(สำเนา)

19 พฤศจิกายน 2546

เรียน ผู้จัดการ

ธนาคารพาณิชย์ทุกธนาคาร

บริษัทเงินทุนและบริษัทเงินทุนหลักทรัพย์ทุกบริษัท

ที่ ธปท.สนส. (11) ว. 2484/2546 เรื่อง แนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์

1. เหตุผลในการออกหนังสือเวียน

ปัจจุบันสถาบันการเงินมีการให้บริการทางการเงินผ่านสื่ออิเล็กทรอนิกส์ต่างๆ มากขึ้น เพื่อให้สามารถลดต้นทุน ตอบสนองความต้องการของลูกค้าผู้ใช้บริการได้อย่างรวดเร็ว และเพิ่มประสิทธิภาพในการแข่งขัน อย่างไรก็ดี การให้บริการทางการเงินผ่านสื่ออิเล็กทรอนิกส์มีความเสี่ยงที่สำคัญคือ ความเสี่ยงด้านความปลอดภัย (Security Risk) ของข้อมูล ระบบ และเครือข่ายที่ใช้ในการให้บริการ สถาบันการเงินจำเป็นต้องมีนโยบายและกระบวนการรักษาความปลอดภัยที่มีประสิทธิภาพ เพื่อให้สามารถป้องกันระบบให้บริการจากภัยคุกคาม การลักลอบเข้าถึง และการโจรกรรมข้อมูลทั้งของสถาบันการเงินและลูกค้า ซึ่งเป็นสาเหตุของความเสียหายทางการเงิน ความเสียหายต่อชื่อเสียง และสามารถนำไปสู่การขาดความเชื่อมั่นต่อระบบให้บริการของระบบสถาบันการเงินโดยรวมได้

ธนาคารแห่งประเทศไทยจึงเห็นควรออกแนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อให้สถาบันการเงินใช้เป็นแนวทางในการกำหนดนโยบายและกระบวนการในการรักษาความปลอดภัยสำหรับการให้บริการการเงินทางอิเล็กทรอนิกส์ เพื่อให้บริการดังกล่าวมีความปลอดภัย เป็นที่น่าเชื่อถือ และเป็นการรักษาผลประโยชน์ของลูกค้าสถาบันการเงิน

2. ขอบเขตการถือปฏิบัติ

ธนาคารพาณิชย์ บริษัทเงินทุน และบริษัทเงินทุนหลักทรัพย์ทุกแห่งที่ให้บริการการเงินทางอิเล็กทรอนิกส์ควรนำแนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ ไปใช้เป็นแนวทางในการกำหนดนโยบายและกระบวนการในการรักษาความปลอดภัยสำหรับการให้บริการการเงินทางอิเล็กทรอนิกส์ ทั้งนี้ แนวปฏิบัติฉบับนี้มุ่งเน้นการรักษาความปลอดภัยของการให้บริการการเงินผ่านเครือข่ายสาธารณะ (Public Network) เช่น เครือข่ายอินเทอร์เน็ต และเครือข่ายการสื่อสารแบบไร้สาย ซึ่งต้องมีการเชื่อมต่อกับเครือข่ายภายในของ

สถาบันการเงิน จึงมีความเสี่ยงสูงที่จะเกิดภัยคุกคามในรูปแบบต่างๆ โดยเฉพาะจากผู้บุกรุกซึ่งสามารถสร้างความเสียหายต่อสถาบันการเงินได้ อย่างไรก็ดี สถาบันการเงินสามารถนำแนวปฏิบัตินี้ไปประยุกต์ใช้กับการให้บริการการเงินทางอิเล็กทรอนิกส์ที่กระทำผ่านช่องทางอื่นที่มีความเสี่ยงต่ำกว่าได้

3. เนื้อหา

สาระสำคัญของแนวปฏิบัติได้แก่

1. <u>นโยบายการรักษาความปลอดภัย</u>

คณะกรรมการสถาบันการเงินมีหน้าที่กำหนดนโยบายการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ที่เป็นลายลักษณ์อักษรและอนุมัติกระบวนการรักษาความปลอดภัยที่ฝ่ายจัดการเสนอ เมื่อคณะกรรมการอนุมัตินโยบายและกระบวนการรักษาความปลอดภัยแล้ว คณะกรรมการต้องกำหนดให้มีผู้บริหารและพนักงานที่รับผิดชอบในการดำเนินการให้เป็นไปตามนโยบายและกระบวนการที่ได้รับการอนุมัติ นอกจากนั้น คณะกรรมการต้องจัดให้มีการประเมินประสิทธิภาพของนโยบายและกระบวนการรักษาความปลอดภัยอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัย

2. <u>กระบวนการหลักในการรักษาความปลอดภัย</u>

กระบวนการหลักในการรักษาความปลอดภัยที่สถาบันการเงินต้องกำหนดไว้ในนโยบายการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ประกอบด้วยกระบวนการควบคุมการเข้าถึงระบบให้บริการและข้อมูล การตรวจสอบตัวตนลูกค้าและการป้องกันการปฏิเสธความรับผิด การรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูล การรักษาความลับของข้อมูล การรักษาความพร้อมใช้ของระบบให้บริการ การติดตามตรวจสอบความผิดปกติและความล่อแหลมของระบบให้บริการ และการแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการได้รับความเสียหายจากภัยคุกคาม

3. <u>กระบวนการเสริมการรักษาความปลอดภัยให้มีประสิทธิภาพ</u>

สถาบันการเงินควรจัดให้มีการฝึกอบรมและให้ความรู้อย่างต่อเนื่องแก่ผู้บริหารและพนักงานทุกระดับที่เกี่ยวข้องกับการให้บริการ เพื่อให้สามารถปฏิบัติตามนโยบายและกระบวนการรักษาความปลอดภัยได้อย่างมีประสิทธิภาพ นอกจากนั้น ควรให้ข้อมูลและคำแนะนำที่เป็นประโยชน์แก่ลูกค้า รวมทั้งจัดให้มีกระบวนการควบคุมภายในที่เหมาะสมกับการให้บริการการเงินทางอิเล็กทรอนิกส์ ซึ่งจะช่วยเสริมให้นโยบายและกระบวนการรักษาความปลอดภัยมีประสิทธิภาพมากยิ่งขึ้น

4. วันเริ่มต้นการถือปฏิบัติ

ให้ถือปฏิบัติตามแนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ตั้งแต่บัดนี้เป็นต้นไป

ขอแสดงความนับถือ

(ม.ร.ว. ปรีดิยาธร เทวกุล)
ผู้ว่าการ

สิ่งที่ส่งมาด้วย แนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์

ฝ่ายกลยุทธ์สถาบันการเงิน
โทร. 0-2283-6938, 0-2283-5839

หมายเหตุ [ ] ธนาคารจะจัดให้มีการประชุมชี้แจงในวันที่.....ณ.....
[X] ไม่มีการจัดประชุมชี้แจง

แนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์

วัตถุประสงค์

เพื่อให้คณะกรรมการและผู้บริหารของสถาบันการเงินใช้เป็นแนวทางในการกำหนดนโยบายและกระบวนการในการรักษาความปลอดภัยสำหรับการให้บริการการเงินทางอิเล็กทรอนิกส์ ซึ่งรวมถึงการบริหารความเสี่ยงต่างๆ ที่อาจเกิดขึ้น เพื่อให้บริการการเงินทางอิเล็กทรอนิกส์ของสถาบันการเงินมีความปลอดภัยและเป็นการรักษาผลประโยชน์ของลูกค้า

คำจำกัดความ

“การให้บริการการเงินทางอิเล็กทรอนิกส์” หมายถึง การให้บริการการเงินผ่านสื่ออิเล็กทรอนิกส์ต่างๆ ซึ่งลูกค้าผู้ใช้บริการสามารถทำรายการได้เอง

“บริการการเงิน” หมายถึง ธุรกรรมทางการเงินและธุรกรรมที่เกี่ยวข้องที่สถาบันการเงินได้รับอนุญาตให้ดำเนินการได้ เช่น การให้บริการโอนเงิน การให้บริการชำระค่าสินค้าและบริการ การแสดงข้อมูลในบัญชีของลูกค้าผู้ใช้บริการ การร้องขอ ตรวจสอบ ยืนยัน เปลี่ยนแปลงแก้ไขข้อมูลของลูกค้าผู้ใช้บริการ การรับส่งคำสั่งหรือข้อมูลกับลูกค้าผู้ใช้บริการเพื่อประโยชน์ในการให้บริการและการทำธุรกรรมทางการเงิน เป็นต้น

“สื่ออิเล็กทรอนิกส์” หมายถึง อุปกรณ์หรือเครื่องมือที่สถาบันการเงินใช้เป็นช่องทางในการให้บริการการเงินทางอิเล็กทรอนิกส์ เช่น สื่อบันทึกข้อมูล อุปกรณ์สื่อสาร เครื่องคอมพิวเตอร์และเครือข่ายรูปแบบต่างๆ เป็นต้น

“ระบบให้บริการ” หมายถึง ระบบเทคโนโลยีสารสนเทศและระบบเทคโนโลยีอื่นๆ ที่เกี่ยวข้องกับการให้บริการการเงินทางอิเล็กทรอนิกส์ เช่น ระบบฐานข้อมูล (Database System) โปรแกรมระบบงาน (Applications) ระบบปฏิบัติการ (Operating System) ระบบเครือข่าย (Network System) เป็นต้น

“เทคโนโลยีรักษาความปลอดภัย” หมายถึง เทคนิค เครื่องมือทางคอมพิวเตอร์หรือเครื่องมือทางอิเล็กทรอนิกส์ต่างๆ ที่สถาบันการเงินใช้ในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์

บทนำ

- ในปัจจุบันสถาบันการเงินทั่วโลกแข่งขันกันให้บริการแก่ลูกค้าในทุกรูปแบบ การเสนอบริการทางการเงินผ่านสื่ออิเล็กทรอนิกส์เป็นช่องทางที่สถาบันการเงินและลูกค้าหันมาให้

ความสนใจมากขึ้น เนื่องจากมีความสะดวกรวดเร็วและลูกค้าสามารถทำธุรกรรมได้ทุกที่ทุกเวลา โดยไม่ต้องเดินทางมาที่ทำการของสถาบันการเงิน ในส่วนของการให้บริการการเงินผ่านเครือข่ายอินเทอร์เน็ต (Internet) สถาบันการเงินหลายแห่งได้ให้บริการแก่ลูกค้าแล้ว หลังจากได้รับอนุญาตจากธนาคารแห่งประเทศไทยตามประกาศเรื่อง การใช้เครือข่ายอินเทอร์เน็ต (Internet) ในการประกอบธุรกิจของสถาบันการเงิน

- อย่างไรก็ดี สถาบันการเงินที่สนใจจะเสนอบริการการเงินผ่านสื่ออิเล็กทรอนิกส์ต้องพิจารณาอย่างจริงจังถึงความเหมาะสมในเชิงกลยุทธ์ที่สถาบันการเงินนั้นจะหันมาเสนอบริการผ่านสื่ออิเล็กทรอนิกส์ เนื่องจากการเปลี่ยนแปลงทางเทคโนโลยีเป็นไปอย่างรวดเร็ว สถาบันการเงินต้องใช้เงินลงทุนระยะเริ่มแรกสูงและต้องพิจารณาเลือกใช้เทคโนโลยีให้เหมาะสมกับบริการที่จะเสนอให้แก่ลูกค้า คณะกรรมการสถาบันการเงินต้องพิจารณาถึงความเสี่ยงด้านกลยุทธ์อย่างรอบคอบและไม่ควรตัดสินใจให้บริการเพียงเพราะต้องการให้ทัดเทียมกับสถาบันการเงินอื่น แต่ควรตระหนักถึงกลยุทธ์ที่เหมาะสมกับองค์กร
- แม้ว่าการให้บริการการเงินทางอิเล็กทรอนิกส์จะทำให้สถาบันการเงินสามารถตอบสนองความต้องการของลูกค้าได้รวดเร็วและมีประสิทธิภาพมากขึ้น แต่ก็เป็นการเพิ่มระดับความเสี่ยงประเภทต่างๆ ที่สถาบันการเงินประสบอยู่แล้วให้มากขึ้น โดยเฉพาะอย่างยิ่งความเสี่ยงด้านความปลอดภัย (Security Risk) ของระบบให้บริการ
- **ความเสี่ยงด้านความปลอดภัย คือ ความเสี่ยงที่ระบบให้บริการของสถาบันการเงินจะเกิดความเสียหายจากภัยคุกคามหรือการลักลอบเข้าถึงในลักษณะต่างๆ เช่น การลักลอบเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาตทั้งจากภายในและภายนอกองค์กร (Unauthorized Access) การลักลอบนำข้อมูลที่อยู่ระหว่างการรับส่งไปใช้ การลักลอบเข้าทำธุรกรรมโดยปลอมแปลงข้อมูลการตรวจสอบตัวตน (False Authentication) และการเข้าโจมตีระบบให้บริการจนไม่สามารถทำงานได้ นอกเหนือจากการใช้เทคนิคทางคอมพิวเตอร์ในการลักลอบกระทำการต่างๆ แล้ว ระบบให้บริการของสถาบันการเงินยังอาจได้รับอันตรายจากการใช้วิธีการอื่นหลอกลวงให้สถาบันการเงินหรือลูกค้าผู้ใช้บริการหลงเชื่อ เพื่อที่จะอนุญาตให้เข้าถึงระบบให้บริการหรือให้ข้อมูลสำคัญได้ (Social Engineering)**
- สถาบันการเงินในต่างประเทศได้ประสบปัญหากรณีถูกผู้บุกรุก (Hacker) ลักลอบเข้าถึงระบบข้อมูลและทำความเสียหายให้กับสถาบันการเงินมาแล้ว ความเสียหายดังกล่าวส่งผลกระทบถึงชื่อเสียงของสถาบันการเงิน (Reputational risk) เป็นอย่างมาก หากไม่มีกระบวนการแก้ไขปัญหาและชี้แจงต่อลูกค้าผู้ใช้บริการอย่างรวดเร็วแล้ว ความเสียหายอาจรุนแรงจนถึงขั้นทำให้ลูกค้าขาดความเชื่อมั่นในสถาบันการเงินแล้วถอนเงินฝาก (Deposit Run) ได้

- ผู้กำกับดูแลสถาบันการเงินในหลายประเทศ อาทิ Bank for International Settlements (BIS) Office of the Comptroller of the Currency (OCC) ประเทศสหรัฐอเมริกา Hong Kong Monetary Authority (HKMA) และ Monetary Authority of Singapore (MAS) ได้ตระหนักถึงความเสี่ยงที่มีต่อสถาบันการเงินจากการให้บริการการเงินทางอิเล็กทรอนิกส์ จึงได้ออกแนวปฏิบัติ (Guideline) ให้สถาบันการเงินต้องมีการกำหนดนโยบายและกระบวนการรักษาความปลอดภัยในการให้บริการการเงินทางอิเล็กทรอนิกส์ที่มีประสิทธิภาพ ธนาคารแห่งประเทศไทยได้ศึกษาแนวปฏิบัติดังกล่าวและเห็นว่าปัจจุบันสถาบันการเงินมีความตื่นตัวในการเสนอบริการการเงินทางอิเล็กทรอนิกส์กันมากขึ้น จึงเห็นควรออกแนวปฏิบัติฉบับนี้เพื่อให้สถาบันการเงินตระหนักถึงความปลอดภัยในการให้บริการและใช้เป็นแนวทางในการกำหนดนโยบายและกระบวนการรักษาความปลอดภัยระบบให้บริการของสถาบันการเงิน

- ในการให้บริการการเงินทางอิเล็กทรอนิกส์ สถาบันการเงินจะต้องคำนึงถึงการรักษาความปลอดภัยระบบให้บริการ นับตั้งแต่ภายในสถาบันการเงินเองจนถึงสื่ออิเล็กทรอนิกส์ต่างๆ ที่ลูกค้าใช้ในการเข้าทำรายการธุรกรรม เนื่องจากในต่างประเทศได้เคยเกิดกรณีที่ผู้บุกรุกเจาะระบบของลูกค้าแล้วเข้าไปแก้ไขข้อมูลเพื่อใช้ปลอมตัวเป็นลูกค้าที่เคยเข้าทำธุรกรรมกับสถาบันการเงิน (Cookie Poisoning) จากวิธีการนี้ หากไม่มีการติดตั้งระบบรักษาความปลอดภัยตั้งแต่สื่ออิเล็กทรอนิกส์ที่ลูกค้าใช้ทำรายการแล้วก็อาจเกิดความเสียหายดังกล่าวได้ นอกจากนั้นการให้คำแนะนำแก่ลูกค้าผู้ใช้บริการในด้านการรักษาความปลอดภัยในการใช้บริการก็เป็นสิ่งสำคัญที่จะช่วยเสริมให้กระบวนการรักษาความปลอดภัยของสถาบันการเงินเองมีประสิทธิภาพมากยิ่งขึ้น

หลักการ

- **แนวปฏิบัติฉบับนี้มุ่งเน้นการรักษาความปลอดภัยของการให้บริการการเงินผ่านเครือข่ายสาธารณะ (Public Network) เช่น เครือข่ายอินเทอร์เน็ต (Internet) และเครือข่ายการสื่อสารแบบไร้สาย (Wireless Communication Network) ซึ่งต้องมีการเชื่อมต่อกับเครือข่ายภายใน (Internal Network) ของสถาบันการเงิน จึงมีโอกาสสูงที่จะเกิดภัยคุกคามในรูปแบบต่างๆ โดยเฉพาะจากผู้บุกรุกซึ่งสามารถสร้างความเสียหายต่อสถาบันการเงินได้**

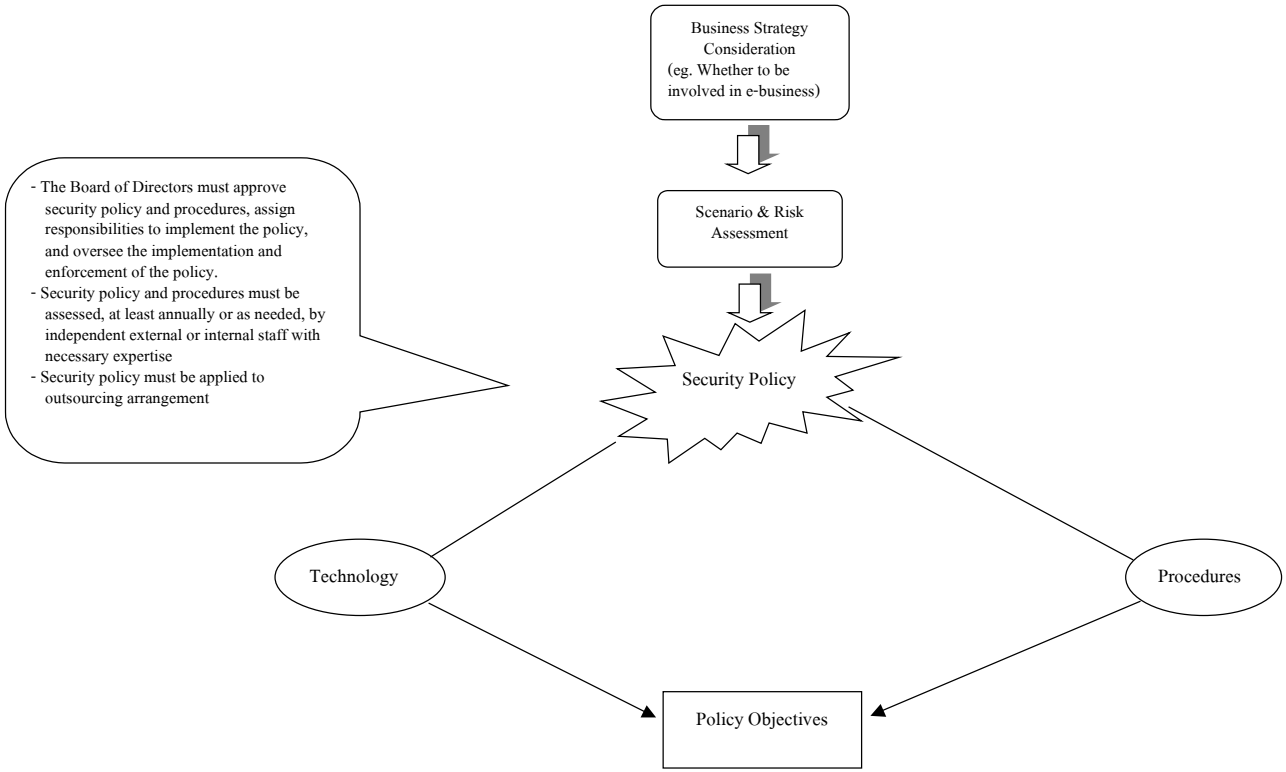
- สถาบันการเงินที่ใช้บริการเครือข่ายสาธารณะเพียงเพื่อเผยแพร่ข้อมูลข่าวสารทางธุรกิจ (Informational Website) ก็ให้พิจารณาประยุกต์ใช้หลักการของแนวปฏิบัตินี้ในการจัดมาตรการรักษาความปลอดภัยที่เหมาะสม เพื่อป้องกันการลักลอบเข้าแก้ไขหรือเปลี่ยนแปลงข้อมูลที่เผยแพร่ ซึ่งจะมีผลกับชื่อเสียงของสถาบันการเงินและอาจมีผลกระทบต่อความเชื่อมั่นของลูกค้าต่อการให้บริการของสถาบันการเงินในอนาคต หากต้องการขยายขอบเขตการให้บริการการเงินทางอิเล็กทรอนิกส์

- สถาบันการเงินสามารถนำแนวปฏิบัตินี้ไปประยุกต์ใช้กับการให้บริการการเงินทางอิเล็กทรอนิกส์ที่กระทำผ่านช่องทางอื่นที่มีความเสี่ยงต่ำกว่าได้ เช่น การให้บริการผ่านเครือข่ายเฉพาะ (Proprietary Network)

เนื้อหาของแนวปฏิบัติสามารถแบ่งเป็น 3 ส่วน ดังนี้

1. ส่วนที่เป็นการกำหนดนโยบายการรักษาความปลอดภัย
2. ส่วนที่เป็นกระบวนการหลักของการรักษาความปลอดภัยระบบให้บริการ ซึ่งรวมถึงเทคโนโลยีรักษาความปลอดภัย ได้แก่
   - 2.1 การควบคุมการเข้าถึงระบบให้บริการและข้อมูล (Access Control)
   - 2.2 การตรวจสอบตัวตนลูกค้าและการป้องกันการปฏิเสธความรับผิด (Authentication & Non-repudiation)
   - 2.3 การรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูล (System & Data Integrity)
   - 2.4 การรักษาความลับของข้อมูล (Data Confidentiality)
   - 2.5 การรักษาความพร้อมใช้ของระบบให้บริการ (System Availability)
   - 2.6 การติดตามตรวจสอบความผิดปกติและความล่อแหลมของระบบให้บริการ (System Detection)
   - 2.7 การแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการได้รับความเสียหายจากภัยคุกคาม (Incident Response & Report)
3. ส่วนเสริมการรักษาความปลอดภัยให้มีประสิทธิภาพ ได้แก่
   - 3.1 การฝึกอบรมและให้ความรู้แก่พนักงาน
   - 3.2 การให้ข้อมูลและคำแนะนำแก่ลูกค้าผู้ใช้บริการ
   - 3.3 การควบคุมภายใน

ทั้งนี้ ภาพรวมของเนื้อหาทั้งหมดในแนวปฏิบัติสามารถนำมาสรุปเป็นแผนภาพเพื่อให้ง่ายต่อการทำความเข้าใจ ดังนี้



Access Control

- Logical access control: access rights, change-control procedure, access logs, review of access rights
- Physical access control: access logs

Technology:
- Firewalls, Web application firewalls
- Application-based Filter, Active Content Filter
- Anti-virus software

Authentication & Non-Repudiation

- Authorization
- Methods are commensurate with risks and transaction types
- Secure authentication databases
- Secure authentication sessions
- Transaction logs
- Regular review of authentication methods

Technology:
- PIN, Password, Smart cards, Security Tokens, Electronic certificates & Electronic signature, Biometrics
- Relevant technology: PKI - Digital Certificate, Digital Signature
- Encryption technology - End-to-end encryption, Transport Encryption
- SSL

System & Data Integrity

- Effective design of systems and technology
- Test systems
- Effective controls during data processing, transmission, and storage
- Change-control procedure

Technology:
- Encryption technology
- SSL
- PKI : Digital Certificate, Digital Signature

Data Confidentiality

- Measures commensurate with the sensitivity of information being transmitted or in storage
- Access to confidential data be authenticated and logged

Technology:
- Encryption technology
- SSL
- PKI : Digital Certificate, Digital Signature

System Availability

- Effective system's capacity, response time, performance, backup and recovery capabilities
- Contingency plan considering business continuity and third party dependencies
- Guideline on IT Contingency Plan to be issued by BOT

System Detection

- Audit logs and transaction logs
- Regular review of logs to detect abnormalities and intrusion attempts which should be promptly reported to management
- Vulnerabilities detection and correction
- Penetration testing for high-risk services

Technology:
- IDS, Network Scanner, Security Alert, Network Analyzer
- Anti-virus software

Incident response & Reporting

- Incident response plan covering
  - Risk assessment and impact analysis
  - Identification of incidents as soon as possible
  - Action plan, responsibilities and reporting procedure
  - Technical assistance
  - Public relations and communications
  - Evidence collecting
  - Formal written report

Technology:
- IDS, Network Scanner, Security Alert, Network Analyzer
- Anti-virus software

Employee Education & Training

- Security training to enhance security awareness as well as skills and knowledge to effectively comply with the security policy
- Keep abreast of new security threats and technological advancements

Consumer Education

- Device protection
- Useful technical information
- Help desk service
- Security training
- Disclosure of Terms & Conditions and comply with the BOT's EFT regulation

Internal Controls

- Legal compliance
- Appropriate HRM
- Clear operational and control procedures
- Audit trails
- Maintenance of audit trails and important documents

สนสว90คส5400125461120ด

รายละเอียดของแนวปฏิบัติ

1. <u>นโยบายการรักษาความปลอดภัย</u>

1.1 คณะกรรมการสถาบันการเงินมีหน้าที่โดยตรงในการกำหนดนโยบายการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ที่เป็นลายลักษณ์อักษรและอนุมัติกระบวนการรักษาความปลอดภัยที่ฝ่ายจัดการเสนอ โดยอย่างน้อยจะต้องพิจารณาถึงความเหมาะสมเชิงกลยุทธ์และต้องเข้าใจถึงความเสี่ยงที่อาจเกิดขึ้น ทั้งนี้ คณะกรรมการสถาบันการเงินอาจมอบหมายให้คณะกรรมการที่รับผิดชอบด้านงานเทคโนโลยีสารสนเทศ หรือคณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการบริหาร หรือที่ปรึกษาภายนอกที่มีความเชี่ยวชาญมาช่วยจัดทำก่อนเสนอให้คณะกรรมการสถาบันการเงินอนุมัติก็ได้

1.2 ในการกำหนดนโยบายการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ มีปัจจัยที่ต้องคำนึงถึงคือ ความสมดุลของกระบวนการรักษาความปลอดภัยกับความเสี่ยงที่อาจเกิดจากธุรกรรมที่ให้บริการ รวมทั้งต้องคำนึงถึงการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็วมากด้วย

1.3 เมื่อมีการอนุมัตินโยบายและกระบวนการรักษาความปลอดภัยแล้ว คณะกรรมการสถาบันการเงินต้องกำหนดให้มีผู้บริหารและพนักงานที่รับผิดชอบในการดำเนินการให้เป็นไปตามนโยบายและกระบวนการที่ได้รับการอนุมัติไว้ มีการสื่อสารให้พนักงานได้รับทราบอย่างทั่วถึง มีการติดตามดูแลให้พนักงานและผู้ที่เกี่ยวข้องกับระบบให้บริการปฏิบัติตามนโยบายและกระบวนการรักษาความปลอดภัยอย่างเคร่งครัด รวมทั้งมีการตรวจสอบการปฏิบัติตามอย่างเหมาะสม ทั้งนี้ ประสิทธิภาพของกระบวนการรักษาความปลอดภัยขึ้นอยู่กับการมีนโยบายที่ชัดเจน มีการสื่อสารอย่างทั่วถึง และมีการบังคับใช้อย่างเหมาะสม หากมีการส่งเสริมให้ผู้บริหารและพนักงานทุกระดับมีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความปลอดภัยและความรับผิดชอบของพนักงานแล้วย่อมก่อให้เกิดผลดีในทางปฏิบัติ

1.4 คณะกรรมการสถาบันการเงินต้องจัดให้มีการประเมินประสิทธิภาพของนโยบายและกระบวนการรักษาความปลอดภัยอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัย เช่น มีการออกผลิตภัณฑ์และบริการใหม่ มีการเปลี่ยนแปลงเทคโนโลยีที่ใช้ หรือมีการลักลอบเข้าถึงระบบให้บริการ (Hacking Incidents) ทั้งนี้ การประเมินสามารถกระทำได้โดยผู้เชี่ยวชาญจากภายนอกหรือภายในองค์กรที่ไม่เป็นผู้พัฒนาหรือปฏิบัติการระบบ นอกจากนั้น สถาบันการเงินควรมีการติดตามความก้าวหน้าทางเทคโนโลยีอย่างใกล้ชิดเพื่อนำมาพัฒนานโยบายและกระบวนการรักษาความปลอดภัยให้มีประสิทธิภาพมากขึ้น

1.5 ในกรณีที่สถาบันการเงินมีการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) เพื่อให้บริการการเงินทางอิเล็กทรอนิกส์ไม่ว่าทั้งหมดหรือบางส่วน คณะกรรมการสถาบันการเงินต้องจัดให้มีการประเมินประสิทธิภาพของกระบวนการรักษาความปลอดภัยของผู้ให้บริการเพื่อให้เป็นไปตามนโยบายการรักษาความปลอดภัยที่ได้กำหนดไว้ รวมทั้งให้ถือปฏิบัติตามหนังสือเวียนที่ ธปท.สนส.(01)ว. 1191/2546 ลงวันที่ 14 พฤษภาคม 2546 เรื่อง แนวปฏิบัติในการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) ด้วย

2. <u>กระบวนการหลักในการรักษาความปลอดภัย</u>

เนื่องจากการให้บริการการเงินทางอิเล็กทรอนิกส์ผ่านเครือข่ายสาธารณะ เช่น เครือข่ายอินเทอร์เน็ต และเครือข่ายการสื่อสารแบบไร้สาย มีโครงสร้างในลักษณะเปิด ซึ่งสถาบันการเงินต้องมีการเชื่อมโยงเครือข่ายภายในกับเครือข่ายสาธารณะ ระบบให้บริการจึงมีความเสี่ยงสูงที่จะได้รับภัยคุกคามจากผู้บุกรุก (Hackers) ในรูปแบบต่างๆ ที่สามารถสร้างความเสียหายต่อสถาบันการเงินได้ เช่น การลักลอบเข้าถึงเครือข่ายภายในที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ตโดยเลียนแบบ IP Address การโจมตีระบบให้บริการโดยใส่ข้อมูลจำนวนมากเข้าสู่ Website เป้าหมายเพื่อให้ระบบทำงานไม่ได้หรือให้เปิดเผยข้อมูลที่สำคัญ การลักลอบส่งโปรแกรมแฝงเข้าระบบให้บริการเพื่อปลอมแปลงข้อมูล หรือการโจมตีระบบให้บริการโดยไวรัสคอมพิวเตอร์ เป็นต้น

สถาบันการเงินจึงจำเป็นต้องมีกระบวนการรักษาความปลอดภัยที่ดีและเลือกใช้เทคโนโลยีสำหรับการรักษาความปลอดภัยที่มีประสิทธิภาพและเป็นที่ยอมรับตามมาตรฐานที่เกี่ยวข้อง เพื่อป้องกันภัยคุกคามต่างๆ และเมื่อเกิดภัยคุกคามก็สามารถควบคุมความเสียหายและแก้ไขปัญหาที่เกิดขึ้นได้ ทั้งนี้ กระบวนการหลักในการรักษาความปลอดภัยที่สถาบันการเงินต้องกำหนดไว้ในนโยบายการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ประกอบด้วย

2.1 <u>การควบคุมการเข้าถึงระบบให้บริการและข้อมูล (Access Control)</u>

กระบวนการและเทคโนโลยีที่ใช้ควบคุมการเข้าถึงระบบให้บริการต้องสามารถป้องกันการลักลอบเข้าถึงโดยผู้ที่ไม่มีสิทธิทั้งจากภายในและภายนอกองค์กร โดยมีการควบคุมการเข้าถึงสถานที่ตั้งของระบบให้บริการและอุปกรณ์สำคัญ (Physical Access Control) และมีการควบคุมการเข้าถึงระบบให้บริการและข้อมูลด้วยวิธีการทางคอมพิวเตอร์ (Logical Access Control) ทั้งนี้ กระบวนการดังกล่าวควรครอบคลุมถึง

1) การกำหนดสิทธิการเข้าถึงระบบให้บริการให้เหมาะสมกับการเข้าใช้บริการของลูกค้าและหน้าที่ความรับผิดชอบของพนักงานในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

2) การกำหนดให้ผู้มีอำนาจเท่านั้นที่จะเข้าแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงต่างๆ ได้

3) การบันทึกรายละเอียดการเข้าถึงระบบให้บริการ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบให้บริการไว้เพื่อเป็นหลักฐานการตรวจสอบในกรณีเกิดปัญหา

ตัวอย่างเทคโนโลยีที่ใช้ในการป้องกันการลักลอบเข้าถึง ได้แก่

- Firewall ประเภทต่างๆ ทั้งในระดับเครือข่าย (Network) และโปรแกรมระบบงาน (Application) ซึ่งใช้เพื่อตรวจสอบและสกัดกั้นข้อมูลหรือคำสั่งที่แปลกปลอมเข้ามาในระบบให้บริการ

- เครื่องมือที่ใช้ในการตรวจสอบและสกัดกั้นโปรแกรมหรือข้อมูลที่แปลกปลอมเข้ามาในระบบให้บริการ เช่น Application-based Filter, Active Content Filter

- โปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-virus Software)

2.2 <u>การตรวจสอบตัวตนลูกค้าและการป้องกันการปฏิเสธความรับผิด (Authentication & Non-repudiation)</u>

กระบวนการและเทคโนโลยีที่ใช้ในการตรวจสอบตัวตนและป้องกันการปฏิเสธความรับผิด (Authentication & Non-repudiation) นอกจากจะเป็นประโยชน์กับสถาบันการเงินในการพิสูจน์ตัวตนของลูกค้าก่อนอนุญาตให้ใช้บริการแล้ว ยังเป็นประโยชน์กับลูกค้าในการพิสูจน์ว่าตนเป็นผู้ทำธุรกรรมกับสถาบันการเงินในกรณีมีข้อพิพาทเกิดขึ้น ทั้งนี้ กระบวนการดังกล่าวควรครอบคลุมถึง

1) การจัดให้มีวิธีการตรวจสอบตัวตนและสิทธิในการใช้บริการของลูกค้าก่อนอนุญาตให้ใช้บริการ

2) การจัดให้วิธีการตรวจสอบตัวตนที่ใช้มีความเหมาะสมกับระดับความเสี่ยงรูปแบบและมูลค่าของธุรกรรมที่ให้บริการ

3) การจัดให้มีการควบคุมการเข้าถึงและการควบคุมการแก้ไขเปลี่ยนแปลงข้อมูลในฐานข้อมูลที่จัดเก็บข้อมูลที่ใช้ในการตรวจสอบตัวตน (Authentication Database)

4) การตรวจสอบตัวตนลูกค้าต้องกระทำอย่างต่อเนื่องและปลอดภัย หากมีการหยุดชะงักควรเริ่มตรวจสอบตัวตนลูกค้าใหม่

5) การจัดให้มีการบันทึกรายละเอียดการเข้าทำธุรกรรมของลูกค้า (Transaction Log) ไว้ เพื่อใช้เป็นหลักฐานการตรวจสอบ รวมทั้งมีการจัดเก็บบันทึกดังกล่าวอย่างปลอดภัย

6) การจัดให้มีการทบทวนวิธีการตรวจสอบตัวตนอย่างสม่ำเสมอ โดยคำนึงถึงระดับความเสี่ยงและพัฒนาการทางเทคโนโลยีที่เปลี่ยนแปลงไป

ตัวอย่างเทคโนโลยีที่ใช้ในการตรวจสอบตัวตนและป้องกันการปฏิเสธความรับผิด ได้แก่

- รหัสผ่าน (Password) เลขประจำตัว (PIN) อุปกรณ์หรือบัตรที่ใช้เก็บข้อมูลส่วนบุคคล (Tokens or Smart card) ลักษณะทางชีวภาพส่วนบุคคล (Biometric)

- เทคโนโลยีกุญแจสาธารณะ(PKI- Public Key Infrastructure) ที่ใช้สร้าง Digital Certificate และ Digital Signature

- เทคโนโลยีการเข้ารหัสลับ (Encryption Technology) ข้อมูลที่ใช้ตรวจสอบตัวตนลูกค้า

- การใช้ช่องทางที่มีความปลอดภัยสูงในการรับส่งข้อมูลการตรวจสอบตัวตน เช่น Secure Sockets Layer (SSL)

2.3 <u>การรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูล</u>

<u>(System & Data Integrity)</u>

กระบวนการที่ใช้ในการรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูลที่อยู่ระหว่างการรับส่ง การประมวลผล และการจัดเก็บ รวมทั้งการดำเนินการให้ระบบให้บริการสามารถทำงานได้อย่างถูกต้องและสามารถตอบสนองความต้องการของลูกค้าได้อย่างมีประสิทธิภาพควรครอบคลุมถึง

1) การออกแบบระบบให้บริการและการเลือกใช้เทคโนโลยีที่มีประสิทธิภาพ

2) การทดสอบระบบให้บริการให้ทำงานได้อย่างถูกต้องก่อนเริ่มใช้งานหรือทุกครั้งที่มีการเปลี่ยนแปลง

3) การจัดให้มีการควบคุมการทำงานของระบบให้บริการในขั้นตอนที่สำคัญ เช่น ขั้นตอน การประมวลผล การรับส่งและการจัดเก็บข้อมูล เพื่อให้สามารถป้องกันและตรวจสอบการลักลอบเข้าถึงระบบให้บริการได้

4) การจัดให้มีการควบคุมการแก้ไขเปลี่ยนแปลงระบบให้บริการและข้อมูล (Change Control) อย่างรัดกุม

2.4 การรักษาความลับของข้อมูล (Data Confidentiality)

กระบวนการและเทคโนโลยีที่ใช้ในการรักษาความลับของข้อมูล (Data Confidentiality) โดยเฉพาะข้อมูลลูกค้าที่อยู่ระหว่างการรับส่ง การประมวลผลและการจัดเก็บ ควรครอบคลุมถึง

1) การจัดให้มีวิธีการรับส่ง ประมวลผล และจัดเก็บข้อมูลลับในลักษณะที่ปลอดภัยตามระดับความสำคัญของข้อมูล เพื่อป้องกันการพบเห็นและการเข้าแก้ไขเปลี่ยนแปลง

2) การจัดให้มีการควบคุมเพื่อให้ผู้ที่มีสิทธิและได้รับการตรวจสอบตัวตนแล้วเท่านั้นที่จะเข้าถึงหรือเปลี่ยนแปลงข้อมูลลับได้

3) การบันทึกรายละเอียดการเข้าถึงและการแก้ไขเปลี่ยนแปลงข้อมูลลับเพื่อใช้เป็นหลักฐานการตรวจสอบ รวมทั้งจัดเก็บหลักฐานดังกล่าวไว้อย่างปลอดภัย

ตัวอย่างเทคโนโลยีที่ใช้ในการรักษาความถูกต้องเชื่อถือได้และการรักษาความลับของข้อมูล ได้แก่

- เทคโนโลยีการเข้ารหัสลับ (Encryption Technology) สำหรับข้อมูลลับ เช่น การเข้ารหัสลับข้อมูลที่อยู่ระหว่างการรับส่ง (Transport Encryption) การเข้ารหัสลับข้อมูลตั้งแต่ต้นทางถึงปลายทาง (End-to-end Encryption) การเข้ารหัสลับข้อมูลในช่วงจัดเก็บ เป็นต้น

- การใช้ช่องทางที่มีความปลอดภัยสูงในการรับส่งข้อมูลลับ เช่น Secure Sockets Layer (SSL)

- เทคโนโลยีกุญแจสาธารณะ(PKI- Public Key Infrastructure) ที่ใช้สร้าง Digital Certificate และ Digital Signature เพื่อใช้ตรวจสอบตัวตนก่อนการเข้าถึงข้อมูลลับ

2.5 การรักษาความพร้อมใช้ของระบบให้บริการ (System Availability)

กระบวนการที่ใช้รักษาความพร้อมใช้ของระบบให้บริการควรครอบคลุมถึงการดำเนินการให้ระบบให้บริการมีประสิทธิภาพและมีความพร้อมในการให้บริการได้ตลอดเวลา โดยอย่างน้อยสามารถให้บริการได้ตามช่วงเวลาที่ได้ตกลงไว้กับลูกค้า สามารถรองรับการทำธุรกรรมตามความต้องการของลูกค้าได้อย่างพอเพียง ตอบสนองการทำธุรกรรมได้อย่างรวดเร็ว ทั้งในช่วงเวลาปกติและช่วงเวลาที่มีการใช้บริการอย่างหนาแน่น รวมทั้งมีการสำรองข้อมูลอย่างเหมาะสมเพื่อให้สามารถกู้ระบบให้กลับมาทำงานได้ตามปกติอย่างทันท่วงทีในกรณีที่เกิดความเสียหาย

ในการเตรียมการรองรับเหตุการณ์ความเสียหายที่อาจเกิดขึ้นโดยไม่ได้คาดหมาย สถาบันการเงินควรจัดให้มีแผนฉุกเฉินในการรักษาความพร้อมใช้ของการให้บริการ โดยให้คำนึงถึงปัญหาขัดข้องที่เกิดจากระบบขององค์กรภายนอกที่สถาบันการเงินพึ่งพาหรือเชื่อมต่อด้วย

ทั้งนี้ ธนาคารแห่งประเทศไทยอยู่ระหว่างการจัดทำแนวปฏิบัติในการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศของสถาบันการเงิน (IT Contingency Plan) เพื่อให้สถาบันการเงินใช้เป็นแนวทางในการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศเพื่อใช้รองรับเหตุการณ์ความเสียหายต่างๆ ที่ส่งผลกระทบต่อการดำเนินธุรกิจและการให้บริการอย่างต่อเนื่องของสถาบันการเงิน อย่างไรก็ดี ในปัจจุบันธนาคารพาณิชย์ยังคงต้องปฏิบัติตามหนังสือเวียนที่ ธปท.ณศ. (ว) 969/2531 ลงวันที่ 23 มิถุนายน 2531 เรื่อง การจัดทำแผนฉุกเฉินและระบบคอมพิวเตอร์สำรองต่อไป

2.6 <u>การติดตามตรวจสอบความผิดปกติและความล่อแหลมของระบบให้บริการ (System Detection)</u>

กระบวนการและเทคโนโลยีที่ใช้ในการติดตามตรวจสอบความผิดปกติและความล่อแหลมของระบบให้บริการควรคลอบคลุมถึง

1) การจัดให้มีหลักฐานการตรวจสอบสำหรับกิจกรรมที่สำคัญ เช่น การเข้าถึงระบบให้บริการ รายละเอียดการทำธุรกรรมของลูกค้า การเข้าถึงฐานข้อมูลการตรวจสอบตัวตนและการปฏิบัติงานของพนักงาน เป็นต้น รวมทั้งจัดเก็บหลักฐานที่บันทึกไว้อย่างปลอดภัย

2) การติดตามตรวจสอบหลักฐานดังกล่าวอย่างสม่ำเสมอ โดยเฉพาะรายละเอียดการทำธุรกรรมกับลูกค้า (Transaction Log) ซึ่งจะช่วยให้ทราบถึงความผิดปกติและโอกาสที่จะเกิดภัยคุกคามหรือการลักลอบเข้าถึงระบบให้บริการได้ รวมทั้งมีการรายงานให้ผู้บริหารทราบเมื่อพบความผิดปกติ เพื่อสามารถวางแผนป้องกันล่วงหน้าก่อนเกิดเหตุการณ์จริง

3) การตรวจสอบและแก้ไขความล่อแหลม (Vulnerabilities) ของระบบให้บริการอย่างต่อเนื่อง โดยเฉพาะในส่วนของระบบเครือข่าย โปรแกรมระบบงาน และฐานข้อมูล เนื่องจากผู้บุกรุกสามารถใช้ข้อบกพร่องดังกล่าวเป็นช่องทางในการโจมตีหรือลักลอบเข้าถึง ทั้งนี้ ความล่อแหลมส่วนใหญ่ได้รับการเผยแพร่ให้สาธารณชนทราบอย่างต่อเนื่องทาง Website ต่างๆ (Known Vulnerabilities) เพื่อให้ผู้ที่เกี่ยวข้องนำไปใช้ปรับปรุงระบบของตนเองให้มีความปลอดภัยยิ่งขึ้น

4) การทดสอบเจาะระบบ (Penetration Test) เพื่อทดสอบประสิทธิภาพของเทคโนโลยีการรักษาความปลอดภัย โดยเฉพาะสำหรับระบบให้บริการที่มีความเสี่ยงสูง เช่น การให้บริการโอนเงิน

ตัวอย่างเทคโนโลยีที่เกี่ยวข้องกับการตรวจสอบความผิดปกติและความล่อแหลม ได้แก่

- ระบบตรวจจับการบุกรุก (Intrusion Detection System - IDS)
- เทคโนโลยีที่ใช้ในการตรวจสอบโปรแกรมหรือข้อมูลที่แปลกปลอมเข้ามาในระบบให้บริการ เช่น Network Scanner, Network Analyzer, Security Alert ต่างๆ
- โปรแกรมตรวจสอบและป้องกันไวรัสคอมพิวเตอร์ (Anti-virus Software)

2.7 <u>การแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการได้รับความเสียหายจากภัยคุกคาม (Incident Response & Report)</u>

กระบวนการแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการได้รับความเสียหายจากภัยคุกคามหรือการลักลอบเข้าถึง (Hacking Incidents) ควรครอบคลุมถึง

1) การประเมินโอกาสที่ภัยคุกคามและการลักลอบเข้าถึงจะเกิดขึ้นในกรณีต่างๆ รวมทั้งประเมินความเสียหายและผลกระทบจากเหตุการณ์ดังกล่าว

2) แนวทางในการรับรู้ปัญหาที่เกิดขึ้นอย่างทันท่วงที

3) ขั้นตอนการแก้ไขปัญหา การกำหนดทีมผู้รับผิดชอบซึ่งควรได้รับการฝึกฝนให้วิเคราะห์และจัดการกับปัญหาต่างๆ ที่เกิดขึ้น รวมทั้งวิธีการรายงานต่อผู้บริหาร

4) การจัดเตรียมข้อมูลและขั้นตอนการขอความช่วยเหลือในกรณีฉุกเฉินจากผู้เชี่ยวชาญทั้งจากภายในและภายนอกองค์กร โดยเฉพาะความช่วยเหลือทางเทคนิค

5) การสื่อสารและประชาสัมพันธ์เพื่อชี้แจงและทำความเข้าใจกับพนักงาน สื่อมวลชน และลูกค้าผู้ใช้บริการอย่างรวดเร็วเกี่ยวกับปัญหาที่เกิดขึ้นและวิธีการแก้ไขที่ได้ดำเนินการไปแล้ว เพื่อรักษาภาพพจน์และชื่อเสียงของสถาบันการเงิน รวมทั้งสร้างความเชื่อมั่นแก่ลูกค้าผู้ใช้บริการและผู้มีส่วนเกี่ยวข้อง

6) การรวบรวมหลักฐานต่างๆ ที่เป็นประโยชน์ในการดำเนินคดีกับผู้บุกรุก เช่น หลักฐานที่บันทึกการเข้าถึงข้อมูลและส่วนต่างๆ ของระบบให้บริการ เครื่องคอมพิวเตอร์ที่ผู้บุกรุกใช้เป็นเครื่องมือติดต่อสื่อสาร ข้อมูลบัญชีที่ผู้บุกรุกใช้ถ่ายโอนเงิน ข้อมูลที่แสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วัน เวลา และอื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสาร เป็นต้น

7) การจัดทำรายงานที่เป็นลายลักษณ์อักษร เพื่อเสนอต่อคณะกรรมการสถาบันการเงิน ทั้งนี้ คณะกรรมการสถาบันการเงินอาจมอบหมายให้คณะกรรมการที่รับผิดชอบด้านงานเทคโนโลยีสารสนเทศ หรือคณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการตรวจสอบทำหน้าที่พิจารณารายงานดังกล่าวแทนก็ได้ อย่างไรก็ดี ในกรณีที่เป็นความเสียหายที่มีนัยสำคัญและมีผลกระทบต่อชื่อเสียงและการดำเนินงานของสถาบันการเงิน ให้คณะกรรมการชุดย่อยที่ได้รับมอบหมายนั้นเสนอรายงานดังกล่าวให้คณะกรรมการสถาบันการเงินทราบด้วย

รายงานที่จัดทำเป็นลายลักษณ์อักษรควรมีสาระสำคัญดังนี้

7.1) วัน เวลา และสถานที่ที่ระบบให้บริการได้รับความเสียหายจากภัยคุกคามหรือการลักลอบเข้าถึง

7.2) ลักษณะ วิธีการที่ใช้ในการลักลอบเข้าถึง และผู้บุกรุก (กรณีทราบ)

7.3) สาเหตุและลักษณะความเสียหายที่เกิดขึ้น โดยระบุถึงข้อมูล ระบบงาน หรือสื่ออิเล็กทรอนิกส์ที่ได้รับความเสียหาย

7.4) การประเมินความเสียหายที่เกิดขึ้น

7.5) การแก้ไขปัญหาที่ได้ดำเนินการแล้วและแนวทางที่จะดำเนินการต่อไป

7.6) รายละเอียดของผู้รับผิดชอบในจุดที่เกิดภัยคุกคามหรือการลักลอบเข้าถึง เช่น ชื่อ ตำแหน่ง ที่อยู่ หมายเลขโทรศัพท์และหน้าที่ความรับผิดชอบ

ทั้งนี้ สถาบันการเงินต้องจัดให้มีข้อมูลสำหรับการเข้าตรวจสอบโดยธนาคารแห่งประเทศไทย

ตัวอย่างเทคโนโลยีที่ใช้ในการแก้ไขปัญหาภัยคุกคามและการลักลอบเข้าถึง ได้แก่

- ระบบตรวจจับการบุกรุก (Intrusion Detection System - IDS)
- เทคโนโลยีที่ใช้ในการตรวจสอบโปรแกรมหรือข้อมูลที่แปลกปลอมเข้ามาในระบบให้บริการ เช่น Network Scanner ที่ถูกออกแบบให้สามารถจัดการกับปัญหาหรือความผิดปกติที่เกิดขึ้น (โปรดดูภาคผนวก 1 <u>ตัวอย่างเทคโนโลยีการรักษาความปลอดภัยสำหรับการให้บริการการเงินทางอิเล็กทรอนิกส์</u>)

3. <u>กระบวนการเสริมการรักษาความปลอดภัยให้มีประสิทธิภาพ</u>

3.1 <u>การฝึกอบรมและให้ความรู้แก่พนักงาน</u>

สถาบันการเงินควรจัดให้มีการพัฒนา ฝึกอบรมและให้ความรู้อย่างต่อเนื่องแก่ผู้บริหารและพนักงานทุกระดับที่เกี่ยวข้องกับการให้บริการ เพื่อให้ตระหนักถึงความปลอดภัยในการให้บริการและสามารถปฏิบัติตามนโยบายและกระบวนการรักษาความปลอดภัยได้อย่างมีประสิทธิภาพ นอกจากนั้น ผู้บริหารและพนักงานที่เกี่ยวข้องควรมีการติดตามพัฒนาการทางเทคโนโลยีและภัยคุกคามใหม่ๆ ที่เกิดขึ้นอย่างใกล้ชิด รวมทั้งเผยแพร่ข้อมูลที่เป็นประโยชน์แก่พนักงานอื่นในองค์กรด้วย

3.2 <u>การให้คำแนะนำแก่ลูกค้าผู้ใช้บริการ</u>

สถาบันการเงินควรให้ข้อมูลและคำแนะนำที่เป็นประโยชน์แก่ลูกค้า เช่น วิธีการใช้บริการอย่างปลอดภัย ข้อมูลทางเทคนิคหรือวิธีการรักษาความปลอดภัยเครื่องคอมพิวเตอร์และอุปกรณ์ที่ลูกค้าใช้ในการทำธุรกรรม เนื่องจากผู้บุกรุกสามารถเจาะระบบของลูกค้าเพื่อ

โจรกรรมข้อมูลและปลอมตัวเป็นลูกค้าเข้าทำธุรกรรมกับสถาบันการเงินได้ คำแนะนำควรรวมถึงการให้ลูกค้าระมัดระวังการใช้หรือ Download Software จากแหล่งที่ไม่เป็นที่รู้จักหรือน่าสงสัย เนื่องจากอาจมีโปรแกรมของผู้บุกรุกแฝงมาด้วย (โปรดดูภาคผนวก 2 การให้คำแนะนำแก่ลูกค้าผู้ใช้บริการ)

การให้ข้อมูลและคำแนะนำดังกล่าวควรใช้ภาษาที่เข้าใจง่ายและเปิดเผยไว้บน Website ของสถาบันการเงินโดยให้ลูกค้าสามารถเรียกดูได้โดยสะดวก และเพื่ออำนวยความสะดวกให้แก่ลูกค้า สถาบันการเงินอาจจัดให้มี Help Desk เพื่อทำหน้าที่ตอบปัญหาและให้คำแนะนำต่างๆ แก่ลูกค้าในการใช้บริการการเงินทางอิเล็กทรอนิกส์ด้วย นอกจากนั้น สถาบันการเงินอาจจัดให้มีการฝึกอบรมลูกค้าผู้ใช้บริการ เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับวิธีการรักษาความปลอดภัยในส่วนที่เกี่ยวข้องกับลูกค้าผู้ใช้บริการ รวมทั้งระบบการรักษาความปลอดภัยของสถาบันการเงินที่ลูกค้าผู้ใช้บริการควรทราบ ซึ่งเป็นการให้ความรู้และความมั่นใจในการใช้บริการการเงินทางอิเล็กทรอนิกส์ได้อีกทางหนึ่ง

นอกจากนั้น สถาบันการเงินควรเปิดเผยข้อตกลงและเงื่อนไขในการให้บริการให้ลูกค้าทราบ และมีวิธีการให้ลูกค้าแสดงการยอมรับข้อตกลงและเงื่อนไขดังกล่าวก่อนตัดสินใจใช้บริการ โดยในการให้บริการโอนเงิน ให้ธนาคารพาณิชย์ถือปฏิบัติตามหนังสือเวียนที่ ธปท.งก. (ว) 1230/2537 ลงวันที่ 5 กรกฎาคม 2537 เรื่อง หลักเกณฑ์การโอนเงินทางอิเล็กทรอนิกส์ ทั้งนี้จนกว่า ธปท. จะทำการปรับปรุงหลักเกณฑ์ดังกล่าว

3.3 การควบคุมภายใน

สถาบันการเงินควรจัดให้มีกระบวนการควบคุมภายในที่เหมาะสมกับการให้บริการการเงินทางอิเล็กทรอนิกส์ อาทิ ระมัดระวังไม่ให้การให้บริการการเงินทางอิเล็กทรอนิกส์ขัดต่อกฎหมายและข้อบังคับของทางการอื่นที่เกี่ยวข้อง ทั้งในเรื่องของวิธีการดำเนินงานและเทคโนโลยีที่ใช้ มีการบริหารพนักงานที่เกี่ยวข้องโดยใช้หลักการแบ่งแยกหน้าที่ (Segregation of Duties) อย่างเหมาะสม มีขั้นตอนและวิธีการปฏิบัติงานที่ชัดเจน มีการควบคุมการปฏิบัติงานอย่างเหมาะสม มีการบันทึกหลักฐานการปฏิบัติงานของพนักงาน รวมทั้งมีการเก็บรักษาหลักฐานและเอกสารสำคัญเกี่ยวกับการให้บริการไว้อย่างปลอดภัย

ภาคผนวก 1

ตัวอย่างเทคโนโลยีการรักษาความปลอดภัยสำหรับการให้บริการการเงินทางอิเล็กทรอนิกส์

ก. เทคโนโลยีการรักษาความปลอดภัยระบบให้บริการ

เทคโนโลยีการรักษาความปลอดภัยระบบให้บริการ ซึ่งต้องมีการเชื่อมต่อเครือข่ายภายในกับเครือข่ายภายนอก โดยเฉพาะเครือข่ายอินเทอร์เน็ต (Internet) หรือเครือข่ายการสื่อสารแบบไร้สาย (Wireless Communication Network) มีดังนี้

1. Firewall

Firewall เป็นเทคโนโลยีที่ใช้ป้องกันการลักลอบเข้าถึงเครือข่ายภายใน โดยจะทำหน้าที่ตรวจสอบและอนุญาตให้เฉพาะข้อมูลที่เกี่ยวข้องผ่านเข้าและออกจากเครือข่าย รวมทั้งสกัดกั้นข้อมูลหรือคำสั่งที่มาจากแหล่งที่น่าสงสัย

ประสิทธิภาพของ Firewall ขึ้นอยู่กับการออกแบบ การติดตั้ง การควบคุม และการบำรุงรักษา โดยควรมีการกำหนดกระบวนการออกแบบ การติดตั้ง การควบคุม และการบำรุงรักษา Firewall ให้ชัดเจนและเป็นลายลักษณ์อักษร รวมทั้งควรมีกระบวนการตรวจสอบและปรับปรุงอย่างต่อเนื่อง เพื่อเป็นการเพิ่มประสิทธิภาพในการทำงานของ Firewall

แนวปฏิบัติในการใช้ Firewall เพื่อรักษาความปลอดภัยระบบให้บริการควรรวมถึง

1.1 การติดตั้ง External Firewall เพื่อควบคุมการรับส่งข้อมูลระหว่างเครือข่ายภายนอกและ Web Server

1.2 การติดตั้ง Internal Firewall เพื่อควบคุมการรับส่งข้อมูลระหว่าง Web Server และเครือข่ายภายใน

1.3 การจัดให้ Firewall ที่ใช้ในแต่ละชั้นเป็นคนละชนิดกัน เพื่อให้ยากต่อการลักลอบเข้าถึง

1.4 การกำหนดวิธีการดำเนินการเกี่ยวกับ Firewall ไว้อย่างชัดเจนและเป็นลายลักษณ์อักษร เช่น การติดตั้ง การตั้งค่า (Configuration) การควบคุม และการบำรุงรักษา เพื่อประโยชน์ในการติดตามดูแลและสามารถนำมาใช้งานได้ทันทีเมื่อเกิดเหตุการณ์ความเสียหาย

2. เทคโนโลยีการเข้ารหัสลับ (Encryption Technology)

เทคโนโลยีการเข้ารหัสลับเป็นวิธีการที่สามารถรักษาความลับและความถูกต้องเชื่อถือได้ของข้อมูล โดยการแปลงข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถเข้าใจได้ ทั้งนี้ ประสิทธิภาพของการเข้ารหัสลับขึ้นอยู่กับสมการทางคณิตศาสตร์ที่ใช้เข้ารหัส (Cryptographic Algorithms) ความยาวของกุญแจเข้ารหัส (Cryptographic key) และกระบวนการในการบริหารจัดการกุญแจ

การใช้เทคโนโลยีการเข้ารหัสลับควรพิจารณาให้เหมาะสมกับระดับความเสี่ยง ระดับความสำคัญของข้อมูล และระดับความปลอดภัยที่ต้องการ โดยคำนึงถึงประเด็นสำคัญดังนี้

2.1 Encryption Algorithm ที่ใช้ควรได้รับการทดสอบจนเป็นที่ยอมรับตามมาตรฐานด้านความปลอดภัย เช่น TripleDES, AES128/192/256, SSL/RC4/128, RSA1024+ ซึ่งสถาบันการเงินควรติดตามพัฒนาการด้าน Encryption Algorithm อย่างใกล้ชิดด้วย

2.2 การจัดให้มีกระบวนการในการบริหารจัดการกุญแจ (Key Management) ที่มีประสิทธิภาพ โดยการดำเนินการเกี่ยวกับกุญแจทุกประเภท เช่น การสร้าง การจัดเก็บ การจัดส่ง และการเปลี่ยน ควรกระทำอย่างปลอดภัยและมีการควบคุมที่เหมาะสม

2.3 การจัดให้มีการควบคุมการรับส่งข้อมูลที่มีประสิทธิภาพ โดยการรับส่งข้อมูลระหว่างสถาบันการเงินกับลูกค้าผู้ใช้บริการควรกระทำผ่านช่องทางที่มีความปลอดภัยสูง เช่น Secure Sockets Layer (SSL) การรับส่งข้อมูลลับหรือข้อมูลสำคัญต่างๆ เช่น รหัสผ่านของลูกค้าผู้ใช้บริการควรใช้วิธีการเข้ารหัสลับตั้งแต่จุดที่ลูกค้าเริ่มป้อนข้อมูลไปจนถึง Server ในเครือข่ายภายในที่ทำการประมวลผล (End-to-end Encryption) รวมถึงมีการเข้ารหัสลับข้อมูลสำคัญระหว่างรับส่ง (Transport Encryption)

2.4 การจัดให้มีการรักษาความปลอดภัย Hardware และ Software ที่ใช้ในการเข้ารหัสและถอดรหัสลับ

3. <u>ระบบตรวจจับการบุกรุก (Intrusion Detection System)</u>

ระบบตรวจจับการบุกรุกเป็นเทคโนโลยีที่ใช้ตรวจจับความผิดปกติหรือความพยายามที่จะโจมตีหรือลักลอบเข้าถึงเครือข่ายภายในหรือฐานข้อมูล โดยการวิเคราะห์ข้อมูลที่ไหลผ่านเครือข่ายและเปรียบเทียบกับรูปแบบข้อมูลที่เป็นการลักลอบเข้าถึง หรือโดยการวิเคราะห์พฤติกรรมการทำงานของเครือข่ายที่แตกต่างไปจากพฤติกรรมการทำงานแบบปกติ

ระบบตรวจจับการบุกรุกควรได้รับการติดตั้งที่ Server ที่สำคัญหรือที่เครือข่ายภายใน รวมทั้งจัดให้มีกระบวนการรายงานให้ผู้ที่รับผิดชอบทราบในกรณีพบความผิดปกติหรือความพยายามที่จะลักลอบเข้าถึง

4. <u>เทคโนโลยีการรักษาความปลอดภัยอื่นๆ</u>

4.1 ติดตั้ง Active Content Filter หรือเครื่องมือที่สามารถตรวจสอบและสกัดกั้นโปรแกรม รหัส ไฟล์ หรือจดหมายอิเล็กทรอนิกส์ที่อาจเป็นอันตรายไม่ให้เข้าสู่เครือข่ายภายใน

4.2 ติดตั้ง Web Application Firewall หรือ Scanner เพื่อตรวจสอบและสกัดกั้นคำสั่งหรือรหัสต่างๆ ที่อาจเป็นอันตรายไม่ให้เข้าสู่เครือข่ายภายในระดับ Web Application Layer

4.3 ติดตั้งโปรแกรมป้องกันไวรัส เพื่อป้องกันความเสียหายต่อระบบให้บริการ

ข. <u>เทคโนโลยีการตรวจสอบตัวตนลูกค้าผู้ใช้บริการ</u>

เทคโนโลยีสำหรับการตรวจสอบตัวตนที่ใช้กันอยู่ในปัจจุบันสามารถสรุปได้ดังนี้

1. <u>รหัสผ่านและเลขประจำตัว (Passwords and Personal Identification Numbers)</u>

เป็นวิธีการตรวจสอบตัวตนที่ใช้กันมากที่สุด เนื่องจากสะดวกและง่ายต่อการใช้งาน โดยในการเข้าใช้บริการ ลูกค้าต้องป้อนชื่อและรหัสผ่านซึ่งเป็นรหัสลับส่วนตัวของลูกค้าให้ระบบดำเนินการตรวจสอบก่อนเข้าใช้บริการ ประสิทธิภาพของระบบให้บริการที่ใช้รหัสผ่านเป็นวิธีการตรวจสอบตัวตนขึ้นอยู่กับการเก็บรักษารหัสผ่าน การกำหนดรูปแบบและความยาวของรหัสผ่าน และการควบคุมต่างๆ ที่เกี่ยวข้อง

ระบบให้บริการที่ใช้รหัสผ่านเป็นวิธีการตรวจสอบตัวตนควรดำเนินการดังนี้

- ให้คำแนะนำแก่ลูกค้าและพนักงานเกี่ยวกับการกำหนดและการเก็บรักษารหัสผ่าน
- กำหนดรูปแบบและความยาวของรหัสผ่านให้เหมาะสมกับระดับความเสี่ยงของธุรกรรม ซึ่งโดยทั่วไปรหัสผ่านควรมีความยาวตั้งแต่ 8 ตัวอักษรขึ้นไป และใช้ตัวเลข ตัวพยัญชนะและอักขระพิเศษผสมกัน
- ไม่ใช้ชื่อบุคคล ชื่อสถานที่ หรือคำศัพท์ที่มีอยู่ในพจนานุกรมทั้งภาษาไทยและภาษาอังกฤษ ในการกำหนดรหัสผ่าน
- งดให้บริการแก่ผู้ใช้งานที่ Login ผิดเกินกว่าจำนวนครั้งที่กำหนด
- หยุดให้บริการเมื่อระบบไม่ได้ถูกใช้งานช่วงเวลาหนึ่ง
- กำหนดอายุการใช้งานของรหัสผ่านอย่างเหมาะสม
- จัดให้มีกระบวนการที่ปลอดภัยในการสร้าง การรับส่ง และการจัดเก็บรหัสผ่าน โดยรหัสผ่านควรได้รับการเข้ารหัสลับทั้งในระหว่างการรับส่งและการจัดเก็บ
- แยกฐานข้อมูลที่เก็บรหัสผ่านออกจากฐานข้อมูลอื่น รวมทั้งมีการรักษาความปลอดภัยอย่างเพียงพอ

2. <u>ใบรับรองลายมือชื่ออิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์</u>

ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) คือ อักษร อักขระ ตัวเลข เสียง หรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

ใบรับรองลายมือชื่ออิเล็กทรอนิกส์ (Electronic Certificate) คือ ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใด ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์

เทคโนโลยี Public Key Infrastructure (PKI) ซึ่งเป็นเทคโนโลยีที่ใช้ในการตรวจสอบตัวตน รักษาความถูกต้องและความลับของข้อมูลได้อย่างมีประสิทธิภาพ โดยสามารถนำมาใช้สร้างลายมือชื่ออิเล็กทรอนิกส์และใบรับรองได้ เรียกว่า Digital Signature และ Digital Certificate

เทคโนโลยี PKI อยู่บนพื้นฐานของการใช้กุญแจสาธารณะ (Public Key) และกุญแจส่วนตัว (Private Key) ซึ่งสร้างขึ้นโดยใช้สมการทางคณิตศาสตร์ (Algorithms) ที่ได้รับการทดสอบจนเป็นที่ยอมรับในด้านความปลอดภัย กุญแจสาธารณะถูกเก็บไว้ที่ผู้ประกอบการออกใบรับรองลายมือชื่ออิเล็กทรอนิกส์ (Certificate Authority) ส่วนกุญแจส่วนตัวถูกเก็บไว้อย่างเป็นความลับในเครื่องคอมพิวเตอร์หรือ Smart card ของเจ้าของลายมือชื่ออิเล็กทรอนิกส์ กุญแจส่วนตัวนี้จะใช้สร้าง Digital Signature ในเวลาที่ลูกค้าส่งข้อมูลให้สถาบันการเงิน

Digital Signature เป็นลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นจากกุญแจส่วนตัวของบุคคลหนึ่ง และสามารถใช้ยืนยันตัวบุคคลนั้นโดยการใช้กุญแจสาธารณะของบุคคลนั้นมาตรวจสอบตัวตน ผู้ประกอบการออกใบรับรองที่เป็นผู้เก็บรักษากุญแจสาธารณะของบุคคลนั้นจะทำหน้าที่จัดส่งกุญแจสาธารณะให้แก่คู่กรณีที่ต้องการตรวจสอบตัวตน พร้อมกับออกใบรับรองลายมือชื่ออิเล็กทรอนิกส์เพื่อยืนยันว่ากุญแจสาธารณะเป็นของบุคคลนั้น

ระบบให้บริการที่ใช้เทคโนโลยี PKI เป็นวิธีการตรวจสอบตัวตนควรดำเนินการดังนี้

- จัดให้มีการตรวจสอบใบรับรองลายมือชื่ออิเล็กทรอนิกส์ที่ได้รับก่อนที่จะเริ่มอนุญาตให้บริการทำธุรกรรม เช่น มีการตรวจสอบกับข้อมูลใบรับรองที่ถูกยกเลิก (Revocation List) ที่เป็นปัจจุบัน

- จัดให้มีการรักษาความปลอดภัยระบบงานและเครื่องคอมพิวเตอร์ที่รองรับการตรวจสอบตัวตนโดยเทคโนโลยี PKI

- จัดให้มีบันทึกการทำงานของระบบงานและเครื่องคอมพิวเตอร์ที่รองรับการตรวจสอบตัวตนโดยเทคโนโลยี PKI

3. <u>Tokens/Smart card</u>

เป็นการตรวจสอบตัวตนโดยใช้สิ่งที่ลูกค้าเป็นเจ้าของ เช่น บัตรต่างๆ ที่สามารถฝัง Chip (Smart card) ควบคู่กับการใช้รหัสผ่านหรือลักษณะทางชีวภาพ (Biometrics) ของลูกค้า วิธีการนี้จึงมีความปลอดภัยสูงกว่าการใช้รหัสผ่านเพียงอย่างเดียวในการตรวจสอบตัวตน

ระบบให้บริการที่ใช้ Tokens/Smart card เป็นวิธีการตรวจสอบตัวตนควรดำเนินการดังนี้

- จัดให้มีกระบวนการสร้างและจัดส่ง Tokens/Smart card ที่ปลอดภัย
- กำหนดอายุการใช้งานของ Tokens/Smart card วิธีการเปลี่ยนทดแทน และวิธีการยกเลิกที่เหมาะสม
- งดให้บริการแก่ผู้ใช้งานที่ Login ผิดเกินกว่าจำนวนครั้งที่กำหนด
- จัดให้มีกฎเกณฑ์และข้อตกลงในการใช้ Tokens/Smart card รวมทั้งชี้แจงให้ลูกค้าทราบถึงวิธีการใช้ Tokens/Smart card อย่างปลอดภัย

4. ลักษณะทางชีวภาพ (Biometrics)

เป็นการตรวจสอบตัวตนโดยใช้ลักษณะเฉพาะของลูกค้า เช่น เสียง ลายนิ้วมือ ลักษณะมือ ลูกตา และใบหน้า เป็นต้น ลักษณะเฉพาะดังกล่าวจะถูกจัดเก็บไว้เพื่อใช้เปรียบเทียบและตรวจสอบตัวตนลูกค้าก่อนการให้บริการทำธุรกรรม

ระบบให้บริการที่ใช้ลักษณะทางชีวภาพเป็นวิธีการตรวจสอบตัวตน ควรดำเนินการดังนี้

- จัดให้มีกระบวนการที่ปลอดภัยในการบันทึกลักษณะทางชีวภาพของลูกค้า
- จัดให้มีการเข้ารหัสลับลักษณะทางชีวภาพทั้งในระหว่างการรับส่งและการจัดเก็บ
- งดให้บริการแก่ผู้ใช้งานที่ Login ผิดเกินกว่าจำนวนครั้งที่กำหนด

ภาคผนวก 2

การให้คำแนะนำแก่ลูกค้าผู้ใช้บริการ

สถาบันการเงินควรให้คำแนะนำที่เป็นประโยชน์แก่ลูกค้าผู้ใช้บริการเพื่อให้เข้าใจและตระหนักถึงความสำคัญของการรักษาความปลอดภัยในการใช้บริการ โดยควรรวมถึงคำแนะนำดังต่อไปนี้

1) แนะนำลูกค้าผู้ใช้บริการไม่ให้เปิดเผยข้อมูลเลขประจำตัวและรหัสผ่านให้บุคคลอื่นทราบ ไม่เขียนหรือจดรหัสผ่านไว้ในที่ที่เห็นได้ง่าย ทำลายเอกสารที่ใช้แจ้งเลขประจำตัวและรหัสผ่าน รวมทั้งแนะนำลูกค้าผู้ใช้บริการให้ระมัดระวังการถูกแอบอ้างหรือหลอกลวงให้เปิดเผยข้อมูลเลขประจำตัวและรหัสผ่าน

2) แนะนำลูกค้าผู้ใช้บริการเกี่ยวกับวิธีการกำหนดรหัสผ่านอย่างปลอดภัย มีการเปลี่ยนรหัสผ่านเป็นประจำ และแนะนำให้ลูกค้าผู้ใช้บริการทราบถึงช่องทางในการแจ้งให้สถาบันการเงินทราบทันทีที่พบว่าข้อมูลเลขประจำตัวหรือรหัสผ่านเกิดปัญหา

3) แนะนำลูกค้าผู้ใช้บริการให้ตรวจสอบ Address ของ Website ของสถาบันการเงินให้ถูกต้องก่อนเริ่มทำธุรกรรม เพื่อป้องกันกรณีที่มีการปลอมแปลง Website

4) แนะนำลูกค้าผู้ใช้บริการให้ตรวจสอบความถูกต้องของรายการธุรกรรม เช่น จำนวนเงิน วันที่ทำรายการ เลขที่บัญชี และยอดเงินในบัญชี อย่างสม่ำเสมอ เพื่อป้องกันรายการธุรกรรมผิดปกติที่อาจเกิดขึ้น

5) แนะนำลูกค้าผู้ใช้บริการให้รู้จักการรักษาความปลอดภัยเครื่องคอมพิวเตอร์ของตนเอง เช่น

- ติดตั้งและใช้งานโปรแกรมป้องกันไวรัสที่มีการปรับปรุงฐานข้อมูลไวรัสให้ทันสมัยและใช้บริการกรองไวรัสทางอินเทอร์เน็ตที่เชื่อถือได้
- มีการควบคุมการเข้าถึงข้อมูลส่วนตัว
- มีการเข้าและออกจากระบบให้บริการอย่างถูกต้อง
- ไม่ละทิ้งเครื่องคอมพิวเตอร์หรืออุปกรณ์ในระหว่างการทำธุรกรรมและออกจากระบบให้บริการอย่างถูกต้อง เมื่อทำธุรกรรมเสร็จสิ้น
- ใช้เครื่องคอมพิวเตอร์และอุปกรณ์ที่เหมาะสมกับระบบการรักษาความปลอดภัยของสถาบันการเงิน
- หลีกเลี่ยงการใช้เครื่องคอมพิวเตอร์และอุปกรณ์ที่ไม่ได้มาตรฐานหรือมาจากแหล่งที่เชื่อถือไม่ได้
- หลีกเลี่ยงการใช้เครื่องคอมพิวเตอร์สาธารณะในการทำธุรกรรมทางการเงิน
- หลีกเลี่ยงการเข้าไปใน Website ที่น่าสงสัย

- หลีกเลี่ยงการเปิดเผยข้อมูลส่วนตัว ข้อมูลทางการเงิน หรือข้อมูลบัตรเครดิต แก่ Website ที่ไม่รู้จักหรือเชื่อถือไม่ได้

- หลีกเลี่ยงการเปิดจดหมายอิเล็กทรอนิกส์ที่ไม่รู้จักหรือน่าสงสัย (Junk Emails)

- หลีกเลี่ยงการติดตั้ง Download หรือใช้ Software จากแหล่งที่ไม่รู้จักหรือไม่สามารถตรวจสอบแหล่งที่มาได้ เนื่องจากระบบของลูกค้าผู้ใช้บริการอาจได้รับโปรแกรมไวรัสหรือโปรแกรมอื่นๆ ที่ผู้บุกรุกสามารถใช้ในการลักลอบเข้าถึงติดมาด้วย

6) ชี้แจงให้ลูกค้าผู้ใช้บริการทราบถึงขอบเขตความรับผิดชอบทั้งในส่วนของสถาบันการเงินและในส่วนของลูกค้าผู้ใช้บริการ