ประกาศสำนักงานเขตพื้นที่การศึกษาประถมศึกษากาญจนบุรี เขต ๒
เรื่อง มาตรการในการเผยแพร่ข้อมูลต่อสาธารณะผ่านเว็บไซต์ของสำนักงานเขตพื้นที่การศึกษา

.....

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากาญจนบุรี เขต ๒ เป็นหน่วยงานทางการศึกษาที่ดูแล บริหารงาน ให้บริการกับโรงเรียน ผู้บริหารสถานศึกษา คณะครู คณะนักเรียน ในท้องที่ ๓ อำเภอ คือ อำเภอพนมทวน อำเภอท่ามะกา และอำเภอห้วยกระเจา จังหวัดกาญจนบุรี เพื่อเป็นการบริหารงานและให้บริการกับหน่วยงานละบุคลดังกล่าว ยังต้องให้บริการกับหน่วยงานอื่น ๆ บุคคลภายนอก ตลอดประชาชนทั่วไป

การให้บริการด้านข้อมูลอิเล็กทรอนิกส์ เพื่อให้ผู้ใช้บริการจากภายนอกและภายในเป็นสิ่งจำเป็นอย่างยิ่ง แต่สิ่งที่ตามมาคือความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ สำนักงานเขตพื้นที่การศึกษาประถมศึกษากาญจนบุรี เขต ๒ จึงมีมาตรการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ เพื่อให้เกิดความมั่นคงและถูกต้องของข้อมูลดังกล่าว

๑. ระบบรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ จึงต้องมีมาตรการดังต่อไปนี้

๑.๑ การระบุตัวบุคคล และอำนาจหน้าที่ (Authentication & Authorization) คือ การระบุ ตัวบุคคลที่ติดต่อว่าเป็น บุคคลตามที่ได้กล่าวอ้างไว้จริง และมีอำนาจหน้าที่ตามที่ได้กล่าวอ้างไว้จริง (เปรียบเทียบได้กับการแสดงตัวด้วยบัตรประจำตัวซึ่งมีรูปติดอยู่ด้วย หรือ การใช้ระบบล็อกซึ่งผู้ที่จะเปิดได้จะต้องมีกุญแจอยู่เท่านั้นเป็นต้น)

๑.๒ การรักษาความลับของข้อมูล (Confidentiality) คือ การรักษาความลับของข้อมูลที่เก็บไว้หรือส่งผ่านทางเครือข่ายโดยป้องกันไม่ให้ผู้อื่นที่ไม่มีสิทธิ์ลักลอบดูได้ (เปรียบเทียบได้กับ การปิดผนึกซองจดหมาย การใช้ซองจดหมายที่ทึบแสง การเขียนหมึกที่มองไม่เห็น เป็นต้น)

๑.๓ การรักษาความถูกต้องของข้อมูล (Integrity) คือ การป้องกันไม่ให้ข้อมูลถูกแก้ไข โดยตรวจสอบไม่ได้ (เปรียบเทียบได้กับ การเขียนด้วยหมึกซึ่งถ้าถูกลบแล้วจะก่อให้เกิดรอยลบขึ้น เป็นต้น)

๑.๔ การป้องกันการปฏิเสธ หรือ อ้าง ความรับผิดชอบ (Non-repudiation) คือ การป้องกันการปฏิเสธว่าไม่ได้มีการส่ง หรือ รับข้อมูล จากฝ่ายต่างๆที่เกี่ยวข้อง หรือ การป้องกันการอ้างที่เป็นเท็จว่าได้ รับหรือ ส่งข้อมูล (เปรียบเทียบได้กับการส่งจดหมายลงทะเบียน เป็นต้น)

๒. เทคโนโลยีในการรักษาความปลอดภัย

๒.๑ ความปลอดภัยของเครือข่าย (Networks Security)

- เพื่อปกป้องความปลอดภัยของเครือข่ายภายในองค์กรจากเครือข่ายภายนอกที่ไม่น่าเชื่อถือ
- การใช้ firewalls

๒.๒ การพิสูจน์ตัวตน (Authentication)

- เพื่อให้มั่นใจได้ว่าฝ่ายที่กาลังติดต่อด้วยนั้นเป็นบุคคลที่ถูกต้อง ไม่ใช่ผู้แอบอ้าง
- การใช้รหัสผ่าน

๒.๓ การเข้ารหัส (Encryption)

- ใช้ในการปกป้องข้อมูลที่ส่งผ่านเส้นทางสาธารณะ
- SSL Protocol, Public-key cryptography

๒.๔ นโยบายและการจัดการระบบความปลอดภัย (Security Policy and Management)

- ครอบคลุมถึงระบบการบริหารบุคคล วิธีการเข้าถึงตัว server และอื่น ๆ
- เป็นส่วนสำคัญในการทำให้ระบบพาณิชย์อิเล็กทรอนิกส์ปลอดภัยอย่างแท้จริง

๓. ความรู้เพิ่มเติมของข้อมูลอิเล็กทรอนิกส์

๓.๑ ลายมือชื่อดิจิทัล (Digital Signature) คือข้อมูลอิเล็กทรอนิกส์ที่ได้จากการเข้ารหัสข้อมูลด้วยกุญแจส่วนตัวของผู้ส่งซึ่งเปรียบเสมือนเป็นลายมือชื่อของผู้ส่ง คุณสมบัติของลายมือชื่อดิจิทัล นอกจากจะสามารถ ระบุตัวบุคคล และเป็นกลไกการป้องกันการปฏิเสธความรับผิดชอบแล้ว ยังสามารถป้องกันข้อมูลที่ส่งไปไม่ให้ถูกแก้ไข หรือหากถูกแก้ไขไปจากเดิมก็สามารถล่วงรู้ได้

๓.๒ ใบรับรองดิจิทัล (Digital Certificate) จะถูกนำมาใช้สำหรับยืนยันในตอนทำธุรกรรมว่าเป็นบุคคลนั้น ๆจริง ตามที่ได้อ้างไว้ ซึ่งออกโดยองค์กรกลางที่เป็นที่เชื่อถือ เรียกว่า องค์กรรับรองความถูกต้อง (Certification Authority) ซึ่งรายละเอียดในใบรับรองดิจิทัลทั่วไปมีดังต่อไปนี้

๑) ข้อมูลระบุผู้ที่ได้รับการรับรอง ได้แก่ ชื่อ องค์กร ที่อยู่

๒) ข้อมูลระบุผู้ออกใบรับรอง ได้แก่ ลายมือชื่อดิจิทัลขององค์กรที่ออกใบรับรอง หมายเลขประจำตัวของผู้ออกใบรับรอง

๓) กุญแจสาธารณะของผู้ที่ได้รับการรับรอง

๔) วันหมดอายุของใบรับรองดิจิทัล

๕) ระดับชั้นของใบรับรองดิจิทัล ซึ่งมีทั้งหมด ๔ ระดับ ในระดับ ๔ จะมีกระบวนการตรวจสอบเข้มงวดที่สุด และต้องการข้อมูลมากที่สุด

๖) หมายเลขประจำตัวของใบรับรองดิจิทัล

๓.๓ ประเภทของใบรับรองดิจิทัล แบ่งออกเป็น ๓ ประเภท คือ

๑) ใบรับรองเครื่องแม่ข่าย

๒) ใบรับรองตัวบุคคล

๓) ใบรับรองสำหรับองค์รับรองความถูกต้อง

ประกาศ ณ วันที่

(นายอาดุลย์ พรมแสง)
ผู้อำนวยการสำนักงานเขตพื้นที่การศึกษาประถมศึกษาสงขลา เขต ๓ ปฏิบัติราชการในตำแหน่ง
ผู้อำนวยการสำนักงานเขตพื้นที่การศึกษาประถมศึกษากาญจนบุรี เขต ๒