เอกสารประกอบการสอน สัปดาห์ที่ 3
เรื่อง จริยธรรมและความปลอดภัยของระบบคอมพิวเตอร์

สาระสำคัญ

เทคโนโลยีสารสนเทศเป็นเครื่องมือของการเรียนรู้ ขณะเดียวกันก็สามา รถส่งผลกระทบต่อสังคมได้เช่นกัน โดยเฉพาะประเด็นเกี่ยวกับจริยธรรมของการใช้ระบบสารสนเทศ รวมถึงความมั่นคงและความปลอดภัยของข้อมูล การใช้เทคโนโลยีสารสนเทศหากไม่มีกฎ ระเบียบ และกฎหมายควบคุมแล้ว ก็อาจก่อให้เกิดปัญหาต่อสังคมได้ ดังนั้นหน่วยงานที่ใช้ระบบสารสนเทศจึงจำเป็นที่จะต้องสร้างระบบป้องกัน ซึ่งผู้บริหารจะต้องมีความเข้าใจ ป้องกัน และหาแนวทางแก้ ไข นอกจากนี้หน่วยงานต่าง ๆ จะต้องร่วมมือกันกำหนดนโยบายเกี่ยวกับจริยธรรมการใช้สารสนเทศ

วัตถุประสงค์

เมื่อจบบทเรียนนี้แล้ว นักศึกษาสามารถ

1. มีจิตสำนึกในเรื่องของสิทธิ์การเข้าถึงข้อมูล
2. อธิบายประเภทและตัวเสี่ยงของอาชญากรรมคอมพิวเตอร์
3. บอกวิธีการป้องกันอาชญากรรมทางคอมพิวเตอร์
4. นำความรู้เกี่ยวกับจริยธรรมและความปลอดภัยไปใช้ในชีวิตประจำวัน

เนื้อหา

1. ความหมายของจริยธรรม

จริยธรรม หมายถึง หลักของความถูกต้องและความผิดที่บุคคลใช้เป็นแนวทางในการปฏิบัติ

2. ประเด็นทางจริยธรรม

ในระบบสารสนเทศคอมพิวเตอร์ แบ่งประเด็นจริยธรรมออกเป็น 4 ประเภท คือ

2.1 ความเป็นส่วนตัว (privacy)

2.2 ความถูกต้อง (accuracy)

2.3 ความเป็นเจ้าของ (property)

2.4 การเข้าถึงข้อมูล (accessibility)

3. <u>อาชญากรรมคอมพิวเตอร์</u>

เป็นการกระทำที่ผิดกฎหมายโดยการใช้คอมพิวเตอร์ หรือการทำลายระบบคอมพิวเตอร์ เช่น

3.1 การเข้าถึงและการใช้คอมพิวเตอร์ที่ผิดกฎหมาย ได้แก่ Hacker, Cracker

3.2 การเปลี่ยนแปลงและการทำลายข้อมูล เช่น ไวรัสคอมพิวเตอร์ เวิร์ม

3.3 การขโมยข้อมูล/ข่าวสาร

3.4 การสแกมทางคอมพิวเตอร์

4. <u>แนวทางปฏิบัติเพื่อป้องกันอาชญากรรมคอมพิวเตอร์</u>

- ควรระวังในการให้ข้อมูล
- การกำหนดรหัสผ่าน
- การติดตั้ง anti-virus
- การสำรองข้อมูล
- การจดลิขสิทธิ์และสิทธิบัตร

5. <u>ตัวอย่างของเทคโนโลยีในปัจจุบันที่ใช้ป้องกันอาชญากรรมคอมพิวเตอร์</u>