ใบความรู้ที่ 3.1
เรื่อง การใช้เทคโนโลยีสารสนเทศอย่างสร้างสรรค์

ภัยคุกคามจาก Social Network

http://gg.gg/c9grc

การใช้เทคโนโลยีสารสนเทศอย่างได้ปลอดภัย

ในปัจจุบันเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่มีจำนวนมากมายมหาศาล มีอิทธิพลในการดำเนินชีวิตประจำวันของมนุษย์ จะเห็นได้จากในทุกพื้นที่มีสัญญาณอินเตอร์ อุปกรณ์ในการใช้งานต่างๆ ก็มีราคาถูก มนุษย์จึงมีโอกาสที่จะเข้าถึงข้อมูลสารสนเทศต่างๆ ได้อย่างทั่วถึง ผลกระทบของเทคโนโลยีสารสนเทศมีทั้งด้านดีหากใช้ถูกวิธี แต่หากใช้ไม่ถูกวิธีภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศจะส่งผลเสียได้มากเช่นกัน อาจมีผู้ไม่ประสงค์ดีใช้สื่อออนไลน์เป็นช่องทางในการสร้างความเสียหายให้กับคนอื่นหรือตัวผู้ใช้เองที่กระทำการโดยรู้เท่าไม่ถึงการณ์ จึงเสี่ยงต่อการกระทำผิดกฎหมายที่เกี่ยวกับเทคโนโลยีสารสนเทศ ดังนั้นการใช้เทคโนโลยีสารสนเทศให้ปลอดภัยควรปฏิบัติตน ดังนี้

1. ไม่เปิดเผยข้อมูลส่วนตัว เช่น เลขประจำตัวประชาชน เบอร์โทรศัพท์ รหัสผ่านเข้าเฟส
2. ไม่ส่งหลักฐานส่วนตัวของตนเองและคนในครอบครัวให้ผู้อื่น เช่น สำเนาบัตรประชาชน เอกสารต่างๆ รวมถึงรหัสบัตรต่างๆ เช่น เอทีเอ็ม บัตรเครดิต ฯลฯ
3. ไม่ควรโอนเงินให้ใครอย่างเด็ดขาด ต้องตรวจสอบก่อนการโอนเงินทุกครั้ง
4. ไม่ออกไปพบเพื่อนที่รู้จักทางอินเทอร์เน็ต เว้นเสียแต่ว่าได้รับอนุญาตจากพ่อแม่ผู้ปกครอง และควรมีผู้ใหญ่หรือเพื่อนไปด้วยหลายๆ คน เพื่อป้องกันการลักพาตัว หรือการกระทำมิดีมิร้ายต่างๆ
5. ระมัดระวังการซื้อสินค้าทางอินเทอร์เน็ต รวมถึงคำโฆษณาชวนเชื่ออื่นๆ เด็กต้องปรึกษาพ่อแม่ผู้ปกครอง โดยต้องใช้วิจารณญาณ พิจารณาความน่าเชื่อถือของผู้ขาย
6. จัดการกับอีเมล์ขยะ เพื่อแยกแยะประเภทของอีเมล์ เราจึงต้องทำความเข้าใจ และเรียนรู้ที่จะคัดกรองจดหมายอิเล็กทรอนิกส์ด้วยตัวเอง เพื่อกันไม่ให้มาปะปนกับจดหมายดีๆ เพราะอาจมีไวรัสแอบแฝงมา
7. จัดการกับไวรัสคอมพิวเตอร์คอมพิวเตอร์ทุกเครื่องจำเป็นต้องมีโปรแกรมสแกนดักจับและฆ่าไวรัส เนื่องจากไวรัสพัฒนาเร็วมาก ต้องอัพเดทโปรแกรมจำกัดไวรัสบ่อยๆ
8. ไม่บันทึกชื่อผู้ใช้และรหัสผ่านขณะใช้เครื่องคอมพิวเตอร์สาธารณะ
9. ไม่ควรแชร์และสนับสนุนข้อมูลที่ไม่เหมาะสม เช่น การโพสเครื่องดื่มแอลกอฮอล์ การแชร์ข้อมูลก่อให้เกิดความแตกแยกในสังคมเพจปลอม ข้อมูลที่หยาบคาย
10. ไม่ควรบันทึกภาพวิดีโอ หรือเสียงที่ไมเหมาะสมบนคอมพิวเตอร์ หรือบนมือถือเพราะภาพ เสียง หรือวีดีโอนั้นๆ รั่วไหลได้
11. ไม่แชร์เรื่องราวหรือข่าวสารที่ไม่เป็นความจริง “ชัวร์ก่อนแชร์”

การรักษาความปลอดภัยข้อมูลและสารสนเทศมีความสำคัญ ผู้ดูแลระบบจะต้องความตระหนักถึงการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Data Confidentiality) ข้อมูลถูกเก็บเป็นความลับ (Data

Integrity) และข้อมูลมีความถูกต้องและน่าเชื่อถือ (System Availability) ด้วยประโยชน์ที่หลากหลายของการเข้าถึงได้ทุกที่ ทุกเวลา บนเครือข่ายอินเทอร์เน็ต สิ่งที่ต้องพึงระวังคือ ภัยคุกคามที่มีผลกระทบต่อความปลอดภัยในชีวิตและทรัพย์สิน ของบุคคลและหน่วยงาน ทั้งในรูปแบบการโจรกรรมข้อมูลส่วนบุคคลอันเป็นความลับ

ภัยคุกคาม (Threat) คือ วัตถุ สิ่งของ ตัวบุคคล หรือสิ่งอื่นใดที่เป็นตัวแทนของการกระทำอันตรายต่อทรัพย์สินขององค์กร หรือสิ่งที่อาจจะก่อให้เกิดเสียหายต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน (ความลับ (Confidentiality), ความสมบูรณ์ (Integrity), ความพร้อมใช้ (Availability))ภัยคุกคามที่ถูกทำให้เกิดขึ้นโดยเจตนา ได้แก่ ภัยคุกคามที่ถูกทำให้เกิดขึ้นโดยไม่เจตนา ภัยคุกคามที่เกิดจากภัยธรรมชาติ และภัยคุกคามที่เกิดจากผู้ใช้ในองค์กรเอง มีรูปแบบภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ดังนี้

1. การโจมตี (Attack) คือการกระทำบางอย่างที่อาศัยความได้เปรียบจากช่องโหว่ของระบบ โดยมีจุดมุ่งหมายเพื่อเข้าควบคุมการทำงานของระบบทำให้ระบบเกิดความเสียหาย โจรกรรมสารสนเทศ เช่น Malicious Code หรือ Malmare, Virus, Worm, Trojan, Spyware, Backdoor, Rootkit, Denial-of-Service (Dos), Spam

2. การดักรับข้อมูล เป็นรูปแบบการโจมตีโดยการตั้งชื่อ Wireless Network หรือที่เรียกว่า SSID ให้มีชื่อเหมือนกับ Network เดิมที่มีอยู่ เช่น ICT Free Wi-Fi แล้วแฮกเกอร์จะสามารถเห็นข้อมูลที่รับส่งกัน

การป้องกันภัยคุกคาม ควรปฏิบัติ ดังนี้

1. หลีกเลี่ยงการใช้งาน Free Wi-Fi ในพื้นที่สาธารณะ

2. หากจำเป็นต้องใช้งาน Free Wi-Fi ให้ใช้งานเฉพาะจำเป็น ไม่ควรเข้าถึงระบบที่มีความสำคัญ เช่น ระบบ e-Banking ระบบอีเมลล์

3. พิจารณาการใช้งานระบบที่มีความสำคัญที่มีการเข้ารหัสลับ เช่น เว็บไซต์ที่มีการใช้งาน https

4. ไม่ใช้ Password ที่คาดเดาได้ง่าย เช่น คำที่มีใน Dictionary

5. ใช้การผสมอักขระที่ซับซ้อน

6. เปลี่ยน Password อย่างสม่ำเสมอ เมื่อถึงเวลาที่เหมาะสม เช่น ทุกๆ 90 วัน

7. ตั้ง Password ซึ่งผสมอักษรภาษาอังกฤษตัวเล็ก อักษรภาษาอังกฤษตัวใหญ่ ตัวเล็ก และตัวอักขระพิเศษ

การใช้เทคโนโลยีสารสนเทศอย่างมีความรับผิดชอบ

การใช้เทคโนโลยีสารสนเทศนั้นผู้ใช้งานจะต้องคำนึงถึงผลกระทบที่จะตามมา ต้องรับผิดชอบในการใช้เทคโนโลยีสารสนเทศ ดังนี้

1. เทคโนโลยีสารสนเทศกับความรับผิดชอบต่อสังคม

1.1 ความรับผิดชอบต่อสังคมระดับบุคคล

- ใช้เทคโนโลยีสารสนเทศอย่างมีจริยธรรมและถูกต้องตามกฎหมาย
- ใช้เทคโนโลยีสารสนเทศอย่างสร้างสรรค์และเป็นมิตรที่ดีกับคนอื่น
- ใช้เทคโนโลยีสารสนเทศเพื่อก่อให้เกิดความรักสามัคคีในหมู่คณะ
- ใช้เทคโนโลยีสารสนเทศเพื่อสร้างกิจกรรมทางสังคมที่เป็นประโยชน์
- ใช้เทคโนโลยีสารสนเทศที่เป็นมิตรกับสิ่งแวดล้อมรักษาสิ่งแวดล้อมและคำนึงถึงการประหยัดพลังงาน

1.2 ความรับผิดชอบต่อสังคมระดับองค์กร (Corporate Social Responsibility: CSR) หมายถึง การดำเนินธุรกิจควบคู่ไปกับการใส่ใจดูแลรักษาสิ่งแวดล้อมในชุมชนและสังคมภายใต้หลักจริยธรรม

การกำกับดูแลที่ดี (good governance) เพื่อนำไปสู่การดำเนินธุรกิจที่ประสบความสำเร็จอย่างยั่งยืนในการดำเนินธุรกิจอย่างมีความรับผิดชอบต่อสังคมนั้น

2. เทคโนโลยีสารสนเทศกับสิ่งแวดล้อม

2.1 เป้าหมายของกรีนไอที

- การออกแบบจากแหล่งกำเนิดไปยังแหล่งกำเนิดการใช้งานของสิ่งต่างๆก็จะเป็นวัฏจักรของผลิตภัณฑ์โดยการสร้างผลิตภัณฑ์ให้สามารถนำกลับมาใช้งานใหม่ได้ (recycle)
- การลดข้อมูลเป็นการลดทิ้งและมลพิษโดยการเปลี่ยนรูปแบบของการนำไปสร้างผลิตภัณฑ์และการบริโภค
- พัฒนาสิ่งใหม่ๆ เป็นการพัฒนาเพื่อเทคโนโลยีไม่ว่าจะเป็นการนำซากสัตว์มาเป็น
- ความสามารถในการดำรงชีวิตสร้างศูนย์กลางทางด้านเศรษฐศาสตร์ให้เหมาะสมกับเทคโนโลยีและผลิตภัณฑ์
- พลังงานต้องรับรู้ข่าวสารทางด้านเทคโนโลยีสีเขียวรวมไปถึงการพัฒนาของเชื้อเพลิง
- สภาพสิ่งแวดล้อมนำไปสู่การค้นหาสำหรับผลิตภัณฑ์ใหม่เพื่อค้นหาสิ่งที่บรรลุและวิธีที่ทำให้เกิดการกระทบกับสภาพแวดล้อมน้อยที่สุด

3. สภาพแวดล้อมที่ได้รับผลกระทบจากการใช้งานระบบไอที

เครื่องคอมพิวเตอร์ที่ใช้งานอยู่นี้ก่อให้เกิดปัญหาต่อสภาพแวดล้อม แต่พอเครื่องคอมพิวเตอร์หมดอายุการใช้งานกลายเป็น “ขยะอิเล็กทรอนิกส์” ซึ่งอุปกรณ์บางอย่างก็ไม่สามารถย่อยสลายได้

การสร้างและแสดงสิทธิความเป็นเจ้าของผลงาน

ลิขสิทธิ์ (Copyright)

ลิขสิทธิ์ หมายถึง สิทธิแต่เพียงผู้เดียวที่จะกระทำการใด ๆ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ริเริ่มโดยการใช้สติปัญญาความรู้ ความสามารถ และความวิริยะอุตสาหะของตนเองในการสร้างสรรค์ โดยไม่ลอกเลียนงานของผู้อื่น โดยงานที่สร้างสรรค์ต้องเป็นงานตามประเภทที่กฎหมายลิขสิทธิ์ให้คุ้มครอง โดยผู้สร้างสรรค์จะได้รับความคุ้มครองทันทีที่สร้างสรรค์โดยไม่ต้องจดทะเบียนการแจ้งข้อมูลลิขสิทธิ์ต่อกรมทรัพย์สินทางปัญญา มิได้เป็นการรับรองสิทธิ์ของเจ้าของลิขสิทธิ์แต่อย่างใด แต่เป็นเพียงการแจ้งต่อหน่วยงานราชการว่าตนเองเป็นเจ้าของสิทธิ์ในผลงานลิขสิทธิ์ที่แจ้งไว้เท่านั้น โดยผู้แจ้งต้องรับรองตนเองว่าเป็นเจ้าของผลงานที่นำมาแจ้งข้อมูลลิขสิทธิ์และหนังสือรับรองที่กรมทรัพย์สินทางปัญญาออกให้ ก็มิได้รับรองว่าผู้แจ้งเป็นเจ้าของงานลิขสิทธิ์แต่อย่างใด หากมีข้อโต้แย้งเกี่ยวกับความเป็นเจ้าของลิขสิทธิ์ ผู้แจ้งจำเป็นต้องพิสูจน์ความเป็นเจ้าของลิขสิทธิ์นั้นเอง ลิขสิทธิ์ให้ความคุ้มครองแก่งานสร้างสรรค์ 9 ประเภทตามที่กฎหมายกำหนด ได้แก่

1. งานวรรณกรรม เช่น หนังสือ จุลสาร สิ่งเขียน สิ่งพิมพ์ คำปราศรัย โปรแกรมคอมพิวเตอร์
2. งานนาฏกรรม เช่น งานที่เกี่ยวกับการรำ การเต้น การทำท่า หรือการแสดงประกอบขึ้นเป็นเรื่องราว รวมถึงการแสดงโดยวิธีใบ้ด้วย
3. งานศิลปกรรม เช่น งานจิตรกรรม งานประติมากรรม ภาพพิมพ์ งานสถาปัตยกรรม ภาพถ่าย ภาพประกอบ หรืองานสร้างสรรค์รูปทรงสามมิติเกี่ยวกับภูมิประเทศ หรือวิทยาศาสตร์ งานศิลปะประยุกต์ ซึ่งรวมถึงภาพถ่ายและแผนผังของงานดังกล่าวด้วย
4. งานดนตรีกรรม เช่น คำร้อง ทำนอง การเรียบเรียงเสียงประสานรวมถึงโน้ตเพลงที่แยกและเรียบเรียงเสียงประสานแล้ว
5. งานสิ่งบันทึกเสียง เช่น เทปเพลง แผ่นคอมแพ็คดิสก์ (ซีดี) ที่บันทึกข้อมูลเสียง ทั้งนี้ไม่รวมถึงเสียงประกอบภาพยนตร์ หรือเสียงประกอบโสตทัศนวัสดุอย่างอื่น

6. งานโสตทัศนวัสดุ เช่น วีดีโอเทป วีซีดี ดีวีดี แผ่นเลเซอร์ดิสก์ที่บันทึกข้อมูลประกอบด้วยลำดับของภาพหรือภาพและเสียงอันสามารถที่จะนำมาเล่นซ้ำได้อีก

7. งานภาพยนตร์ เช่น ภาพยนตร์ รวมทั้งเสียงประกอบของภาพยนตร์นั้นด้วย (ถ้ามี)

8. งานแพร่เสียงแพร่ภาพ เช่น การกระจายเสียงวิทยุ การแพร่เสียง หรือภาพทางโทรทัศน์

9. งานอื่นใดในแผนกวรรณคดี แผนกวิทยาศาสตร์ หรือแผนกศิลปะ

นอกจากผลงานที่กล่าวมาข้างต้น ยังมีอีกหลายอย่างที่เป็นผลงานที่ไม่ถือว่าเป็นลิขสิทธิ์ มีดังนี้

1. ข่าวประจำวันและข้อเท็จจริงต่างๆ ที่มีลักษณะเป็นเพียงข่าวสาร เช่น วัน เวลา สถานที่ ชื่อบุคคล จำนวนคน ปริมาณ เป็นต้น ทั้งนี้ หากมีการนำข้อมูลดังกล่าวมาเรียบเรียงจนมีลักษณะเป็นงานวรรณกรรม อาทิ การวิเคราะห์ข่าว บทความ ผลงานนั้นอาจจะได้รับความคุ้มครองในลักษณะของงานวรรณกรรม

2. รัฐธรรมนูญ และกฎหมาย

3. ระเบียบ ข้อบังคับ ประกาศ คำสั่ง คำชี้แจง และหนังสือโต้ตอบของกระทรวง ทบวง กรม หรือหน่วยงานอื่นใดของรัฐหรือของท้องถิ่น

4. คำพิพากษา คำสั่ง คำวินิจฉัย และรายงานของทางราชการ

5. คำแปลและการรวบรวมสิ่งต่างๆ ตามข้อ 3.1 - 3.4 ซึ่งกระทรวง ทบวง กรม หรือหน่วยงานอื่นใดของรัฐหรือของท้องถิ่นจัดทำขึ้น

6. ความคิด ขั้นตอน กรรมวิธี ระบบ วิธีใช้หรือทำงาน แนวความคิด หลักการ การค้นพบ หรือทฤษฎีทางวิทยาศาสตร์ หรือคณิตศาสตร์

การแจ้งข้อมูลลิขสิทธิ์ เอกสารที่ใช้ประกอบการแจ้งข้อมูลลิขสิทธิ์

1. สำเนาบัตรประชาชน พร้อมรับรองสำเนาถูกต้อง (กรณีเป็นบุคคลธรรมดา)

2. สำเนาหนังสือรับรองนิติบุคคล ที่นายทะเบียนออกให้ไม่เกิน 6 เดือน ของเจ้าของลิขสิทธิ์ (กรณีเป็นนิติบุคคล)

3. ผลงานหรือภาพถ่ายงานลิขสิทธิ์ จำนวน 1 ชุด

4. หนังสือมอบอำนาจติดอากรแสตมป์ 30 บาท พร้อมสำเนาบัตรประชาชนของผู้รับมอบอำนาจ (รับรองสำเนาถูกต้อง)

5. หน่วยงานหรือองค์กรของรัฐบาลใช้สำเนาหนังสือแต่งตั้งผู้บริหารหน่วยงานหรือองค์กรฯ รวมทั้งสำเนาบัตรประชาชนของผู้ยื่นคำขอ (รับรองสำเนาถูกต้อง)

การกำหนดสิทธิ์การใช้ข้อมูล

การใช้งานเทคโนโลยีสารสนเทศ จะต้องมีการรักษาความปลอดภัย มีวัฒนาการของมาตรการรักษาความปลอดภัยของข้อมูล ดังนี้

1. การรักษาความปลอดภัยด้านกายภาพ (Physical Security) ในอดีตข้อมูลที่สำคัญจะอยู่ในรูปแบบวัตถุโดยจะถูกบันทึกไว้บนแผ่นหินแผ่นหนังหรือกระดาษแต่บุคคลสำคัญส่วนใหญ่ไม่นิยมบันทึกข้อมูลที่สำคัญมากๆ ลงบนสื่อถาวรและไม่สนทนาเกี่ยวกับข้อมูลกับคนที่ไม่ไว้ใจ ถ้าต้องส่งข้อมูลไปที่อื่นต้องมีผู้คุ้มกันติดตามไปด้วยเพราะภัยอันตรายจะอยู่ในรูปแบบทางกายภาพ เช่น การขโมย

2. การรักษาความปลอดภัยด้านการสื่อสาร (Communication Security) การรักษาความปลอดภัยด้านการสื่อสารถูกพัฒนามาอย่างต่อเนื่อง โดยเฉพาะในช่วงสงครามที่ข้อมูลข่าวสารเป็นปัจจัยสำคัญของชัยชนะ เช่น ยุคของจูเลียสซีซาร์ (ยุคศตวรรษที่ 2) มีการคิดค้นวิธีใช้สำหรับ “ซ่อน” ข้อมูลหรือการเข้ารหัสข้อมูล (Encryption) เรียกว่า รหัสซีซาร์ (Caesar cipher) ซึ่งจัดเป็นวิธีเข้ารหัสที่ง่ายและแพร่หลายที่สุด โดยใช้หลักการแทนที่ตัวอักษร โดยตัวอักษรในข้อความต้นฉบับแต่ละตัวจะถูกแทนด้วยตัวอักษรที่อยู่ใน

ลำดับถัดไปตามจำนวนที่แน่นอน เช่น ถ้าเข้ารหัสโดยเลื่อนไป 3 ตัวอักษร ตัวอักษร B ในต้นฉบับก็จะถูกแทนด้วยตัวอักษร E เป็นต้น

3. การรักษาความปลอดภัยการแผ่รังสี (Emissions Security) ในช่วงทศวรรษ 1950 มีการค้นพบว่าอุปกรณ์และสายสัญญาณที่ใช้ในการรับส่งข้อมูลนั้นมีการแผ่รังสีออกมา และสามารถใช้อุปกรณ์ตรวจจับและแปลงกลับมาเป็นข้อมูลได้ จึงมีการกำหนดมาตรฐานเกี่ยวกับการแผ่รังสีชื่อ เทมเพสต์(Tempest : Transient Electromagnetic Pulse Emanations Standard) ควบคุมการแผ่รังสีของอุปกรณ์คอมพิวเตอร์เพื่อลดการแผ่รังสีที่อาจถูกใช้ในการดักจับข้อมูลได้

4. การรักษาความปลอดภัยคอมพิวเตอร์(Computer Security) ช่วงทศวรรษ 1970 มีการพัฒนาแม่แบบสำหรับการรักษาความปลอดภัยของคอมพิวเตอร์ ซึ่งจะแบ่งระดับความปลอดภัยออกเป็น 4 ชั้นคือ ไม่ลับ ลับ ลับมาก และลับที่สุด ผู้ที่สามารถเข้าถึงข้อมูลในระดับใดระดับหนึ่งได้จะต้องมีสิทธิ์เท่ากับหรือสูงกว่าชั้นความลับของข้อมูลนั้น ดังนั้นผู้ที่มีสิทธิ์น้อยกว่าชั้นความลับของไฟล์จะไม่สามารถเข้าถึงไฟล์นั้นได้ แนวคิดนี้ได้ถูกนำไปใช้ในกระทรวงกลาโหมของสหรัฐอเมริกาโดยได้ชื่อว่ามาตรฐาน 5200.28 หรือ ออเรนจ์บุ๊ค (Orange Book) ซึ่งได้กำหนดระดับความปลอดภัยของคอมพิวเตอร์ออกเป็นระดับต่างๆ คือ D, C1, C2, B1, B2, B3, A1 ในแต่ระดับออเรนจ์บุ๊คได้กำหนดฟังก์ชันต่างๆ ที่ระบบต้องมี ระบบที่ต้องการใบรับรองว่าจัดอยู่ในระดับใดระบบนั้นต้องมีทั้งฟังก์ชันต่างๆ ที่กำหนดในระดับนั้นๆ

5. การรักษาความปลอดภัยเครือข่าย (Network Security) เมื่อคอมพิวเตอร์เชื่อมต่อกันเข้าเป็นเครือข่าย ปัญหาใหม่ก็เกิดขึ้น เช่น การสื่อสารคอมพิวเตอร์เปลี่ยนจาก WAN มาเป็น LAN ซึ่งมีแบนด์วิธที่สูงมากอาจมีหลายเครื่องที่เชื่อมต่อเข้ากับสื่อเดียวกัน การเข้ารหัสโดยใช้เครื่องเข้ารหัสเดี่ยวๆ อาจไม่ได้ผลในปี1987 จึงได้มีการใช้มาตรฐาน TNI หรือเรดบุ๊ค (Red Book) ซึ่งได้เพิ่มส่วนที่เกี่ยวข้องกับเครือข่ายเข้าไป

6. การรักษาความปลอดภัยข้อมูล (Information Security) อาจกล่าวได้ว่าไม่มีวิธีการใดที่สามารถแก้ปัญหาเกี่ยวกับการรักษาความปลอดภัยได้ทั้งหมด ความปลอดภัยที่ดีต้องใช้ทุกวิธีการที่กล่าวมาร่วมกัน จึงจะสามารถให้บริการการรักษาความปลอดภัยข้อมูลได้ จึงต้องมีการกำหนดสิทธิ์การเข้าใช้งานของแต่ละบุคคลเพื่อความปลอดภัยของข้อมูล เช่น กำหนดสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานที่ให้สามารถดูได้แต่ไม่สามารถแก้ไขได้

อ้างอิง :

https://sites.google.com/a/msts.ac.th/kittithat/contact/social-network/kar-chi-thekhnoloyi-dicithal-thi-plxdphay-laea-kd-ktika-maryath-ni-kar-chi-thekhnoloyi-dicithal

http://www.ecpat-thailand.org/th/make%20it%20safe.html

http://thedctmike.blogspot.com/2013/01/technology-lesson-10_22.html

http://tuipi.tu.ac.th/tuip02.php

https://www.ipthailand.go.th/th/copyright-001.html

https://sites.google.com/site/ges0503chiwitkabthekhnoloyi/bth-thi-5-khwam-mankhng-plxdphay-khxng-rabb-sarsnthes/3-prawati-khxng-kar-raksa-khwam-plxdphay-khxng-khxmul

http://www.erp.mju.ac.th/acticleDetail.aspx?qid=549