เอกสารประกอบการสอน
รหัสวิชา CPE5019
กฎหมายและจริยธรรมสำหรับวิศวกร
Law and Ethics for Engineers

โดย

ผศ.ดร.พรภวิษย์ บุญศรีเมือง

สาขาวิศวกรรมคอมพิวเตอร์
คณะเทคโนโลยีอุตสาหกรรมม
มหาวิทยาลัยราชภัฏสวนสุนันทา
Suan Sunandha Rajabhat University

บทนำและหลักการเบื้องต้น

การใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์จำเป็นจะต้องมีความตระหนักรู้ และมีความเข้าใจระบบการทำงานของหน่วยงานว่ามีระบบงานสารสนเทศและเครือข่ายที่สามารถเชื่อมต่ออินเทอร์เน็ต ทั้งภายในหน่วยงานและการเชื่อมต่อไปยังภายนอกองค์

1.ผู้เกี่ยวข้องในการให้บริการข้อมูล

2.ผู้ใช้บริการข้อมูล

3.การใช้งาน ระบบงาน การสื่อสารเชื่อมต่อทั้งในและต่างประเทศ

4.ภัยคุกคามที่อาจเกิดขึ้น แนวทางป้องกันหรือการสร้างความตระหนักที่พึงระวังการปฏิบัติตามข้อปฏิบัติ หรือกฎหมายที่เกี่ยวข้องจึงเป็นสิ่งจำเป็น

5. การบริหารจัดการเพื่อแก้ไขปัญหา การควบคุม เช่นการเข้าถึง การใช้งาน

เช่นเครื่องคอมพิวเตอร์ส่วนบุคคล การควบคุมการส่งข้อมูลข่าวสาร e-mail

การใช้เทคโนโลยีสารสนเทศ หมายถึง กระบวนการต่างๆ และระบบงานที่ช่วยให้ได้ สารสนเทศหรือข่าวสารที่ต้องการ โดยจะรวมถึง

1.เครื่องมือและอุปกรณต่าง ๆหมายถึงเครื่องคอมพิวเตอร์ เครื่องใช้สำนักงาน

อุปกรณค์มนาคมต่างๆรวมทั้งซอฟต์แวรทั้งระบบ สำเร็จรูปและพัฒนาขึ้นโดยเฉพาะด้าน

2.กระบวนการในการนำอุปกรณ์ครื่องมือต่างๆ ข้างต้นมาใช้งาน

รวบรวมข้อมูลจัดเก็บประมวลผลและแสดงผลลัพธ์รูปแบบต่างๆ ที่สามารถนำไปใช้ประโยชน์ได้ต่อไป

ในปัจจุบันการใช้งานเทคโนโลยีสารสนเทศเป็นสิ่งจำเป็นสาหรับทุกองค์กร การเชื่อมโยงสารสนเทศผ่านทางคอมพิวเตอร์ ทำให้สิ่งที่มีค่ามากที่สุดของระบบ คือ ข้อมูลและสารสนเทศ อาจถูกจารกรรม ถูกปรับเปลี่ยน ถูกเข้าถึงโดยเจ้าของไม่รู้ตัว ถูกปิดกั้นขัดขวางให้ไม่สามารถเข้าถึงข้อมูลได้ หรือถูกทำลายเสียหายไป ซึ่งสามารถ เกิดขึ้นได้ไม่ยากบนโลกของเครือข่าย ด้วยความล้ำสมัยของอุปกรณ์ที่มีความสามารถเชื่อมต่อผ่านแบบไร้สายได้

ปัจจุบันมีกฎหมายที่เกี่ยวข้องด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร

1. กฎหมายเกี่ยวกับการกระทาความผิดเกี่ยวกับ คอมพิวเตอร์ (Computer Crime Law) เพื่อกาหนด มาตรการทางอาญาในการลงโทษผู้กระทำผิดต่อระบบ การทำงานของคอมพิวเตอร์ ระบบข้อมูล และระบบ เครือข่าย ทั้งนี้เพื่อเป็นหลักประกันสิทธิเสรีภาพ และ การคุ้มครองการอยู่ร่วมกันของสังคมมนุษย์

2.กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions Law) เพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยกระดาษ อัน เป็นการรองรับนิติสัมพันธ์ต่าง ๆ ซึ่งแต่เดิมอาจจะจัดทาขึ้นในรูปแบบของหนังสือ ให้เท่าเทียมกับนิติสัมพันธ์รูปแบบใหม่ที่จัดทาขึ้นให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

3.กฎหมายอื่นๆที่เกี่ยวข้องเช่น

3.1 กฎหมายลิขสิทธิ์

3.2 กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบคุคล(Data Protection Law)

3.3 กฎหมายคุ้มครองผู้บริโภค

3.3 กฎหมายว่าด้วย การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศสาหรับองค์กร

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายความว่า

การดำรงไว้ซึ่งความลับ(Confidentiality) ความถูกต้อง (Integrity) และ สภาพพร้อมใช้งาน (Availability)ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความ ถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธ ความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

การรักษาความมั่นคงปลอดภัยของข้อมูล (Data security) หมายถึง การป้องกันข้อมูลในบริบทของ การรักษาความลับ บูรณภาพ และความพร้อมใช้งานของข้อมูล ซึ่งสามารถใช้แทน การรักษาความมั่นคงปลอดภัยของสารสนเทศได้

การปกป้องข้อมูล (Data protection) หมายถึงการป้องกันข้อมูลส่วนบุคคลต่อการ ประสงค์ร้ายของบุคคลที่สาม

เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง การเกิดเหตุการณ์ หรือสภาพของบริการ ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือ มาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคง ปลอดภัย

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

การควบคุมโดยการออกระเบียบหรือแนวทางปฏิบัติ

1. มีการประกาศใช้ แนวนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยขององค์กร การนำแนวนโยบายไปปฏิบัติ ออกมาเช่น การรักษาความมั่นคงปลอดภัย มีแนวทางการป้องกันทางด้านไซเบอร์ สร้างขั้นตอนปฏิบัติ

2. การจัดองค์กร และการรักษาความปลอดภัยสาหรับระบบสารสนเทศ

2.1.การจัดองค์การการวางโครงสร้างขององค์กรที่สามารถเอื้ออานวยให้แผนงานที่จัดทาขึ้นไปสู่สัมฤทธิ์ผล โดยกำหนดอานาจหน้าที่และความรับผิดชอบ ของกลุ่มบุคคลในองค์กร เพื่อให้งานเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ

2.2. การพัฒนาระบบงานควบคุมดูแลและปฏิบัติงานที่เกี่ยวกับเรื่อง ความมั่นคงปลอดภัย และการใช้งาน เครื่องมืออุปกรณ์ ในการสื่อสารข้อมูล

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทาธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. 2549 กาหนดให้หน่วยงานต้องจัดทาแนวนโยบายและแนวปฏิบัติใน การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

แนวทางและมาตรการที่จะต้องกาหนดใหเป็นไปตามข้อกฎหมาย

ควรให้ความสาคัญ ในประเด็น ดังนี้

1. การเข้าถึงหรือควบคุมการใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศ

จัดทำานโยบายการควบคุมการเข้าถึงสารสนเทศเป็นลายลักษณ์อักษร

2. จัดให้มีการสารองข้อมูลสารสนเทศที่สาคัญ อย่างสม่ำเสมอ เพื่อให้อยู่ในสภาพพร้อมการใช้งาน

กำหนดหน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับการดำเนินการจัดทำแผน มีการเตรียมพร้อม

3. การปฏิบัติตามข้อบังคับของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฯ

กำหนดมาตรการป้องกันระบบคอมพิวเตอร์สาหรับจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

จัดให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามอุปกรณ์ที่เกี่ยวข้องกับการใช้งาน

ในกรณีเกิดการกระทาความผิดขึ้นในองค์กร : ควรมีผังกระบวนการแสดงขั้นตอนการปฏิบัติเมื่อเกิด เหตุการณ์ พร้อมทั้งระบุผู้รับผิดชอบในการปฏิบัติในแต่ละขั้นตอนเป็นเฉพาะกรณีไป เช่นการคุกคามจากผู้ไม่ประสงค์ดีเข้า เปลี่ยนแปลงหน้าเว็บไซต์ขององค์กร โดยกรณีเช่นนี้ การวิเคราะห์และการประเมินเหตุการณ์ การปฏิบัติงานเพื่อแก้ไขปัญหาก็ จะสามารถดำเนินการได้ทันต่อสถานการณ์ ในเมื่อมีความพร้อมและกระบวนการที่ชัดเจน

การปฏิบัติตามข้อกาหนดทางด้านกฎหมาย และข้อบังคับต่างๆ ที่เกี่ยวกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

-เพื่อลดความเสี่ยงที่อาจเกิดขึ้นได้จากการปฏิบัติงานระบบสารสนเทศ

-เพื่อให้ระบบสารสนเทศมีความปลอดภัยจากการใช้เทคโนโลยีสารสนเทศที่ไม่เหมาะสม หรือไม่ถูกต้อง

- เพื่อเป็นกรอบการดำเนินงานด้านการรักษาความปลอดภัยสารสนเทศขององค์กร

- เพื่อให้ผู้ใช้งานตระหนักถึงภัยคุกคาม และความปลอดภัยด้านเทคโนโลยีสารสนเทศ

กำหนดเงื่อนไขนโยบายความปลอดภัยระบบสารสนเทศสาหรับผู้ทางาน (Acceptable Use Policy: AUP)เพื่อเป็นกรอบที่กำหนดให้ผู้ใช้งานทางาน ร่วมกัน โดยมีเป้าหมายเพื่อนาไปพัฒนาเป็นมาตรฐาน กระบวนการ แนวทาง ขั้นตอนปฏิบัติที่เหมาะสมให้ระบบสารสนเทศเกิดความมั่นคง และปลอดภัยตาม พื้นฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ คือ การรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อม ใช้งาน (Availability) ซึ่งผู้ใช้งานทุกระดับต้องให้ความสาคัญ

เอกสารอ้างอิงและเว็บไซต์อ้างอิง

๑.๑) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม http://www.mict.go.th/ สอบถามข้อมูล /แจ้งข้อมูลเว็บไซต์ที่ไม่เหมาะสม

๑.๒) กองบังคับการปราบปรามการกระทาความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี(ปอท.) http://www.tcsd.in.th/ แจ้งความดาเนินคดี

๑.๓) ความรู้ด้านภัยร้ายจากอินเทอร์เน็ต www.catcyfence.com