Chapter 8

จริยธรรมและความปลอดภัย

2

บทนี้มีอะไรบ้าง ?

8.1 ความหมายของจริยธรรม

8.2 กรอบความคิดเรื่องจริยธรรม

8.3 การคุ้มครองความเป็นส่วนตัว

8.4 การคุ้มครองทางทรัพย์สินทางปัญญา

8.5 อาชญากรรมคอมพิวเตอร์ (Computer Crime)

8.6 การรักษาความปลอดภัยของระบบคอมพิวเตอร์

3

8.1 ความหมายของจริยธรรม

คำจำกัดความของจริยธรรมมีอยู่มากมาย เช่น

"หลักของศีลธรรมในแต่ละวิชาชีพเฉพาะ"

"มาตรฐานของการประพฤติ ปฏิบัติในวิชาชีพที่ได้รับ"

"ข้อตกลงกันในหมู่ประชาชนในการกระทำสิ่งที่ถูก และหลีกเลี่ยงการกระทำที่ผิด"

สรุป

จริยธรรม (Ethics) คือ หลักของความถูกและผิด ที่บุคคลใช้เป็นแนวทางในการปฏิบัติ

4

8.2 กรอบความคิดเรื่องจริยธรรม

หลักปรัชญาเกี่ยวกับจริยธรรม มีดังนี้

1. ปฏิบัติต่อคนอื่นเหมือนอย่างที่ต้องการให้ผู้อื่นปฏิบัติต่อตน
2. ถ้าการกระทำอย่างหนึ่งไม่เหมาะที่ทุกคนจะปฏิบัติ ดังนั้น การกระทำดังกล่าว ก็ไม่เหมาะที่คนใดคนหนึ่งจะปฏิบัติด้วย
3. ถ้าการกระทำใดไม่พึงปฏิบัติซ้ำ ๆ กันหลายครั้ง การกระทำนั้น ก็ไม่ควรนำมาปฏิบัติเลยแม้แต่ครั้งเดียว
4. ถ้าสิ่งใดสิ่งหนึ่งที่สร้างขึ้นโดยคนอื่นและมีประโยชน์ต่อคนใดคนหนึ่ง คนๆ นั้นพึงให้คุณค่าและผลตอบแทนแก่ผู้ที่คิดค้นหรือสร้างขึ้นมา

5

8.2 กรอบความคิดเรื่องจริยธรรม

R.O. Mason และคณะ (2001) ได้จำแนกประเด็นเกี่ยวข้องกับเทคโนโลยีสารสนเทศเป็น 4 ประเภท คือ

1. ประเด็นความเป็นส่วนตัว (Privacy)
2. ประเด็นความถูกต้องแม่นยำ (Accuracy)
3. ประเด็นของความเป็นเจ้าของ (Property)
4. ประเด็นของความเข้าถึงได้ของข้อมูล (Accessibility)

8.3 การคุ้มครองความเป็นส่วนตัว

ความเป็นส่วนตัวคือสิทธิที่อยู่ตามลำพังและสิทธิที่เป็นอิสระจากการถูกรบกวนโดยไม่มีเหตุอันควร ความเป็นส่วนตัวของข้อมูลสารสนเทศ คือ สิทธิในการตัดสินใจว่าเมื่อใดข้อมูลสารสนเทศของบุคคลหนึ่ง จะสามารถเปิดเผยให้กับผู้อื่นได้ และภายใต้ขอบเขตอย่างไร

8.3 การคุ้มครองความเป็นส่วนตัว

แนวทางการพัฒนาคุ้มครองความเป็นส่วนตัว

ความถูกต้องแม่นยำของข้อมูล

- ข้อมูลส่วนตัว ควรจะได้รับการตรวจสอบก่อนจะนำเข้าสู่ฐานข้อมูล
- ข้อมูลควรมีความถูกต้องแม่นยำ และมีความทันสมัย
- แฟ้มข้อมูลควรทำให้บุคคลสามารถเข้าถึง (ข้อมูลของตน) และตรวจสอบความถูกต้องได้

8.3 การคุ้มครองความเป็นส่วนตัว

แนวทางการพัฒนาคุ้มครองความเป็นส่วนตัว

ความลับของข้อมูล

- ควรมีมาตรการป้องกันความปลอดภัยของข้อมูลบุคคล ไม่ว่าจะเป็นทางด้านเทคนิค และการบริหาร
- บุคคลที่สามไม่สมควรได้รับอนุญาตให้เข้าถึงข้อมูลโดยปราศจากการรับรู้หรืออนุญาตของเจ้าของ ยกเว้นโดยข้อกำหนดของกฎหมาย
- ข้อมูลไม่ควรถูกเปิดเผยด้วยเหตุผลที่ไม่ตรงกับวัตถุประสงค์ในการเก็บข้อมูล

8.4 การคุ้มครองทางทรัพย์สินทางปัญญา

ทรัพย์สินทางปัญญาเป็นทรัพย์สินที่จับต้องไม่ได้ ที่สร้างสรรค์ขึ้นโดยปัจเจกชน หรือนิติบุคคล ซึ่งอยู่ภายใต้ความคุ้มครองของกฎหมายลิขสิทธิ์ กฎหมายความลับทางการค้า และกฎหมายสิทธิบัตร

ลิขสิทธิ์ (Copyright) หมายถึง สิทธิ์แต่ผู้เดียวที่จะกระทำการใด ๆ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น ซึ่งเป็นสิทธิ์ในการป้องกันการคัดลอกหรือทำซ้ำในงานเขียน งานศิลป์ หรืองานด้านศิลปะอื่น ตามพระราชบัญญัติดังกล่าว**ลิขสิทธิ์ทั่วไปมีอายุห้าสิบปี** นับแต่งานได้สร้างสรรค์ขึ้น หรือนับแต่ได้มีการโฆษณาเป็นครั้งแรก

สิทธิ์บัตร (Patent) หมายถึง หนังสือสำคัญที่ออกให้เพื่อคุ้มครองการประดิษฐ์ หรือการออกแบบผลิตภัณฑ์ ตามที่กฎหมายกำหนดไว้ โดย**สิทธิบัตรมีอายุ 20 ปี** นับแต่วันขอรับสิทธิบัตร

8.5 อาชญากรรมคอมพิวเตอร์

ปัจจุบัน อาชญากรรมคอมพิวเตอร์มีความก้าวหน้าและพัฒนาไปมากโดยเฉพาะอย่างยิ่งระบบอินเทอร์เน็ต ทำให้อาชญากรรมคอมพิวเตอร์ระบาดไปทั่วโลก ซึ่งบางครั้งทำให้เกิดความเสียหายด้านทรัพย์สินเงินทองจำนวนมหาศาล

สำหรับเครื่องคอมพิวเตอร์ อาจจะเป็นไปได้ทั้ง

1. เครื่องคอมพิวเตอร์ในฐานะเป็นเครื่องประกอบอาชญากรรม คือ ใช้คอมพิวเตอร์เป็นเครื่องมือในการเข้าถึงข้อมูลข่าวสาร และทำลายระบบคอมพิวเตอร์อื่น

8.5 อาชญากรรมคอมพิวเตอร์

2. เครื่องคอมพิวเตอร์ในฐานะเป้าหมายของอาชญากรรม
   - 2.1 การเข้าถึงและการใช้คอมพิวเตอร์ที่ไม่ถูกกฎหมาย ซึ่งมีทั้ง Hacker และ Criminal Hacker (Cracker)
   - 2.2 การเปลี่ยนแปลงและทำลายข้อมูล โดย
     - ☑ virus : เป็นโปรแกรมที่ต้องทำงานร่วมกับโปรแกรมอื่น
     - ☑ worms : เป็นโปรแกรมอิสระที่สามารถจำลองโปรแกรมเองได้
   - 2.3 การขโมยข้อมูลข่าวสารและเครื่องมือ
   - 2.4 การหลอกลวงทางคอมพิวเตอร์ (Computer-related Scams)

8.6 การรักษาความปลอดภัยของระบบคอมพิวเตอร์

การรักษาความปลอดภัยให้ระบบสารสนเทศมีความปลอดภัย และยังช่วยลดข้อผิดพลาด การทำลายระบบสารสนเทศ มีระบบการควบคุมที่สำคัญ 3 ประการ คือ

1. การควบคุมระบบสารสนเทศ
2. การควบคุมกระบวนการทำงาน
3. การควบคุมอุปกรณ์อำนวยความสะดวก

8.6 การรักษาความปลอดภัยของระบบคอมพิวเตอร์

การควบคุมสารสนเทศ

- การควบคุมอินพุท
- การควบคุมการประมวลผล
- การควบคุมฮาร์ดแวร์
- การควบคุมซอร์ฟแวร์
- การควบคุมเอาท์พุท

8.6 การรักษาความปลอดภัยของระบบคอมพิวเตอร์

การควบคุมความจำสำรอง

- มอบหมายให้หน่วยงานอื่นรับผิดชอบข้อมูลขององค์การ
- การใช้รหัสผ่านในการเข้าถึงข้อมูล
- การสร้างแบ็คอัพไฟล์ข้อมูล

8.6 การรักษาความปลอดภัยของระบบคอมพิวเตอร์

การควบคุมกระบวนการทำงาน

- การมีการทำงานที่เป็นมาตรฐานและคู่มือ
- การอนุมัติเพื่อพัฒนาระบบ
- การมีแผนการป้องกันการเสียหาย
- การตรวจสอบระบบสารสนเทศ

8.6 การรักษาความปลอดภัยของระบบคอมพิวเตอร์

การควบคุมอุปกรณ์อำนวยความสะดวกอื่น

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