วย หลักฐานทางกายภาพ (Physical Evidence) หลักฐานเอกสาร (Documentary Evidence) หลักฐานการวิเคราะห์(Analytical Evidence) และหลักฐานคำรับรอง (Testimonial Evidence) ซึ่งหลักฐานเหล่านั้นต้องเชื่อถือได้ (Reliable) เพียงพอ (Sufficient) มีความเกี่ยวข้อง (Relevant) และมีประโยชน์(Useful)

การควบคุมและวัตถุประสงค์การควบคุม ประกอบด้วย

ขั้นตอน	วัตถุประสงค์การควบคุม	วิธีการ/เครื่องมือในการควบคุม
รับคำขอ/คำสั่งซื้อ (Input)	ความเป็นจริงของรายการ ความครบถ้วนของรายการ	ให้เลขที่ลำดับคำขอ หลักฐาน ผู้สั่งซื้อ ควบคุมจำนวนรายการที่รับเข้า (ใช้ระบบ)
การกำหนด/คำนวณราคา	ความถูกต้องของราคาตามอัตราที่กำหนดไว้	บันทึกตารางราคาในระบบ สอบทานการบันทึก หรือ หน่วยงานกำหนดราคา

ขั้นตอน	วัตถุประสงค์การควบคุม	วิธีการ/เครื่องมือในการควบคุม
รับชำระ	ครบถ้วนและถูกต้องตามอัตราที่กำหนด	ออกใบรับ
การบันทึกรายการ	ครบถ้วน และถูกต้อง ตามที่รับมาจริง	ระบบบันทึก รายงานประจำวัน
ออกหลักฐาน	เป็นจริง ถูกต้อง ครบถ้วน	Pre-number
จัดเก็บ	ความครบถ้วน	จำกัดผู้รับผิดชอบ ตรวจนับ (กับรายงาน)

หลักการควบคุมภายใน – การตรวจสอบ

- การประเมินความเสี่ยง
- การกำหนดอำนาจ และหน้าที่
- การมอบหมายงาน คุณสมบัติผู้รับผิดชอบ
- กำหนดหลักเกณฑ์และขั้นตอน การปฏิบัติงาน
- การบันทึกข้อมูล และสื่อสาร
- การติดตามผล

ประเภทของการควบคุม Type of Control

- การควบคุมแบบป้องกัน (Preventive Control)
- การควบคุมแบบตรวจจับ (Detective Control)
- การควบคุมแบบสั่งการ (Directive Control)
- การควบคุมแบบทดแทน (Compensate Control)

การรับคำร้อง /คำสั่งซื้อ

- Control Procedure : ให้ลำดับเลข คำร้อง/PO ที่รับเข้ามาในแต่ละวัน
- Test of Control : มีผู้ทำหน้าที่ ตรวจทานว่า ได้ลำดับเลขที่หรือไม่? (Monitoring)

การกำหนดตารางราคา

- Control Procedure : การแบ่งแยกหน้าที่ (ผู้ทำ/ผู้อนุมัติ)/Password Control/ระบบบังคับออกรายงานการแก้ไข
- Test of Control : สิทธิการเข้าระบบ/รายงานการแก้ไข/การสอบทานรายงานการแก้ไขของหัวหน้างาน/หัวหน้างาน ตรวจดูข้อมูลในระบบ เป็นครั้งคราว

การรับชำระ : เป็นเงินสด

- Control Procedure : บันทึกรายการรับ/ออกใบรับ
- Test of Control : รายการที่บันทึกกับสำเนาใบเสร็จ/มีผู้สอบทานข้อมูลกับสำเนาใบเสร็จทุกสิ้นวันทำการ (Monitoring)/ออกใบเสร็จเรียงตามลำดับ/มีผู้สอบทานสำเนาว่าเรียงตามลำดับ

การรับชำระ : เข้าบัญชี

- Control Procedure : หลักฐานการเข้าบัญชี (สำเนา Pay-in)/เช็ค Pay-in กับ Statement/ประทับตรา “ผ่าน” ใน Pay-in/ออกใบเสร็จรับเงิน

การรับชำระ : รับชำระด้วยเช็ค

- Control Procedure : ขีดคร่อม ระบุชื่อองค์กร/บันทึกการรับเช็ค/สอบทาน Pay-in กับ บันทึก

วิชาที่ ๓ การตรวจสอบวงจรรายจ่าย โดย อาจารย์รินทร์ วัฒกานน์

● ภาพรวมระบบงาน

วงจรรายจ่ายประกอบด้วยกิจกรรมที่เกี่ยวข้องกับการจัดซื้อจัดหา รวมถึงการชำระเงินค่าสินค้า หรือบริการ ซึ่งถือเป็นวงจรที่สำคัญสำหรับทุกกิจการ หากการควบคุมวงจรรายจ่ายไม่มีประสิทธิภาพ อาจส่งผลให้ระบบสินค้าคงคลังล้นหรือขาด และอาจเกิดการทุจริตในการจ่ายเงินเจ้าหนี้หรือผู้ขาย

ความเสี่ยงของวงจรรายจ่าย ประกอบด้วย

- ความเสี่ยงทั่วไป เช่น ไม่มีการแยกหน้าที่ความรับผิดชอบอย่างพอเพียง ไม่มีการจัดทำระเบียบการปฏิบัติงาน และไม่มีการควบคุมการเข้าถึงข้อมูล ซึ่งอาจนำไปสู่การทุจริตหรือความผิดพลาด
- ความเสี่ยงเฉพาะ เช่น มีการทุจริตในการสั่งซื้อสินค้าหรือบริการ ซื้อสินค้าอย่างไม่เหมาะสม ตรวจรับสินค้าที่ไม่ตรงกับที่สั่งซื้อ และทุจริตในการจ่ายเงินให้แก่ผู้ขาย

● แนวทางการควบคุม ได้แก่

๑) การควบคุมทั่วไป

๑.๑) แบ่งแยกหน้าที่อย่างเหมาะสม

จุดประสงค์ : ผู้ปฏิบัติงานได้รับสิทธิเหมาะสมตามงานที่ได้รับมอบหมาย

วิธีการควบคุม : มีการแบ่งแยกหน้าที่ความรับผิดชอบระหว่างหน่วยจัดหา จัดซื้อ รับพัสดุ และบัญชี

๑.๒) การควบคุมการเข้าถึงข้อมูลหลักผู้ขาย

จุดประสงค์	วิธีการควบคุม
- การเข้าถึงกระบวนการหรือข้อมูลของวงจรรายจ่ายถูกจำกัดไว้เฉพาะผู้ที่เกี่ยวข้องที่ได้รับสิทธิ์เท่านั้น - การสร้างหรือขอเปลี่ยนแปลงข้อมูลหลักผู้ขายต้องได้รับอนุมัติและมีการนำเข้าอย่างครบถ้วน ถูกต้องและไม่ซ้ำซ้อน	- มีการกำหนดสิทธิ์ของผู้ปฏิบัติงานในระบบอย่างเหมาะสมตามอำนาจหน้าที่ - การขอสร้าง ขอลบหรือขอเปลี่ยนแปลงข้อมูลหลักผู้ขาย ต้องมีการกรอกแบบฟอร์มขอเปลี่ยนแปลงและได้รับอนุมัติอย่างครบถ้วนสมบูรณ์ - การขอเปลี่ยนแปลงข้อมูลหลักมีการบันทึก จัดเก็บและตรวจสอบความสมเหตุสมผล มีการสอบทานข้อมูลอย่างสม่ำเสมอ

๑.๓) การจัดทำระเบียบการปฏิบัติงาน

จุดประสงค์ : การจัดซื้อจัดหามีการควบคุมและเป็นมาตรฐานเดียวกัน

วิธีการควบคุม : มีการจัดทำระเบียบปฏิบัติงานเกี่ยวกับ นโยบายการจัดซื้อ ผู้มีอำนาจในการอนุมัติ วิธีคัดเลือกผู้ขาย การทำสัญญา การประเมินผู้ขาย ขั้นตอนการจัดหา ขั้นตอนการตรวจรับ

๒) การควบคุมเฉพาะ เป็นการควบคุมใน ๕ กระบวนงาน ได้แก่

๒.๑) การควบคุมการจัดซื้อจัดหา

จุดประสงค์	วิธีการควบคุม
- การขอจัดซื้อจัดหาปฏิบัติตามกฎระเบียบอย่างเคร่งครัด - การซื้อสินค้าและบริการได้รับการอนุมัติอย่างถูกต้อง	- มีการทำเอกสารอย่างเป็นทางการโดยระบุรายละเอียดอย่างครบถ้วน ชัดเจน และผ่านการอนุมัติอย่างถูกต้อง - กำหนดจุดสั่งซื้อ และแจ้งจัดซื้อเมื่อถึงจุดที่กำหนด - ตรวจสอบรายการวัสดุคงคลังก่อนแจ้งจัดหา เพื่อรักษาระดับสินค้าในคลังให้มีปริมาณที่เหมาะสม

จุดประสงค์	วิธีการควบคุม
	- ปฏิบัติตามขั้นตอนการคัดเลือกผู้ขายที่ดีที่สุดตามที่ระบุในกฎระเบียบปฏิบัติ -มีการแบ่งแยกหน้าที่ของผู้จัดหาและผู้ตรวจรับออกจากกัน - จัดทำทะเบียนประวัติผู้ขาย รวมถึงราคาและปริมาณของที่สั่งซื้อ

๒.๒) การควบคุมการสั่งซื้อ

จุดประสงค์	วิธีการควบคุม
- การสั่งซื้อได้ปฏิบัติตามกฎระเบียบอย่างเคร่งครัด - การสั่งซื้อสินค้าและบริการได้รับการอนุมัติอย่างถูกต้อง	- มีการทำเอกสารอย่างเป็นทางการโดยระบุรายละเอียดอย่างครบถ้วน ชัดเจน และผ่านการอนุมัติอย่างถูกต้อง - ใบสั่งซื้อควรมีข้อมูลครบถ้วน และมีเลขที่เรียงลำดับพิมพ์ไว้ล่วงหน้า - มีการเช็คซ้ำว่าใบสั่งซื้อได้ถูกส่งไปยังผู้ขายที่ถูกคัดเลือกไว้อย่างถูกต้อง

๒.๒) การควบคุมการรับของ

จุดประสงค์ : สินค้าหรือบริการที่รับถูกต้องครบถ้วนตรงกับที่สั่งซื้อและคุณภาพได้มาตรฐาน

วิธีการควบคุม :
- ผู้รับสินค้าตรวจนับและตรวจเช็คสินค้าเทียบกับใบส่งของและใบสั่งซื้อ
- กำหนดผู้มีอำนาจในการตรวจรับและควรลงนามผู้ตรวจรับร่วมกันอย่างน้อย ๒ คน
- จัดทำรายงานสิ่งที่ผิดปกติ เช่น สินค้าไม่ครบ เสียหาย หรือไม่ได้คุณภาพ
- ควรมีเอกสารลดหนี้จากผู้ขายเมื่อมีการคืนสินค้า

๒.๓) การควบคุมการบันทึกบัญชีเจ้าหนี้

จุดประสงค์ : มีการบันทึกบัญชีอย่างถูกต้อง ครบถ้วน และทันกาล

วิธีการควบคุม :
- มีการบันทึกบัญชีอย่างทันกาล และได้รับการอนุมัติอย่างถูกต้องหลังจากการที่ตรวจรับและตรวจเช็คเอกสารเรียบร้อยแล้ว
- เจ้าหน้าที่บัญชีตรวจเช็คความครบถ้วนถูกต้องของตัวเลขในบัญชีฝั่งเจ้าหนี้ก่อนจะทำการยืนยันในระบบ

๒.๔) การควบคุมการจ่ายเงิน

จุดประสงค์ : ชำระหนี้ไปยังผู้ขายอย่างถูกต้อง ครบถ้วน และทันกาล

วิธีการควบคุม :
- มีการตรวจสอบและอนุมัติการชำระหนี้
- ชำระหนี้ให้ทันตามกำหนดเวลาและเงื่อนไขของผู้ขาย
- ใบสำคัญที่ชำระเงินแล้วจะต้องทำเครื่องหมายเพื่อป้องกันการจ่ายซ้ำ
- เก็บเอกสารหลักฐานการทำจ่ายเพื่อเป็นหลักฐานและเพื่อการตรวจสอบ

● ภาพรวมของระบบการจัดซื้อจัดจ้าง GFMIS ระบบการจัดซื้อจัดจ้าง GFMIS เริ่มใช้จริงเมื่อวันที่ ๑ ตุลาคม ๒๕๔๗ เป็นระบบบริหารการคลังภาครัฐที่ครอบคลุมด้านรายรับ รายจ่าย การกู้เงิน เงินคงคลัง บัญชีต้นทุน บัญชีทรัพย์สินถาวร การจัดซื้อจัดจ้าง การอนุมัติ การเบิกจ่าย ฯลฯ โดยใช้ระบบปฏิบัติการ SAP R/3 ซึ่งเป็นระบบที่มีการบูรณาการและสามารถปรับปรุงข้อมูลเป็นแบบทันทีทันใด โดยการกำหนดสิทธิ์ตามหน้าที่ ซึ่งทำ

ให้งานจัดซื้อระบบ GFMIS สามารถทำการติดตามสถานะได้ทันที และเชื่อมโยงกับระบบที่เกี่ยวข้องได้ เช่น การตรวจสอบขั้นตอนการจัดทำใบขอสั่งซื้อ (PO) สามารถบันทึกบัญชีและการรับสินทรัพย์โดยอัตโนมัติ ในขั้นตอนการบันทึกรับพัสดุ และข้อมูลผู้ขายยังได้ถูกจัดเก็บเป็นข้อมูลกลางที่ส่วนราชการใช้ร่วมกันได้

● กระบวนการอัตโนมัติ Blockchain เป็นเทคโนโลยีที่ใช้ในการทำธุรกรรมโดยไม่ต้องผ่านบุคคลที่สาม (ไม่ต้องผ่านคนกลาง) และมีความปลอดภัยสูง ซึ่งข้อดีของการใช้เทคโนโลยี Blockchain คือ เป็นกระบวนการอัตโนมัติ ไม่ต้องใช้กระดาษ รวดเร็ว ปลอดภัย น่าเชื่อถือและสามารถตรวจสอบได้

● การวิเคราะห์ข้อมูล (Data Analytics) ขั้นตอนการวิเคราะห์ข้อมูล ประกอบด้วย

- การทำความเข้าใจเกี่ยวกับธุรกิจ (Business Understanding) เป็นขั้นตอนแรกที่สำคัญมาก เพราะต้องทำความเข้าใจว่าปัญหาคืออะไร ต้องการคำตอบของปัญหาในทิศทางหรือลักษณะใด หากไม่เข้าใจปัญหาอย่างถ่องแท้จะทำให้ขั้นตอนต่อไปดำเนินไปในทิศทางที่ไม่ถูกต้อง ซึ่งนอกจากจะไม่ได้คำตอบที่ต้องการแล้ว ยังสูญเสียเวลาและทรัพยากรไปโดยไร้ประโยชน์ด้วย

- การทำความเข้าใจเกี่ยวกับข้อมูล (Data Understanding) เป็นการทำความเข้าใจว่าข้อมูลที่จะนำมาใช้ควรมีลักษณะอย่างไร แหล่งข้อมูลอยู่ที่ใดและที่สำคัญที่สุดคือค่าใช้จ่ายหรือต้นทุน (Costs of Data) ที่จะได้มาซึ่งข้อมูลเหล่านั้นมีค่าใช้จ่ายเท่าไร รวมทั้งควรต้องประเมินมูลค่าของประโยชน์ที่จะได้รับจากการนำเอาข้อมูลดังกล่าวมาใช้

- การเตรียมข้อมูล (Data Preparation) โดยปกติระบบประมวลผลข้อมูล นำเข้าข้อมูล จะอยู่ในรูปแบบที่จำกัด (Fixed Known Format) แต่ในความเป็นจริงข้อมูลส่วนใหญ่ ไม่ได้จัดเก็บในลักษณะดังกล่าวจึงต้องการกระบวนการแปลงข้อมูล (Data Transformation) หรือเปลี่ยนชนิดข้อมูล (Data Conversion) เพื่อให้ข้อมูลอยู่ในลักษณะหรือรูปแบบที่ง่ายต่อการนำไปประมวลผลหรือวิเคราะห์ต่อไป

- การสร้างแบบจำลอง (Modeling) คือ การสร้างรูปแบบความสัมพันธ์ (Relational Pattern) อาจจะอยู่ในรูปของแบบจำลองบนซอฟต์แวร์ (Computer Model) หรือสมการความสัมพันธ์ (Equation) ก็ได้

- การประเมินผล (Evaluation) หลังจากที่ได้แบบจำลองแล้ว ต้องทำการประเมินผลว่าแบบจำลองนั้นมีความถูกต้องแม่นยำมากน้อยเพียงใด โดยอาจทดลองในระบบเสมือน (Simulation) หรือนำไปประมวลผลกับข้อมูลจริงที่มีอยู่เพื่อเปรียบเทียบผล ของการวิเคราะห์ว่าถูกต้องเป็นร้อยละเท่าใด

- การนำไปใช้งาน (Deployment) หลังจากที่ได้แบบจำลองที่มีคุณภาพและความถูกต้องแม่นยำตามที่เราต้องการก็สามารถนำไปใช้งานจริง โดยอาจต้องมีการปรับแต่งเพื่อความเหมาะสมในสภาวะจริง อีกทั้งยังต้องติดตั้งร่วมกับระบบอื่นๆ เช่น ระบบช่วยการตัดสินใจ (Decision Support System) อย่างไรก็ตามหลังจากการติดตั้งแล้วควรมีการปรับปรุงแบบจำลองเป็นระยะๆ (Periodic Update) เพราะแท้จริงแล้วการทำเหมืองข้อมูลไม่มีที่สิ้นสุด

ข้อดีของการใช้การข้อมูล (Data Analytics) ในการตรวจสอบ คือ สามารถเพิ่มขอบเขตในการตรวจสอบ ไม่ต้องใช้กระดาษ รวดเร็วปลอดภัย น่าเชื่อถือและสามารถตรวจสอบได้ ได้ข้อเสนอแนะใหม่ๆที่มีประโยชน์ครบถ้วน ถูกต้องและตรงประเด็น ที่สำคัญ คือสามารถเพิ่มความถี่ในการตรวจสอบได้

● การตรวจสอบทุจริต กระบวนการคัดเลือกผู้ขาย

- กรณีผู้ขายปลอม : ผู้ขายมีเบอร์โทร และ/หรือที่อยู่ตรงกัน ผู้ขายมีชื่อกรรมการคนเดียวกัน ผู้ขายมีที่อยู่เป็นตู้ ปณ.
- กรณีคิดราคาเกินจริง : ตรวจสอบราคามาตรฐาน ตรวจสอบคุณภาพของงาน
- กรณีมีผลประโยชน์ร่วมกัน : ผู้ขายและพนักงานมีเบอร์โทร และ/หรือที่อยู่ตรงกัน มีชื่อพนักงานเป็นกรรมการบริษัทของผู้ขาย

วิชาที่ ๔ ระบบปฏิบัติการ (Information System Operation) โดย อาจารย์ภิธันปต์ ถิรสัตยาพิทักษ์

ปัจจุบันระบบสารสนเทศส่วนใหญ่ขององค์กรทำการติดต่อกับภายนอกด้วยระบบออนไลน์บนเครือข่ายอินเทอร์เน็ต ทำให้สารสนเทศขององค์กรเกิดความไม่มั่งคนปลอดภัย มีความเสี่ยงต่อการถูกคุกคาม บุกรุกและโจมตีจากแฮกเกอร์และไวรัสคอมพิวเตอร์

ดังนั้น องค์กรควรมีมาตรการป้องกันความเสี่ยงต่อการเกิดความไม่มั่นคงปลอดภัยกับสารสนเทศที่เป็นมาตรฐานสากลเพื่อจัดการควบคุมสารสนเทศขององค์กรให้มีความมั่นคงปลอดภัยโดยการกำหนดเป็นแนวนโยบายและแนวปฏิบัติสำหรับใช้รักษาความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร ซึ่งเป็นกระบวนการรวบรวมข้อควรปฏิบัติสำหรับบุคลากรที่ปฏิบัติงานร่วมกับระบบเทคโนโลยีสารสนเทศ เพื่อเป็นนโยบายที่จะทำให้บุคลากรและบุคคลภายนอกที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศขององค์กรได้ตระหนักถึงความสำคัญ และรับทราบถึงบทบาทหน้าที่ ความรับผิดชอบของตนเองต่อการรักษาความมั่นคงปลอดภัยสารสนเทศ และปฏิบัติตามมาตรการควบคุมความเสี่ยงที่ได้กำหนดขึ้น

แนวทางปฏิบัติการจัดทำแนวนโยบายแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ คือ

๑) ต้องจัดทำแนวนโยบายแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศที่เป็นลายลักษณ์อักษรโดยผู้บริหารองค์กร ผู้ที่เกี่ยวข้องจากฝ่ายเทคโนโลยีสารสนเทศ และจากทุกฝ่ายงานต้องมีส่วนร่วมในการจัดทำแนวนโยบายฯ

๒) ต้องได้รับอนุมัติจากคณะกรรมการบริหารหรือผู้บริหารระดับสูงขององค์กร

๓) ต้องทบทวนและปรับปรุงแนวนโยบายฯ ให้เป็นปัจจุบันอยู่เสมอ โดยต้องมีการประเมินความเสี่ยงอย่างน้อยปีละครั้ง ซึ่งต้องมีการระบุความเสี่ยงที่เกี่ยวข้อง การจัดลำดับความสำคัญของข้อมูลและระบบคอมพิวเตอร์ การกำหนดระดับความเสี่ยงที่ยอมรับได้ และการกำหนดมาตรการหรือวิธีปฏิบัติในการควบคุมความเสี่ยง

๔) ต้องจัดเก็บแนวนโยบายฯ ที่เป็นลายลักษณ์อักษร ไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้องสามารถเข้าถึงได้โดยง่าย

๕) จัดให้มีการเผยแพร่แนวนโยบายฯ ให้กับบุคลากรภายใน ผู้ให้บริการภายนอก และผู้ที่เกี่ยวข้องรับทราบและนำไปปฏิบัติโดยเคร่งครัด

วัตถุประสงค์เพื่อให้มีการกำหนดกรอบการบริหารจัดการการปฏิบัติงานและการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศภายในองค์กร

๑) การกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

๒) การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties)

➢ การสร้างความมั่นคงปลอดภัยให้กับองค์กรในระดับบุคลากร เป็นการกำหนดมาตรการเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดของบุคลากร โดยมีหลักการ ดังนี้

- ขั้นตอนของการว่าจ้างต้องมีการกำหนดบทบาทหน้าที่ความรับผิดชอบทางด้านความปลอดภัยไว้ในสัญญาอย่างชัดเจน และติดตามผลการปฏิบัติงานเป็นรายบุคคล
- กำหนดข้อตกลงการรักษาความลับขององค์กรโดยห้ามมิให้นำข้อมูลขององค์กรไปเผยแพร่ให้แก่บุคคลอื่น ซึ่งข้อตกลงดังกล่าวจะต้องสอดคล้องกันกับสัญญาการว่าจ้าง
- อบรมให้พนักงานทราบและตระหนักถึงความสำคัญของการรักษาความปลอดภัยสารสนเทศ เพื่อเป็นแนวทางในการปฏิบัติงานที่สนับสนุนนโยบายความปลอดภัยขององค์กร
- รายงานผลกรณีที่เกิดเหตุการณ์ต่างๆ อันส่งผลกระทบต่อความปลอดภัยขององค์กร ให้แก่ผู้บริหารได้รับทราบโดยด่วน เพื่อพิจารณาหาแนวทางแก้ไข

➢ การกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศ

- องค์กรต้องกำหนดสิทธิ์ในการเข้าถึงระบบสารสนเทศต่างๆขององค์กรโดยกำหนดสิทธิ์ให้ตามบทบาทหน้าที่ความรับผิดชอบ เช่น การเข้าใช้งานระบบอินเทอร์เน็ตขององค์กร การเข้าใช้ระบบงานต่างๆ (Applications) ขององค์กร

- ผู้ที่ประสงค์ขอเข้าใช้งานระบบสารสนเทศต่างๆ ขององค์กรจะต้องดำเนินการขออนุญาตเพื่อเข้าใช้งานตามขั้นตอนที่องค์กรกำหนดไว้

- รายชื่อสำหรับเข้าใช้ระบบงานฯ (User Login) และรหัสผ่าน (Password) ถือว่าเป็นทรัพย์สินสำคัญขององค์กรที่ผู้ถือครองจะต้องเก็บรักษาเป็นอย่างดี และต้องปกปิดเป็นความลับ

➢ จัดทำทะเบียนบัญชีรายชื่อผู้มีสิทธิ์ใช้งานระบบสารสนเทศ

- หน่วยงานที่มีหน้าที่ควบคุมการใช้งานระบบสารสนเทศและเจ้าของระบบงานต่างๆ จะต้องจัดทำทะเบียนบัญชีรายชื่อผู้มีสิทธิ์เข้าใช้งานระบบสารสนเทศขององค์กร เพื่อเป็นหลักฐานในการตรวจสอบว่ามีผู้ละเมิดเข้าใช้งานระบบสารสนเทศขององค์กรโดยไม่ได้รับอนุญาตหรือเข้าใช้งานมากกว่าสิทธิ์ที่ได้รับอนุญาตหรือไม่

- ผู้ที่มีส่วนเกี่ยวข้องในการจัดทำทะเบียนบัญชีรายชื่อผู้มีสิทธิ์เข้าใช้งานระบบสารสนเทศจะต้องทำการทบทวนรายชื่อให้เป็นปัจจุบันอย่างน้อยปีละ ๒ ครั้ง

- ผู้ที่ดูแลระบบงาน IT จะต้องทำการถอดถอนสิทธิ์ในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้

➢ กระบวนการตรวจสอบระบบเทคโนโลยีสารสนเทศ (Steps of IT Audit)

๑) การกำหนดขอบเขตงานตรวจสอบระบบเทคโนโลยีสารสนเทศ คือ การระบุเรื่องการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยขอบเขตงานตรวจสอบอาจเป็นได้ทั้งระบบงานกระบวนการ หรือการปฏิบัติตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒) การวางแผนงานตรวจสอบระบบเทคโนโลยีสารสนเทศ คือ การวางแผนงานตรวจสอบของหน่วยงาน โดยมีรายละเอียดประกอบด้วย

- การวางแผนในรายละเอียดของโครงการตรวจสอบเทคโนโลยีสารสนเทศ เพื่อนำไปจัดทำและนำเสนอรายละเอียดแผนงาน
- การชี้แจงและทำความเข้าใจในเบื้องต้นภายในทีมงานตรวจสอบ โดยจัดประชุมชี้แจงยืนยันบทบาทหน้าที่ของสมาชิกในทีมตรวจสอบ

๓) การปฏิบัติงานตรวจสอบระบบเทคโนโลยีสารสนเทศ มีรายละเอียดการปฏิบัติงาน ดังนี้

- ทำการประเมินความเสี่ยงและการควบคุมที่เกี่ยวข้องกับการดำเนินงานด้วยเทคโนโลยีสารสนเทศ
- การประเมินประสิทธิผลของมาตรการควบคุม

๔) การสรุปผลงานตรวจสอบระบบเทคโนโลยีสารสนเทศ มีขั้นตอนดังนี้

- ปรึกษาหารือและยืนยันความเข้าใจสำหรับประเด็นที่ตรวจพบกับหน่วยรับตรวจ
- จัดทำรายงานผลการตรวจสอบฉบับสมบูรณ์นำเสนอผู้บริหารองค์กร
- จัดเตรียมเอกสารการประชุมและนำเสนอรายงานผลการตรวจสอบต่อผู้บริหารหรือผู้บริหารระดับสูงขององค์กร
- จัดทำหนังสือแจ้งผลการตรวจสอบให้หน่วยรับตรวจรับทราบ เพื่อดำเนินการปรับปรุงแก้ไขตามประเด็นที่ตรวจพบ

๕) การติดตามและประเมินผล

- การติดตามและประเมินผล เป็นองค์ประกอบหนึ่งของกรอบงานการควบคุม เพื่อให้มั่นใจในการนำการควบคุมไปใช้ให้เกิดประสิทธิภาพ ประสิทธิผล และมีการปรับปรุงให้ทันสมัยอยู่เสมอ ซึ่งผู้ที่มีหน้าที่รับผิดชอบจะทำการติดตามผลระหว่างการปฏิบัติงาน

- การติดตามประเมินผลการควบคุมด้าน IT เป็นกระบวนการที่ต้องจัดทำอย่างต่อเนื่อง เพื่อให้ทันต่อการเปลี่ยนแปลงของสภาพแวดล้อมและปัจจัยภายนอกที่เกิดขึ้นตลอดเวลา

➢ Business Continuity Management : BCM คือ องค์รวมของกระบวนการบริหารซึ่งชี้บ่งภัยคุกคามต่อองค์กร และผลกระทบของภัยคุกคามนั้นต่อการดำเนินธุรกิจ และให้แนวทางในการสร้างขีดความสามารถให้องค์กรมีความยืดหยุ่น เพื่อการตอบสนองและปกป้องผลประโยชน์ของผู้มีส่วนได้ส่วนเสีย ชื่อเสียงภาพลักษณ์ และกิจกรรมที่สร้างมูลค่าที่มีประสิทธิผล

➢ แผนสำรองฉุกเฉิน (Contingency Plan) แผนในภาพรวมในการรับมือกับเหตุการณ์ ฉุกเฉินที่เกิดขึ้นนอกเหนือจากความคาดหมาย มีรายละเอียดเกี่ยวกับ การตรวจสอบ การตอบสนอง การกอบกู้ระบบงาน แนวทางในการรับมือเหตุการณ์ที่สร้างความเสี่ยงให้กับระบบและสินทรัพย์ต่างๆ และทำให้กลับสู่ภาวะปกติโดยมีการสูญเสียน้อยที่สุด

➢ องค์ประกอบของแผนสำรองฉุกเฉิน

- แผนรับมือเหตุฉุกเฉิน (Incident Response Plan)
- แผนรับมือภัยพิบัติ (Disaster Recovery Plan)
- แผนการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan)

➢ การกำหนดหลักเกณฑ์การบริหารความต่อเนื่องทางธุรกิจ ต้องมีความเหมาะสม น่าเชื่อถือ มีประสิทธิภาพ เกิดประโยชน์ที่ดีที่สุดแก่ลูกค้า และผู้ใช้บริการ บุคลากรขององค์กรสามารถปฏิบัติงานได้ถูกต้องตรงตามหน้าที่ ต้องไม่ก่อให้เกิดความเสี่ยงที่จะทำให้องค์กรฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย กฎเกณฑ์ และมาตรฐานการประกอบธุรกิจที่เกี่ยวข้อง

➢ แผนความต่อเนื่องของธุรกิจ (Business Continuity Plan : BCP) เป็นแผนที่องค์กรต้องจัดทำขึ้นเพื่อให้องค์กรสามารถดำเนินภารกิจไปได้อย่างต่อเนื่องแม้ว่าจะเกิดเหตุการณ์ใดๆ ที่ส่งผลกระทบให้การดำเนินภารกิจหลักขององค์กรต้องหยุดชะงักลงก็ตาม เป็นการสร้างแผนเพื่อลดความเสี่ยงต่อเหตุการณ์ที่ไม่คาดคิด ซึ่งประกอบด้วยการดำเนินการด้วยมือ (Manual) หรืออัตโนมัติ (Automation) เพื่อให้มั่นใจว่าระบบงานที่สำคัญขององค์กรสามารถทำงานได้อย่างต่อเนื่อง

➢ แผนกู้คืนระบบสารสนเทศหลังเหตุการณ์ความเสียหาย (Disaster Recovery Plan : DRP) เป็นการสร้างแผนเพื่อดำเนิน การกู้คืนกระบวนการทำงานของเทคโนโลยีสารสนเทศ(IT) ให้สามารถทำงานได้ตามปกติหลังจากเกิดเหตุการณ์ความเสียหายขึ้น

วิชาที่ ๕ การพัฒนาและดูแลระบบสารสนเทศ โดย อาจารย์ภิธันปต์ ถิรสัตยาพิทักษ์

แนวคิดการพัฒนาระบบงานสารสนเทศ (Information System Development Concepts) การพัฒนาระบบงานสารสนเทศในองค์กรมักจะเริ่มต้นจากการศึกษาและหาความต้องการของเจ้าของระบบงาน หรือผู้ใช้ระบบ โดยผู้ที่พัฒนาระบบงาน จะต้องเก็บรวบรวมข้อมูลความต้องการต่างๆ เพื่อนำมาวิเคราะห์ออกแบบเป็นระบบงาน ดังนั้นหากผู้พัฒนาระบบสามารถรวบรวมข้อมูลความต้องการได้อย่างถูกต้องสมบูรณ์ครบถ้วนให้ได้มากที่สุดเท่าที่จะทำได้ก็จะส่งผลให้ระบบงานที่จะพัฒนาถูกต้องสมบูรณ์ตรงกับความต้องการของเจ้าของระบบงาน

เหตุผลสำคัญที่นำไปสู่การพัฒนาระบบใหม่ เพื่อปรับปรุงบริการแก่ผู้ใช้บริการ เพิ่มประสิทธิภาพการทำงาน เพิ่มกระบวนการควบคุมการทำงาน ลดต้นทุนการดำเนินการ และต้องการสารสนเทศที่มากขึ้นเพื่อเพียงพอต่อการตัดสินใจ

แนวทางการพัฒนาระบบสารสนเทศมีหลายวิธี อาจจะจัดทำขึ้นเองโดยอาศัยบุคลากรฝ่ายคอมพิวเตอร์ขององค์กร การว่าจ้างบริษัทที่รับพัฒนาระบบงานจากภายนอก (Outsourcing) ทำการพัฒนาระบบร่วมกับบุคลากรฝ่ายคอมพิวเตอร์ขององค์กร การว่าจ้างบริษัทที่รับพัฒนาระบบงานจากภายนอก (Outsourcing) ทำการพัฒนาให้ทั้งหมด หรือการจัดหาซอฟต์แวร์สำเร็จรูป

วงจรการพัฒนาระบบ (System Development Life Cycle : SDLC) ประกอบด้วย

ขั้นตอนที่ ๑. การวางแผนโครงการ (Project Planning Phase) ประกอบด้วยการกำหนดปัญหา การศึกษาความเป็นไปได้ การยื่นข้อเสนอรายงานเสนอผู้บริหารเพื่อยืนยันโครงการ และการวางแผนและควบคุมกิจกรรม และการบริหารโครงการ

ขั้นตอนที่ ๒. การวิเคราะห์ (Analysis Phase) ประกอบด้วยการศึกษาระบบงานเดิม การรวบรวมวิเคราะห์ความต้องการ การสร้างแบบจำลองกระบวนการ และการสร้างแบบจำลองข้อมูล

ขั้นตอนที่ ๓. การออกแบบ (Design Phase) ประกอบด้วยการออกแบบรายงาน การออกแบบหน้าจอโต้ตอบกับผู้ใช้ การออกแบบฝังงานระบบ รายละเอียดโปรแกรม ฐานข้อมูล และไฟล์ข้อมูลที่เกี่ยวข้อง

ขั้นตอนที่ ๔. การดำเนินงาน (Implementation Phase) เป็นขั้นตอนที่จะทำให้ระบบเกิดผลด้วยการสร้างระบบขึ้นมา ซึ่งเกี่ยวข้องกับกิจกรรมต่างๆ ดังต่อไปนี้

- การเขียนโปรแกรม (Coding) การเขียนโปรแกรม เป็นการสร้างระบบขึ้นมาใช้งาน โดยผู้รับผิดชอบคือโปรแกรมเมอร์ ด้วยการเขียนโปรแกรมให้เป็นไปตามมาตรฐานที่นักวิเคราะห์ระบบได้กำหนดไว้ มีขั้นตอนการเขียนโปรแกรม คือ ศึกษาจากเอกสารต่างๆ ออกแบบโปรแกรม เขียนโปรแกรม ทดสอบโปรแกรม และจัดทำเอกสารประกอบโปรแกรม
- การทดสอบ (Testing) เป็นขั้นตอนของการทดสอบระบบก่อนที่จะนำไปใช้งานจริง โดยนำเอาระบบหรือโปรแกรมที่สร้างมาทดสอบกับข้อมูลเบื้องต้นเสียก่อน การตรวจสอบระบบทั้ง 2 ประเภทตรวจสอบ Syntax ตรวจสอบ Objective มีขั้นตอนการทดสอบ คือ การทดสอบหน่วยย่อย (Unit Testing) การทดสอบด้วยการนำโปรแกรมมาประกอบรวมกัน (Integration Testing) การทดสอบทั้งระบบ (System Testing) การทดสอบการยอมรับในระบบ (Acceptance Testing)
- การติดตั้ง (Installation) การติดตั้งเพื่อใช้งานใหม่ทันที (Direct Installation) การติดตั้งแบบคู่ขนาน (Parallel Installation) การติดตั้งระบบแบบเป็นระยะ (Phased Installation)
- การจัดทำเอกสารคู่มือใช้งาน (Documentation)
- การฝึกอบรม (Training)
- การประเมินผลระบบ (System Evaluation)

ขั้นตอนที่ ๕ การบำรุงรักษา (Maintenance) ระบบที่ถูกพัฒนาขึ้นมาใช้งานทุกระบบ จะต้องมีรอบระยะของการบำรุงรักษา ไม่ว่าจะเป็นการปรับปรุงแก้ไขข้อผิดพลาดที่เกิดจากการทำงานของระบบ หรือจากความต้องการขอผู้ใช้ที่เปลี่ยนแปลงไป การบำรุงรักษาระบบสามารถทำได้โดย การบำรุงรักษาด้วยการแก้ไขให้ถูกต้อง (Corrective Maintenance) การบำรุงรักษาด้วยการปรับระบบให้สามารถรองรับสภาพแวดล้อมใหม่ที่เปลี่ยนแปลงไป(Adaptive Maintenance) การบำรุงรักษาด้วยการปรับปรุงให้ระบบมีประสิทธิภาพดียิ่งขึ้น (Perfective Maintenance) และ การบำรุงรักษาด้วยการป้องกัน (Preventive Maintenance)

วิชาที่ ๖ การรักษาความปลอดภัยของระบบสารสนเทศ โดย อาจารย์ภิธันปต์ ถิรสัตยาพิทักษ์

ช่องทางการโจรกรรมทรัพย์สินในยุค ๔.๐ ไม่จำเป็นต้องบุกรุกเข้ามาโจรกรรมทรัพย์สินในอาคารสถานที่อีกต่อไป แต่เป็นการบุกรุกคุกคามเพื่อโจรกรรมทรัพย์สินทางช่องทาง Cyber

ข้อมูลที่สำคัญระดับบุคคล ได้แก่ ข้อมูลและไฟล์ที่เป็นส่วนตัว ข้อมูลบัตรประจำตัวประชาชน ข้อมูลเลขบัญชีธนาคาร User, Password สำหรับเข้าสู่ระบบที่สำคัญๆ รูปบุคคล และเสียง

ข้อมูลสำคัญระดับองค์กร ได้แก่ ข้อมูลลูกค้า ข้อมูลที่เกี่ยวข้องกับบริการและสินค้าขององค์กร ข้อมูลทางการเงินและบัญชี ข้อมูลสูตรทางการผลิต ข้อมูลกระบวนการทางธุรกิจ User, Password สำหรับเข้าสู่ระบบที่สำคัญๆขององค์กร

องค์กรจะต้องมีมาตรการป้องกันความเสี่ยงที่เป็นมาตรฐานสากลมาประยุกต์ใช้เพื่อจัดการความมั่นคงปลอดภัยสารสนเทศโดยการกำหนดเป็นแนวนโยบายแนวปฏิบัติในการการรักษาความมั่นคงปลอดภัยสารสนเทศและให้ยึดถือปฏิบัติโดยเคร่งครัดทั่วทั้งองค์กร

องค์ประกอบหลักของการรักษาความปลอดภัย ประกอบด้วย ๓ ประการด้วยกัน ซึ่งนิยมใช้ตัวย่อว่า C-I-A มาจากคำว่า Confidentiality (การรักษาความลับของสารสนเทศ) Integrity (การรักษาความคงสภาพเดิมของสารสนเทศ) และ Availability (การรักษาความพร้อมใช้งานของสารสนเทศ)

- การรักษาความลับของสารสนเทศ C : เป็นการปกป้องรักษาสารสนเทศขององค์กรไว้เป็นความลับเพื่อให้มั่นใจว่าสารสนเทศขององค์กร สามารถล่วงรู้ เข้าถึง และใช้งานได้เฉพาะผู้ที่ได้รับอนุญาต และมีสิทธิ์ตามที่องค์กรกำหนดไว้เท่านั้น
- การรักษาความคงสภาพเดิมของสารสนเทศ I : เป็นการปกป้องรักษาสารสนเทศขององค์กรเพื่อให้มั่นใจว่าข้อมูลมีความถูกต้อง และสมบูรณ์ครบถ้วน ไม่ถูกแก้ไข เปลี่ยนแปลงนับตั้งแต่สารสนเทศถูกสร้างขึ้นหรือถูกทำลายจากผู้ที่ไม่มีสิทธิ์ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม
- การรักษาความพร้อมใช้งานของสารสนเทศ A : เป็นการปกป้องรักษาสารสนเทศขององค์กรเพื่อให้มั่นใจว่าสารสนเทศมีความพร้อมที่จะให้ผู้ที่มีสิทธิ์เข้าถึงสารสนเทศสามารถเข้าถึงและใช้งานสารสนเทศได้ทุกเมื่อที่ต้องการ

ประเภทความไม่มั่นคงปลอดภัยด้าน IT มี ๔ ประเภท คือ

๑) ความไม่ปลอดภัยจากเทคโนโลยี เป็นความไม่ปลอดภัยที่เกิดขึ้นจากระบบเทคโนโลยีที่มีความสลับซับซ้อนมากขึ้น มีการทำงานที่เป็นอัตโนมัติมากยิ่งขึ้น ซึ่งหากขาดการควบคุม ติดตามตรวจสอบที่ดีพอก็จะทำให้ระบบคอมพิวเตอร์และอุปกรณ์ดิจิทัลต่างๆ อาจถูกคุกคามและโจมตีจาก Hacker หรือโปรแกรมไม่ประสงค์ดี (Malware)

๒) ความไม่ปลอดภัยจากบุคคลและผู้ปฏิบัติงาน เป็นความไม่ปลอดภัยที่เกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศหรือใช้ข้อมูลต่างๆขององค์กรเกกว่าอำนาจหน้าที่ที่มีอยู่เนื่องจากการกำหนดบทบาทหน้าที่ความรับผิดชอบที่ไม่ชัดเจน ซึ่งอาจทำให้เกิดความเสียหายต่อสารสนเทศหรือต่อการดำเนินงานขององค์กรได้

๓) ความไม่ปลอดภัยจากกระบวนการและการบริหารจัดการ เป็นความไม่ปลอดภัยที่ส่งผลกระทบต่อการดำเนินงานด้านสารสนเทศจากแนวนโยบายแนวปฏิบัติในการบริหารจัดการที่ไม่ได้ถูกจัดทำ หรือถูกปรับปรุงให้เหมาะสมสอดคล้องกับสภาวะแวดล้อมที่ถูกเปลี่ยนแปลงไปขององค์กร ตลอดทั้งการประกาศและการบังคับใช้อย่างจริงจัง

๔) ความไม่ปลอดภัยจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความไม่ปลอดภัยที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม แผ่นดินไหว โรคระบาด ไฟไหม้ อาคารถล่มการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

ความจำเป็นของการรักษาความมั่นคงปลอดภัยด้านไอที (IT Security issues and Trends)

- การพิสูจน์ตัวตน (Authentication) เพื่อให้มั่นใจว่าทั้งผู้รับและผู้ส่งเป็นตัวจริง
- การเข้ารหัสลับ (Cryptography) เพื่อปกป้องการรักษาความลับของข้อมูล (Confidential) ไม่ให้ถูกเปิดเผยออกไป
- การให้สิทธิ (Authorization) เพื่อที่จะรับประกันว่าผู้ใช้ทุกฝ่ายมีสิทธิทำธุรกรรมได้
- การตรวจสอบความถูกต้อง (Integrity) เพื่อที่จะรับประกันได้ว่า การทำธุรกรรมไม่ได้ถูกเปลี่ยนแปลง หรือทำให้เสียหาย
- การไม่ปฏิเสธความรับผิดชอบ (Non-repudiation) เพื่อที่จะจัดให้มีหลักฐาน

การควบคุมความปลอดภัย

- การควบคุมทางด้านกายภาพ (Physical Control) - บัตรเข้าออก - การควบคุมประตูปิดเปิด - การจำกัดพื้นที่ในการเข้าใช้ - เจ้าหน้าที่ รปภ. - คล้องด้วยโซ่และใส่กุญแจ - ระบบโทรทัศน์วงจรปิด (CCTV)
- การควบคุมทางด้านตรรกะ (Logical Control) - การเข้ารหัส - อุปกรณ์ไฟร์วอลล์ - อุปกรณ์ IDS/IPS - โปรแกรมป้องกันไวรัส - การควบคุมรหัสผ่าน - ระบบตรวจสอบข้อมูลจำเพาะบุคคล - การบันทึก Log
- การควบคุมทางด้านการบริหารจัดการ (Administration control)

- นโยบายและขั้นตอนปฏิบัติ ด้านการรักษาความปลอดภัยสารสนเทศ - การบริหารความเสี่ยง - การอบรมความตระหนักด้านความปลอดภัย – การแบ่งแยกหน้าที่การทำงานให้ชัดเจน –การทบทวนงานด้านความปลอดภัย และการตรวจสอบ-ระบบการแจ้งเตือน (Information Security Incident Management, Problem Management)

การติดตามและประเมินผลการควบคุมความไม่ปลอดภัย

การติดตามและประเมินผล เป็นองค์ประกอบหนึ่งของกรอบงานการควบคุม เพื่อให้มั่นใจในการนำการควบคุมไปใช้ให้เกิดประสิทธิภาพประสิทธิผล และมีการปรับปรุงให้ทันสมัยอยู่เสมอ ซึ่งผู้บริหารมีหน้าที่รับผิดชอบในการติดตามผลระหว่างการปฏิบัติงาน ในขณะที่ผู้ตรวจสอบมีหน้าที่ในการประเมินผลเป็นครั้งคราว การติดตามประเมินผลการควบคุมด้าน IT เป็นกระบวนการที่ต้องจัดทำอย่างต่อเนื่อง เพื่อให้ทันต่อการเปลี่ยนแปลงของสภาพแวดล้อมและปัจจัยภายนอกที่เกิดขึ้นตลอดเวลา

แนวคิดการบริหารจัดการ การรักษาความมั่นคงปลอดภัยสารสนเทศในองค์กรให้เกิดความยั่งยืน

- การจัดทำแนวนโยบาย แนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศและควรทำการปรับปรุงทุกๆ ปี
- จัดหามาตรการควบคุมบริหารจัดการความเสี่ยงที่มีประสิทธิผลและมีการสำรวจความเสี่ยงอย่างสม่ำเสมอ
- สร้างความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศให้เกิดขึ้นกับบุคลากรทั่วทั้งองค์กร

วิชาที่ ๗ ระบบจัดการฐานข้อมูล โดย อาจารย์ภิธันปต์ ถิรสัตยาพิทักษ์

ฐานข้อมูล (Database) คือ การเก็บรวบรวมข้อมูลอย่างเป็นระบบ รวมถึงความสามารถที่จะนำข้อมูลนั้นออกมาใช้ร่วมกันได้โดยไม่มีการซ้ำซ้อนของข้อมูล

นิยามและคำศัพท์พื้นฐานเกี่ยวกับฐานข้อมูล

- บิท (Bit) หมายถึง หน่วยของข้อมูลที่มีขนาดเล็กที่สุดประกอบด้วยเลข 0,1 เป็นเลขฐาน 2
- ไบท์ (Byte) หมายถึง หน่วยของข้อมูลที่เกิดจากการนำบิทมารวมกันเป็นตัวอักษร (Character) หรือ 8 bit รวมกัน เป็น 1 byte
- เขตข้อมูล (Field) หมายถึง หน่วยของข้อมูลที่ประกอบขึ้นจากตัวอักขระตั้งแต่หนึ่งตัวขึ้นไปมารวมกันแล้วได้ความหมายของสิ่งใดสิ่งหนึ่ง เช่น ชื่อ ที่อยู่ เป็นต้น
- ระเบียน (Record) หมายถึง หน่วยของข้อมูลที่เกิดจากการนเอาเขตข้อมูลหลาย ๆ เขตข้อมูลมารวมกัน เพื่อเกิดเป็นข้อมูลเรื่องใดเรื่องหนึ่ง เช่น ข้อมูลของนักศึกษา 1 ระเบียน (1 คน) จะประกอบด้วย รหัสประจำตัวนักศึกษา ชื่อนักศึกษา และที่อยู่เป็นต้น
- แฟ้มข้อมูล (File) หมายถึงหน่วยของข้อมูลที่เกิดจากการนำข้อมูลหลาย ๆ ระเบียนที่เป็นเรื่องเดียวกันมารวมกัน เช่น แฟ้มข้อมูลนักศึกษา แฟ้มข้อมูลลูกค้า แฟ้มข้อมูลพนักงาน
- ฐานข้อมูล (Database) หมายถึง การเอาหลายๆ File หรือ Table มารวมกัน

ปัญหาระบบฐานข้อมูลแบบเก่า

ปัญหาระบบฐานข้อมูลแบบเก่า อาจเกิดจากข้อมูลซ้ำซ้อน ความผูกพันระหว่างโปรแกรมกับข้อมูล ขาดความคล่องตัว ขาดระบบรักษาความปลอดภัย การไม่สามารถใช้ข้อมูลร่วมกันและความพร้อมใช้งาน

ระบบจัดการฐานข้อมูล หมายถึงซอฟต์แวร์ที่ช่วยในการจัดเก็บข้อมูลไว้ในที่ที่กำหนดไว้ ทั้งนี้เพื่อช่วยให้การบริหารจัดการข้อมูลเหล่านั้นเป็นไปอย่างมีประสิทธิภาพ และสามารถช่วยอำนวยความสะดวกให้แก่โปรแกรมประยุกต์ (Application Program) ในการเข้าถึงฐานข้อมูล ที่ได้จัดเก็บไว้ ระบบการจัดการฐานข้อมูล ประกอบด้วย แอพพลิเคชันฐานข้อมูล ระบบจัดการฐานข้อมูล ดาด้าเบสเซิร์ฟเวอร์ ข้อมูล และ ผู้บริหารฐานข้อมูล

การออกแบบฐานข้อมูล มีความสำคัญต่อการจัดการระบบฐานข้อมูล (DBMS) ทั้งนี้เนื่องจากข้อมูลที่อยู่ภายในฐานข้อมูลจะต้องศึกษาถึงความสัมพันธ์ของข้อมูล โครงสร้างของข้อมูลการเข้าถึงข้อมูลและกระบวนการที่โปรแกรมประยุกต์จะเรียกใช้ฐานข้อมูล ดังนั้น เราจึงสามารถแบ่งวิธีการสร้างฐานข้อมูลได้ ๓ ประเภท คือ

๑. รูปแบบข้อมูลแบบลำดับขั้น หรือโครงสร้างแบบลำดับขั้น (Hierarchical data model) เป็นวิธีการสร้างฐานข้อมูล ที่ได้รับความนิยมมาก ในการพัฒนาฐานข้อมูลบนเครื่องคอมพิวเตอร์ขนาดใหญ่และขนาดกลาง โดยที่โครงสร้างข้อมูลจะสร้างรูปแบบเหมือนต้นไม้โดยความสัมพันธ์เป็นแบบหนึ่งต่อหลาย (One-to-Many)

๒. รูปแบบข้อมูลแบบเครือข่าย (Network data Model)เป็นฐานข้อมูลแบบเครือข่ายมีความคล้ายคลึงกับฐาน ข้อมูลแบบลำดับขั้น ต่างกันที่โครงสร้างแบบเครือข่าย อาจจะมีการติดต่อหลายต่อหนึ่ง(Many-to-one) หรือ หลายต่อหลาย (Many-to-many) กล่าวคือลูก (Child) อาจมีพ่อแม่ (Parent) มากกว่าหนึ่ง สำหรับตัวอย่างฐานข้อมูลแบบเครือข่ายให้ลองพิจารณาการจัดการข้อมูลของห้องสมุด ซึ่งรายการจะประกอบด้วยชื่อเรื่อง ผู้แต่ง สำนักพิมพ์ ที่อยู่ ประเภท

๓. รูปแบบความสัมพันธ์ข้อมูล (Relation data model) เป็นลักษณะการออกแบบฐานข้อมูลโดยจัดข้อมูลให้อยู่ในรูปของตารางที่มีระบบคล้ายแฟ้ม โดยที่ข้อมูลแต่ละแถว (Row) ของตารางจะแทนเรคอร์ด (Record) ส่วนข้อมูลแนวดิ่งจะแทนคอลัมน์ (Column) ซึ่งเป็นขอบเขตของข้อมูล (Field) โดยที่ตารางแต่ละตาราง

ที่สร้างขึ้นจะเป็นอิสระ ดังนั้น ผู้ออกแบบฐานข้อมูลจะต้องมีการวางแผนถึงตารางข้อมูลที่จำเป็นต้องใช้ เช่นระบบฐานข้อมูลบริษัทแห่งหนึ่ง ประกอบด้วย ตารางประวัติพนักงาน ตารางแผนกและตารางข้อมูลโครงการ แสดงประวัติพนักงาน ตารางแผนก และตารางข้อมูลโครงการ

ขั้นตอนการออกแบบระบบฐานข้อมูล ประกอบด้วย

- การรวบรวมและวิเคราะห์ความต้องการในการใช้ข้อมูล
- การเลือกระบบจัดการฐานข้อมูล
- การออกแบบฐานข้อมูลในระดับแนวคิด
- การนำฐานข้อมูลที่ออกแบบในระดับแนวคิดเข้าสู่ระบบจัดการฐานข้อมูล
- การออกแบบฐานข้อมูลในระดับกายภาพ
- การนำฐานข้อมูลไปใช้และการประเมินผล

การสร้างระบบรักษาความปลอดภัยของฐานข้อมูล โดยการสร้างข้อมูลให้เป็นความลับ ด้วยการ

- เข้ารหัส (Coding) คือ กระบวนการแปลงรูปแบบของ ข้อมูลให้อยู่ในรูปที่บุคคลอื่นๆ ไม่สามารถรู้เนื้อหาของข้อมูล ยกเว้นบุคคลที่เป็นผู้รับ
- การบีบอัด (Compression) มักใช้กับข้อมูลประเภทตัวเลขหรือข้อมูลที่แปลงเป็นเลขฐานสองแล้ว ยังช่วยประหยัดเนื้อที่ในการจัดเก็บและเวลาในการส่งข้อมูลด้วย
- การแทนค่า (Substitution) คล้ายการเข้ารหัส แต่จะเป็นการกำหนดค่าที่จะแทนล่วงหน้า
- การสลับตำแหน่งข้อมูล (Transposition) ไม่ได้เปลี่ยนแปลงข้อมูล แต่ใช้การสลับตำแหน่ง

การรักษาความปลอดภัยฐานข้อมูล จะต้องดำเนินการตามขั้นตอน ดังนี้

๑) ความเสี่ยงและวิธีการสร้างความปลอดภัยให้ฐานข้อมูล
๒) การกำหนดนโยบายและขั้นตอนปฏิบัติในการใช้งานข้อมูล
๓) การสร้างความปลอดภัยให้กับฐานข้อมูล
๔) การตรวจสอบตัวตนผู้ใช้งาน
๕) นโยบายและขั้นตอนปฏิบัติในการดูแลระบบ
๖) การใช้งานค่า Configuration เริ่มต้นที่ปลอดภัย
๗) การตรวจสอบการทำงาน
๘) แผนการสำรองข้อมูลและการกู้คืนระบบ
๙) วิธีการสร้างความปลอดภัยให้กับโปรแกรมฐานข้อมูล
๑๐) ระบบและวิธีการตรวจสอบสิทธิของโปรแกรมฐานข้อมูล
๑๑) กระบวนการตรวจสอบสิทธิของโปรแกรมฐานข้อมูล

วิชาที่ ๘ ระบบการสื่อสารข้อมูล โดย อาจารย์ภิธันปต์ ถิรสัตยาพิทักษ์

การสื่อสารข้อมูล คือ การถ่ายโอนหรือแลกเปลี่ยนข้อมูล (Transmission) กันระหว่างต้นทางและปลายทางโดยผ่านทางอุปกรณ์เครือข่าย โดยอาศัยอาศัยสื่อกลาง (Transmission Line) ในการนำข้อมูลจากต้นทางไปยังปลายทาง การสื่อสารข้อมูล จะหมายรวมไปถึงสัญญาณภาพ เสียง วีดีโอ และสัญญาณอื่นๆ ทุกชนิด

ประโยชน์ของการสื่อสารข้อมูล เพื่อการบริหารและการจัดการ เพื่อการบริการ เพื่อธุรกิจและการเงิน เพื่อการแลกเปลี่ยนข่าวสาร และเพื่อการบันเทิง

องค์ประกอบของการสื่อสารข้อมูล การสื่อสารข้อมูลเป็นการแลกเปลี่ยนข่าวสารหรือข้อมูลกันระหว่างอุปกรณ์ที่ใช้ในการสื่อสาร ซึ่งประกอบด้วย

๑)ผู้ส่ง (Sender) เป็นอุปกรณ์ที่สามารถใช้ส่งข้อมูลได้ เช่นคอมพิวเตอร์ โทรศัพท์ กล้องวีดิโอ โทรศัพท์มือถือ เป็นต้น

๒)ผู้รับ (Receiver) เป็นอุปกรณ์สำหรับรับข้อมูลได้ เช่น คอมพิวเตอร์ โทรศัพท์ กล้องวีดิโอ โทรศัพท์มือถือ เป็นต้น

๓)ข้อมูล/ข่าวสาร (Message) สามารถเป็นไปได้ทั้งข้อความตัวเลข ภาพ เสียง วีดิโอ

๔)สื่อที่ใช้ในการส่ง (Media) เป็นสื่อกลางที่ใช้ในการส่งข้อมูลระหว่างผู้ส่งกับผู้รับ เช่น สายเคเบิล เส้นใยแก้วนำแสง คลื่นไมโครเวฟ แสงอินฟราเรด คลื่นวิทยุ ดาวเทียม เป็นต้น

๕)โปรโตคอล (Protocol) เป็นกฎเกณฑ์หรือข้อกำหนดที่ใช้ในซอฟต์แวร์ของการสื่อสารข้อมูลภายในเครือข่าย ซึ่งเป็นข้อตกลงของผู้ส่งและผู้รับก่อนการส่งข้อมูล เพื่อให้สามารถรับส่งข้อมูลกันได้

ทิศทางการสื่อสารข้อมูล มี ๓ รูปแบบ คือ

- การสื่อสารแบบทางเดียว (Simplex) ช่องสัญญาณอนุญาตให้ส่งข้อมูลได้ช่องทางเดียวหรือหลายช่องทางจากผู้ส่งไปยังผู้รับ ข้อมูลจะถูกส่งไปในทางเดียว
- การสื่อสารแบบทางใดทางหนึ่ง (Half - duplex) การส่งข้อมูลผ่านช่องสัญญาณเดียวกันสามารถส่งได้สองทาง แต่ต้องสลับกันจะส่งในเวลาเดียวกันไม่ได้ ช่วงเวลาที่ส่งข้อมูลไปเรียกว่า reaction time เมื่อมีการตอบกลับต้องกดสวิตซ์เพื่อเปลี่ยนสถานะจากผู้รับเป็นผู้ส่ง เรียกว่า line turnaround
- การสื่อสารแบบสองทาง (Full - duplex) มีช่องสัญญาณ ๒ ช่องและอุปกรณ์ปลายทางสามารถรับและส่งข้อมูลได้พร้อมกันโดยไม่ต้องเสียเวลาในการสับสวิตซ์ไปมา

รูปแบบของสัญญาณข้อมูล ข้อมูลที่ถูกส่งผ่านหรือถ่ายทอดจากต้นทางไปยังปลายทาง ไม่ว่าจะเป็นข้อความ ภาพ หรือเสียง จะต้องถูกแปลงให้อยู่ในรูปแบบของสัญญาณ (Signal)รูปแบบของสัญญาณข้อมูลในการสื่อสารมี ๒ รูปแบบ

- สัญญาณอนาลอก (Analog signal) สัญญาณข้อมูลมีลักษณะต่อเนื่อง (continuous) มีการเปลี่ยนแปลงค่าอย่างต่อเนื่องทั้งทางด้านความถี่และขนาด (VOLUME) ได้แก่ สัญญาณไฟฟ้ากระแสสลับหรือ AC สัญญาณเสียง(VOICE) เป็นต้น
- สัญญาณดิจิทัล (Digital signal) สัญญาณประกอบด้วยข้อมูลที่เป็นตัวเลข 0 และ 1 ที่เรียกว่า Binary digit หรือบิต (bit) และมีลักษณะของสัญญาณข้อมูลที่สามารถแยกข้อมูลที่อยู่ติดกันออกจากกันได้โดยง่าย

คุณลักษณะของระบบสื่อสารข้อมูล ๗ ประการ

๑) Performance สมรรถนะในการสื่อสารข้อมูลซึ่งสามารถวัดได้หลายวิธี แต่วิธีทั่วไปที่ใช้คือวัด Response time (ระยะเวลาตั้งแต่การส่ง Massage จนถึงการตอบรับ) และ Throughput (จำนวน Massage ที่สามารถส่งหรือรับได้ในช่วงเวลาหนึ่ง)

๒) Consistency การทำงานของระบบมีความแน่นอนสามารถคาดการณ์ได้

๓) Flexibility ความยืดหยุ่นของระบบที่สามารถขยายหรือเปลี่ยนแปลงได้ โดยมีผลกระทบต่อผู้ใช้น้อยที่สุด

๔) Availability ระบบสามารถใช้งานได้อย่างต่อเนื่องตลอดเวลาทำงาน

๕) Reliability ความน่าเชื่อถือของระบบ ระบบสามารถทำงานได้โดยมีค่า Mean time between failure (MTBF) ระยะเวลาคาดว่าระบบจะล่มหรือหยุดทำงาน และค่า Mean timeto repair (MTTR) ระยะเวลาในการแก้ไขระบบให้กลับสู่สภาพเดิม ค่าทั้งสองจะต้องมีค่าน้อยที่สุด โดยต้องมี Fault Tolerance หรือความทนทานต่อการเสียหายมากเท่าที่จะมากได้

๖) Recovery ระบบสามารถกู้คืนให้ทำงานให้เป็นปกติได้

๗) Security ระบบจะต้องมีความปลอดภัย

การสื่อสารข้อมูลผ่านช่องทางสื่อสารมักมีข้อผิดพลาดเนื่องจากการลักลอบดักฟัง การเปลี่ยนแปลงสัญญาณและเสียงรบกวน ข้อผิดพลาดดังกล่าวสามารถตรวจพบและแก้ไขโดยเทคนิค

❖ การตรวจทวนซ้ำ เป็นการตรวจทวนสัญญาณจากต้นทางว่าที่ปลายทางได้รับสัญญาณตรงกับที่ส่งไปหรือไม่

❖ การตรวจพาริตี้บิต เป็นวิธีการเติมบิตพิเศษ 0 หรือ 1 ไปกับกลุ่มข้อมูล เมื่อส่งไปถึงปลายทางก็จะตรวจสอบว่าเป็นจำนวนคี่หรือคู่ตรงกับลักษณะที่ส่งมาหรือไม่

❖ การแก้ไขข้อผิดพลาด ซึ่งมี ๒ วิธีคือ ๑) การส่งสัญญาณ ๒ ชุดไปพร้อมกัน และ ๒) การส่งสัญญาณซ้ำเมื่อการส่งครั้งแรกผิดพลาด

ส่วนประกอบของระบบเครือข่าย ประกอบด้วย

- เครื่องคอมพิวเตอร์แม่ข่าย (Host, File Server)
- เครื่องคอมพิวเตอร์ลูกข่าย (Workstation, Client)
- อุปกรณ์เครือข่าย (Network Equipment)
- ระบบปฏิบัติการเครือข่าย (Network Operating System : NOS)
- หมายเลขไอพีแอดเดรส (IP Address)

ระบบเครือข่าย

- ระบบเครือข่ายเฉพาะบริเวณ (Local Area Network หรือ LAN) เป็นเครือข่ายคอมพิวเตอร์ขนาดเล็กของผู้ใช้กลุ่มเล็ก ๆ กลุ่มหนึ่ง โดยทั่วไปเครือข่ายจะอยู่ภายในอาคารเดียวกันหรือกลุ่มอาคารที่อยู่ติดกัน มีระยะทางไม่เกิน ๒–๓ กิโลเมตร โดยมีวัตถุประสงค์หลักคือ การใช้อุปกรณ์ส่วนกลางร่วมกัน การใช้โปรแกรมหรือข้อมูลร่วมกัน และการรับส่งข้อมูลอิเล็กทรอนิกส์ระหว่างกัน เครือข่ายเฉพาะบริเวณมีลักษณะเฉพาะที่แตกต่างกับเครือข่ายแบบอื่น ๓ ประการคือ ขนาด เทคโนโลยีที่ใช้ในการรับ-ส่งข้อมูล และรูปแบบโครงสร้างเครือข่าย

- ระบบเครือข่ายบริเวณกว้าง (Wide Area Network หรือ WAN) เป็นเครือข่ายที่มีขนาดใหญ่ขึ้นไปอีกระดับหนึ่งโดยเป็นการรวมเอาเครือข่ายทั้ง LAN และMAN มาเชื่อมต่อกันเป็นเครือข่ายเดียว ดังนั้น เครือข่ายจึงครอบคลุมพื้นที่กว้าง บางครั้งครอบคลุมไปทั่วประเทศหรือทั่วทั้งโลก ตัวอย่างเช่นอินเตอร์เน็ตก็จัดว่าเป็นเครือข่าย WAN ประเภทหนึ่ง แต่เป็นเครือข่ายสาธารณะที่ไม่มีใครเป็นเจ้าของทั้งหมด สำหรับเครือข่าย WAN ของบริษัทหรือหน่วยงานเอกชน เรามักเรียกอีกชื่อหนึ่งว่า Enterprise Network

- ระบบเครือข่ายไร้สาย (Wireless LAN : WLAN) หมายถึง เทคโนโลยีที่ช่วยให้การติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ ๒ เครื่อง หรือกลุ่มของเครื่องคอมพิวเตอร์สามารถสื่อสารกันได้ ร่วมถึงการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่ายคอมพิวเตอร์ด้วยเช่นกัน โดยปราศจากการใช้

สายสัญญาณในการเชื่อมต่อ แต่จะใช้คลื่นวิทยุเป็นช่องทางการสื่อสารแทนการรับส่งข้อมูลระหว่างกันจะผ่านอากาศ ทำให้ไม่ต้องเดินสายสัญญาณ และติดตั้งใช้งานได้สะดวกขึ้น ข้อดีและข้อเสียเครือข่ายไร้สาย คือ

ข้อดี คือ ความสะดวกสบายในการใช้งาน สามารถใช้ได้ทุกที่ตามที่ต่างๆ และ ต้นทุนต่ำ

ข้อเสีย คือ ความปลอดภัย ประสิทธิภาพของเครือข่าย แบนด์วิดช์ต่ำกว่าระบบสาย

ความปลอดภัยในการใช้งานระบบเครือข่าย

- การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control) ผู้บริหารระบบต้องกำหนดสิทธิ์ให้กับผู้ที่ใช้งานเท่าที่จำเป็น ในการเข้าใช้ระบบสารสนเทศต้องจัดทำกลไกควบคุมการเข้าใช้ด้วยผู้ใช้ในเวลาเดียวกันเพียงหนึ่งเดียว (Single User Session) โดยมีระบบการตรวจสอบสิทธิ์การเข้าถึง (Access Right) และมีการปรับปรุงให้ถูกต้องเหมาะสมอยู่เสมอ และต้องจัดทำรายการควบคุมสิทธิ์ในการเข้าใช้ระบบสารสนเทศของผู้ใช้แต่ละคน (Access Control List) โดยมีการบันทึกเพื่อตรวจสอบการเข้าใช้ระบบสารสนเทศ เพื่อรายงานให้ผู้รับผิดชอบทราบถึงความผิดปกติที่เกิดขึ้น

- การควบคุมการใช้รหัสผ่านและกุญแจอิเล็กทรอนิกส์ ผู้ใช้งานต้องปฏิบัติตามนโยบายรหัสผ่านอย่างเคร่งครัด โดยรหัสผ่านที่ใช้ในการติดต่อต้องมีการกำหนดการเข้ารหัส (Encryption) และมีการบันทึกการเข้าใช้เพื่อตรวจสอบสิ่งผิดปกติที่เกิดขึ้น

- การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server) ระบบคอมพิวเตอร์แม่ข่ายต้องมีการกำหนดผู้รับผิดชอบอย่างชัดเจน มีระบบการสำรองข้อมูลและโปรแกรมระบบงานอย่างเพียงพอ รวมถึงกำหนดรอบในการตรวจสอบความปลอดภัยอยู่อย่างสม่ำเสมอ และมีการตรวจสอบความเพียงพอของระบบงาน ในกรณีที่มีการติดตั้งเครื่องแม่ข่ายใหม่ต้องพิจารณาระบบปฏิบัติการและแอพพลิเคชั่นให้ทันสมัยที่สุด มีการติดตั้ง Patch เพื่อปิดช่องโหว่อย่างสม่ำเสมอ รวมถึงต้องมีการทดสอบซอฟต์แวร์เกี่ยวกับความปลอดภัยก่อนการติดตั้งและหลังจากที่ติดตั้งไปแล้ว

- การบริหารจัดการ และการตรวจสอบระบบเครือข่าย (Network) ระบบเครือข่ายต้องมีการแบ่งแยกเครือข่ายอย่างเป็นสัดส่วน และมีการออกแบบเครือข่ายเพื่อป้องกันผู้บุกรุก มีระบบตรวจสอบผู้บุกรุก ป้องกันไวรัส และการใช้งานที่ผิดปกติที่ผ่านเข้ามายังระบบเครือข่าย (Firewall/IDS/IPS)

- การเข้าถึงสารสนเทศจากระยะไกล (Remote Access) ผู้ที่เข้าใช้ระบบสารสนเทศจากทางไกลต้องถูกระบุสิทธิ์อย่างเป็นลายลักษณ์อักษรจากฝ่ายความปลอดภัยระบบเทคโนโลยีสารสนเทศและผู้รับผิดชอบระบบงานที่เกี่ยวข้อง ในการติดต่อจะต้องมีระบบการพิสูจน์ตัวตน (Authentication)และการเข้ารหัสข้อมูล (Encryption) ที่ได้มาตรฐาน รวมทั้งต้องมีหน่วยงานที่ทำหน้าที่ตรวจสอบบันทึกการเข้าใช้ เพื่อติดตาม และตรวจสอบสิ่งที่ผิดปกติ องค์กรต้องไม่อนุญาตให้ใช้โมเด็มในการเชื่อมต่อเครือข่ายสื่อสารภายในองค์กร หากจำเป็นต้องใช้ จะต้องได้รับการอนุมัติ

แนวปฏิบัติการใช้งานระบบอินเทอร์เน็ต (Internet)

- ผู้ใช้บริการต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น และห้ามผู้ใช้บริการทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากหน่วยงานที่ดูแลด้านการรักษาความปลอดภัยระบบสารสนเทศเป็นลายลักษณ์อักษรแล้ว

- ผู้ใช้บริการต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของหน่วยงาน และต้องไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา

พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับหน่วยงาน เป็นต้น

- ห้ามผู้ใช้บริการเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet) ผู้ใช้บริการต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) ซึ่งรวมถึงการดาวน์โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา
- ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้บริการต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน
- ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้บริการต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคคลากรของหน่วยงานอื่นๆ
- หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ผู้ใช้บริการทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

วิชาที่ ๙ พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ โดย อาจารย์ภิธันปต์ ถิรสัตยาพิทักษ์

โครงสร้างของพระราชบัญญัติ ในบททั่วไป ประกอบด้วย ๖ หมวด ดังนี้

หมวด ๑ ธุรกรรมทางอิเล็กทรอนิกส์

หมวด ๒ ลายมือชื่ออิเล็กทรอนิกส์

หมวด ๓ ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

หมวด ๔ ธุรกรรมอิเล็กทรอนิกส์ภาครัฐ

หมวด ๕ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

หมวด ๖ บทกำหนดโทษ

เหตุผลในการประกาศใช้ พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ฯ เพื่อรองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ ที่ใช้ทำธุรกรรมหรือสัญญา ให้มีผลเช่นเดียวกับการทำสัญญาตามหลักเกณฑ์ที่ประมวลกฎหมายแพ่งและพาณิชย์กำหนดไว้ ได้แก่ การทำเป็นหนังสือ หลักฐานเป็นหนังสือ การลงลายมือชื่อ กล่าวคือ ถ้ามีการทำสัญญาระหว่างบุคคลที่ใช้ข้อมูลอิเล็กทรอนิกส์ หรือลายมือชื่ออิเล็กทรอนิกส์ ตามความหมายของกฎหมายแล้ว ถือว่า การทำสัญญานั้นได้ทำตามหลักเกณฑ์ของประมวลกฎหมายแพ่งและพาณิชย์ อันเป็นผลให้ สัญญานั้นสมบูรณ์หรือใช้บังคับได้ตามกฎหมาย และสามารถนำไปใช้เป็นพยานหลักฐานในการฟ้องร้อง และศาลสามารถรับฟัง ซึ่งน้ำหนัก และมีผลในการพิจารณาคดีทั้ง คดีแพ่ง คดีอาญา เป็นต้น

คำนิยาม

ธุรกรรม หมายความว่า การกระทำใดๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์ หรือในการดำเนินงานของรัฐตามที่กำหนดในหมวด

อิเล็กทรอนิกส์ หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้าคลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่างๆเช่นว่านั้น

ธุรกรรมทางอิเล็กทรอนิกส์ หมายความว่าธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน

ข้อความ หมายความว่า เรื่องราวหรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ

ข้อมูลอิเล็กทรอนิกส์ หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

ลายมือชื่ออิเล็กทรอนิกส์ หมายความว่าอักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

ระบบข้อมูล หมายความว่า กระบวนการประมวลผลด้วยเครื่องมืออิเล็กทรอนิกส์สำหรับสร้าง ส่ง รับ เก็บรักษา หรือประมวลผลข้อมูลอิเล็กทรอนิกส์

การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ หมายความว่า การส่งหรือรับข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์โดยใช้มาตรฐานที่กำหนดไว้ล่วงหน้า

ผู้ส่งข้อมูล หมายความว่า บุคคลซึ่งเป็นผู้ส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ก่อนจะมีการเก็บรักษาข้อมูลเพื่อส่งไปตามวิธีการที่ผู้นั้นกำหนด โดยบุคคลนั้นอาจจะส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง หรือมีการส่ง

หรือสร้างข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนบุคคลนั้นก็ได้ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

ผู้รับข้อมูล หมายความว่า บุคคลซึ่งผู้ส่งข้อมูลประสงค์จะส่งข้อมูลอิเล็กทรอนิกส์ให้และได้รับข้อมูลอิเล็กทรอนิกส์นั้น ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

บุคคลที่เป็นสื่อกลาง หมายความว่า บุคคลซึ่งกระทำการในนามผู้อื่นในการส่ง รับ หรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์อันใดอันหนึ่งโดยเฉพาะ รวมถึงให้บริการอื่นที่เกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้น

ใบรับรอง หมายความว่า ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใด ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์

เจ้าของลายมือชื่อ หมายความว่า ผู้ซึ่งถือข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์

หมวดและมีมาตราที่ต้องพิจารณาเป็นพิเศษ คือ

หมวด ๑ ธุรกรรมทางอิเล็กทรอนิกส์

มาตรา ๗ ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใดเพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

มาตรา ๘ ภายใต้บังคับบทบัญญัติแห่งมาตรา ๙ ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว

มาตรา ๘ เพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ ในกรณีที่กฎหมายกำหนดให้ต้องมีการปิดอากรแสตมป์ หากได้มีการชำระเงินแทนหรือดำเนินการอื่นใดด้วยวิธีการทางอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่หน่วยงานของรัฐซึ่งเกี่ยวข้องประกาศกำหนด ให้ถือว่าหนังสือหลักฐานเป็นหนังสือ หรือเอกสาร ซึ่งมีลักษณะเป็นตราสารนั้นได้มีการปิดอากรแสตมป์และขีดฆ่าตามกฎหมายนั้นแล้ว ในการนี้ในการกำหนดหลักเกณฑ์และวิธีการของหน่วยงานของรัฐดังกล่าว คณะกรรมการจะกำหนดกรอบและแนวทางเพื่อเป็นมาตรฐานทั่วไปไว้ด้วยก็ได้

มาตรา ๙ ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า

(๑) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ

(๒) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

วิธีการที่เชื่อถือได้ตาม (๒) ให้คำนึงถึง

ก. ความมั่นคงและรัดกุมของการใช้วิธีการหรืออุปกรณ์ในการระบุตัวบุคคล สภาพพร้อมใช้งานของทางเลือกในการระบุตัวบุคคล กฎเกณฑ์เกี่ยวกับลายมือชื่อที่กำหนดไว้ในกฎหมายระดับความมั่นคงปลอดภัยของการใช้ลายมือชื่ออิเล็กทรอนิกส์ การปฏิบัติตามกระบวนการในการระบุตัวบุคคลผู้เป็นสื่อกลาง ระดับของการยอมรับหรือไม่ยอมรับวิธีการที่ใช้ในการระบุตัวบุคคลในการทำธุรกรรม วิธีการระบุตัวบุคคล ณ ช่วงเวลาที่มีการทำธุรกรรมและติดต่อสื่อสาร

ข. ลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำ จำนวนครั้งหรือความสม่ำเสมอในการทำธุรกรรมประเพณีทางการค้าหรือทางปฏิบัติ ความสำคัญ มูลค่าของธุรกรรมที่ทำ หรือ

ค. ความรัดกุมของระบบการติดต่อสื่อสาร (เพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑)ให้นำความในวรรคหนึ่งมาใช้บังคับกับการประทับตราของนิติบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์ ด้วยโดยอนุโลม (เพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑)

มาตรา ๑๐ ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว

(๑) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และ

(๒) สามารถแสดงข้อความนั้นในภายหลังได้ความถูกต้องของข้อความตาม (๑) ให้พิจารณาถึงความครบถ้วนและไม่มีการเปลี่ยนแปลงใดของข้อความ เว้นแต่การรับรองหรือบันทึกเพิ่มเติม หรือการเปลี่ยนแปลงใดๆ ที่อาจจะเกิดขึ้นได้ตามปกติในการติดต่อสื่อสารการเก็บรักษา หรือการแสดงข้อความซึ่งไม่มีผลต่อความถูกต้องของข้อความนั้น

ในการวินิจฉัยความน่าเชื่อถือของวิธีการรักษาความถูกต้องของข้อความตาม (๑) ให้พิเคราะห์ถึงพฤติการณ์ที่เกี่ยวข้องทั้งปวง รวมทั้งวัตถุประสงค์ของการสร้างข้อความนั้น

มาตรา ๑๐ (เพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑)ในกรณีที่มีการทำสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ตามวรรคหนึ่งสำหรับใช้อ้างอิงข้อความของข้อมูลอิเล็กทรอนิกส์ หากสิ่งพิมพ์ออกนั้นมีข้อความถูกต้องครบถ้วนตรงกับข้อมูลอิเล็กทรอนิกส์ และมีการรับรองสิ่งพิมพ์ออกโดยหน่วยงานที่มีอำนาจตามที่คณะกรรมการประกาศกำหนดแล้ว ให้ถือว่าสิ่งพิมพ์ออกดังกล่าวใช้แทนต้นฉบับได้

มาตรา ๑๑ ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้นให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะหรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง

ให้นำความในวรรคหนึ่งมาใช้บังคับกับสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ด้วย (แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑)

มาตรา ๑๒ ภายใต้บังคับบทบัญญัติมาตรา ๑๐ ในกรณีที่กฎหมายกำหนดให้เก็บรักษาเอกสารหรือข้อความใด ถ้าได้เก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการเก็บรักษาเอกสารหรือข้อความตามที่กฎหมายต้องการแล้ว

(๑) ข้อมูลอิเล็กทรอนิกส์นั้นสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง

(๒) ได้เก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นให้อยู่ในรูปแบบที่เป็นอยู่ในขณะที่สร้าง ส่ง หรือได้รับข้อมูลอิเล็กทรอนิกส์นั้น หรืออยู่ในรูปแบบที่สามารถแสดงข้อความที่สร้าง ส่ง หรือได้รับให้ปรากฏอย่างถูกต้องได้ และ

(๓) ได้เก็บรักษาข้อความส่วนที่ระบุถึงแหล่งกำเนิด ต้นทาง และปลายทางของข้อมูลอิเล็กทรอนิกส์ตลอดจนวันและเวลาที่ส่งหรือได้รับข้อความดังกล่าว ถ้ามี

ความในวรรคหนึ่ง มิให้ใช้บังคับกับข้อความที่ใช้เพียงเพื่อวัตถุประสงค์ในการส่งหรือรับข้อมูลอิเล็กทรอนิกส์

หน่วยงานของรัฐที่รับผิดชอบในการเก็บรักษาเอกสารหรือข้อความใด อาจกำหนดหลักเกณฑ์รายละเอียดเพิ่มเติมเกี่ยวกับการเก็บรักษาเอกสารหรือข้อความนั้นได้ เท่าที่ไม่ขัดหรือแย้งกับบทบัญญัติในมาตรานี้

มาตรา ๑๒/๑ (เพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑) ให้นำบทบัญญัติในมาตรา ๑๐ มาตรา ๑๑ และมาตรา ๑๒ มาใช้บังคับกับเอกสารหรือข้อความที่ได้มีการจัดทำหรือแปลงให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ในภายหลังด้วยวิธีการทางอิเล็กทรอนิกส์ และการเก็บรักษาเอกสารและข้อความดังกล่าวด้วยโดยอนุโลม

การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ตามวรรคหนึ่งให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนด

หมวด ๒ ลายมือชื่ออิเล็กทรอนิกส์

มาตรา ๒๖ ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

(๑) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นได้เชื่อมโยงไปยังเจ้าของลายมือชื่อโดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้

(๒) ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(๓) การเปลี่ยนแปลงใดๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้และ

(๔) ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่ออิเล็กทรอนิกส์เป็นไปเพื่อรับรองความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์

มาตรา ๒๗ ในกรณีมีการใช้ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์เพื่อสร้างลายมือชื่ออิเล็กทรอนิกส์ที่จะมีผลตามกฎหมาย เจ้าของลายมือชื่อต้องดำเนินการดังต่อไปนี้

(๑) ใช้ความระมัดระวังตามสมควรเพื่อมิให้มีการใช้ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

(๒) แจ้งให้บุคคลที่คาดหมายได้โดยมีเหตุอันควรเชื่อว่าจะกระทำการใดโดยขึ้นอยู่กับลายมือชื่ออิเล็กทรอนิกส์หรือให้บริการเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ ทราบโดยมิชักช้า เมื่อ

(ก) เจ้าของลายมือชื่อรู้หรือควรได้รู้ว่าข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นสูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(ข) เจ้าของลายมือชื่อรู้จากสภาพการณ์ที่ปรากฏว่ากรณีมีความเสี่ยงมากพอที่ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ สูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบหรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(๓) ในกรณีมีการออกใบรับรองสนับสนุนการใช้ลายมือชื่ออิเล็กทรอนิกส์ จะต้องใช้ความระมัดระวังตามสมควรให้แน่ใจในความถูกต้องและสมบูรณ์ของการแสดงสาระสำคัญทั้งหมดซึ่งกระทำโดยเจ้าของลายมือชื่อเกี่ยวกับใบรับรองนั้นตลอดอายุใบรับรอง หรือตามที่มี

หมวด ๔ ธุรกรรมอิเล็กทรอนิกส์ภาครัฐ

มาตรา ๓๕ คำขอ การอนุญาต การจดทะเบียนคำสั่งทางปกครอง การชำระเงิน การประกาศหรือการดำเนินการใดๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับและให้ถือว่ามีผล โดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด ทั้งนี้ ในพระราชกฤษฎีกาอาจกำหนดให้บุคคลที่เกี่ยวข้องต้องกระทำหรืองดเว้นกระทำการใดๆ หรือให้หน่วยงานของรัฐออกระเบียบเพื่อกำหนดรายละเอียดในบางกรณีด้วยก็ได้

เทคโนโลยีการสร้างลายมือชื่อที่มีความน่าเชื่อถือ

๑. การใช้เทคโนโลยี PKI สร้างลายมือชื่อดิจิทัล (Digital signatures)

๒. การใช้เทคโนโลยีชีวภาพสร้างสิ่งที่ใช้ระบุตัวบุคคล (Biometric devices) เช่น เครื่องสแกนฝ่ามือ เครื่องสแกนใบหน้า เครื่องสแกนลายนิ้วมือ ระบบจดจำเสียง เครื่องสแกนม่านตา เป็นต้น

๓. อื่นๆ เช่น รหัส PIN, Tokens หรือ Ring networkการทำลายเซ็นมือให้เป็นลายเซ็นดิจิตอล e-mail address เป็นต้น

ปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ ด้วย PKI

ลายมือชื่ออิเล็กทรอนิกส์ที่ใช้ในการยืนยันและตรวจสอบ จะต้องมีมาตรการสร้างความเชื่อมั่นความปลอดภัยต่อผู้ทำธุรกรรมว่าข้อมูลจะไม่ถูกเผยแพร่ หรือถูกหลอกลวงจากอีกฝ่าย และต้องสร้างความเชื่อมั่นปลอดภัยแก่อีกฝ่ายเช่นกันว่าลูกค้าหรือผู้ทำธุรกรรมด้วยมีตัวตนจริงเทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI) เป็นวิธีหนึ่งที่ทำให้การทำธุรกรรมทางอิเล็กทรอนิกส์มีความปลอดภัย

เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI)

PKI คือระบบที่ได้รวบรวมบริการพื้นฐานต่างๆเข้าไว้ด้วยกัน ซึ่งประกอบไปด้วยองค์ประกอบต่างๆ ได้แก่ ระบบการเข้ารหัส (Cryptography) ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate)ลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) ซึ่งองค์ประกอบเหล่านี้จะจัดตั้งขึ้นโดยองค์กรที่ทำธุรกรรม หรือโดยองค์กรที่เป็นกลางซึ่งเรียกว่า ผู้ประกอบการรับรอง (Certification Authority)หรือผู้ให้บริการรับรอง (Certification Service Provider) เทคโนโลยี PKI สามารถตอบสนองความต้องการพื้นฐานด้านความปลอดภัยของการทำธุรกรรมอิเล็กทรอนิกส์

ผู้ออกใบรับรองอิเล็กทรอนิกส์(Certification Authority : CA)

ผู้ออกใบรับรองอิเล็กทรอนิกส์ จะเป็นผู้ตรวจสอบสถานะและออกใบรับรองอิเล็กทรอนิกส์ให้แก่ผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ และ CAจะเป็นผู้รับรองความมีตัวตนของคู่ทำธุรกรรม

หน้าที่ผู้ออกใบรับรองอิเล็กทรอนิกส์

๑. สร้างคู่กุญแจ (Key pairs) ตามคำขอของผู้ขอใช้บริการ

๒. ออกใบรับรองอิเล็กทรอนิกส์เพื่อยืนยันตัวบุคคลของผู้ขอใช้บริการ

๓. จัดเก็บกุญแจสาธารณะ (Public Key) ในฐานข้อมูล

๔. เปิดเผยกุญแจสาธารณะต่อสาธารณชนที่ติดต่อผ่านทางระบบเครือข่าย

๕. ยืนยันตัวบุคคลที่เป็นเจ้าของกุญแจสาธารณะตามคำขอของบุคคลทั่วไป

๖. เปิดเผยรายชื่อใบรับรองฯ ที่ถูกยกเลิกแล้ว (Certificate Revocation List หรือ CRL) เพื่อเป็นการบอกแก่สาธารณชนว่าใบรับรองฯ นั้น ไม่สามารถนำมาใช้ได้อีกต่อไป

รายละเอียดข้อมูลใน Digital Certificate ด้วยการเข้ารหัส และ ลายมือชื่อดิจิตอล ในการทำธุรกรรมสามารถรักษาความลับของข้อมูล และสามารถระบุตัวบุคคลได้ระดับหนึ่ง เพื่อเพิ่มระดับความปลอดภัยในการระบุตัวบุคคล โดยสร้างความเชื่อถือมากขึ้นด้วยใบรับรองดิจิตอล (Digital Certificate) ซึ่งออกโดยองค์กรกลางที่เป็นที่เชื่อถือเรียกว่า องค์กรรับรองความถูกต้อง (Certification Authority) จะถูกนำมาใช้สำหรับยืนยันในการทำธุรกรรมว่าเป็นบุคคลนั้นๆ จริงตามที่ได้อ้างไว้ ใบรับรองดิจิตอลจะประกอบด้วยข้อมูลดังต่อไปนี้

- หมายเลขของใบรับรอง (serial number)
- วิธีการที่ใช้ในการเข้ารหัสข้อมูล (algorithm)
- หน่วยงานที่ออกใบรับรอง (issuer)
- เวลาเริ่มใช้ใบรับรอง (starting time)
- เวลาที่ใบรับรองหมดอายุ (expiring time)
- ผู้ได้รับการรับรอง (subject)
- กุญแจสาธารณะของผู้ได้รับการรับรอง (subject ' s public key)
- ลายมือชื่อดิจิตอลของหน่วยงานที่ออกใบรับรอง (CA signature

วิชาที่ ๑๐ ความรู้เกี่ยวกับกฎหมายด้านการพิทักษ์สิทธิของบุคคล โดย อาจารย์ภิธันปต์ ถิรสัตยาพิทักษ์

ลักษณะการก่ออาชญากรรมทางคอมพิวเตอร์ เป็นการเจาะระบบรักษาความปลอดภัยทางกายภาพ การเจาะระบบสื่อสาร การเจาะเข้าสู่ระบบรักษาความปลอดภัยของซอฟต์แวร์ต่างๆ การเจาะเข้าสู่ระบรักษาความปลอดภัยของระบบปฏิบัติการ (OS) และการเจาะผ่านระบบรักษาความปลอดภัยส่วนบุคคล

รูปแบบการก่ออาชญากรรม คอมพิวเตอร์ยอดนิยม ได้แก่

- การขโมยข้อมูลทางระบบอินเตอร์เน็ต
- การลักลอบเข้าใช้บริการระบบคอมพิวเตอร์ของผู้อื่น
- การละเมิดลิขสิทธิ์ซอฟต์แวร์
- การเผยแพร่ภาพ เสียง ลามก อนาจาร และข้อมูลที่ไม่เหมาะสมทางระบบอินเตอร์เน็ต
- การใช้คอมพิวเตอร์ฟอกเงิน
- การก่อกวน ทำลายระบบสาธารณูปโภค
- การหลอกลวงให้ร่วมค้าขายหรือลงทุนปลอม
- การล้วงข้อมูลความลับส่วนบุคคลแล้วนำข้อมูลนั้นมาแสวงหาผลประโยชน์
- การใช้ระบบคอมพิวเตอร์แอบโอนเงินจากบัญชีผู้อื่นเข้าบัญชีตัวเอง

เหตุผลในการประกาศบังคับใช้ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

- ป้องกันและปราบปรามผู้ที่ทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้
- ป้องกันและปราบปรามผู้ที่ทำให้การทำงานของระบบคอมพิวเตอร์ผิดพลาดไปจากคำสั่งที่กำหนด
- ป้องกันและปราบปรามผู้ที่ใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ
- ป้องกันและปราบปรามผู้ที่ใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ที่ก่อให้ เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน

การกำหนดฐานความผิด มีเจตนารมณ์เพื่อกำหนดฐานความผิดและบทลงโทษสำหรับการกระทำความผิดต่อความลับ (Confidentiality) ความครบถ้วน (Integrity) หรือสภาพพร้อมใช้งาน (Availability) ของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ รวมทั้งความผิดที่เกี่ยวข้องกับการกระทำความผิดทางคอมพิวเตอร์อื่นๆ เช่น การเผยแพร่ภาพอันไม่เหมาะสมและการตัดต่อภาพ เป็นต้น และเพื่อกำหนดเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่

คำนิยามศัพท์

ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

ข้อมูลจราจรทางคอมพิวเตอร์ หมายความว่าข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

ผู้ให้บริการ หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่นผู้ให้บริการ ครอบคลุมทั้งหน่วยงานภาครัฐบาล และเอกชน ไม่เฉพาะแต่ “ISP” หรือผู้ให้บริการอินเทอร์เน็ตอย่างเดียว แต่หมายรวมถึง

- ผู้ประกอบการธุรกิจโทรคมนาคม ระบบโทรศัพท์ ระบบดาวเทียม ระบบวงจรเช่า หรือบริการสื่อสารไร้สาย
- องค์กรหรือหน่วยงานที่จัดตั้งและให้บริการเครือข่าย Internet, Intranet และ Extranet ทั้งผ่านสายและไร้สาย รวมถึงร้านอินเทอร์เน็ต คาเฟ่ สถาบันการศึกษา
- ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ ต่าง ๆ (Host Service Provider)
- ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านโปรแกรมต่าง ๆ เช่น Web Board หรือ Web Service ต่าง ๆ

ผู้ใช้บริการ หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

พนักงานเจ้าหน้าที่ หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

รัฐมนตรี หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

เหตุผลในการประกาศบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

เนื่องจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกัน และปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ซึ่งมีรูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้น จึงมีการการปรับปรุงบทบัญญัติในส่วนที่เกี่ยวข้องกับ

- ❖ ผู้รักษาการตามกฎหมาย
- ❖ กำหนดฐานความผิดขึ้นใหม่
- ❖ แก้ไขเพิ่มเติมฐานความผิดเดิมและบทกำหนดโทษของความผิด
- ❖ การปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์
- ❖ กำหนดให้มีคณะกรรมการเปรียบเทียบซึ่งมีอำนาจเปรียบเทียบความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
- ❖ เพิ่มเติมอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ให้เหมาะสมยิ่งขึ้น

เนื้อหาใน **มาตรา ๑๑ แก้ไขใน (ฉบับที่ ๒) พ.ศ. ๒๕๖๐**

มาตรา ๔ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ต้องระวางโทษปรับไม่เกินสองแสนบาท

ให้รัฐมนตรีออกประกาศกำหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับและลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย

เนื้อหาใน **มาตรา ๑๒ แก้ไขใน (ฉบับที่ ๒) พ.ศ. ๒๕๖๐**

มาตรา ๕ ให้ยกเลิกความในมาตรา ๑๒ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท

มาตรา ๖ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๒/๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

มาตรา ๑๒/๑ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นเหตุให้เกิดอันตรายแก่บุคคลอื่นหรือทรัพย์สินของผู้อื่นต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท”

เนื้อหาใน **มาตรา ๑๓ แก้ไขใน (ฉบับที่ ๒) พ.ศ. ๒๕๖๐**

มาตรา ๗ ให้เพิ่มความต่อไปนี้เป็นวรรคสองวรรคสาม วรรคสี่ และวรรคห้าของมาตรา ๑๓ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย ก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นนั้นด้วย

ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรคหนึ่งหรือวรรคสอง และตามวรรคสามหรือวรรคสี่ด้วย ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระทงเดียว”

เนื้อหาใน **มาตรา ๑๔ แก้ไขใน (ฉบับที่ ๒) พ.ศ. ๒๕๖๐**

มาตรา ๘ ให้ยกเลิกความในมาตรา ๑๔ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำ ทั้งปรับ และให้เป็นความผิดอันยอมความได้"

เนื้อหาใน **มาตรา ๑๕ แก้ไขใน (ฉบับที่ ๒) พ.ศ. ๒๕๖๐**

มาตรา ๙ ให้ยกเลิกความในมาตรา ๑๕ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๕ ผู้ให้บริการผู้ใดให้ความร่วมมือยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์

เนื้อหาใน **มาตรา ๑๖ แก้ไขใน (ฉบับที่ ๒) พ.ศ. ๒๕๖๐**

มาตรา ๑๐ ให้ยกเลิกความในมาตรา ๑๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอายผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง

ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสองเป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็นการติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิดความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งหรือวรรคสองตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรสหรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย”

มาตรา ๑๑ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๖/๑ และมาตรา ๑๖/๒ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“มาตรา ๑๖/๑ ในคดีความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖ ซึ่งมีคำพิพากษาว่าจำเลยมีความผิด ศาลอาจสั่ง

(๑) ให้ทำลายข้อมูลตามมาตราดังกล่าว

(๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์หรือสื่ออื่นใด ตามที่ศาลเห็นสมควร โดยให้จำเลยเป็นผู้ชำระค่าโฆษณาหรือเผยแพร่

(๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น

มาตรา ๑๖/๒ ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา ๑๖/๑ ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ในมาตรา ๑๔ หรือมาตรา ๑๖ แล้วแต่กรณี”