จริยธรรมและความปลอดภัย

เทคโนโลยีสารสนเทศมีผลกระทบต่อสังคมเป็นอย่างมาก โดยเฉพาะประเด็นจริยธรรมที่เกี่ยวกับระบบสารสนเทศที่จำเป็นต้องพิจารณารวมทั้งเรื่องความปลอดภัยของระบบสารสนเทศการใช้เทคโนโลยีสารสนเทศหากไม่มีกรอบจริยธรรมกำกับไว้แล้ว สังคมย่อมจะเกิดปัญหาต่าง ๆ ตามมาไม่สิ้นสุด รวมทั้งปัญหาอาชญากรรมคอมพิวเตอร์ด้วย ดังนั้นหน่วยงานที่ใช้ระบบสารสนเทศจึงจำเป็นต้องสร้างระบบความปลอดภัยเพื่อป้องกันปัญหาดังกล่าว

ประเด็นเกี่ยวกับจริยธรรม

คำจำกัดความของจริยธรรมมีอยู่มากมาย เช่น “หลักของศีลธรรมใ นแต่ละวิชาชีพเฉพาะ” “มาตรฐานของการประพฤติปฏิบัติในวิชาชีพที่ได้รับ” “ข้อตกลงกันในหมู่ประชาชนในการกระทำสิ่งที่ถูกและหลีกเลี่ยงการกระทำสิ่งที่ผิด” หรืออาจสรุปได้ว่า จริยธรรม (Ethics) หมายถึง หลักของความถูกและความผิดที่บุคคลใช้เป็นแนวทางในการปฏิบัติ (Laudon & Laudon, 1999:105)

กรอบความคิดเรื่องจริยธรรม

หลักปรัชญาเกี่ยวกับจริยธรรม มีดังนี้ (Laudon & Laudon, 1999)

R.O. Mason และคณะ ได้จำแนกประเด็นเกี่ยวกับจริยธรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเป็น 4 ประเภทคือ ความเป็นส่วนตัว (Privacy) ความถูกต้องแม่นยำ (Accuracy) ความเป็นเจ้าของ (Property) และความสามารถในการเข้าถึงได้ (Accessibility) (O’Brien, 1999: 675; Turban, et al., 2001: 512)

1) ประเด็นความเป็นส่วนตัว (Privacy) คือ การเก็บรวบรวม การเก็บรักษา และการเผยแพร่ข้อมูลสารสนเทศเกี่ยวกับปัจเจกบุคคล

2) ประเด็นความถูกต้องแม่นยำ (Accuracy) ได้แก่ ความถูกต้องแม่นยำของการเก็บรวบรวมและวิธีการปฏิบัติกับข้อมูลสารสนเทศ

3) ประเด็นของความเป็นเจ้าของ (Property) คือ กรรมสิทธิ์และมูลค่าของข้อมูลสารสนเทศ (ทรัพย์สินทางปัญญา)

4) ประเด็นของความเข้าถึงได้ (Accessibility) คือ สิทธิในการเข้าถึงข้อมูลสารสนเทศได้และการจ่ายค่าธรรมเนียมในการเข้าถึงข้อมูลสารสนเทศ

การคุ้มครองความเป็นส่วนตัว (Privacy)

- ความเป็นส่วนตัวของบุคคลต้องได้ดุลกับความต้องการของสังคม
- สิทธิของสาธารณชนอยู่เหนือสิทธิความเป็นส่วนตัวของปัจเจกชน

การคุ้มครองทางทรัพย์สินทางปัญญา

ทรัพย์สินทางปัญญาเป็นทรัพย์สินที่จับต้องไม่ได้ที่สร้างสรรค์ขึ้นโดยปัจเจกชน หรือนิติบุคคล ซึ่งอยู่ภายใต้ความคุ้มครองของกฎหมายลิขสิทธิ์ กฎหมายความลับทางการค้า และกฎหมายสิทธิบัตร

ลิขสิทธิ์ (copyright) ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 หมายถึง สิทธิ์แต่ผู้เดียวที่จะกระทำการใด ๆ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น ซึ่งเป็นสิทธิ์ในการป้องกันการคัดลอกหรือทำซ้ำในงานเขียน งานศิลป์ หรืองานด้านศิลปะอื่น ตามพระราชบัญญัติดังกล่าวลิขสิทธิ์ทั่วไปมีอายุห้าสิบปีนับแต่งานได้สร้างสรรค์ขึ้น หรือนับแต่ได้มีการโฆษณาเป็นครั้งแรกในขณะที่ประเทศสหรัฐอเมริกาจะมีอายุเพียง 28 ปี

สิทธิบัตร (patent) ตามพระราชบัญญัติสิทธิบัตร พ.ศ. 2522 หมายถึง หนังสือสำคัญที่ออกให้เพื่อคุ้มครองการประดิษฐ์ หรือการออกแบบผลิตภัณฑ์ ตามที่กฎหมายบัญญัติไว้ โดยสิทธิบัตรการประดิษฐ์มีอายุยี่สิบปีนับแต่วันขอรับสิทธิบัตร ในขณะที่ประเทศสหรัฐอเมริกาจะคุ้มครองเพียง 17 ปี

อาชญากรรมคอมพิวเตอร์ (Computer Crime)

อาชญากรรมคอมพิวเตอร์อาศัยความรู้ในการใช้เครื่องมือคอมพิวเตอร์หรืออุปกรณ์อื่น โดยสามารถทำให้เกิดความเสียหายด้านทรัพย์สินเงินทองจำนวนมหาศาลมากกว่าการปล้นธนาคารเสียอีก นอกจากนี้อาชญากรรมประเภทนี้ยากที่จะป้องกัน และบางครั้งผู้ได้รับความเสียหายอาจจะไม่รู้ตัวด้วยซ้ำ

- เครื่องคอมพิวเตอร์ในฐานะเป็นเครื่องประกอบอาชญากรรม
- เครื่องคอมพิวเตอร์ในฐานะเป็นเป้าหมายของอาชญากรรม
- การเข้าถึงและการใช้คอมพิวเตอร์ที่ไม่ถูกกฎหมาย
- การเปลี่ยนแปลงและการทำลายข้อมูล
- การขโมยข้อมูลข่าวสารและเครื่องมือ
- การสแกมทางคอมพิวเตอร์ (computer-related scams)

การรักษาความปลอดภัยของระบบคอมพิวเตอร์

การควบคุมที่มีประสิทธิผลจะทำให้ระบบสารสนเทศมีความปลอดภัยและยังช่วยลดข้อผิดพลาด การฉ้อฉล และการทำลายระบบสารสนเทศที่มีการเชื่อมโยงเป็นระบบอินเทอร์เน็ตด้วย

ระบบการควบคุมที่สำคัญมี 3 ประการ คือ การควบคุมระบบสารสนเทศ การควบคุมกระบวนการทำงาน และการควบคุมอุปกรณ์อำนวยความสะดวก (O'Brien, 1999: 656)

การควบคุมระบบสารสนเทศ (Information System Controls)

- การควบคุมอินพุท
- การควบคุมการประมวลผล
- การควบฮาร์ดแวร์ (Hardware Controls)
- การควบคุมซอฟท์แวร์ (Software Controls)
- การควบคุมเอาท์พุท (Output Controls)
- การควบคุมความจำสำรอง (Storage Controls)

การควบคุมกระบวนการทำงาน (Procedural Controls)

- การมีการทำงานที่เป็นมาตรฐาน และมีคู่มือ
- การอนุมัติเพื่อพัฒนาระบบ
- แผนการป้องกันการเสียหาย
- ระบบการตรวจสอบระบบสารสนเทศ (Auditing Information Systems)

การควบคุมอุปกรณ์อำนวยความสะดวกอื่น (Facility Controls)

- ความปลอดภัยทางเครือข่าย (Network Security)
- การแปลงรหัส (Encryption)
- กำแพงไฟ (Fire Walls)
- การป้องกันทางกายภาพ (Physical Protection Controls)
- การควบคุมด้านชีวภาพ (Biometric Control)
- การควบคุมความล้มเหลวของระบบ (Computer Failure Controls)