# ใบความรู้ที่ 2

# ความปลอดภัยของข้อมูล

**การจัดการความปลอดภัยของข้อมูล**

|  |
| --- |
| ข้อมูลสารสนเทศ เป็นสินทรัพย์สำคัญทางธุรกิจ ที่ต้องดูแลบำรุงรักษา และป้องกันอย่างดี ปัจจุบันบริษัทฯ ได้กำหนดความปลอดภัยระบบข้อมูลสารสนเทศ โดยการนำเทคโนโลยีความปลอดภัยที่สำคัญมาใช้ในองค์กร เพื่อช่วยในการทำงาน และลดความเสี่ยงด้านความปลอดภัย ในระดับที่เหมาะสม และเกิดประสิทธิภาพต่อการทำงานสูงสุด          บริษัทได้ตระหนักถึงความสำคัญของข้อมูลสารสนเทศ โดยให้มีการบริหารจัดการให้ระบบข้อมูลมีลักษณะคงความเป็น C I A  คือ  **1. การรักษาความลับ** (Confidentiality) ให้บุคคลผู้มีสิทธิเท่านั้น เข้าถึงเรียกดูข้อมูลได้ ต้องมีการควบคุมการเข้าถึง ข้อมูลเป็นความลับต้องไม่เปิดเผยกับผู้ไม่มีสิทธิ  **2. ความถูกต้องแท้จริง** (Integrity) มีเกราะป้องกันความถูกต้องครบถ้วนสมบูรณ์ของข้อมูล และวิธีการประมวลผล ต้องมีการควบคุมความผิดพลาด ไม่ให้ผู้ไม่มีสิทธิมาเปลี่ยนแปลงแก้ไข  **3. ความสามารถพร้อมใช้เสมอ** (Availability) ให้บุคคลผู้มีสิทธิเท่านั้นเข้าถึงข้อมูลได้ทุกเมื่อที่ต้องการ ต้องมีการควบคุมไม่ให้ระบบล้มเหลว มีสมรรถภาพทำงานต่อเนื่อง ไม่ให้ผู้ไม่มีสิทธิมาทำให้ระบบหยุดการทำงาน  **ความปลอดภัยของข้อมูลสารสนเทศ (Information Security)**  บริษัทฯ มีนโยบายให้ความปลอดภัยและการรักษาความลับของข้อมูล โดยบริษัทฯ ใช้ระบบรักษาความปลอดภัยที่มีมาตรฐานสูงทั้งในด้านเทคโนโลยีและกระบวนการเพื่อป้องกันการโจรกรรมข้อมูลที่เป็นความลับ บริษัทฯ ได้กำหนดให้มีระบบความปลอดภัยที่มีประสิทธิภาพ เพื่อให้มั่นใจได้ว่าเว็บไซต์และข้อมูลของบริษัทฯ มีการรักษาความปลอดภัยที่ได้มาตรฐาน รวมถึงการเลือกใช้ Firewall System, Anti-Virus System ที่มีมาตรฐานความปลอดภัยสูง รวมทั้งได้ใช้เทคโนโลยี เข้ารหัสข้อมูลที่ระดับ 128 บิท (128 Bit Encryption) ซึ่งเป็นการเข้ารหัสข้อมูลระดับสูงสำหรับการทำธุรกรรมผ่านบริการทางอินเทอร์เน็ต นอกจากนี้ บริษัทฯ ยังกำหนดให้ลูกค้าต้องลงทะเบียนก่อนจึงจะสามารถใช้บริการได้  บริษัทฯ ได้มีการเลือกใช้เทคโนโลยีระบบคอมพิวเตอร์ที่มีระบบการรักษาความปลอดภัยในขั้นพื้นฐานที่เป็นมาตรฐานสากลอยู่แล้ว และเสริมด้วยการทำงานด้านอุปกรณ์ความปลอดภัยเฉพาะอีกชั้น และโดยหลักการทั่วไปในการควบคุมและรักษาความปลอดภัยให้กับระบบข้อมูลข่าวสาร ได้แก่การควบคุมส่วนต่าง ๆ ของระบบอย่างรัดกุม วิธีการที่ใช้ในการควบคุมมีดังนี้  **1.  การควบคุมรักษาความปลอดภัยโดยตัวซอฟต์แวร์ (Software Control)**   โดยมีระดับวิธีการ 3 วิธีคือ  -  การควบคุมจากระบบภายในของซอฟต์แวร์ (Internal Program Control) คือการที่       โปรแกรมนั้นได้มีการควบคุมสิทธิการเข้าถึง และสิทธิในการใช้ข้อมูลภายในระบบ ซึ่งถูกจัดเก็บไว้ในระบบฐานข้อมูลภายในระบบเอง  -  การควบคุมความปลอดภัยโดยระบบปฏิบัติการ (Operating System Control) คือการควบคุมสิทธิการเข้าถึงและการใช้ข้อมูลในส่วนต่าง ๆ ภายในระบบคอมพิวเตอร์ของผู้ใช้คนหนึ่ง และจำแนกแตกต่างจากผู้ใช้คนอื่น ๆ  -  การควบคุมและการออกแบบโปรแกรม (Development Control) คือการควบคุมตั้งแต่การออกแบบ การทดสอบก่อนการใช้งานจริง  **2. การควบคุมความปลอดภัยของระบบโดยฮาร์ดแวร์ (Hardware Control)**   โดยเลือกใช้เทคโนโลยีทางด้านฮาร์ดแวร์ ที่สามารถควบคุมการเข้าถึง และป้องกันการทำงานผิดพลาด ด้วยอุปกรณ์ภายในตัวเอง  **3. การใช้นโยบายในการควบคุม (Policies)**  โดยมีการประกาศใช้นโยบาย และการปรับปรุงนโยบายให้มีการทำงานสอดคล้องกับการดำเนินธุรกิจ และสภาพแวดล้อมที่เปลี่ยนแปลง โดยมีผลบังคับใช้ทั้งองค์กร  **4. การป้องกันทางกายภาพ (Physical Control)**   การมีมาตรการการเข้าถึงศูนย์คอมพิวเตอร์ และเครื่องคอมพิวเตอร์ที่สำคัญได้เฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น รวมทั้งมีระบบสำรองข้อมูลอย่างสม่ำเสมอ  **มาตรการและอุปกรณ์ที่ใช้ในนโยบายระบบความปลอดภัย**  **การจัดการด้านความปลอดภัยของระบบเครือข่าย Counter Service จะประกอบด้วยองค์ประกอบ 3 ส่วนดังนี้**  **1. โครงสร้างพื้นฐานด้านความปลอดภัย**  a.การติดตั้งระบบ Firewall บริษัทฯ ได้ติดตั้ง Firewall ซึ่งเป็นเทคโนโลยีที่ทำการป้องกันผู้บุกรุกเข้า-ออกระบบ และกำหนดโซนการให้บริการ การเข้าถึงข้อมูล ที่เหมาะสม - กำหนดขอบเขต และโซนการทำงานที่เหมาะสม - กำหนดบริการ และการเข้าถึงระบบสำหรับผู้ที่ได้รับอนุญาตเท่านั้น  b.การติดตั้งระบบ Anti-Virus เพื่อทำการป้องกัน และกำจัดไวรัสที่มีการอัพเดตข้อมูลอย่างสม่ำเสมอ  c.การติดตั้งระบบ SSL บริษัทฯ เลือกใช้ SSL เวอร์ชั่นล่าสุด ซึ่งบริษัท และธนาคารชั้นนำส่วนใหญ่เลือกใช้ เนื่องจากมีประสิทธิภาพในการรักษาความปลอดภัยขั้นสูง  หน้าที่ของ SSL คือ สลับที่ข้อมูลและแปลงเป็นรหัสตัวเลขทั้งหมด ยิ่งความละเอียดในการเข้ารหัสมีมากเท่าไร ความปลอดภัยก็ยิ่งสูงขึ้นเท่านั้น ระดับความละเอียดของการเข้ารหัสมีหน่วยเป็น บิท  โดยเว็บไซท์บริษัทฯ ได้ใช้การเข้ารหัสระดับ 128 บิท ซึ่งถือว่าเป็นระดับที่บริษัท และธนาคารชั้นนำของโลกใช้อยู่  d.การติดตั้งระบบปฏิบัติการที่มีระดับความปลอดภัยที่ระดับ C2 โดยการติดตั้ง และเปิดใช้เฉพาะบริการที่เหมาะสม และจำเป็นเท่านั้น  e.การติดตั้งระบบ Web Server และการกำหนดค่าพารามิเตอร์ที่เหมาะสม  **2. การตั้งค่าและใช้งานอย่างเหมาะสม (Hardening)**  a.  Hardening  b.  Patch Management  c.   Authentication  d.   Backup  **3. การตรวจสอบ (Audit)**     การตรวจสอบการใช้งานทั่วไป |