ประกาศธนาคารแห่งประเทศไทย

ที่ สนส. 27/2551

เรื่อง การอนุญาตให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ให้บริการการเงินทางอิเล็กทรอนิกส์

---

1. เหตุผลในการออกประกาศ

บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ซึ่งเป็นผู้ให้บริการทางการเงินมีการนำเทคโนโลยีสารสนเทศเข้ามาใช้ในการดำเนินงานอย่างต่อเนื่อง เพื่อพัฒนาศักยภาพของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ให้มีประสิทธิภาพและรวดเร็วในการตอบสนองความต้องการของผู้ใช้บริการที่เปลี่ยนแปลงไป ซึ่งการเลือกใช้เทคโนโลยีที่เหมาะสมจะทำให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์สามารถลดต้นทุนและเพิ่มประสิทธิภาพการทำงานได้จริง เป็นที่น่าเชื่อถือและเป็นการพิทักษ์รักษาประโยชน์ของประชาชนผู้ใช้บริการ

การใช้เทคโนโลยีสารสนเทศ แม้จะช่วยให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ลดต้นทุนการให้บริการ เพิ่มประสิทธิภาพ เกิดความรวดเร็วและสร้างความสะดวกสบายให้กับผู้ใช้บริการก็จริง แต่การใช้เทคโนโลยีดังกล่าวก็ก่อให้เกิดความเสี่ยงเช่นกัน ดังนั้น การควบคุมดูแลรักษาความปลอดภัยจึงเป็นสิ่งสำคัญ เนื่องจากเมื่อเกิดความเสียหายจากระบบเทคโนโลยีดังกล่าวอาจก่อให้เกิดความเสียหายแก่บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์เองทั้งในด้านจำนวนเงินและชื่อเสียงที่ไม่สามารถประเมินค่าได้ รวมถึงการฉ้อโกงรูปแบบใหม่ ๆ ที่เมื่อเกิดขึ้นแล้วจะเป็นไปอย่างรวดเร็วและเกิดความเสียหายอย่างมากและมีผลกระทบในวงกว้างต่อระบบการเงินของประเทศได้

ธนาคารแห่งประเทศไทยตระหนักถึงความสำคัญดังกล่าว จึงออกหลักเกณฑ์ให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ผู้ใช้เทคโนโลยีสารสนเทศในการให้บริการการเงินถือปฏิบัติตามหลักเกณฑ์ และแนวปฏิบัติต่าง ๆ ที่เหมาะสมกับการให้บริการการเงินทางอิเล็กทรอนิกส์

การออกประกาศฉบับนี้ เพื่ออ้างอิงอำนาจตามกฎหมายให้สอดคล้องกับพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 และเป็นการรวบรวมประกาศกระทรวงการคลังที่เกี่ยวข้องมาประมวลให้อยู่ในฉบับเดียวกัน โดยให้ขอบเขตธุรกิจที่บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ได้รับอนุญาตยังคงเป็นไปตามขอบเขตที่ได้รับอนุญาตอยู่เดิม

ฝนสป33-กส35002-25510803

กส 350	วันที่ 3 ส.ค. 2551

เนื่องจากพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 มีผลยกเลิกกฎหมายว่าด้วยการประกอบธุรกิจเงินทุน ธุรกิจหลักทรัพย์และธุรกิจเครดิตฟองซิเอร์ ดังนั้น กฎกระทรวง ประกาศต่าง ๆ ที่ออกโดยอาศัยอำนาจตามกฎหมายดังกล่าวจึงสิ้นผลบังคับใช้เมื่อธนาคารแห่งประเทศไทยได้ออกประกาศฉบับนี้

2. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา 36 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ธนาคารแห่งประเทศไทยออกหลักเกณฑ์เกี่ยวกับการให้บริการการเงินทางอิเล็กทรอนิกส์ตามข้อกำหนดในประกาศนี้

3. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

4. ประกาศและหนังสือเวียนที่ยกเลิก ตามเอกสารแนบ 1

5. เนื้อหา

5.1 รูปแบบธุรกรรมการให้บริการทางการเงิน

การนำเทคโนโลยีใหม่ ๆ มาใช้เพื่อช่วยในการให้บริการการเงินนั้น บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์จะต้องขออนุญาตตามที่ธนาคารแห่งประเทศไทยกำหนดก่อนการให้บริการ ทั้งในส่วนของเทคโนโลยีใหม่ที่ยังไม่เคยนำมาใช้ และการพัฒนาเทคโนโลยีเดิมเพื่อเพิ่มขีดความสามารถในการให้บริการทางการเงิน

ปัจจุบันรูปแบบการให้บริการทางการเงินที่ธนาคารแห่งประเทศไทยอนุญาตให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ดำเนินการได้ตามหลักเกณฑ์ที่ธนาคารแห่งประเทศไทยกำหนด ได้แก่ การใช้บริการเครือข่ายอินเทอร์เน็ต (Internet) ในการประกอบธุรกิจของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ ตามเอกสารแนบ 2 ซึ่งได้ให้บริการหรือทำธุรกรรมผ่านเครือข่ายดังกล่าว ทั้งนี้ บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ต้องได้รับอนุญาตจากธนาคารแห่งประเทศไทยก่อนการดำเนินการ สำหรับบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ที่ได้รับอนุญาตจากธนาคารแห่งประเทศไทยอยู่เดิมแล้ว ให้ทำได้ต่อไปตามที่ได้รับอนุญาต

5.2 การรักษาความปลอดภัย

5.2.1 การให้บริการทางการเงินผ่านสื่ออิเล็กทรอนิกส์ มีความเสี่ยงที่สำคัญคือ ความเสี่ยงด้านความปลอดภัย (Security Risk) ของข้อมูล ระบบ และเครือข่ายที่ใช้ในการให้บริการ บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์จำเป็นต้องมีนโยบายและกระบวนการรักษาความปลอดภัยที่มีประสิทธิภาพ เพื่อให้สามารถป้องกันระบบการให้บริการจากภัยคุกคาม การลักลอบเข้าถึง และการโจรกรรมข้อมูลทั้งของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์เองและลูกค้า ซึ่งเป็นสาเหตุของความเสียหายทางการเงิน ความเสียหายต่อชื่อเสียง และสามารถนำไปสู่การขาดความเชื่อมั่นต่อระบบการให้บริการของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์โดยรวมได้

ธนาคารแห่งประเทศไทยจึงเห็นว่าบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ควรมีแนวทางในการกำหนดนโยบายและกระบวนการในการรักษาความปลอดภัยสำหรับการให้บริการการเงินทางอิเล็กทรอนิกส์ เพื่อให้บริการดังกล่าวมีความปลอดภัย เป็นที่น่าเชื่อถือ และเป็นการรักษาผลประโยชน์ของลูกค้าบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ ดังนั้น จึงได้ออกแนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ เพื่อเป็นแนวทางสำหรับบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ ตามเอกสารแนบ 3

5.2.2 การจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ เพื่อให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์มีแนวทางในการกำหนดนโยบายและกระบวนการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ เพื่อเตรียมรองรับเหตุการณ์และลดผลกระทบต่าง ๆ ที่อาจเกิดขึ้น รวมทั้งฟื้นฟูระบบเทคโนโลยีสารสนเทศของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ให้กลับคืนสู่สภาพปกติได้ภายในเวลาที่เหมาะสม ซึ่งทำให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์สามารถดำเนินธุรกิจได้อย่างต่อเนื่องหรือได้รับผลกระทบน้อยที่สุดหลังจากเกิดเหตุการณ์หยุดชะงัก อันเป็นการสร้างความเชื่อมั่นให้กับลูกค้าและผู้มีส่วนได้ส่วนเสียในการให้บริการของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ ธนาคารแห่งประเทศไทยจึงได้ออกแนวปฏิบัติในการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ (แผนฉุกเฉินด้าน IT) ตามเอกสารแนบ 4

5.3 การควบคุมภายใน

การที่บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ได้นำคอมพิวเตอร์มาใช้ในการประมวลผลข้อมูลธุรกิจการเงินหรือใช้เป็นเครื่องมือสำคัญในการให้บริการทางการเงินใหม่ ๆ ซึ่งอาจก่อให้เกิดความเสี่ยงและความเสียหายแก่การดำเนินธุรกิจของบริษัทเงินทุนและบริษัท

เครดิตฟองซิเอร์ได้ หากมิได้มีการตระเตรียมในการควบคุมและตรวจสอบไว้ล่วงหน้าอย่างมีประสิทธิภาพเพียงพอ ธนาคารแห่งประเทศไทยจึงกำหนดมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัย เกี่ยวกับการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์เพื่อให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ได้ใช้เป็นแนวปฏิบัติและสามารถปรับใช้ให้เหมาะสมกับสภาพโครงสร้างธุรกิจและสิ่งแวดล้อม ตามมาตรฐานขั้นต่ำการควบคุมภายในและการรักษาความปลอดภัยเกี่ยวกับการประมวลข้อมูลด้วยระบบคอมพิวเตอร์ ตามเอกสารแนบ 5 อันจะช่วยป้องกันหรือบรรเทาความเสียหายที่อาจเกิดขึ้นจากการนำคอมพิวเตอร์มาใช้ในการประมวลผลข้อมูลให้มีความปลอดภัยและมั่นคงอย่างเพียงพอได้ตามสมควร

5.4 การดำเนินการอื่น ๆ

การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) เนื่องด้วยสถาบันการเงินส่วนใหญ่ได้มีการใช้บริการดังกล่าวอย่างแพร่หลายมากขึ้น เพื่อลดต้นทุน เพิ่มขีดความสามารถในการดำเนินงานและพัฒนาศักยภาพการให้บริการให้ทันต่อพัฒนาการของเทคโนโลยีที่มีการเปลี่ยนแปลงอย่างรวดเร็ว ซึ่งบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ที่ใช้บริการดังกล่าว ขอให้ปฏิบัติตามประกาศธนาคารแห่งประเทศไทยว่าด้วยการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) เพื่อให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์สามารถใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และเป็นการพิทักษ์รักษาประโยชน์ของประชาชนผู้ใช้บริการ

5.5 รูปแบบการฉ้อโกงทางการเงินและแนวทางป้องกัน

เพื่อให้ลูกค้าผู้ใช้บริการมีความรู้เท่าทันต่อเหตุการณ์ มีความปลอดภัยเมื่อใช้บริการ ลดผลกระทบและความเสียหายต่อธุรกิจของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ และเป็นการรักษาความเชื่อมั่นของลูกค้าในการใช้บริการการเงินทางอิเล็กทรอนิกส์ของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์

บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ที่ให้บริการธนาคารผ่านเครือข่ายอินเทอร์เน็ต ควรเพิ่มความระมัดระวังในการให้บริการจากการทุจริตผ่านเครือข่ายอินเทอร์เน็ตด้วยวิธี Phishing รวมทั้งจัดให้มีมาตรการป้องกันและแจ้งเตือนลูกค้าเกี่ยวกับการทุจริตที่อาจเกิดขึ้น ตามเอกสารแนบ 6

5.6 กฎหมายที่เกี่ยวข้องกับการให้บริการการเงินทางอิเล็กทรอนิกส์

การบริหารความเสี่ยงทางด้านการให้บริการการเงินทางอิเล็กทรอนิกส์นั้น ยังมีกฎเกณฑ์ที่บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์จำเป็นต้องศึกษาเพิ่มเติมเพื่อใช้ในการบริหารความเสี่ยงของตนและส่งเสริมให้การทำธุรกรรมด้านการธนาคารอิเล็กทรอนิกส์มีความปลอดภัยและเป็นมาตรฐานสากล เช่น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 (ตามเอกสารแนบ 7) และBank for International Settlements (BIS) โดย Basle Committee on Banking Supervision ได้ดำเนินการจัดทำและเผยแพร่ Risk Management Principles for Electronic Banking (ตามเอกสารแนบ 8)

6. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ 3 สิงหาคม 2551

(นางธาริษา วัฒนเกส)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

เอกสารแนบ 1

ประกาศและหนังสือเวียนที่ยกเลิก

ที่	วันที่ลงในประกาศธนาคารแห่งประเทศไทย / หนังสือเวียน	ประเภท	เลขที่	เรื่อง
1	22 ตุลาคม 2535	หนังสือเวียน	ธปท. งศ. (ว) 1850/2535	การกำหนดมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยเกี่ยวกับการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์
2	22 มกราคม 2544	ประกาศกระทรวงการคลัง		การใช้บริการเครือข่ายอินเทอร์เน็ต (Internet) ในการประกอบธุรกิจของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ (หนังสือเวียนนำส่งที่ สนส. (01) ว. 59/2544 ลงวันที่ 14 กุมภาพันธ์ 2544)
3	5 มีนาคม 2545	หนังสือเวียน	ธปท.สนส. (11)ว. 525/2545	การนำส่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544
4	8 มีนาคม 2545	หนังสือเวียน	ธปท.สนส. (11)ว. 559/2545	การนำส่ง Risk Management Principles for Electronic Banking ที่จัดทำโดย Bank for International Settlements (BIS)
5	19 พฤศจิกายน 2546	หนังสือเวียน	ธปท.สนส. (11)ว. 2484/2546	แนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์

ที่	วันที่ลงในประกาศธนาคารแห่งประเทศไทย / หนังสือเวียน	ประเภท	เลขที่	เรื่อง
6	12 ตุลาคม 2548	หนังสือเวียน	ธปท.ฝนส. (21)ว. 1953/2548	แนวปฏิบัติในการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ (แผนฉุกเฉินด้าน IT)

เอกสารแนบ 2

การใช้บริการเครือข่ายอินเทอร์เน็ต (Internet) ในการประกอบธุรกิจ
ของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์

ด้วยบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์มีการเพิ่มช่องทางในการให้บริการแก่ลูกค้ามากขึ้น โดยเฉพาะการนำเทคโนโลยีต่าง ๆ เข้ามาช่วยในการให้บริการแก่ลูกค้า เพื่อความสะดวก รวดเร็ว และลดต้นทุนในการดำเนินงาน

ธนาคารแห่งประเทศไทยกำหนดหลักเกณฑ์ในการอนุญาตให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ใช้บริการเครือข่ายอินเทอร์เน็ต (Internet) ในการประกอบธุรกิจของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ได้ ดังต่อไปนี้

1. การใช้บริการเครือข่ายอินเทอร์เน็ต (Internet) ในการประกอบธุรกิจเงินทุนและธุรกิจเครดิตฟองซิเอร์ ต้องได้รับอนุญาตจากธนาคารแห่งประเทศไทยก่อนดำเนินการ

ทั้งนี้ ไม่รวมถึงการใช้บริการเครือข่ายอินเทอร์เน็ต (Internet) เพื่อเป็นการให้ข้อมูลข่าวสารของกิจการลักษณะเช่นเดียวกับการโฆษณา หรือเผยแพร่ธุรกิจที่ให้บริการ เช่น ขั้นตอนปฏิบัติในการขอกู้ยืมเงิน แบบคำขอกู้ยืมเงิน เอกสารหลักฐานที่จำเป็นต้องใช้ แบบคำขอซื้อตั๋วสัญญาใช้เงิน อัตราดอกเบี้ย เป็นต้น ทั้งกรณีที่กระทำเป็นการทั่วไปหรือเป็นการเฉพาะแก่ลูกค้ารายหนึ่งรายใด ให้กระทำได้โดยไม่ต้องขออนุญาตต่อธนาคารแห่งประเทศไทย

สำหรับบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ที่ได้รับอนุญาตจากธนาคารแห่งประเทศไทย ในการใช้บริการเครือข่ายอินเทอร์เน็ต (Internet) ประกอบธุรกิจเงินทุนและธุรกิจเครดิตฟองซิเอร์แล้วนั้น ให้สามารถใช้บริการเครือข่ายอินเทอร์เน็ต (Internet) ให้บริการธุรกรรมต่าง ๆ ได้ ตามที่ได้รับอนุญาต

2. ในการขออนุญาต ให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ยื่นคำขออนุญาตต่อธนาคารแห่งประเทศไทยตามแบบที่ธนาคารแห่งประเทศไทยกำหนด (ภาคผนวก 1 ท้ายเอกสารแนบ 2) พร้อมทั้งรายละเอียด ดังนี้

2.1 แผนรองรับการประกอบธุรกรรมผ่านเครือข่ายอินเทอร์เน็ต (Internet) โดยอย่างน้อยแผนดังกล่าวต้องมีมาตรการดูแลความปลอดภัยของระบบและข้อมูล การประเมินความเสี่ยงและแผนรองรับในกรณีเกิดปัญหา การพัฒนาทางด้านเทคโนโลยีของระบบและการรักษา

ความปลอดภัย การพัฒนาและฝึกอบรมพนักงาน ระบบการควบคุมภายใน การแก้ไขปัญหาทางด้านกฎหมายที่อาจเกิดขึ้น โดยคำนึงถึงสิทธิและผลประโยชน์ของลูกค้าผู้ใช้บริการ

ทั้งนี้ ต้องพร้อมที่จะอธิบายหรือชี้แจงเพิ่มเติมและปฏิบัติตามที่ธนาคารแห่งประเทศไทยสั่งการ และ

2.2 จัดให้มีและมอบเอกสารหลักฐานสำหรับธุรกรรมที่กระทำแก่ลูกค้า เพื่อใช้เป็นหลักฐานตามกฎหมาย รวมทั้งต้องเก็บรักษาสำเนาไว้ให้ธนาคารแห่งประเทศไทยตรวจสอบได้

3. เมื่อบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ ยื่นคำขอและรายละเอียดตามข้อ 2 แล้ว ให้มีผลเป็นการอนุญาตเมื่อพ้นกำหนด 60 วันนับแต่วันยื่นคำขอ เว้นแต่ธนาคารแห่งประเทศไทยจะมีข้อทักท้วงหรือให้ชี้แจงเพิ่มเติมเป็นลายลักษณ์อักษร ให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ได้รับอนุญาตเมื่อได้รับแจ้งการอนุญาตจากธนาคารแห่งประเทศไทย

4. หลักเกณฑ์ในการประกอบธุรกิจ

4.1 เมื่อบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ได้รับอนุญาตตามข้อ 3 แล้ว บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์สามารถใช้บริการเครือข่ายอินเทอร์เน็ต (Internet) ในการประกอบธุรกิจของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ได้ ภายในขอบเขต ดังต่อไปนี้

4.1.1 บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์สามารถใช้บริการเครือข่ายอินเทอร์เน็ต (Internet) ในการประกอบธุรกรรมอื่น ๆ ที่ได้รับอนุญาตเพิ่มเติมได้ โดยไม่ต้องขออนุญาตใช้เครือข่ายอินเทอร์เน็ต (Internet) ในการประกอบธุรกิจอีก ทั้งนี้ ต้องมีการปรับปรุงแผนรองรับการประกอบธุรกรรมดังกล่าวด้วย

4.1.2 บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์สามารถแสดงเครื่องหมายการค้า (Logo) หรือข้อความของธุรกิจอื่นบน Website ของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ เพื่ออำนวยความสะดวกให้ลูกค้าผู้ใช้บริการทราบว่ามีธุรกิจอื่นใดที่สามารถทำธุรกรรมด้านการเงินผ่านบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์หรือเพื่อเป็นช่องทางให้ลูกค้าผู้ใช้บริการเลือกเข้า Website ของธุรกิจอื่นได้ ยกเว้นหน้าจอภาพแรกซึ่งเป็นหน้าจอภาพหลักของ Website ให้แสดงเฉพาะบริการของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ เท่านั้น

ทั้งนี้ บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ต้องไม่หารายได้จากการแสดงเครื่องหมายการค้า (Logo) หรือข้อความของธุรกิจอื่นดังกล่าว ซึ่งเสมือนเป็นการโฆษณาให้ธุรกิจอื่น และต้องไม่กระทำการใด ๆ ในลักษณะที่เป็นการโฆษณาหรือชี้ชวนให้ลูกค้าผู้ใช้บริการเข้าไปใช้บริการใน Website ของธุรกิจอื่นที่บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์มีการเชื่อมโยง

4.1.3 บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ต้องไม่ให้กระทำขั้นตอนการซื้อขายสินค้าหรือบริการของธุรกิจอื่นบน Website ของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์

4.2 ในการคิดค่าธรรมเนียมการให้บริการผ่านเครือข่ายอินเทอร์เน็ต (Internet) จากลูกค้าผู้ใช้บริการและธุรกิจอื่น บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ต้องจัดให้เป็นไปตามกลไกตลาดเพื่อให้เกิดการแข่งขันและต้องคำนึงถึงความเป็นธรรมต่อลูกค้าผู้ใช้บริการ

4.3 หากมีข้อสัญญาระหว่างบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์กับลูกค้าผู้ใช้บริการ หรือระหว่างบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์กับธุรกิจอื่น กำหนดให้บริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ต้องปฏิบัติอย่างไร ให้บริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ปฏิบัติตามสัญญาดังกล่าว และหากมีข้อสัญญาจำกัดความรับผิดของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ ข้อสัญญาดังกล่าวต้องไม่จำกัดความรับผิดเพื่อกลฉ้อฉลหรือประมาทเลินเล่ออย่างร้ายแรงและต้องไม่ขัดต่อกฎหมาย

ภาคผนวก 1 ท้ายเอกสารแนบ 2

คำขออนุญาตการใช้บริการเครือข่ายอินเทอร์เน็ต (Internet) ประกอบธุรกิจฯ

ทำที่ .....

วันที่ .....

เรียน ผู้ว่าการธนาคารแห่งประเทศไทย

ด้วย.....ประสงค์จะขออนุญาตเพื่อใช้บริการเครือข่ายอินเทอร์เน็ต (Internet) ในการประกอบธุรกิจ ตามรายละเอียดแผนรองรับการประกอบธุรกรรมผ่านเครือข่ายอินเทอร์เน็ต (Internet) และเอกสารหลักฐานสำหรับธุรกรรมที่ให้บริการ ซึ่งระบุในเอกสารที่ส่งมาพร้อมคำขอนี้ ได้แก่

(1) .....

(2) .....

(3) .....

(4) .....

(5) .....

ในกรณีที่ธนาคารแห่งประเทศไทยขอรายละเอียดหรือข้อมูลใด ๆ เพิ่มเติม ข้าพเจ้าจะไปชี้แจงและ/หรือจัดส่งรายละเอียดหรือข้อมูลเพิ่มเติมตามความต้องการของธนาคารแห่งประเทศไทย นอกจากนี้ ในกรณีที่ธนาคารแห่งประเทศไทยกำหนดเงื่อนไขใด ๆ ไม่ว่าก่อนหรือภายหลังจากได้รับอนุญาตแล้ว เพื่อให้ข้าพเจ้ากระทำหรือละเว้นการกระทำ ข้าพเจ้าต้องดำเนินการตามเงื่อนไขดังกล่าวโดยเคร่งครัด

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาต

ลงชื่อ .....

(.....)

ผู้มีอำนาจลงนามแทนบริษัท

<u>เอกสารหลักฐานประกอบคำขออนุญาตการใช้บริการเครือข่ายอินเทอร์เน็ต (Internet) ประกอบธุรกิจ</u>

รายละเอียดที่ต้องส่งพร้อมคำขออนุญาตฯ อย่างน้อยต้องประกอบด้วย

1. แผนรองรับการประกอบธุรกรรมผ่านเครือข่ายอินเทอร์เน็ต (Internet)

1.1 มาตรการรักษาความปลอดภัยของระบบและข้อมูล
(โปรดระบุเทคโนโลยีที่ใช้ประกอบด้วย)

1.2 การประเมินความเสี่ยง

1.3 แผนรองรับกรณีเกิดปัญหา

1.4 การพัฒนาด้านเทคโนโลยีของระบบและการรักษาความปลอดภัย

1.5 การพัฒนาและฝึกอบรมพนักงาน

1.6 ระบบควบคุมภายใน

1.7 การแก้ไขปัญหาทางด้านกฎหมายที่อาจเกิดขึ้นได้ โดยคำนึงถึงสิทธิและผลประโยชน์ของลูกค้าผู้ใช้บริการ

2. เอกสารหลักฐานสำหรับธุรกรรมผ่านเครือข่ายอินเทอร์เน็ต (Internet) ที่ให้บริการ

เอกสารแนบ 3

แนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์

---

1. เหตุผลในการออกแนวปฏิบัติ

1.1 การเสนอบริการทางการเงินผ่านสื่ออิเล็กทรอนิกส์เป็นช่องทางที่บริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์และลูกค้าหันมาให้ความสนใจมากขึ้น เนื่องจากมีความสะดวกรวดเร็วและลูกค้าสามารถทำธุรกรรมได้ทุกที่ทุกเวลาโดยไม่ต้องเดินทางมาที่ทำการของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ ในส่วนของการให้บริการการเงินผ่านเครือข่ายอินเทอร์เน็ต (Internet) บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์หลายแห่งได้ให้บริการแก่ลูกค้าแล้ว หลังจากได้รับอนุญาตจากธนาคารแห่งประเทศไทย

1.2 อย่างไรก็ดี บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ที่สนใจจะเสนอบริการการเงินผ่านสื่ออิเล็กทรอนิกส์ต้องพิจารณาอย่างจริงจังถึงความเหมาะสมในเชิงกลยุทธ์ที่บริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์นั้นจะหันมาเสนอบริการผ่านสื่ออิเล็กทรอนิกส์ เนื่องจากการเปลี่ยนแปลงทางเทคโนโลยีเป็นไปอย่างรวดเร็ว บริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ต้องใช้เงินลงทุนระยะเริ่มแรกสูงและต้องพิจารณาเลือกใช้เทคโนโลยีให้เหมาะสมกับบริการที่จะเสนอให้แก่ลูกค้า คณะกรรมการบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ต้องพิจารณาถึงความเสี่ยงด้านกลยุทธ์อย่างรอบคอบและไม่ควรตัดสินใจให้บริการเพียงเพราะต้องการให้ทัดเทียมกับบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์อื่น แต่ควรตระหนักถึงกลยุทธ์ที่เหมาะสมกับองค์กร

1.3 แม้ว่าการให้บริการการเงินทางอิเล็กทรอนิกส์จะทำให้บริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์สามารถตอบสนองความต้องการของลูกค้าได้รวดเร็วและมีประสิทธิภาพมากขึ้น แต่ก็เป็นการเพิ่มระดับความเสี่ยงประเภทต่างๆ ที่บริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ประสบอยู่แล้วให้มากขึ้น โดยเฉพาะอย่างยิ่งความเสี่ยงด้านความปลอดภัย (Security Risk) ของข้อมูล ระบบ และเครือข่ายที่ใช้ในการให้บริการ

1.4 ความเสี่ยงด้านความปลอดภัย คือ ความเสี่ยงที่ระบบให้บริการของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์จะเกิดความเสียหายจากภัยคุกคามหรือการลักลอบเข้าถึงในลักษณะต่าง ๆ เช่น การลักลอบเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาตทั้งจากภายในและภายนอกองค์กร (Unauthorized Access) การลักลอบนำข้อมูลที่อยู่ระหว่างการรับส่งไปใช้ การลักลอบเข้าทำธุรกรรม

โดยปลอมแปลงข้อมูลการตรวจสอบตัวตน (False Authentication) และการเข้าโจมตีระบบให้บริการจนไม่สามารถทำงานได้ นอกเหนือ จากการใช้เทคนิคทางคอมพิวเตอร์ในการลักลอบกระทำการต่างๆ แล้ว ระบบให้บริการของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ยังอาจได้รับอันตรายจากการใช้วิธีการอื่นหลอกลวงให้บริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์หรือลูกค้าผู้ใช้บริการหลงเชื่อ เพื่อที่จะอนุญาตให้เข้าถึงระบบให้บริการหรือให้ข้อมูลสำคัญได้ (Social Engineering)

1.5 สถาบันการเงินในต่างประเทศได้ประสบปัญหากรณีถูกผู้บุกรุก (Hacker) ลักลอบเข้าถึงระบบข้อมูลและทำความเสียหายให้กับสถาบันการเงินมาแล้ว ความเสียหายดังกล่าวส่งผลกระทบถึงชื่อเสียงของสถาบันการเงิน (Reputational risk) เป็นอย่างมาก หากไม่มีกระบวนการแก้ไขปัญหาและชี้แจงต่อลูกค้าผู้ใช้บริการอย่างรวดเร็วแล้ว ความเสียหายอาจรุนแรงจนถึงขั้นทำให้ลูกค้าขาดความเชื่อมั่นในบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์แล้วถอนเงินฝาก (Deposit Run) ได้

1.6 ในการให้บริการการเงินทางอิเล็กทรอนิกส์ บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์จะต้องคำนึงถึงการรักษาความปลอดภัยระบบให้บริการ นับตั้งแต่ภายในบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์เองจนถึงสื่ออิเล็กทรอนิกส์ต่างๆ ที่ลูกค้าใช้ในการเข้าทำรายการธุรกรรม เนื่องจากในต่างประเทศได้เคยเกิดกรณีที่ผู้บุกรุก เจาะระบบของลูกค้าแล้วเข้าไปแก้ไขข้อมูลเพื่อใช้ปลอมตัวเป็นลูกค้าที่เคยเข้าทำธุรกรรมกับบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ (Cookie Poisoning) จากวิธีการนี้ หากไม่มีการติดตั้งระบบรักษาความปลอดภัยตั้งแต่สื่ออิเล็กทรอนิกส์ที่ลูกค้าใช้ทำรายการแล้วก็อาจเกิดความเสียหายดังกล่าวได้ นอกจากนั้น การให้คำแนะนำแก่ลูกค้าผู้ใช้บริการในด้านการรักษาความปลอดภัยในการใช้บริการก็เป็นสิ่งสำคัญที่จะช่วยเสริมให้กระบวนการรักษาความปลอดภัยของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์เองมีประสิทธิภาพมากยิ่งขึ้น

2. เนื้อหา

2.1 ในแนวปฏิบัตินี้

“บริษัท” หมายความว่า บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ ตามมาตรา 4 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551

“การให้บริการการเงินทางอิเล็กทรอนิกส์” หมายถึง การให้บริการการเงินผ่านสื่ออิเล็กทรอนิกส์ต่างๆ ซึ่งลูกค้าผู้ใช้บริการสามารถทำรายการได้เอง

“บริการการเงิน” หมายถึง ธุรกรรมทางการเงินและธุรกรรมที่เกี่ยวข้องที่บริษัทได้รับอนุญาตให้ดำเนินการได้ เช่น การแสดงข้อมูลในบัญชีของลูกค้าผู้ใช้บริการ การร้องขอ ตรวจสอบ ยืนยัน เปลี่ยนแปลง แก้ไขข้อมูลของลูกค้าผู้ใช้บริการ การรับส่งคำสั่งหรือข้อมูลกับลูกค้าผู้ใช้บริการเพื่อประโยชน์ในการให้บริการและการทำธุรกรรมทางการเงิน เป็นต้น

“สื่ออิเล็กทรอนิกส์” หมายถึง อุปกรณ์หรือเครื่องมือที่บริษัทใช้เป็นช่องทางในการให้บริการการเงินทางอิเล็กทรอนิกส์ เช่น สื่อบันทึกข้อมูล อุปกรณ์สื่อสาร เครื่องคอมพิวเตอร์ และเครือข่ายรูปแบบต่าง ๆ เป็นต้น

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

“เทคโนโลยีรักษาความปลอดภัย” หมายถึง เทคนิค เครื่องมือทางคอมพิวเตอร์หรือเครื่องมือทางอิเล็กทรอนิกส์ต่างๆ ที่บริษัทใช้ในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์

2.2 หลักการ

2.2.1 แนวปฏิบัติฉบับนี้มุ่งเน้นการรักษาความปลอดภัยของการให้บริการการเงินผ่านเครือข่ายสาธารณะ (Public Network) เช่น เครือข่ายอินเทอร์เน็ต (Internet) และเครือข่าย การสื่อสารแบบไร้สาย (Wireless Communication Network) ซึ่งต้องมีการเชื่อมต่อกับเครือข่ายภายใน (Internal Network) ของบริษัท จึงมีโอกาสสูงที่จะเกิดภัยคุกคามในรูปแบบต่างๆ โดยเฉพาะจากผู้บุกรุกซึ่งสามารถสร้างความเสียหายต่อบริษัทได้

2.2.2 บริษัทที่ใช้บริการเครือข่ายสาธารณะเพียงเพื่อเผยแพร่ข้อมูลข่าวสารทางธุรกิจ (Informational Website) ก็ให้พิจารณาประยุกต์ใช้หลักการของแนวปฏิบัตินี้ในการจัดมาตรการรักษาความปลอดภัยที่เหมาะสม เพื่อป้องกันการลักลอบเข้าแก้ไขหรือเปลี่ยนแปลงข้อมูลที่เผยแพร่ ซึ่งจะมีผลกับชื่อเสียงของบริษัทและอาจมีผลกระทบต่อความเชื่อมั่นของลูกค้าต่อการให้บริการของบริษัทในอนาคต หากต้องการขยายขอบเขตการให้บริการการเงินทางอิเล็กทรอนิกส์

2.2.3 บริษัทสามารถนำแนวปฏิบัตินี้ไปประยุกต์ใช้กับการให้บริการการเงินทางอิเล็กทรอนิกส์ที่กระทำผ่านช่องทางอื่นที่มีความเสี่ยงต่ำกว่าได้ เช่น การให้บริการผ่านเครือข่ายเฉพาะ (Proprietary Network)

2.3 เนื้อหาของแนวปฏิบัติสามารถแบ่งเป็น 3 ส่วน ดังนี้

2.3.1 ส่วนที่เป็นการกำหนดนโยบายการรักษาความปลอดภัย

2.3.2 ส่วนที่เป็นกระบวนการหลักของการรักษาความปลอดภัยระบบให้บริการ ซึ่งรวมถึงเทคโนโลยีรักษาความปลอดภัย ได้แก่

(1) การควบคุมการเข้าถึงระบบให้บริการและข้อมูล (Access Control)

(2) การตรวจสอบตัวตนลูกค้าและการป้องกันการปฏิเสธความรับผิด (Authentication & Non-repudiation)

(3) การรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูล (System & Data Integrity)

(4) การรักษาความลับของข้อมูล (Data Confidentiality)

(5) การรักษาความพร้อมใช้ของระบบให้บริการ (System Availability)

(6) การติดตามตรวจสอบความผิดปกติและความล่อแหลมของระบบให้บริการ (System Detection)

(7) การแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการได้รับความเสียหายจากภัยคุกคาม (Incident Response & Report)

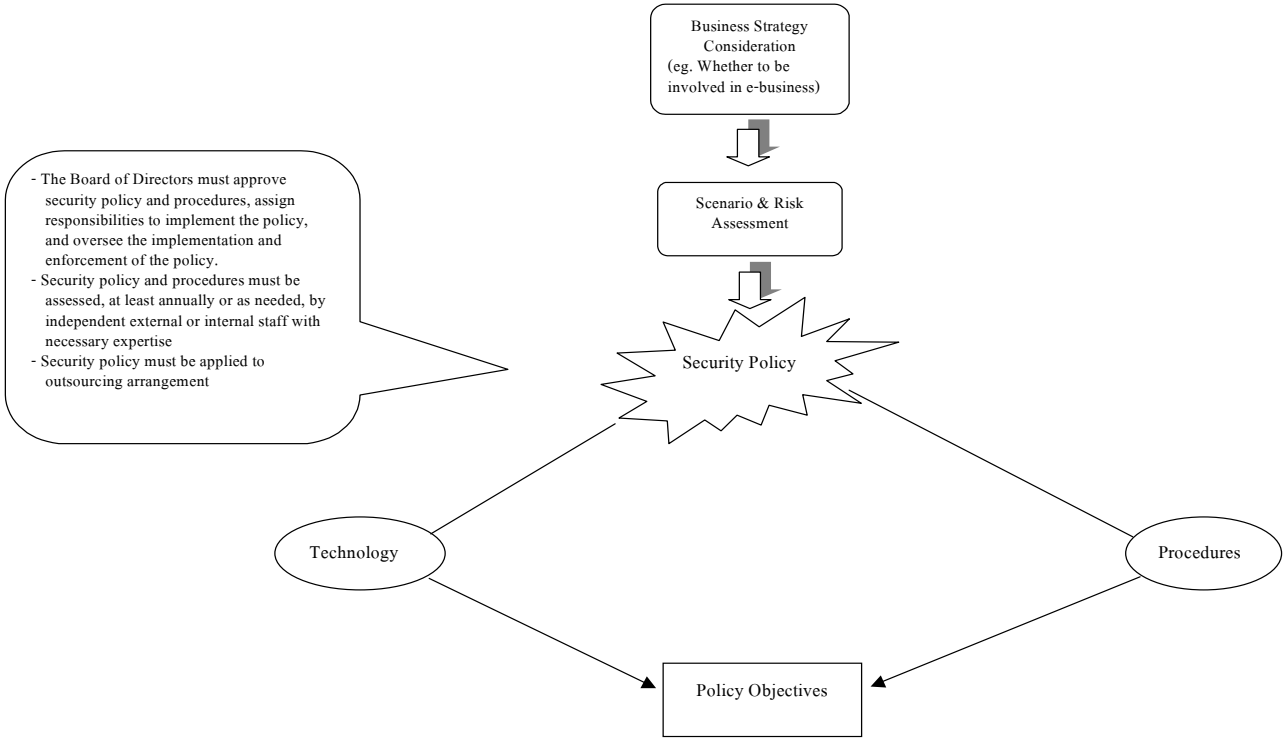
2.3.3 ส่วนเสริมการรักษาความปลอดภัยให้มีประสิทธิภาพ ได้แก่

(1) การฝึกอบรมและให้ความรู้แก่พนักงาน

(2) การให้ข้อมูลและคำแนะนำแก่ลูกค้าผู้ใช้บริการ

(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

3. รายละเอียดของแนวปฏิบัติ

3.1 นโยบายการรักษาความปลอดภัย

3.1.1 คณะกรรมการบริษัทมีหน้าที่โดยตรงในการกำหนดนโยบายการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ที่เป็นลายลักษณ์อักษรและอนุมัติกระบวนการรักษาความปลอดภัยที่ฝ่ายจัดการเสนอ โดยอย่างน้อยจะต้องพิจารณาถึงความเหมาะสมเชิงกลยุทธ์และต้องเข้าใจถึงความเสี่ยงที่อาจเกิดขึ้น ทั้งนี้ คณะกรรมการบริษัทอาจมอบหมายให้คณะกรรมการที่รับผิดชอบด้านงานเทคโนโลยีสารสนเทศ หรือคณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการบริหาร หรือที่ปรึกษาภายนอกที่มีความเชี่ยวชาญมาช่วยจัดทำก่อนเสนอให้คณะกรรมการบริษัทอนุมัติก็ได้

3.1.2 ในการกำหนดนโยบายการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ มีปัจจัยที่ต้องคำนึงถึงคือ ความสมดุลของกระบวนการรักษาความปลอดภัยกับความเสี่ยงที่อาจเกิดจากธุรกรรมที่ให้บริการ รวมทั้งต้องคำนึงถึงการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็วมากด้วย

3.1.3 เมื่อมีการอนุมัตินโยบายและกระบวนการรักษาความปลอดภัยแล้ว คณะกรรมการบริษัทต้องกำหนดให้มีผู้บริหารและพนักงานที่รับผิดชอบในการดำเนินการให้เป็นไปตามนโยบายและกระบวนการที่ได้รับการอนุมัติไว้ มีการสื่อสารให้พนักงานได้รับทราบอย่างทั่วถึง มีการติดตามดูแลให้พนักงานและผู้ที่เกี่ยวข้องกับระบบให้บริการปฏิบัติตามนโยบายและกระบวนการรักษาความปลอดภัยอย่างเคร่งครัด รวมทั้งมีการตรวจสอบการปฏิบัติตามอย่างเหมาะสม ทั้งนี้ ประสิทธิภาพของกระบวนการรักษาความปลอดภัยขึ้นอยู่กับการมีนโยบายที่ชัดเจน มีการสื่อสารอย่างทั่วถึง และมีการบังคับใช้อย่างเหมาะสม หากมีการส่งเสริมให้ผู้บริหารและพนักงานทุกระดับมีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความปลอดภัยและความรับผิดชอบของพนักงานแล้วย่อมก่อให้เกิดผลดีในทางปฏิบัติ

3.1.4 คณะกรรมการบริษัทต้องจัดให้มีการประเมินประสิทธิภาพของนโยบายและกระบวนการรักษาความปลอดภัยอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัย เช่น มีการออกผลิตภัณฑ์และบริการใหม่ มีการเปลี่ยนแปลงเทคโนโลยีที่ใช้ หรือมีการลักลอบเข้าถึงระบบให้บริการ (Hacking Incidents) ทั้งนี้ การประเมินสามารถกระทำได้โดยผู้เชี่ยวชาญจากภายนอกหรือภายในองค์กรที่ไม่เป็นผู้พัฒนาหรือปฏิบัติการ

ระบบ นอกจากนั้น บริษัทควรมีการติดตามความก้าวหน้าทางเทคโนโลยีอย่างใกล้ชิดเพื่อนำมาพัฒนานโยบายและกระบวนการรักษาความปลอดภัยให้มีประสิทธิภาพมากขึ้น

3.1.5 ในกรณีที่บริษัทมีการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) เพื่อให้บริการการเงินทางอิเล็กทรอนิกส์ไม่ว่าทั้งหมดหรือบางส่วน คณะกรรมการบริษัทต้องจัดให้มีการประเมินประสิทธิภาพของกระบวนการรักษาความปลอดภัยของผู้ให้บริการเพื่อให้เป็นไปตามนโยบายการรักษาความปลอดภัยที่ได้กำหนดไว้ รวมทั้งให้ถือปฏิบัติตามประกาศว่าด้วย การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) ด้วย

3.2 กระบวนการหลักในการรักษาความปลอดภัย

เนื่องจากการให้บริการการเงินทางอิเล็กทรอนิกส์ผ่านเครือข่ายสาธารณะ เช่น เครือข่ายอินเทอร์เน็ต และเครือข่ายการสื่อสารแบบไร้สาย มีโครงสร้างในลักษณะเปิด ซึ่งบริษัทต้องมีการเชื่อมโยงเครือข่ายภายในกับเครือข่ายสาธารณะ ระบบให้บริการจึงมีความเสี่ยงสูง ที่จะได้รับภัยคุกคามจากผู้บุกรุก (Hackers) ในรูปแบบต่างๆ ที่สามารถสร้างความเสียหายต่อบริษัทได้ เช่น การลักลอบเข้าถึงเครือข่ายภายในที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ตโดยเลียนแบบ IP Address การโจมตีระบบให้บริการโดยใส่ข้อมูลจำนวนมากเข้าสู่ Website เป้าหมายเพื่อให้ระบบทำงานไม่ได้หรือให้เปิดเผยข้อมูลที่สำคัญ การลักลอบส่งโปรแกรมแฝงเข้าระบบให้บริการเพื่อปลอมแปลงข้อมูล หรือการโจมตีระบบให้บริการโดยไวรัสคอมพิวเตอร์ เป็นต้น

บริษัทจึงจำเป็นต้องมีกระบวนการรักษาความปลอดภัยที่ดีและเลือกใช้เทคโนโลยีสำหรับการรักษาความปลอดภัยที่มีประสิทธิภาพและเป็นที่ยอมรับตามมาตรฐานที่เกี่ยวข้อง เพื่อป้องกันภัยคุกคามต่างๆ และเมื่อเกิดภัยคุกคามก็สามารถควบคุมความเสียหายและแก้ไขปัญหาที่เกิดขึ้นได้ ทั้งนี้ กระบวนการหลักในการรักษาความปลอดภัยที่บริษัทต้องกำหนดไว้ในนโยบายการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ประกอบด้วย

3.2.1 การควบคุมการเข้าถึงระบบให้บริการและข้อมูล (Access Control)

กระบวนการและเทคโนโลยีที่ใช้ควบคุมการเข้าถึงระบบให้บริการต้องสามารถป้องกันการลักลอบเข้าถึงโดยผู้ที่ไม่มีสิทธิทั้งจากภายในและภายนอกองค์กร โดยมีการควบคุมการเข้าถึงสถานที่ตั้งของระบบให้บริการและอุปกรณ์สำคัญ (Physical Access Control) และ

มีการควบคุมการเข้าถึงระบบให้บริการและข้อมูลด้วยวิธีการทางคอมพิวเตอร์ (Logical Access Control) ทั้งนี้ กระบวนการดังกล่าวควรครอบคลุมถึง

(1) การกำหนดสิทธิการเข้าถึงระบบให้บริการให้เหมาะสมกับการเข้าใช้บริการของลูกค้าและหน้าที่ความรับผิดชอบของพนักงานในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

(2) การกำหนดให้ผู้มีอำนาจเท่านั้นที่จะเข้าแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงต่างๆ ได้

(3) การบันทึกรายละเอียดการเข้าถึงระบบให้บริการ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบให้บริการไว้เพื่อเป็นหลักฐานการตรวจสอบในกรณีเกิดปัญหา

ตัวอย่างเทคโนโลยีที่ใช้ในการป้องกันการลักลอบเข้าถึง ได้แก่

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

- เครื่องมือที่ใช้ในการตรวจสอบและสกัดกั้นโปรแกรมหรือข้อมูลที่แปลกปลอม เข้ามาในระบบให้บริการ เช่น Application-based Filter, Active Content Filter

- โปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-virus Software)

3.2.2 การตรวจสอบตัวตนลูกค้าและการป้องกันการปฏิเสธความรับผิด (Authentication & Non-repudiation)

กระบวนการและเทคโนโลยีที่ใช้ในการตรวจสอบตัวตนและป้องกันการปฏิเสธความรับผิด (Authentication & Non-repudiation) นอกจากจะเป็นประโยชน์กับบริษัทในการพิสูจน์ตัวตนของลูกค้าก่อนอนุญาตให้ใช้บริการแล้ว ยังเป็นประโยชน์กับลูกค้าในการพิสูจน์ว่าตนเป็นผู้ทำธุรกรรมกับบริษัทในกรณีมีข้อพิพาทเกิดขึ้น ทั้งนี้ กระบวนการดังกล่าวควรครอบคลุมถึง

(1) การจัดให้มีวิธีการตรวจสอบตัวตนและสิทธิในการใช้บริการของลูกค้าก่อนอนุญาตให้ใช้บริการ

(2) การจัดให้วิธีการตรวจสอบตัวตนที่ใช้มีความเหมาะสมกับระดับความเสี่ยง รูปแบบและมูลค่าของธุรกรรมที่ให้บริการ

(3) การจัดให้มีการควบคุมการเข้าถึงและการควบคุมการแก้ไขเปลี่ยนแปลงข้อมูลในฐานข้อมูลที่จัดเก็บข้อมูลที่ใช้ในการตรวจสอบตัวตน (Authentication Database)

(4) การตรวจสอบตัวตนลูกค้าต้องกระทำอย่างต่อเนื่องและปลอดภัย หากมีการหยุดชะงักควรเริ่มตรวจสอบตัวตนลูกค้าใหม่

(5) การจัดให้มีการบันทึกรายละเอียดการเข้าทำธุรกรรมของลูกค้า (Transaction Log) ไว้ เพื่อใช้เป็นหลักฐานการตรวจสอบ รวมทั้งมีการจัดเก็บบันทึกดังกล่าวอย่างปลอดภัย

(6) การจัดให้มีการทบทวนวิธีการตรวจสอบตัวตนอย่างสม่ำเสมอ โดยคำนึงถึงระดับความเสี่ยงและพัฒนาการทางเทคโนโลยีที่เปลี่ยนแปลงไป

ตัวอย่างเทคโนโลยีที่ใช้ในการตรวจสอบตัวตนและป้องกันการปฏิเสธความรับผิดได้แก่

- 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)

3.2.3 การรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูล (System & Data Integrity)

กระบวนการที่ใช้ในการรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูลที่อยู่ระหว่างการรับส่ง การประมวลผล และการจัดเก็บ รวมทั้งการดำเนินการให้ระบบให้บริการสามารถทำงานได้อย่างถูกต้องและสามารถตอบสนองความต้องการของลูกค้าได้อย่างมีประสิทธิภาพควรครอบคลุมถึง

(1) การออกแบบระบบให้บริการและการเลือกใช้เทคโนโลยีที่มีประสิทธิภาพ

(2) การทดสอบระบบให้บริการให้ทำงานได้อย่างถูกต้องก่อนเริ่มใช้งาน หรือทุกครั้งที่มีการเปลี่ยนแปลง

(3) การจัดให้มีการควบคุมการทำงานของระบบให้บริการในขั้นตอนที่สำคัญ เช่น ขั้นตอน การประมวลผล การรับส่งและการจัดเก็บข้อมูล เพื่อให้สามารถป้องกันและตรวจสอบการลักลอบเข้าถึงระบบให้บริการได้

(4) การจัดให้มีการควบคุมการแก้ไขเปลี่ยนแปลงระบบให้บริการและข้อมูล (Change Control) อย่างรัดกุม

3.2.4 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) การเข้ารหัสลับข้อมูลตั้งแต่ ต้นทางถึงปลายทาง (End-to-end Encryption) การเข้ารหัสลับข้อมูลในช่วงจัดเก็บ เป็นต้น

- การใช้ช่องทางที่มีความปลอดภัยสูงในการรับส่งข้อมูลลับ เช่น Secure Sockets Layer (SSL)

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

3.2.5 การรักษาความพร้อมใช้ของระบบให้บริการ (System Availability)

กระบวนการที่ใช้รักษาความพร้อมใช้ของระบบให้บริการควรครอบคลุมถึงการดำเนินการให้ระบบให้บริการมีประสิทธิภาพและมีความพร้อมในการให้บริการได้ตลอดเวลา โดยอย่างน้อยสามารถให้บริการได้ตามช่วงเวลาที่ได้ตกลงไว้กับลูกค้า สามารถรองรับการทำธุรกรรมตามความต้องการของลูกค้าได้อย่างพอเพียง ตอบสนองการทำธุรกรรมได้อย่างรวดเร็วทั้งในช่วงเวลาปกติและช่วงเวลาที่มีการใช้บริการอย่างหนาแน่น รวมทั้งมีการสำรองข้อมูลอย่างเหมาะสมเพื่อให้สามารถกู้ระบบให้กลับมาทำงานได้ตามปกติอย่างทันท่วงทีในกรณีที่เกิดความเสียหาย

ในการเตรียมการรองรับเหตุการณ์ความเสียหายที่อาจเกิดขึ้นโดยไม่ได้คาดหมาย บริษัทควรจัดให้มีแผนฉุกเฉินในการรักษาความพร้อมใช้ของการให้บริการ โดยให้คำนึงถึงปัญหาขัดข้องที่เกิดจากระบบขององค์กรภายนอกที่บริษัทพึ่งพาหรือเชื่อมต่อด้วย ทั้งนี้ให้บริษัทปฏิบัติตามตามประกาศฉบับนี้ เรื่อง แนวปฏิบัติในการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ (แผนฉุกเฉินด้าน IT) (เอกสารแนบ 4)

3.2.6 การติดตามตรวจสอบความผิดปกติและความล่อแหลมของระบบให้บริการ (System Detection)

กระบวนการและเทคโนโลยีที่ใช้ในการติดตามตรวจสอบความผิดปกติและความล่อแหลมของระบบให้บริการควรคลอบคลุมถึง

(1) การจัดให้มีหลักฐานการตรวจสอบสำหรับกิจกรรมที่สำคัญ เช่น การเข้าถึงระบบให้บริการ รายละเอียดการทำธุรกรรมของลูกค้า การเข้าถึงฐานข้อมูลการตรวจสอบตัวตน และการปฏิบัติงานของพนักงาน เป็นต้น รวมทั้งจัดเก็บหลักฐานที่บันทึกไว้อย่างปลอดภัย

(2) การติดตามตรวจสอบหลักฐานดังกล่าวอย่างสม่ำเสมอ โดยเฉพาะรายละเอียดการทำธุรกรรมกับลูกค้า (Transaction Log) ซึ่งจะช่วยให้ทราบถึงความผิดปกติและโอกาสที่จะเกิดภัยคุกคามหรือการลักลอบเข้าถึงระบบให้บริการได้ รวมทั้งมีการรายงานให้ผู้บริหารทราบเมื่อพบความผิดปกติ เพื่อสามารถวางแผนป้องกันล่วงหน้าก่อนเกิดเหตุการณ์จริง

(3) การตรวจสอบและแก้ไขความล่อแหลม (Vulnerabilities) ของระบบให้บริการอย่างต่อเนื่อง โดยเฉพาะในส่วนของระบบเครือข่าย โปรแกรมระบบงาน และฐานข้อมูล เนื่องจาก ผู้บุกรุกสามารถใช้ข้อบกพร่องดังกล่าวเป็นช่องทางในการโจมตีหรือลักลอบเข้าถึง ทั้งนี้ความล่อแหลมส่วนใหญ่ได้รับการเผยแพร่ให้สาธารณชนทราบอย่างต่อเนื่องทาง Website ต่าง ๆ

(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)

3.2.7 การแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการได้รับความเสียหายจากภัยคุกคาม (Incident Response & Report)

กระบวนการแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการได้รับความเสียหายจากภัยคุกคามหรือการลักลอบเข้าถึง (Hacking Incidents) ควรครอบคลุมถึง

(1) การประเมินโอกาสที่ภัยคุกคามและการลักลอบเข้าถึงจะเกิดขึ้นในกรณีต่างๆ รวมทั้งประเมินความเสียหายและผลกระทบจากเหตุการณ์ดังกล่าว

(2) แนวทางในการรับรู้ปัญหาที่เกิดขึ้นอย่างทันท่วงที

(3) ขั้นตอนการแก้ไขปัญหา การกำหนดทีมผู้รับผิดชอบซึ่งควรได้รับการฝึกฝนให้วิเคราะห์และจัดการกับปัญหาต่างๆ ที่เกิดขึ้น รวมทั้งวิธีการรายงานต่อผู้บริหาร

(4) การจัดเตรียมข้อมูลและขั้นตอนการขอความช่วยเหลือในกรณีฉุกเฉินจากผู้เชี่ยวชาญทั้งจากภายในและภายนอกองค์กร โดยเฉพาะความช่วยเหลือทางเทคนิค

(5) การสื่อสารและประชาสัมพันธ์เพื่อชี้แจงและทำความเข้าใจกับพนักงาน สื่อมวลชน และลูกค้าผู้ใช้บริการอย่างรวดเร็วเกี่ยวกับปัญหาที่เกิดขึ้นและวิธีการแก้ไขที่ได้ดำเนินการไปแล้ว เพื่อรักษาภาพพจน์และชื่อเสียงของบริษัท รวมทั้งสร้างความเชื่อมั่นแก่ลูกค้าผู้ใช้บริการและผู้มีส่วนเกี่ยวข้อง

(6) การรวบรวมหลักฐานต่าง ๆ ที่เป็นประโยชน์ในการดำเนินคดีกับผู้บุกรุก เช่น หลักฐานที่บันทึกการเข้าถึงข้อมูลและส่วนต่าง ๆ ของระบบให้บริการ เครื่องคอมพิวเตอร์ที่ผู้บุกรุก ใช้เป็นเครื่องมือติดต่อสื่อสาร ข้อมูลบัญชีที่ผู้บุกรุกใช้ถ่ายโอนเงิน ข้อมูลที่แสดงถึงแหล่งกำเนิดต้นทาง ปลายทาง เส้นทาง วัน เวลา และอื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสาร เป็นต้น

(7) การจัดทำรายงานที่เป็นลายลักษณ์อักษร เพื่อเสนอต่อคณะกรรมการบริษัท ทั้งนี้ คณะกรรมการบริษัทอาจมอบหมายให้คณะกรรมการที่รับผิดชอบด้านงานเทคโนโลยีสารสนเทศ หรือคณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการตรวจสอบทำหน้าที่พิจารณารายงานดังกล่าวแทนก็ได้ อย่างไรก็ดี ในกรณีที่เป็นความเสียหายที่มีนัยสำคัญ และมีผลกระทบต่อชื่อเสียงและการดำเนินงานของบริษัท ให้คณะกรรมการชุดย่อยที่ได้รับมอบหมายนั้นเสนอรายงานดังกล่าวให้คณะกรรมการบริษัททราบด้วย

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 บริษัทต้องจัดให้มีข้อมูลสำหรับการเข้าตรวจสอบโดยธนาคารแห่งประเทศไทย

ตัวอย่างเทคโนโลยีที่ใช้ในการแก้ไขปัญหาภัยคุกคามและการลักลอบเข้าถึง ได้แก่

- ระบบตรวจจับการบุกรุก (Intrusion Detection System - IDS)
- เทคโนโลยีที่ใช้ในการตรวจสอบโปรแกรมหรือข้อมูลที่แปลกปลอมเข้ามาในระบบให้บริการ เช่น Network Scanner ที่ถูกออกแบบให้สามารถจัดการกับปัญหาหรือความ

ผิดปกติที่เกิดขึ้น (ภาคผนวก 1 ท้ายเอกสารแนบ 3 ตัวอย่างเทคโนโลยีการรักษาความปลอดภัยสำหรับการให้บริการการเงินทางอิเล็กทรอนิกส์)

3.3 กระบวนการเสริมการรักษาความปลอดภัยให้มีประสิทธิภาพ

3.3.1 การฝึกอบรมและให้ความรู้แก่พนักงาน

บริษัทควรจัดให้มีการพัฒนา ฝึกอบรมและให้ความรู้อย่างต่อเนื่องแก่ผู้บริหารและพนักงานทุกระดับที่เกี่ยวข้องกับการให้บริการ เพื่อให้ตระหนักถึงความปลอดภัย ในการให้บริการและสามารถปฏิบัติตามนโยบายและกระบวนการรักษาความปลอดภัยได้อย่างมีประสิทธิภาพ นอกจากนั้น ผู้บริหารและพนักงานที่เกี่ยวข้องควรมีการติดตามพัฒนาการทางเทคโนโลยีและภัยคุกคามใหม่ ๆ ที่เกิดขึ้นอย่างใกล้ชิด รวมทั้งเผยแพร่ข้อมูลที่เป็นประโยชน์แก่พนักงานอื่นในองค์กรด้วย

3.3.2 การให้คำแนะนำแก่ลูกค้าผู้ใช้บริการ

บริษัทควรให้ข้อมูลและคำแนะนำที่เป็นประโยชน์แก่ลูกค้า เช่น วิธีการใช้บริการอย่างปลอดภัย ข้อมูลทางเทคนิคหรือวิธีการรักษาความปลอดภัยเครื่องคอมพิวเตอร์และอุปกรณ์ที่ลูกค้าใช้ในการทำธุรกรรม เนื่องจากผู้บุกรุกสามารถเจาะระบบของลูกค้าเพื่อโจรกรรมข้อมูลและปลอมตัวเป็นลูกค้าเข้าทำธุรกรรมกับบริษัทได้ คำแนะนำควรรวมถึงการให้ลูกค้าระมัดระวังการใช้หรือ Download Software จากแหล่งที่ไม่เป็นที่รู้จักหรือน่าสงสัย เนื่องจากอาจมีโปรแกรมของผู้บุกรุกแฝงมาด้วย (ภาคผนวก 2 ท้ายเอกสารแนบ 3 การให้คำแนะนำ แก่ลูกค้าผู้ใช้บริการ)

การให้ข้อมูลและคำแนะนำดังกล่าวควรใช้ภาษาที่เข้าใจง่ายและเปิดเผยไว้บน Website ของบริษัทโดยให้ลูกค้าสามารถเรียกดูได้โดยสะดวก และเพื่ออำนวยความสะดวกให้แก่ลูกค้า บริษัทอาจจัดให้มี Help Desk เพื่อทำหน้าที่ตอบปัญหาและให้คำแนะนำต่าง ๆ แก่ลูกค้าในการใช้บริการการเงินทางอิเล็กทรอนิกส์ด้วย นอกจากนั้น บริษัทอาจจัดให้มีการฝึกอบรมลูกค้าผู้ใช้บริการ เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับวิธีการรักษาความปลอดภัยในส่วนที่เกี่ยวข้องกับลูกค้าผู้ใช้บริการ รวมทั้งระบบการรักษาความปลอดภัยของบริษัทที่ลูกค้าผู้ใช้บริการควรทราบ ซึ่งเป็นการให้ความรู้และความมั่นใจในการใช้บริการการเงินทางอิเล็กทรอนิกส์ได้อีกทางหนึ่ง

ทั้งนี้ บริษัทควรเปิดเผยข้อตกลงและเงื่อนไขในการให้บริการให้ลูกค้าทราบ และมีวิธีการให้ลูกค้าแสดงการยอมรับข้อตกลงและเงื่อนไขดังกล่าวก่อนตัดสินใจใช้บริการ

3.3.3 การควบคุมภายใน

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

ภาคผนวก 1 ท้ายเอกสารแนบ 3

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 ประสิทธิภาพของ

การเข้ารหัสลับขึ้นอยู่กับสมการทางคณิตศาสตร์ที่ใช้เข้ารหัส (Cryptographic Algorithms) ความยาวของกุญแจเข้ารหัส (Cryptographic key) และกระบวนการในการบริหารจัดการกุญแจ

การใช้เทคโนโลยีการเข้ารหัสลับควรพิจารณาให้เหมาะสมกับระดับความเสี่ยง ระดับความสำคัญของข้อมูล และระดับความปลอดภัยที่ต้องการ โดยคำนึงถึงประเด็นสำคัญดังนี้

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

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

2.3 การจัดให้มีการควบคุมการรับส่งข้อมูลที่มีประสิทธิภาพ โดยการรับส่งข้อมูลระหว่างบริษัทกับลูกค้าผู้ใช้บริการควรกระทำผ่านช่องทางที่มีความปลอดภัยสูง 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. เทคโนโลยีการรักษาความปลอดภัยอื่นๆ

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. เทคโนโลยีการตรวจสอบตัวตนลูกค้าผู้ใช้บริการ

เทคโนโลยีสำหรับการตรวจสอบตัวตนที่ใช้กันอยู่ในปัจจุบันสามารถสรุปได้ดังนี้

1. รหัสผ่านและเลขประจำตัว (Passwords and Personal Identification Numbers)

เป็นวิธีการตรวจสอบตัวตนที่ใช้กันมากที่สุด เนื่องจากสะดวกและง่ายต่อการใช้งาน โดยในการเข้าใช้บริการ ลูกค้าต้องป้อนชื่อและรหัสผ่านซึ่งเป็นรหัสลับส่วนตัวของลูกค้า ให้ระบบดำเนินการตรวจสอบก่อนเข้าใช้บริการ ประสิทธิภาพของระบบให้บริการที่ใช้รหัสผ่านเป็นวิธีการตรวจสอบตัวตนขึ้นอยู่กับการเก็บรักษารหัสผ่าน การกำหนดรูปแบบและความยาวของรหัสผ่าน และการควบคุมต่างๆ ที่เกี่ยวข้อง

ระบบให้บริการที่ใช้รหัสผ่านเป็นวิธีการตรวจสอบตัวตนควรดำเนินการดังนี้

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

- แยกฐานข้อมูลที่เก็บรหัสผ่านออกจากฐานข้อมูลอื่น รวมทั้งมีการรักษาความปลอดภัยอย่างเพียงพอ

2. ใบรับรองลายมือชื่ออิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์

ใบรับรองลายมือชื่ออิเล็กทรอนิกส์ (Electronic Certificate) คือ ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใด ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์

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

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 ในเวลาที่ลูกค้าส่งข้อมูลให้บริษัท

Digital Signature เป็นลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นจากกุญแจส่วนตัวของบุคคลหนึ่ง และสามารถใช้ยืนยันตัวบุคคลนั้นโดยการใช้กุญแจสาธารณะของบุคคลนั้นมาตรวจสอบตัวตน ผู้ประกอบการออกใบรับรองที่เป็นผู้เก็บรักษากุญแจสาธารณะของบุคคลนั้นจะทำหน้าที่จัดส่งกุญแจสาธารณะให้แก่คู่กรณีที่ต้องการตรวจสอบตัวตน พร้อมกับออกใบรับรองลายมือชื่ออิเล็กทรอนิกส์เพื่อยืนยันว่ากุญแจสาธารณะเป็นของบุคคลนั้น

ระบบให้บริการที่ใช้เทคโนโลยี PKI เป็นวิธีการตรวจสอบตัวตนควรดำเนินการดังนี้

- จัดให้มีการตรวจสอบใบรับรองลายมือชื่ออิเล็กทรอนิกส์ที่ได้รับก่อนที่จะเริ่มอนุญาตให้บริการทำธุรกรรม เช่น มีการตรวจสอบกับข้อมูลใบรับรองที่ถูกยกเลิก (Revocation List) ที่เป็นปัจจุบัน

- จัดให้มีการรักษาความปลอดภัยระบบงานและเครื่องคอมพิวเตอร์ที่รองรับการตรวจสอบตัวตนโดยเทคโนโลยี PKI

- จัดให้มีบันทึกการทำงานของระบบงานและเครื่องคอมพิวเตอร์ที่รองรับการตรวจสอบตัวตนโดยเทคโนโลยี PKI

3. Tokens/Smart card

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 วิธีการเปลี่ยนทดแทนและวิธีการยกเลิกที่เหมาะสม

- 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 ท้ายเอกสารแนบ 3

การให้คำแนะนำแก่ลูกค้าผู้ใช้บริการ

บริษัทควรให้คำแนะนำที่เป็นประโยชน์แก่ลูกค้าผู้ใช้บริการเพื่อให้เข้าใจ และตระหนักถึงความสำคัญของการรักษาความปลอดภัยในการใช้บริการ โดยควรรวมถึงคำแนะนำดังต่อไปนี้

1) แนะนำลูกค้าผู้ใช้บริการไม่ให้เปิดเผยข้อมูลเลขประจำตัวและรหัสผ่านให้บุคคลอื่นทราบ ไม่เขียนหรือจดรหัสผ่านไว้ในที่ที่เห็นได้ง่าย ทำลายเอกสารที่ใช้แจ้งเลขประจำตัวและรหัสผ่าน รวมทั้งแนะนำลูกค้าผู้ใช้บริการให้ระมัดระวังการถูกแอบอ้างหรือหลอกลวงให้เปิดเผยข้อมูลเลขประจำตัวและรหัสผ่าน

2) แนะนำลูกค้าผู้ใช้บริการเกี่ยวกับวิธีการกำหนดรหัสผ่านอย่างปลอดภัย มีการเปลี่ยนรหัสผ่านเป็นประจำ และแนะนำให้ลูกค้าผู้ใช้บริการทราบถึงช่องทางในการแจ้งให้บริษัททราบทันทีที่พบว่าข้อมูลเลขประจำตัวหรือรหัสผ่านเกิดปัญหา

3) แนะนำลูกค้าผู้ใช้บริการให้ตรวจสอบ Address ของ Website ของบริษัทให้ถูกต้องก่อนเริ่มทำธุรกรรม เพื่อป้องกันกรณีที่มีการปลอมแปลง Website

4) แนะนำลูกค้าผู้ใช้บริการให้ตรวจสอบความถูกต้องของรายการธุรกรรม เช่น จำนวนเงิน วันที่ทำรายการ เลขที่บัญชี และยอดเงินในบัญชี อย่างสม่ำเสมอ เพื่อป้องกันรายการธุรกรรมผิดปกติที่อาจเกิดขึ้น

5) แนะนำลูกค้าผู้ใช้บริการให้รู้จักการรักษาความปลอดภัยเครื่องคอมพิวเตอร์ของตนเอง เช่น

- ติดตั้งและใช้งานโปรแกรมป้องกันไวรัสที่มีการปรับปรุงฐานข้อมูลไวรัสให้ทันสมัยและใช้บริการกรองไวรัสทางอินเทอร์เน็ตที่เชื่อถือได้
- มีการควบคุมการเข้าถึงข้อมูลส่วนตัว
- มีการเข้าและออกจากระบบให้บริการอย่างถูกต้อง
- ไม่ละทิ้งเครื่องคอมพิวเตอร์หรืออุปกรณ์ในระหว่างการทำธุรกรรมและออกจากระบบให้บริการอย่างถูกต้อง เมื่อทำธุรกรรมเสร็จสิ้น
- ใช้เครื่องคอมพิวเตอร์และอุปกรณ์ที่เหมาะสมกับระบบการรักษาความปลอดภัยของบริษัท
- หลีกเลี่ยงการใช้เครื่องคอมพิวเตอร์และอุปกรณ์ที่ไม่ได้มาตรฐานหรือมาจากแหล่งที่เชื่อถือไม่ได้

- หลีกเลี่ยงการใช้เครื่องคอมพิวเตอร์สาธารณะในการทำธุรกรรมทางการเงิน
- หลีกเลี่ยงการเข้าไปใน Website ที่น่าสงสัย
- หลีกเลี่ยงการเปิดเผยข้อมูลส่วนตัว ข้อมูลทางการเงิน หรือข้อมูลบัตรเครดิตแก่ Website ที่ไม่รู้จักหรือเชื่อถือไม่ได้
- หลีกเลี่ยงการเปิดจดหมายอิเล็กทรอนิกส์ที่ไม่รู้จักหรือน่าสงสัย (Junk Emails)
- หลีกเลี่ยงการติดตั้ง Download หรือใช้ Software จากแหล่งที่ไม่รู้จักหรือไม่สามารถตรวจสอบแหล่งที่มาได้ เนื่องจากระบบของลูกค้าผู้ใช้บริการอาจได้รับโปรแกรมไวรัสหรือโปรแกรมอื่นๆ ที่ผู้บุกรุกสามารถใช้ในการลักลอบเข้าถึงติดมาด้วย

6) ชี้แจงให้ลูกค้าผู้ใช้บริการทราบถึงขอบเขตความรับผิดชอบทั้งในส่วนของบริษัทและในส่วนของลูกค้าผู้ใช้บริการ

เอกสารแนบ 4

แนวปฏิบัติในการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ (แผนฉุกเฉินด้าน IT)

บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ใช้ระบบเทคโนโลยีสารสนเทศในการให้บริการแก่ลูกค้า มีการเชื่อมโยงเครือข่ายทั้งภายในบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์เองและกับองค์กรอื่นทั้งในและต่างประเทศ ดังนั้น หากเกิดเหตุการณ์ที่ส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ไม่ว่าจะเกิดจากภัยทางธรรมชาติ หรืออุบัติเหตุหรือการมุ่งร้ายต่อระบบสถาบันการเงิน เช่น อัคคีภัย อุทกภัย วินาศกรรม โจรกรรม ไวรัสคอมพิวเตอร์ ย่อมมีผลกระทบทันทีต่อธุรกิจของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ ทำให้ไม่สามารถให้บริการลูกค้าได้อย่างต่อเนื่อง รวมทั้งส่งผลกระทบเป็นวงกว้างต่อองค์กรอื่นที่มีเครือข่ายเชื่อมโยงกัน ดังนั้น หากบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ไม่มีกระบวนการรองรับที่ดีแล้ว อาจส่งผลให้ลูกค้าผู้ใช้บริการและผู้มีส่วนได้ส่วนเสีย (Stakeholder) ขาดความเชื่อมั่นต่อบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์นั้นและต่อระบบสถาบันการเงินโดยรวมได้

กระบวนการรองรับเหตุการณ์ความเสียหายดังกล่าวข้างต้นเป็นสิ่งสำคัญที่จะนำมาใช้เมื่อเกิดปัญหาขึ้นกับบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ และหากมีการเตรียมการอย่างดีย่อมจะช่วยลดผลกระทบต่าง ๆ ที่เกิดขึ้นกับบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ และช่วยให้การฟื้นฟูระบบเทคโนโลยีสารสนเทศของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์กลับคืนสู่สภาพปกติได้ภายในเวลาที่ยอมรับได้ ซึ่งเป็นผลต่อความเชื่อมั่นของลูกค้าและผู้มีส่วนได้ส่วนเสียที่มีต่อธุรกิจและการให้บริการของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ ดังนั้น บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์จึงจำเป็นต้องมีแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศที่มีประสิทธิภาพและสามารถนำมาใช้งานได้เมื่อเกิดเหตุการณ์ความเสียหายจริง เพื่อให้บรรลุเป้าหมายที่สำคัญคือความสามารถในการดำเนินธุรกิจและการให้บริการอย่างต่อเนื่อง หรืออย่างน้อยก็ใกล้เคียงกับสภาวะปกติ

เนื้อหา

1. ในแนวปฏิบัตินี้

“บริษัท” หมายความว่า บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ ตามมาตรา 4 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551

"คณะกรรมการบริษัท" หมายถึง คณะกรรมการบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์

2. หลักการ

2.1 ในการจัดทำแผนฉุกเฉินด้าน IT บริษัทต้องคำนึงถึงความเป็นไปได้ในทางปฏิบัติ สามารถนำมาใช้รองรับเหตุการณ์ความเสียหายที่เกิดขึ้นได้จริง โดยให้ถือเป็นส่วนหนึ่งของการดำเนินงานปกติ นอกจากนี้ บริษัทต้องจัดให้มีการทดสอบแผนฉุกเฉินทั้งในระดับหน่วยงานและระดับองค์กรอย่างน้อยปีละหนึ่งครั้ง เพื่อทดสอบว่าแผนฉุกเฉินนั้นสามารถนำมาใช้งานได้จริง และหากบริษัทมีระบบงานที่เชื่อมโยงเครือข่ายหรือใช้บริการจากหน่วยงานภายนอก บริษัทควรจัดให้มีการทดสอบร่วมกันด้วย

2.2 ในการจัดทำแผนฉุกเฉินด้าน IT บริษัทควรคำนึงถึงองค์ประกอบต่าง ๆ ที่จะมีส่วนเกี่ยวข้อง เพื่อให้เหมาะสมกับรูปแบบและความซับซ้อนของการดำเนินธุรกิจ อาทิเช่น ระบบการรักษาความปลอดภัย ระบบการควบคุมภายในของแต่ละบริษัท ประเภทและระดับความเสี่ยงที่อาจเกิดขึ้นต่อบริษัท ลูกค้าผู้ใช้บริการ ผู้มีส่วนได้ส่วนเสีย ระบบสถาบันการเงินและระบบการเงินโดยรวม

2.3 บริษัทต้องคำนึงถึงการบริหารความเสี่ยงที่อาจเกิดขึ้นจากเหตุการณ์ความเสียหายต่าง ๆ ซึ่งนอกจากความเสี่ยงทั่วไป เช่น ความเสี่ยงด้านปฏิบัติการ (Operational Risk) ความเสี่ยงด้านชื่อเสียง (Reputation Risk) แล้ว บริษัทควรคำนึงถึงความเสี่ยงที่เกี่ยวข้องในด้านอื่นเพิ่มเติม ได้แก่

2.3.1 ความเสี่ยงที่มีผลกระทบต่อระบบบริษัท (Systemic Risk) ซึ่งเป็นการเกิดการหยุดชะงักของบริษัทหนึ่ง แต่อาจส่งผลกระทบให้ทั้งระบบบริษัทและระบบการเงินโดยรวมหยุดชะงักได้

2.3.2 ความเสี่ยงจากการพึ่งพาองค์กรอื่นในการดำเนินธุรกิจ (Interdependency Risk) เช่น การใช้บริการด้านการสื่อสารโทรคมนาคม หรือการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น เป็นต้น หากผู้ให้บริการดังกล่าวไม่สามารถให้บริการแก่บริษัทได้ก็จะส่งผลกระทบต่อการดำเนินงานของบริษัทนั้นด้วย

2.3.3 ความเสี่ยงจากการกระจุกตัว (Concentration Risk) ของระบบงานหรือทรัพยากรที่สำคัญ เช่น การกระจุกตัวของระบบการสื่อสารโทรคมนาคม หรือระบบสาธารณูปโภคที่อยู่ในบริเวณใกล้เคียงกับที่ทำการของบริษัท ซึ่งมีโอกาสได้รับความเสียหายพร้อมกัน หรือการกระจุกตัวของผู้ให้บริการภายนอกที่บริษัทหลายแห่งไปใช้บริการร่วมกัน เป็นต้น

2.4 ในกรณีที่บริษัทมีการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) เพื่อสนับสนุนการดำเนินงานของบริษัท คณะกรรมการบริษัทต้องจัดให้มีการประเมินประสิทธิภาพของกระบวนการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศของผู้ให้บริการเพื่อให้สอดคล้องกับนโยบายการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศที่บริษัทได้กำหนดไว้ โดยให้ถือปฏิบัติตามประกาศธนาคารแห่งประเทศไทย เรื่อง การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) ด้วย

3. สาระสำคัญของแนวปฏิบัติฉบับนี้ประกอบด้วย

3.1 บทบาทและความรับผิดชอบของคณะกรรมการบริษัท

3.2 นโยบายและแนวทางในการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ

3.3 กระบวนการหลักในการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ

3.3.1 การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis)

3.3.2 การประเมินความเสี่ยงและการควบคุม (Risk Analysis & Control)

3.3.3 การวางกลยุทธ์สำหรับแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ (IT Contingency Plan Strategy Development)

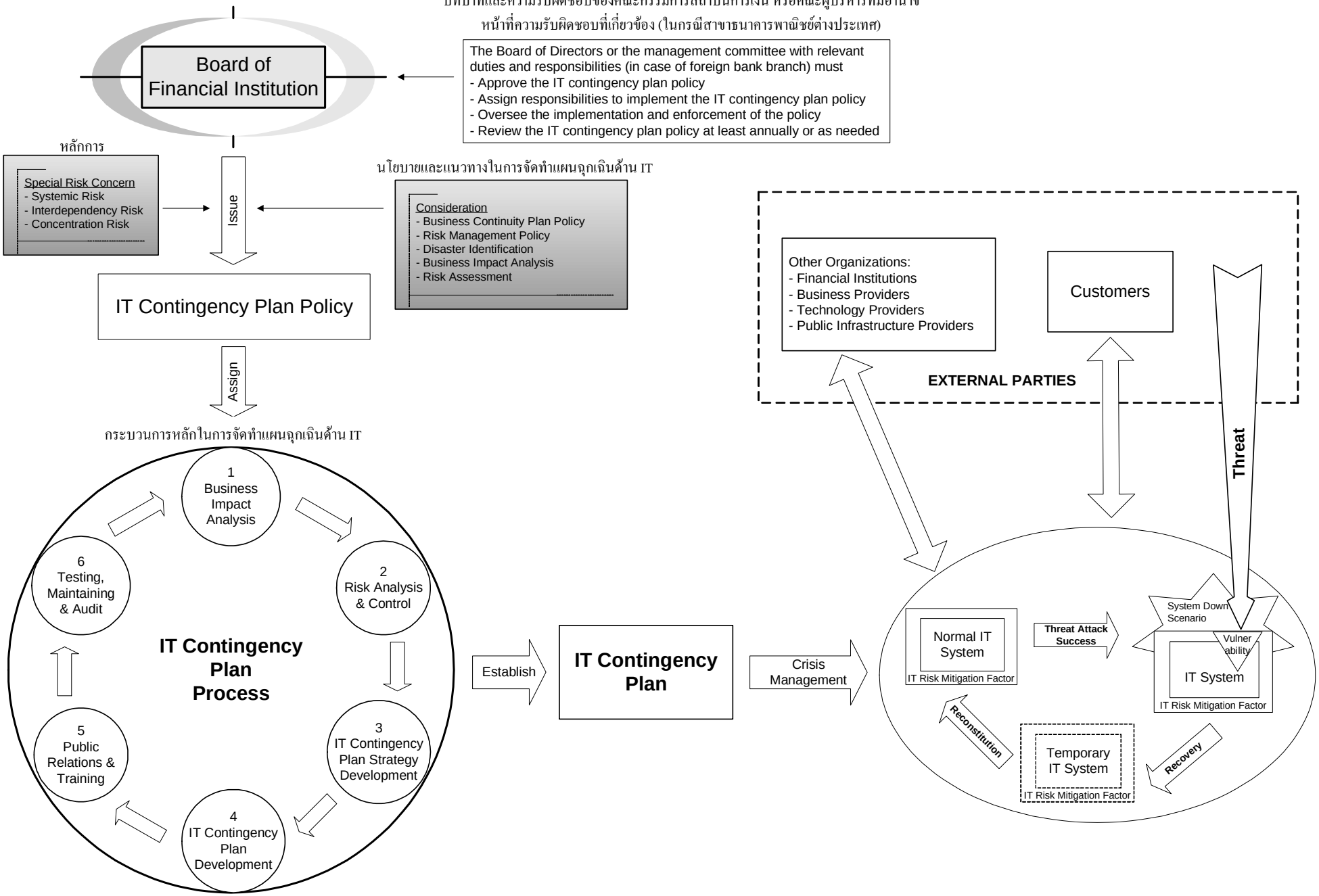
3.3.4 การพัฒนาแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ (IT Contingency Plan Development)

3.3.5 การประชาสัมพันธ์และการฝึกอบรม (Public Relations & Training)

3.3.6 การทดสอบ ปรับปรุงและสอบทานแผน (Testing, Maintaining & Audit)

ทั้งนี้ ภาพรวมของเนื้อหาทั้งหมดในแนวปฏิบัติสามารถนำมาสรุปเป็นแผนภาพเพื่อให้ง่ายต่อการทำความเข้าใจ ดังนี้

บทบาทและความรับผิดชอบของคณะกรรมการสถาบันการเงิน หรือคณะผู้บริหารที่มีอำนาจหน้าที่ความรับผิดชอบที่เกี่ยวข้อง (ในกรณีสาขาธนาคารพาณิชย์ต่างประเทศ)



3. รายละเอียดของแนวปฏิบัติ

3.1 บทบาทและความรับผิดชอบของคณะกรรมการบริษัท

คณะกรรมการบริษัทต้องมีหน้าที่ ดังนี้

3.1.1 กำหนดนโยบายและแนวทางในการจัดทำแผนฉุกเฉินด้าน IT ที่เป็นลายลักษณ์อักษร คณะกรรมการบริษัทอาจมอบหมายให้คณะกรรมการที่รับผิดชอบด้านงานเทคโนโลยีสารสนเทศ หรือคณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการบริหาร ดำเนินการจัดทำนโยบายและแนวทางดังกล่าว และนำเสนอให้คณะกรรมการบริษัทพิจารณาอนุมัติก็ได้

3.1.2 กำหนดให้มีคณะทำงานที่รับผิดชอบในการดำเนินการจัดทำแผนฉุกเฉินด้าน IT ให้เป็นไปตามนโยบายและแนวทางที่ได้กำหนดไว้ และเมื่อคณะทำงานยกร่างแผนฉุกเฉินด้าน IT แล้วเสร็จ ให้เสนอคณะกรรมการบริษัทพิจารณาอนุมัติแผนฉุกเฉินด้าน IT เพื่อใช้เป็นแผนในการดำเนินการต่อไป

3.1.3 ติดตามดูแลให้พนักงานและผู้ที่เกี่ยวข้องปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างเหมาะสม ทั้งในเหตุการณ์จำลอง และเมื่อเกิดเหตุการณ์ความเสียหายขึ้นจริง

3.1.4 จัดให้มีการประเมินประสิทธิภาพของนโยบายและแนวทางในการจัดทำแผนฉุกเฉินด้าน IT อย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับแผนฯ เช่น มีการเปลี่ยนแปลงกลยุทธ์ทางธุรกิจ นโยบายการบริหารความเสี่ยงโดยรวม สภาพแวดล้อมของการดำเนินธุรกิจ หรือทรัพยากรทางเทคโนโลยีสารสนเทศหลัก คณะกรรมการบริษัทจะต้องจัดให้มีการประเมินประสิทธิภาพของนโยบายและแนวทางที่ใช้อยู่โดยพลัน

3.2 นโยบายและแนวทางในการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ

3.2.1 คณะกรรมการบริษัทต้องกำหนดนโยบายและแนวทางการจัดทำแผนฉุกเฉินด้าน IT โดยคำนึงถึงความสอดคล้องกับนโยบายการบริหารความเสี่ยงของบริษัท (Risk Management Policy) รวมทั้งความซับซ้อนของธุรกิจ พัฒนาการทางเทคโนโลยีที่มีการเปลี่ยนแปลงอย่างรวดเร็ว สภาพแวดล้อมทางการเงิน และบทบาทขององค์กรในการรักษาเสถียรภาพของระบบสถาบันการเงินและระบบการเงิน

3.2.2 ในการกำหนดนโยบายและแนวทางการจัดทำแผนฉุกเฉินด้าน IT คณะกรรมการบริษัทต้องพิจารณาให้ครอบคลุมถึง

(1) การระบุเหตุการณ์ความเสียหาย (Disaster Identification) ที่มีโอกาสเกิดขึ้นและมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศที่บริษัทใช้ในการดำเนินธุรกิจ

(2) การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) ที่พึ่งพาเทคโนโลยีสารสนเทศ หากระบบเกิดการหยุดชะงัก

(3) การประเมินและบริหารความเสี่ยงต่าง ๆ (Risk Assessment) ที่อาจเกิดขึ้นจากเหตุการณ์ความเสียหาย รวมทั้ง การกำหนดระดับความเสี่ยงที่ยอมรับได้ ระยะเวลาสูงสุดที่ยอมให้ระบบการดำเนินงานทางธุรกิจและทรัพยากรทางเทคโนโลยีในแต่ละระบบงานหยุดชะงัก

ตัวอย่างรายละเอียดที่ควรกำหนดไว้ในนโยบายและแนวทางการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ ได้แก่ วัตถุประสงค์โดยรวม โครงร่างของแผน ขอบเขตของแผน ขั้นตอนและระยะเวลาในการจัดทำแผน การกำหนดผู้มีหน้าที่จัดทำแผน รวมถึงบทบาทและความรับผิดชอบ การระบุเหตุการณ์ความเสียหายที่มีโอกาสเกิดขึ้น การกำหนดระดับความเสี่ยงที่ยอมรับได้ เกณฑ์ในการบริหารจัดการความเสี่ยง แนวทางการจัดการภาวะฉุกเฉิน แนวทางการประชาสัมพันธ์ให้ผู้ที่เกี่ยวข้องทราบ เป็นต้น

3.2.3 นโยบายและแนวทางในการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ ควรมีกระบวนการวางแผนที่สำคัญ 4 ด้าน คือ

(1) การเตรียมความพร้อมก่อนเกิดเหตุการณ์ความเสียหาย (Disaster Preparedness) เพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ความเสียหายที่มีผลกระทบต่อการดำเนินธุรกิจและการให้บริการของบริษัท เช่น การกำหนดมาตรการป้องกันความเสี่ยง การสร้างความเข้าใจในบทบาทหน้าที่ของพนักงาน เป็นต้น

(2) การตอบสนองต่อสถานการณ์ฉุกเฉิน (Emergency Response) เพื่อควบคุมและจำกัดขอบเขตของความเสียหายและผลกระทบต่อบริษัท ลูกค้าผู้ใช้บริการ ผู้มีส่วนเกี่ยวข้อง และระบบบริษัทโดยรวม เช่น การกำหนดแนวทาง วิธีการควบคุม และการแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น

(3) การดำเนินการเพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง (Business Continuity) เช่น การสำรองข้อมูลและอุปกรณ์สำคัญ (Backup) การกู้ระบบงานและข้อมูลที่เสียหาย (Recovery) การเปิดใช้ศูนย์สำรองและการโยกย้ายพนักงาน เมื่อเกิดเหตุการณ์ความเสียหายจริง เป็นต้น

(4) การกลับคืนสู่การทำงานปกติ (Business Restoration) เพื่อให้ธุรกิจและการให้บริการของบริษัทกลับสู่สภาวะปกติโดยเร็ว เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ การกำหนดกระบวนการในการควบคุม

การติดตั้ง การตั้งค่า และการทดสอบทรัพยากรทางเทคโนโลยีที่ถูกกู้หรือที่นำมาทดแทน การกำหนดแนวทางการประเมินความเสียหาย เป็นต้น

3.2.4 บริษัทต้องแต่งตั้งคณะทำงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT ไว้อย่างชัดเจน โดยคณะทำงานดังกล่าวควรมาจากฝ่ายงานต่าง ๆ ที่เกี่ยวข้องทั้งในด้านงานเทคโนโลยีสารสนเทศและด้านสายงานธุรกิจ และมีการแบ่งแยกหน้าที่ของแต่ละฝ่ายงานอย่างชัดเจนและเหมาะสม ทั้งนี้ ผู้บริหารของแต่ละฝ่ายงานที่เกี่ยวข้องต้องมีส่วนร่วมในการจัดทำแผนฉุกเฉินด้าน IT ด้วย

3.3 กระบวนการหลักในการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ

บริษัทต้องจัดให้มีกระบวนการในการจัดทำแผนฉุกเฉินด้าน IT ที่มีประสิทธิภาพ และสามารถนำแผนฉุกเฉินด้าน IT ดังกล่าวมาใช้รองรับเหตุการณ์ความเสียหายที่เกิดขึ้นได้จริง เพื่อให้บริษัทสามารถดำเนินธุรกิจที่มีการพึ่งพาระบบเทคโนโลยีสารสนเทศได้อย่างต่อเนื่อง ทั้งนี้ กระบวนการหลักในการจัดทำแผนฉุกเฉินด้าน IT ประกอบด้วย

3.3.1 การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) บริษัทต้องมีการประเมินและวิเคราะห์ผลกระทบทางธุรกิจ เพื่อให้ทราบถึงความสัมพันธ์ของการดำเนินงานทางธุรกิจกับระบบเทคโนโลยีสารสนเทศ และผลกระทบจากการหยุดชะงักของระบบเทคโนโลยีสารสนเทศต่อการดำเนินงานนั้น ซึ่งจะทำให้บริษัทสามารถกำหนดลำดับความสำคัญของการดำเนินงานทางธุรกิจและทรัพยากรทางเทคโนโลยีสารสนเทศในการกู้ระบบได้อย่างมีประสิทธิภาพ โดยมีแนวทางดังนี้

(1) วิเคราะห์และระบุการดำเนินงานทางธุรกิจที่ต้องมีการพึ่งพาระบบเทคโนโลยีสารสนเทศทั้งภายในและภายนอกบริษัท จุดที่มีความเสี่ยงต่อการล้มเหลวทั้งระบบ ผลกระทบที่เกิดจากจากการหยุดชะงักทั้งทางด้านการเงินและที่ไม่ใช่ทางด้านการเงิน และระยะเวลาสูงสุดที่ยอมให้การดำเนินงานทางธุรกิจเกิดการหยุดชะงัก

(2) จัดลำดับความสำคัญของการดำเนินงานทางธุรกิจที่จะต้องทำการกู้ระบบ พร้อมทั้งกำหนดระยะเวลาในการกู้ระบบ และเป้าหมายของระบบงานและข้อมูลที่ควรกู้คืนได้ภายหลังเกิดการหยุดชะงัก

(3) กำหนดระดับของความต่อเนื่องทางธุรกิจในแต่ละการดำเนินงานทางธุรกิจ เช่น การให้บริการรับฝาก/ถอนเงินที่สำนักงานของบริษัท มีความต่อเนื่องทางธุรกิจในระดับสูง จึงต้องสามารถดำเนินงานได้ตลอดเวลาทำการ เป็นต้น

(4) วิเคราะห์และระบุทรัพยากรทางเทคโนโลยีสารสนเทศต่าง ๆ ทั้งภายในและภายนอกบริษัทที่จำเป็นในแต่ละการดำเนินงานทางธุรกิจตามที่ได้ระบุไว้ในข้อ 3.3.1 (1) รวมทั้งผลกระทบที่เกิดขึ้นหากทรัพยากรทางเทคโนโลยีสารสนเทศเกิดการหยุดชะงัก และระยะเวลาสูงสุดที่ยอมให้ทรัพยากรทางเทคโนโลยีสารสนเทศหยุดชะงัก

(5) จัดลำดับความสำคัญของทรัพยากรทางเทคโนโลยีสารสนเทศที่ได้ระบุไว้ในข้อ 3.3.1 (4) ที่จะต้องทำการกู้ระบบ กำหนดระยะเวลาในการกู้ระบบ เป้าหมายของระบบงานและข้อมูลที่ควรกู้คืนได้ภายหลังเกิดการหยุดชะงัก และทรัพยากรทางเทคโนโลยีสารสนเทศขั้นต่ำที่จำเป็นต้องใช้ในการกู้ระบบ

3.3.2 การประเมินความเสี่ยงและการควบคุม (Risk Analysis & Control)

บริษัทต้องระบุปัจจัยต่าง ๆ ที่ทำให้เกิดความเสี่ยงหรือผลกระทบต่อระบบเทคโนโลยีสารสนเทศที่การดำเนินงานธุรกิจต้องพึ่งพา และปรับปรุงกระบวนการควบคุมเพื่อให้สามารถลดทอนหรือขจัดผลกระทบที่อาจเกิดขึ้นได้ โดยมีกระบวนการดังนี้

(1) ประเมินความเสี่ยงที่อาจทำให้ทรัพยากรทางเทคโนโลยีสารสนเทศที่ใช้ในการดำเนินงานทางธุรกิจเกิดการหยุดชะงัก โดยระบุเหตุการณ์ที่ทำให้เกิดการหยุดชะงัก สาเหตุหรือแหล่งภัยคุกคามที่ทำให้เกิดการหยุดชะงักทั้งจากภายในและภายนอกบริษัท จุดล่อแหลม ความรุนแรงและความเป็นไปได้ที่ทำให้เกิดเหตุการณ์หยุดชะงัก และระดับการยอมรับความเสี่ยง

(2) วิเคราะห์กระบวนการควบคุมความเสี่ยงที่มีอยู่ และปรับปรุงกระบวนการและทรัพยากรที่จำเป็นในการควบคุมความเสี่ยงที่อาจทำให้เกิดเหตุการณ์หยุดชะงัก รวมถึงการจัดทำการประเมินผลและควบคุมกระบวนการดังกล่าว

3.3.3 การวางกลยุทธ์สำหรับแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ (IT Contingency Plan Strategy Development)

บริษัทต้องมีการกำหนดกลยุทธ์แผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศที่เหมาะสมกับการรองรับเหตุการณ์ที่ทำให้เกิดการหยุดชะงัก สภาพแวดล้อมและทรัพยากรของบริษัท เพื่อให้สามารถครอบคลุมความเสี่ยงและผลกระทบทางธุรกิจที่ได้วิเคราะห์ไว้ และกลยุทธ์ดังกล่าวควรมีความสอดคล้องกับแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของบริษัทด้วย ทั้งนี้ ในการกำหนดทางเลือกของกลยุทธ์แผนฉุกเฉินด้าน IT บริษัทควรพิจารณาประเด็นต่าง ๆ ดังนี้

(1) การบรรลุถึงเป้าหมายที่ได้กำหนดไว้ เช่น ระยะเวลาที่ใช้ในการกู้ระบบ เป้าหมายของระบบงานและข้อมูลที่ควรกู้คืนได้ภายหลังเกิดการหยุดชะงัก และทรัพยากรทางเทคโนโลยีสารสนเทศขั้นต่ำที่จำเป็นสำหรับการกู้ระบบ เป็นต้น

(2) ปัจจัยสำคัญที่สนับสนุนการกำหนดทางเลือกของกลยุทธ์เพื่อให้บริษัทมีทิศทางในการพัฒนาแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศที่บรรลุเป้าหมายที่ได้กำหนดไว้ เช่น การจัดการข้อมูลที่มีความสำคัญ การจัดให้มีระบบเทคโนโลยีสารสนเทศสำรอง บทบาทและหน้าที่ของผู้ปฏิบัติงาน เป็นต้น (ภาคผนวก 1 ท้ายเอกสารแนบ 4 ตัวอย่างปัจจัยที่สนับสนุนการกำหนดทางเลือกของกลยุทธ์แผนฉุกเฉินด้าน IT)

(3) การกำหนดงบประมาณของแต่ละทางเลือกให้มีความเพียงพอและครอบคลุมกิจกรรมที่ต้องดำเนินการทั้งหมด นอกจากนี้ บริษัทอาจจัดให้มีการวิเคราะห์ต้นทุนและผลประโยชน์ที่จะได้รับในแต่ละทางเลือก เพื่อใช้เปรียบเทียบและพิจารณาหาทางเลือกที่เหมาะสม

ตัวอย่างของการกำหนดกลยุทธ์ได้แก่ การกำหนดทางเลือกของการกู้ระบบเทคโนโลยีสารสนเทศระบบหนึ่ง อาจมีสองทางเลือกคือ ทำการกู้ระบบคืนมาโดยการจัดหาอุปกรณ์มาทดแทน หรือมีการย้ายการดำเนินงานเทคโนโลยีสนเทศไปใช้ระบบเทคโนโลยีสารสนเทศสำรอง เป็นต้น

3.3.4 การพัฒนาแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ (IT Contingency Plan Development)

แผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศควรมีรูปแบบและเนื้อหาที่ชัดเจน เพื่อให้เกิดการดำเนินการที่รวดเร็ว และง่ายต่อการปฏิบัติ รวมทั้งควรมีความยืดหยุ่นในการตอบสนองต่อเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้น และการเปลี่ยนแปลงข้อจำกัดต่าง ๆ ทั้งภายในและภายนอก ทั้งนี้ รายละเอียดแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศควรมีส่วนประกอบที่สำคัญดังนี้ (ภาคผนวก 2 ท้ายเอกสารแนบ 4 ตัวอย่างโครงสร้างของแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ)

(1) ข้อมูลสนับสนุนการปฏิบัติงาน

ข้อมูลสนับสนุนการปฏิบัติงานช่วยให้แผนมีความง่ายต่อการเข้าใจ การดำเนินการและการปรับปรุง โดยควรมีรายละเอียดดังนี้ ชื่อแผน วัตถุประสงค์ ขอบเขต ความสัมพันธ์กับแผนอื่น รายละเอียดของระบบเทคโนโลยีสารสนเทศ ผังโครงสร้างของการบังคับบัญชาการดำเนินงานตามแผน การกำหนดผู้ปฏิบัติหน้าที่และความรับผิดชอบ

และผู้ปฏิบัติที่ทำหน้าที่แทนในกรณีที่ผู้ปฏิบัติหน้าที่ที่กำหนดไว้ไม่สามารถปฏิบัติงานได้ รวมถึงการบันทึกการเปลี่ยนแปลงของแผน

(2) การตอบสนองต่อเหตุการณ์ฉุกเฉิน

บริษัทควรมีกระบวนการในการตอบสนองต่อเหตุการณ์ฉุกเฉิน ดังนี้

(2.1) การตรวจจับเหตุการณ์ที่ทำให้เกิดการหยุดชะงักหรืออุบัติภัย และการแจ้งไปยังกลุ่มหรือพนักงานที่เกี่ยวข้องได้อย่างรวดเร็ว

(2.2) การประเมินลักษณะและขนาดของความเสียหายที่เกิดขึ้นกับระบบได้อย่างรวดเร็วและถูกต้อง รวมถึงการแจ้งให้ทราบถึงข้อมูลที่ได้ทำการประเมินไปยังกลุ่มดำเนินงานกู้ระบบหรือพนักงานที่เกี่ยวข้อง

(2.3) การกำหนดขั้นตอนการสั่งการและการตัดสินใจที่ชัดเจน การพิจารณาการจัดตั้งศูนย์บัญชาการ การกำหนดบุคคลหรือกลุ่มคนที่ทำหน้าที่ในการสั่งการและตัดสินใจ รวมถึง แนวทางในการเริ่มต้นการกู้ระบบ และการกำหนดเกณฑ์ในการเริ่มต้นการกู้ระบบ โดยพิจารณาจากปัจจัยต่าง ๆ เช่น ขอบเขตความเสียหายที่มีต่อระบบเทคโนโลยีสารสนเทศ ความปลอดภัยของผู้ปฏิบัติงาน ความสำคัญของระบบเทคโนโลยีสารสนเทศที่มีต่อการดำเนินงาน เป็นต้น

(3) การดำเนินงานในการกู้ระบบ

บริษัทควรพิจารณากระบวนการที่ทำให้สามารถดำเนินงานระบบเทคโนโลยีสารสนเทศได้ชั่วคราว การซ่อมแซมความเสียหายระบบเดิม การฟื้นฟูการปฏิบัติงานในที่เดิมหรือเคลื่อนย้ายไปที่ใหม่ โดยกระบวนการกู้ระบบควรมีลักษณะดังต่อไปนี้

(3.1) มีการกำหนดขั้นตอนในการดำเนินงานกู้ระบบที่ชัดเจน และควรคำนึงถึงการสื่อสารและการประสานงานภายในกลุ่มและระหว่างกลุ่มดำเนินงาน นอกจากนี้ บริษัทควรมีระบบหรือเอกสารสำหรับบันทึกการดำเนินงาน รวมถึงข้อผิดพลาดหรือปัญหาที่เกิดขึ้นหากการดำเนินงานกู้ระบบไม่เป็นไปตามแผน เช่น การใช้เอกสารรายละเอียดการปฏิบัติตามแผน (Checklist) เป็นต้น เพื่อควบคุมให้การดำเนินงานเป็นไปตามขั้นตอน และใช้ในการเปรียบเทียบผลการดำเนินงานกับเป้าหมายที่ได้กำหนดไว้ เพื่อใช้ประเมินและพัฒนาประสิทธิภาพของแผนฉุกเฉินด้าน IT ต่อไป

(3.2) มีลำดับขั้นตอนในการดำเนินงานกู้ระบบที่สอดคล้องกับลำดับความสำคัญในการกู้ระบบที่ได้จากการวิเคราะห์ผลกระทบทางธุรกิจ และระยะเวลาในการกู้ระบบที่ได้กำหนดไว้

(3.3) มีทางเลือกของขั้นตอนในการดำเนินงานกู้ระบบ เพื่อรองรับกรณีที่ไม่สามารถดำเนินการตามขั้นตอนของแผนที่ได้กำหนดไว้ เช่น ขณะที่มีการดำเนินงานกู้ระบบงานหนึ่งปรากฏว่า Server ที่รองรับระบบงานนั้นไม่สามารถดำเนินการได้ตามปกติ เนื่องจากอุปกรณ์บางส่วนของ Server ขัดข้อง ซึ่งบริษัทควรจัดให้มีทางเลือกในการดำเนินงาน เช่น ให้มีการเปลี่ยนอุปกรณ์ที่ขัดข้อง หรือทำการเปลี่ยน Server เป็นต้น บริษัทควรพิจารณาทางเลือกที่ไม่ต้องพึ่งพาระบบเทคโนโลยีสารสนเทศ แต่ต้องจัดให้มีกระบวนการป้องกันความเสี่ยงที่อาจเกิดขึ้นด้วย

(3.4) ในขณะที่ดำเนินการกู้ระบบ บริษัทควรระมัดระวังมิให้มีการข้ามหรือละเลยขั้นตอนที่กำหนดไว้ รวมทั้งไม่ควรมีขั้นตอนที่กำหนดขึ้นใหม่ขณะปฏิบัติงานยกเว้น ขั้นตอนที่ได้รับการอนุญาตจากผู้มีอำนาจสั่งการเพิ่มเติม

(4) การกลับคืนสู่การทำงานปกติ

บริษัทควรพิจารณาถึงกระบวนการที่ยืนยันถึงความพร้อมใช้งานในการกลับคืนสู่การดำเนินงานปกติ ซึ่งอาจเป็นการดำเนินงานโดยใช้ทรัพยากรทางเทคโนโลยีสารสนเทศเดิม หรือใช้ทรัพยากรทางเทคโนโลยีสารสนเทศใหม่ เช่น กระบวนการในการควบคุมการติดตั้ง การตั้งค่าและทดสอบทรัพยากรเทคโนโลยีสารสนเทศที่ถูกกู้หรือทดแทนใหม่ หรือกระบวนการโยกย้ายการดำเนินงานจากระบบเทคโนโลยีสารสนเทศสำรองกลับมายังระบบเทคโนโลยีสารสนเทศหลัก เป็นต้น

(5) การจัดทำเอกสารประกอบการดำเนินงานตามแผน

บริษัทต้องจัดทำเอกสารประกอบการดำเนินงานตามแผนฉุกเฉินด้าน IT และจัดเก็บไว้ในสถานที่ที่ปลอดภัยจากผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ที่ทำให้เกิดการหยุดชะงัก โดยอย่างน้อยที่สุดควรเก็บไว้ที่ผู้ที่มีหน้าที่รับผิดชอบในการสั่งการตามแผนชุดหนึ่ง และเก็บไว้ที่สถานที่สำรองอีกชุดหนึ่ง เพื่อให้สามารถเข้าถึงเอกสารและนำเอกสารดังกล่าวไปใช้ในการดำเนินงานได้ตรงตามแผน

3.3.5 การประชาสัมพันธ์ และการฝึกอบรม (Public Relations & Training)

(1) การประชาสัมพันธ์

บริษัทต้องจัดให้มีการประชาสัมพันธ์แผนฉุกเฉินด้าน IT โดยมีการระบุขั้นตอนและวิธีการประชาสัมพันธ์ที่ชัดเจน เพื่อให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องได้รับทราบถึงรายละเอียดในการจัดทำแผน ขั้นตอนการดำเนินงานตามแผน พนักงานที่เกี่ยวข้องกับแผนและการเปลี่ยนแปลงที่เกิดขึ้น

นอกจากนี้ บริษัทต้องระบุขั้นตอนและวิธีการประชาสัมพันธ์เมื่อเกิดเหตุการณ์ฉุกเฉินแก่ลูกค้าผู้ใช้บริการ เพื่อสร้างความเชื่อมั่นว่าบริษัทยังคงให้บริการอย่างต่อเนื่องได้ เช่น การประชาสัมพันธ์ถึงวิธีการติดต่อสื่อสารกับบริษัท ในกรณีที่การสื่อสารในช่องทางปกติไม่สามารถทำได้ หรือเวลาที่จะเริ่มให้บริการได้อีกครั้งหลังจากเกิดเหตุการณ์หยุดชะงัก เป็นต้น

(2) การฝึกอบรม

บริษัทต้องจัดให้มีการฝึกอบรมแก่พนักงานผู้มีส่วนเกี่ยวข้องกับการดำเนินงานตามแผนอย่างน้อยปีละหนึ่งครั้ง โดยอย่างน้อยควรมีหัวข้อในการอบรมดังนี้ วัตถุประสงค์ของแผน ขั้นตอนการปฏิบัติงานตามแผน การประสานงานและการสื่อสารกันระหว่างกลุ่ม ขั้นตอนในการรายงาน ระบบรักษาความปลอดภัย กระบวนการเฉพาะของแต่ละกลุ่มดำเนินงาน และความรับผิดชอบของแต่ละบุคคล ทั้งนี้ พนักงานที่ผ่านการอบรมแล้วควรมีความเข้าใจและสามารถปฏิบัติตามแผนได้แม้ในกรณีที่ไม่มีเอกสารกำกับการดำเนินงานตามแผน

3.3.6 การทดสอบ ปรับปรุงและสอบทานแผน (Testing, Maintaining & Audit)

(1) การทดสอบแผน

บริษัทต้องจัดให้มีการทดสอบแผนทั้งในระดับหน่วยงานและระดับองค์กรอย่างสม่ำเสมอ อย่างน้อยปีละหนึ่งครั้ง หรือทุกครั้งที่มีการปรับปรุงแผน โดยเฉพาะระบบงานที่หากเกิดเหตุการณ์หยุดชะงักจะมีผลกระทบต่อการให้บริการลูกค้าหรือต่อบริษัททั้งระบบ เช่น ระบบเงินฝาก ระบบการโอนและชำระเงิน เป็นต้น และหากระบบงานนั้นมีการเชื่อมโยงเครือข่ายหรือใช้บริการจากหน่วยงานภายนอก บริษัทควรมีการทดสอบแผนฉุกเฉินร่วมกับหน่วยงานภายนอกที่เกี่ยวข้องด้วย ทั้งนี้ ในการทดสอบแผน บริษัทควรพึงระวังไม่ให้การทดสอบนั้นกระทบต่อการดำเนินงานปกติของบริษัท รวมทั้ง ต้องจัดให้มีการเก็บข้อมูลผลการทดสอบเพื่อเทียบเคียงกับเป้าหมายที่ได้กำหนดไว้ และรายงานผลการทดสอบนั้นต่อคณะกรรมการสถาบันการเงินด้วย เพื่อใช้ในการประเมินผลการทดสอบและพัฒนาประสิทธิภาพของแผนฉุกเฉินด้าน IT

รายละเอียดของการทดสอบที่บริษัทควรกำหนดไว้ในแผนฉุกเฉินของแต่ละระบบงาน ได้แก่ วัตถุประสงค์ในการทดสอบ ขอบเขตของการทดสอบ เหตุการณ์จำลองที่ใช้ทดสอบ ระยะเวลาที่ใช้ในการทดสอบ ขั้นตอนการทดสอบ ทรัพยากรต่าง ๆ ที่ใช้ในการทดสอบ และเกณฑ์วัดความสำเร็จ โดยบริษัทควรพิจารณาให้ครอบคลุมการดำเนินงานและเหตุการณ์จำลองที่ได้ระบุไว้ ทั้งนี้ ในการทดสอบ บริษัทอาจเลือกทดสอบเฉพาะ

บางส่วน หรือทดสอบเต็มรูปแบบก็ได้ อย่างไรก็ดี บริษัทควรทดสอบแบบเต็มรูปแบบ อย่างน้อยปีละหนึ่งครั้ง และในแต่ละครั้ง บริษัทอาจเลือกเหตุการณ์จำลองที่ได้กำหนดไว้มาเพียงเหตุการณ์เดียวในการทดสอบก็ได้

(2) การปรับปรุงแผน

บริษัทต้องมีการกำหนดแผนงาน แนวทางและระยะเวลาในการทบทวนและปรับปรุงแผนฉุกเฉินด้าน IT ไว้อย่างชัดเจน เพื่อให้แผนสามารถใช้งานได้จริง และสอดคล้องกับพัฒนาการทางเทคโนโลยี สถานการณ์ปัจจุบัน นโยบายและกลยุทธ์ของบริษัท โดยบริษัทควรกำหนดให้มีการทบทวนและปรับปรุงแผนฉุกเฉินอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับแผนฉุกเฉิน เช่น การเปลี่ยนแปลงพนักงานที่มีหน้าที่รับผิดชอบในการดำเนินงานตามแผน การเปลี่ยนสภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศ เป็นต้น ทั้งนี้ บริษัทควรคำนึงถึงการปรับปรุงข้อมูลหรือเอกสารที่ได้มีการเผยแพร่ให้แก่พนักงานหรือบุคคลภายนอกให้สอดคล้องกันด้วย

(3) การสอบทานแผน

บริษัทควรจัดให้มีการสอบทานแผนฉุกเฉินด้าน IT เพื่อยืนยันถึงความเหมาะสมของขั้นตอนต่าง ๆ ในการจัดทำแผนให้สามารถใช้งานได้จริง ทั้งนี้ ผู้สอบทานแผนอาจเป็นหน่วยงานภายนอกหรือหน่วยงานภายในบริษัทก็ได้ แต่ต้องมีความเป็นอิสระในการดำเนินการ

ภาคผนวก 1 ท้ายเอกสารแนบ 4

ตัวอย่างปัจจัยที่สนับสนุนการกำหนดทางเลือกของกลยุทธ์แผนฉุกเฉินด้าน IT

1. การจัดการข้อมูลที่มีความสำคัญ

บริษัทควรจัดให้มีกระบวนการจัดการข้อมูลที่มีความสำคัญ เพื่อยืนยันถึงการไม่สูญหาย ความถูกต้องครบถ้วน ความปลอดภัย และการเข้าถึงได้ของข้อมูล หากเกิดเหตุการณ์ที่ทำให้การดำเนินงานหยุดชะงัก โดยบริษัทควรมีกระบวนการดังต่อไปนี้

1. การระบุถึงข้อมูลหรือกลุ่มข้อมูลที่มีความสำคัญต่อการดำเนินงานทางธุรกิจ เช่น ข้อมูลการทำรายการทางการเงินของลูกค้า ข้อมูลที่ใช้ในการบริหารสินทรัพย์ของบริษัท เป็นต้น รวมทั้งข้อมูลที่จำเป็นในการติดตั้งระบบงาน นอกจากนี้ บริษัทควรพิจารณาถึงข้อมูลสำคัญในแต่ละหน่วยงานหรือของพนักงานที่อาจเก็บไว้ในคอมพิวเตอร์ส่วนบุคคลซึ่งมิได้มีการสำรองข้อมูลอย่างเหมาะสมด้วย

2. การสำรองข้อมูลและการนำข้อมูลกลับมาใช้งาน บริษัทควรพิจารณากำหนดวิธีการที่ชัดเจนและมีความเหมาะสมกับความสำคัญของข้อมูลที่ได้กำหนดไว้ นอกจากนี้ บริษัทควรพิจารณาถึงการกำหนดความถี่ในการสำรองข้อมูลและการกำหนดแหล่งเก็บข้อมูลสำรองภายนอก รวมทั้ง การจัดให้มีการทดสอบเพื่อยืนยันความพร้อมและความเหมาะสมในการใช้งาน

3. ในการจัดให้มีแหล่งเก็บข้อมูลสำรองภายนอก บริษัทควรพิจารณาปัจจัยที่เกี่ยวข้อง ได้แก่ สถานที่ตั้งและสภาพแวดล้อม กระบวนการรักษาความปลอดภัย วิธีการเข้าถึงข้อมูลที่จัดเก็บไว้ เป็นต้น

2. การจัดให้มีระบบเทคโนโลยีสารสนเทศสำรอง

บริษัทต้องกำหนดให้มีระบบเทคโนโลยีสารสนเทศสำรองที่สามารถทำงานทดแทนระบบเทคโนโลยีสารสนเทศหลักเมื่อเกิดความเสียหายได้ เพื่อความต่อเนื่องในการดำเนินงานและการให้บริการ โดยระบบเทคโนโลยีสารสนเทศสำรองอาจอยู่ในลักษณะศูนย์ประมวลผลสำรอง (Backup Site) และ/หรือระบบเทคโนโลยีสารสนเทศสำรองเฉพาะบางส่วน เช่น ข้อมูล โปรแกรมระบบงาน เครื่องคอมพิวเตอร์ และอุปกรณ์เครือข่าย เป็นต้น แนวทางสำคัญที่บริษัทควรพิจารณา มีดังนี้

1. ที่ตั้งของระบบเทคโนโลยีสารสนเทศหลักและระบบเทคโนโลยีสารสนเทศสำรองควรอยู่ห่างกันพอสมควร รวมทั้งไม่ควรใช้สาธารณูปโภคจากแหล่งเดียวกัน โดยเน้นหลักการกระจายความเสี่ยง เพื่อป้องกันเหตุการณ์ที่มีผลกระทบในวงกว้าง (Wide area disruption)

2. ระบบเทคโนโลยีสารสนเทศสำรองต้องได้รับการดูแลหรือทดสอบให้สามารถประมวลผลได้จริงตามขั้นตอนและวิธีการในการกู้ระบบงานตามที่ได้ตั้งเป้าหมายไว้ รวมทั้งต้องมีการกำหนดวิธีการสำรองข้อมูล ความถี่และประเภทของข้อมูลให้สอดคล้องกับความจำเป็น ลำดับความสำคัญ และผลกระทบของข้อมูลต่อระบบงานเมื่อเกิดความเสียหาย

3. ระบบเทคโนโลยีสารสนเทศสำรองควรมีความพร้อมใช้งานและสามารถเข้าไปดำเนินงานได้ตลอดเวลา หรืออย่างน้อยที่สุดต้องสามารถทำงานทดแทนได้เมื่อระบบเทคโนโลยีสารสนเทศหลักหยุดชะงัก รวมถึงมีระบบรักษาความปลอดภัยที่เป็นไปตามนโยบายการรักษาความปลอดภัยของบริษัท และสามารถรองรับเหตุการณ์ความเสียหายที่อาจเกิดขึ้นเป็นระยะเวลายาวนานด้วย

ตัวอย่างรูปแบบของระบบเทคโนโลยีสารสนเทศสำรอง ได้แก่

- Active/Backup Model เป็นรูปแบบหนึ่งที่มีระบบเทคโนโลยีสารสนเทศเป็นศูนย์คอมพิวเตอร์หลักในการดำเนินงาน และมีอีกระบบหนึ่งเป็นศูนย์คอมพิวเตอร์สำรอง (Backup System) ซึ่งศูนย์คอมพิวเตอร์สำรองจะเริ่มดำเนินงานได้ก็ต่อเมื่อศูนย์คอมพิวเตอร์หลักไม่สามารถดำเนินงานได้เป็นปกติหรือเกิดการหยุดชะงักขึ้น โดยศูนย์คอมพิวเตอร์สำรองจะมีการติดตั้งอุปกรณ์คอมพิวเตอร์ที่สอดคล้องกับศูนย์คอมพิวเตอร์หลักและโดยมากจะสามารถใช้ปฏิบัติงานได้นานหลายชั่วโมง ทั้งนี้บริษัทอาจใช้บริการศูนย์คอมพิวเตอร์สำรองจากบุคคลภายนอกก็ได้

- Split Operation Model หรือ Active/Active Model เป็นรูปแบบที่มีการแยกสถานที่การดำเนินงานของระบบเทคโนโลยีสารสนเทศหลักออกเป็น 2 แห่งขึ้นไป โดยทำหน้าที่เป็นศูนย์คอมพิวเตอร์สำรองซึ่งกันและกัน ซึ่งแต่ละศูนย์คอมพิวเตอร์มีความสามารถที่จะรองรับการทำงาน บางส่วนหรือทั้งหมดของศูนย์คอมพิวเตอร์อีกแห่งสำหรับช่วงระยะเวลาหนึ่งได้ ซึ่งจะทำให้การดำเนินงานกลับคืนมาได้ในทันทีหรือเกือบทันทีที่ศูนย์คอมพิวเตอร์แห่งใดแห่งหนึ่งเกิดการหยุดชะงัก อย่างไรก็ตาม การดำเนินงานในรูปแบบนี้อาจมีต้นทุนของการดูแลรักษาที่ค่อนข้างสูงเนื่องจากต้องทำการดูแลรักษาและทำการปรับปรุงในหลายสถานที่ที่เป็นที่ตั้งของระบบเทคโนโลยีสารสนเทศหลัก

ทั้งนี้ การตัดสินใจเลือกรูปแบบของระบบเทคโนโลยีสารสนเทศสำรอง บริษัทควรพิจารณาถึงความเหมาะสมกับ ขนาด ความซับซ้อน และลักษณะการดำเนินงานของบริษัท รวมถึงความเสี่ยงต่าง ๆ และแนวทางการบริหารความเสี่ยง สภาพแวดล้อม และต้นทุนของบริษัทด้วย

ภาคผนวก 2 ท้ายเอกสารแนบ 4

ตัวอย่างโครงสร้างของแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ

ตัวอย่างโครงสร้างของแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศนี้จัดทำขึ้นเพื่อให้บริษัทใช้เป็นแนวทางในการจัดทำแผน ซึ่งบริษัทสามารถนำไปปรับใช้ให้ เหมาะสมกับนโยบายและแนวทางในการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ และมีความสอดคล้องกับนโยบายการบริหารความเสี่ยง นโยบายในการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และนโยบายอื่นที่เกี่ยวข้องของบริษัท นอกจากนี้ บริษัทควรพิจารณาปรับใช้ให้เหมาะสมกับสถานการณ์ในปัจจุบันด้วย

โดยทั่วไป ตัวอย่างโครงสร้างของแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศควรมีเนื้อหาครอบคลุมเรื่องต่าง ๆ ดังนี้

ข้อมูลสนับสนุนการปฏิบัติงาน เพื่อให้แผนมีความง่ายต่อความเข้าใจ การดำเนินการ และการปรับปรุง

1. ชื่อแผนฉุกเฉิน ระบุชื่อแผน

2. วัตถุประสงค์ในการจัดทำแผนฉุกเฉิน ระบุวัตถุประสงค์ของแผน ผลกระทบอันอาจจะเกิดจากความเสี่ยงที่มีต่อบริษัท ลูกค้าผู้ใช้บริการ และองค์กรภายนอกอื่น ๆ ที่เกี่ยวข้อง รวมถึง ผลลัพธ์ที่คาดหวังจากการนำแผนดังกล่าวมาใช้

3. ขอบเขตของแผนฉุกเฉิน ระบุขอบเขตของระบบงาน รายละเอียดของกระบวนการทำงาน และส่วนงานที่แผนมีผลบังคับใช้ รวมทั้ง รายละเอียดของงาน (Work Flow)

4. รายละเอียดของระบบเทคโนโลยีสารสนเทศ ระบุชื่อ และโครงสร้างของระบบเทคโนโลยีสารสนเทศ โครงสร้างระบบรักษาความปลอดภัย และการติดต่อสื่อสาร

5. การกำหนดผู้รับผิดชอบสั่งการ ระบุผู้มีอำนาจตัดสินใจ และสั่งการในการนำแผนมาปฏิบัติ โครงสร้างการบังคับบัญชา (ผู้สั่งการ และผู้รับผิดชอบ) บทบาทหน้าที่ และขอบเขตอำนาจความรับผิดชอบ รวมทั้ง การกำหนดผู้รับผิดชอบแทนในกรณีที่ผู้สั่งการในลำดับแรกไม่สามารถปฏิบัติงานได้

6. สถานที่ปฏิบัติงานทดแทน (Alternate Site) ระบุสถานที่ที่เข้าใช้ปฏิบัติงานแทนในกรณีเกิดเหตุวินาศภัยจนเป็นเหตุให้ไม่สามารถใช้สถานที่ทำงานเดิมได้

7. การบันทึกการเปลี่ยนแปลงของแผน (Record of Changes) ระบุวันที่ ชื่อผู้จัดทำหรือแก้ไข ชื่อผู้ตรวจทาน และรายละเอียดโดยย่อเมื่อมีการแก้ไขแผน

<u>แผนการปฏิบัติงาน</u> การระบุสถานการณ์ และเงื่อนไขในการปฏิบัติงานตามแผน รายละเอียดขั้นตอน ทรัพยากรที่ใช้ และข้อจำกัดในการปฏิบัติโดยละเอียด ซึ่งบริษัทควรมีแนวปฏิบัติที่ครอบคลุมการวางแผนที่สำคัญ 4 ด้าน ดังนี้

1. การเตรียมความพร้อมก่อนเกิดเหตุการณ์ความเสียหาย การกำหนดกระบวนการป้องกัน และควบคุมความเสี่ยง เพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ความเสียหาย

2. การตอบสนองต่อเหตุการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหายรวมทั้งผลกระทบอื่น ในขณะที่มีเหตุการณ์ความเสียหายเกิดขึ้น โดยมีกระบวนการดังนี้

ก) <u>เงื่อนไขการเริ่มปฏิบัติตามแผน</u> กำหนด หรือระบุเงื่อนไข สถานการณ์

ข) <u>ระบุขั้นตอนการดำเนินการพื้นฐาน</u> ประเมินสถานการณ์เบื้องต้น สถานที่สาเหตุ และขอบเขตความเสียหาย ระบุวิธีการปฏิบัติงานเพื่อระงับเหตุการณ์ความเสียหาย วิธีการดำเนินงานต่างๆ ที่เกี่ยวข้อง แนวทางการเก็บรักษาข้อมูล เอกสาร ความปลอดภัยของผู้ปฏิบัติงาน การเคลื่อนย้ายอพยพพนักงาน และทรัพยากรทางเทคโนโลยีสารสนเทศที่จำเป็น

ค) <u>ระบุแผนปฏิบัติการด้านการติดต่อสื่อสาร</u> กำหนดวิธีการติดต่อสื่อสารกับหน่วยงาน หรือบุคคลอื่นที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อแจ้งสถานการณ์ และแนวทางการดำเนินงาน หรือสถานที่ติดต่องานฉุกเฉิน รวมทั้งจัดทำรายชื่อของหน่วยงาน หรือผู้ที่มีหน้าที่รับผิดชอบในการดำเนินการช่วยเหลือ ยุติเหตุการณ์ความเสียหายทั้งภายในและภายนอกบริษัท

ง) <u>ระบุความต้องการใช้ทรัพยากรต่างๆ</u> ระบุความต้องการทรัพยากรที่มีความจำเป็น จำนวนแรงงาน สถานที่ อุปกรณ์และเครื่องมือต่าง ๆ ระบบการสื่อสารโทรคมนาคม สาธารณูปโภคให้ชัดเจน

3. การดำเนินการเพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง เป็นแผนปฏิบัติการต่อเนื่องจากแผนในข้อ 2 เพื่อให้ระบบเทคโนโลยีสารสนเทศที่สนับสนุนการดำเนินธุรกิจ

ของบริษัทมีความต่อเนื่องไม่หยุดชะงัก หรือสามารถกลับคืนมาในระยะเวลาการกู้ที่กำหนด และไม่ก่อให้เกิดผลกระทบต่อเนื่องอื่น ๆ โดยมีรายละเอียดดังนี้

ก) เงื่อนไขการเริ่มปฏิบัติตามแผน กำหนด หรือระบุเงื่อนไข เหตุการณ์

ข) ระบุขั้นตอนการดำเนินการพื้นฐาน กำหนดลำดับขั้นตอน ลำดับความสำคัญ และระยะเวลาในการกู้ระบบ ระบุวิธีการปฏิบัติงาน วิธีการนำระบบข้อมูลสำรองมาใช้งาน เพื่อให้เกิดการปฏิบัติงานต่อเนื่องได้โดยทันที

ค) ระบุแผนปฏิบัติการด้านการติดต่อสื่อสาร กำหนดวิธีการติดต่อสื่อสารและประสานงานกับหน่วยงาน หรือบุคคลอื่นที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อแจ้งข้อเท็จจริงและแนวทางการดำเนินงาน หรือสถานที่ติดต่องานชั่วคราว

ง) ระบุความต้องการใช้ทรัพยากรต่างๆ ระบุความต้องการทรัพยากรที่มีความจำเป็นหากมีการกู้ระบบที่ต้องใช้ระยะเวลานาน จำนวนแรงงาน สถานที่ปฏิบัติงานสำรอง อุปกรณ์และเครื่องมือต่าง ๆ ระบบการสื่อสารโทรคมนาคม สาธารณูปโภค

4. การกลับคืนสู่การทำงานปกติ เพื่อฟื้นฟูและจัดระบบงานให้กลับเข้าสู่การดำเนินงานตามปกติ รวมทั้งการสรุปประเมินความเสียหายที่เกิดขึ้น และแนวทางการป้องกันในอนาคตด้วย โดยมีรายละเอียดดังนี้

ก) ระบุขั้นตอนการดำเนินการ ระบุวิธีการปฏิบัติงานเพื่อฟื้นฟูให้เหตุการณ์กลับสู่ภาวะปกติ กระบวนการควบคุมการติดตั้ง การตั้งค่าและทดสอบระบบที่ถูกกู้คืนมาหรือทดแทนใหม่ การรายงานสรุปความเสียหายต่อผู้บังคับบัญชา

ข) ระบุรายชื่อผู้ที่เกี่ยวข้อง จัดทำรายชื่อของหน่วยงาน หรือผู้ที่มีหน้าที่รับผิดชอบทั้งจากภายในและภายนอกในการดำเนินการช่วยเหลือ เพื่อฟื้นฟูให้เหตุการณ์กลับสู่ภาวะปกติ

การประชาสัมพันธ์ และการฝึกอบรม ระบุขั้นตอนและวิธีการประชาสัมพันธ์ให้แก่พนักงานของบริษัทและลูกค้าผู้ใช้บริการ และจัดฝึกอบรมให้แก่หน่วยงานและพนักงานผู้มีส่วนเกี่ยวข้อง ให้รับทราบถึงวัตถุประสงค์ ขั้นตอนการปฏิบัติงาน การประสานงาน การติดต่อสื่อสารระหว่างกลุ่ม ขั้นตอนการรายงาน ระบบรักษาความปลอดภัย และหน้าที่ความรับผิดชอบของตนเองตามแผนฉุกเฉินอย่างชัดเจน

<u>การทดสอบ ปรับปรุงและสอบทานแผนฉุกเฉิน</u>

1. การทดสอบ

ก) <u>กำหนดเวลาการทดสอบแผน</u> กำหนดงวดของการทดสอบแผนที่ชัดเจน รวมถึงกำหนดระยะเวลาที่ใช้ในการทดสอบตั้งแต่เริ่มต้น จนสิ้นสุดกระบวนการทดสอบ

ข) <u>กำหนดเหตุการณ์จำลองที่จะใช้ทดสอบ และรายละเอียด</u> ในการกำหนดรายละเอียดของเหตุการณ์จำลอง ควรระบุวัตถุประสงค์ ขอบเขตของระบบงาน หรือกระบวนการทำงานที่เกี่ยวข้องกับการทดสอบแผนฉุกเฉินทั้งหมด รวมถึงการกำหนดขั้นตอนการทดสอบแผน

ค) <u>กำหนดทรัพยากรต่าง ๆ ที่ใช้ในการทดสอบแผน</u> กำหนดผู้รับผิดชอบที่จะทำหน้าที่ควบคุม ประสานงาน และรับผิดชอบในการจัดการทดสอบแผนฉุกเฉิน รวมถึงสถานที่ และอุปกรณ์เครื่องมือต่างๆ และงบประมาณที่ต้องใช้ด้วย

ง) <u>กำหนดเกณฑ์การประเมินผล</u> กำหนดผู้รับผิดชอบในการประเมินผล เกณฑ์การประเมินผลซึ่งอาจมีความแตกต่างกันไปตามลักษณะของระบบงาน กระบวนการทำงาน และวัตถุประสงค์ของการทดสอบในแต่ละครั้ง

2. การปรับปรุงและสอบทานแผน

ก) <u>กำหนดเวลาการทบทวนแผน</u> กำหนดแผนงาน แนวทาง และระยะเวลาในการทบทวนและปรับปรุงแผนอย่างชัดเจน เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน

ข) <u>กำหนดผู้รับผิดชอบในการสอบทานแผน</u> ควรกำหนดผู้สอบทานแผน เพื่อยืนยันถึงความเหมาะสมของขั้นตอนต่าง ๆ ในการจัดทำแผน

รายละเอียดเพิ่มเติม

รายละเอียดอื่น ๆ ที่ควรมีในแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ มีดังนี้

1. รายชื่อ ที่อยู่ และหมายเลขโทรศัพท์ของพนักงานบริษัทที่มีหน้าที่รับผิดชอบในการปฏิบัติตามแผน

2. รายชื่อหน่วยงาน สถานที่ตั้ง และหมายเลขโทรศัพท์ขององค์กรภายนอกที่เกี่ยวข้อง

3. รายละเอียดการปฏิบัติตามแผน (Checklist)

4. รูปแบบรายงานต่าง ๆ ที่จำเป็น

เอกสารแนบ 5

มาตรฐานขั้นต่ำการควบคุมภายในและการรักษาความปลอดภัยเกี่ยวกับการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์

ในปัจจุบันบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ได้นำคอมพิวเตอร์มาใช้ในการประมวลผลข้อมูลธุรกิจการเงินหรือใช้เป็นเครื่องมือสำคัญในการให้บริการทางการเงินใหม่ ๆ ซึ่งอาจก่อให้เกิดความเสี่ยงและความเสียหายแก่การดำเนินธุรกิจของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ได้ หากมิได้มีการตระเตรียมในการควบคุมและตรวจสอบไว้ล่วงหน้าอย่างมีประสิทธิภาพเพียงพอ อาทิเช่น รายการทางการเงินผิดพลาด การตัดสินใจผิดพลาด การทุจริต หรือธุรกิจหยุดชะงัก บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์จึงควรมีการบริหารและการควบคุมงานด้านคอมพิวเตอร์ อย่างมีระบบและมีประสิทธิภาพ ให้เหมาะสมตามสภาพแวดล้อมที่ได้เปลี่ยนแปลงไปในการประมวลผลข้อมูลด้วยคอมพิวเตอร์

ธนาคารแห่งประเทศไทยจึงกำหนดมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัย เกี่ยวกับการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ เพื่อให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ได้ใช้เป็นแนวปฏิบัติและสามารถปรับใช้ให้เหมาะสมกับสภาพโครงสร้างธุรกิจและสิ่งแวดล้อม อันจะช่วยป้องกันหรือบรรเทาความเสียหายที่อาจเกิดขึ้นจากการนำคอมพิวเตอร์มาใช้ในการประมวลผลข้อมูลให้มีความปลอดภัยและมั่นคงอย่างเพียงพอได้ตามสมควร ทั้งนี้ บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ ที่มีแนวทางการควบคุมงานด้านคอมพิวเตอร์แล้ว มาตรฐานขั้นต่ำในการควบคุมภายในฯ ตามเอกสารแนบนี้จะทำให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์สามารถเปรียบเทียบแนวทางการปฏิบัติที่ถูกต้องและเหมาะสมได้

เนื้อหา

1. ในเอกสารแนบนี้

"บริษัท" หมายความว่า บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ ตามมาตรา 4 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551

2. การนำระบบคอมพิวเตอร์มาใช้ในการประกอบธุรกิจและการประมวลผลข้อมูลของบริษัท อาจก่อให้เกิดความเสียหายที่จะกระทบการดำเนินงานและความมั่นคงของบริษัทได้ อันเนื่องจากสาเหตุที่สำคัญ 4 ประการ ได้แก่

2.1 การพัฒนาคอมพิวเตอร์หรือใช้งานได้ไม่ตรงกับความต้องการ

2.2 ระบบคอมพิวเตอร์เสียหายหรือถูกทำลายโดยอุบัติเหตุหรือเจตนากระทำ

2.3 การทุจริตในระบบคอมพิวเตอร์ (Computer frauds)

2.4 ความผิดพลาดที่เกิดจากการกระทำของพนักงานปฏิบัติงานคอมพิวเตอร์

ดังนั้น การจัดให้มีระบบการควบคุมภายในและการรักษาความปลอดภัยที่เหมาะสม จะสามารถป้องกันหรือจำกัดความเสียหายให้อยู่ในขอบข่ายที่ยอมรับได้

3. การประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ของบริษัท ประเภทระบบการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ของบริษัทตามประกาศฉบับนี้ แบ่งได้เป็น 2 ประเภทใหญ่ ๆ คือ การประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์หลัก (Computer center) และการประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์

3.1 การประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์หลัก หมายถึง ระบบประมวลผลข้อมูลของบริษัท ซึ่งมีฝ่ายหรือแผนกคอมพิวเตอร์รับผิดชอบงานประมวลผลข้อมูลให้แก่ฝ่ายงานอื่น ๆในบริษัท ระบบประมวลผลข้อมูลหลักยังอาจแบ่งย่อยออกเป็น 3 ขนาด คือ

3.1.1 ระบบประมวลผลข้อมูลขนาดเล็ก หมายถึง ระบบประมวลผลข้อมูลของบริษัท ซึ่งปกติใช้คอมพิวเตอร์ขนาดเล็ก (Minicomputer system) ในการประมวลผลโดยมีบริษัทผู้ผลิตหรือผู้ขายเครื่องคอมพิวเตอร์เป็นผู้พัฒนาหรือจัดหาโปรแกรมระบบงาน (Application programs) ให้ทั้งหมด รวมทั้งการฝึกอบรมพนักงานหรือที่เรียกว่า ระบบ Turn Key

3.1.2 ระบบการประมวลข้อมูลขนาดกลาง หมายถึงระบบข้อมูลของบริษัท ซึ่งปกติใช้คอมพิวเตอร์ขนาดเล็กและขนาดกลางในการประมวลผลข้อมูล (Minicomputer และ Super minicomputer) ในการบริหารงานระบบประมวลผลข้อมูลอาจจะมีคณะกรรมการเทคโนโลยีสารสนเทศ (IT Steering Committee) ทำหน้าที่กำหนดนโยบาย แผนงาน และการควบคุมดูแลการดำเนินงานด้านเทคโนโลยีสารสนเทศของบริษัท

3.1.3 ระบบประมวลผลข้อมูลขนาดใหญ่ หมายถึง ระบบประมวลผลข้อมูลของบริษัท ซึ่งปกติจะใช้คอมพิวเตอร์ขนาดใหญ่ (Mainframe หรือ Large scale computer) ในการประมวลผลข้อมูล มีคณะกรรมการเทคโนโลยีสารสนเทศทำหน้าที่บริหารงานระบบประมวลผลของบริษัทกำหนดนโยบาย เป้าหมาย แผนงาน และควบคุมดูแลการดำเนินงานด้านเทคโนโลยีสารสนเทศของบริษัทให้เป็นไปตามมาตรฐานสากล รวมทั้งมีการแบ่งแยกหน้าที่ที่มีความรู้ทางเทคนิคและความชำนาญเฉพาะด้าน

3.2 การประมวลข้อมูลด้วยไมโครคอมพิวเตอร์ เป็นระบบการประมวลผลข้อมูลด้วยคอมพิวเตอร์ที่มีขนาดเล็กที่สุด สำหรับใช้ประจำส่วนงานและหน่วยงานต่าง ๆ ในบริษัท (End user) ปกติจะใช้กับงานโปรแกรมสำเร็จรูป เช่น Microsoft office เป็นต้น

4. มาตรฐานการควบคุมภายในและการรักษาความปลอดภัยเกี่ยวกับการประมวลผลข้อมูลด้วยคอมพิวเตอร์ ธนาคารแห่งประเทศไทยกำหนดแนวทางให้บริษัทที่ใช้ระบบคอมพิวเตอร์ในการให้บริการทางธุรกิจและการประมวลผลข้อมูล ต้องจัดให้มีการควบคุมภายในและการรักษาความปลอดภัยให้เหมาะสมเพื่อป้องกันหรือลดความเสี่ยงต่อความเสียหายที่อาจเกิดขึ้นได้ โดยมีรายละเอียด ดังนี้

4.1 การควบคุมการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์หลัก

4.1.1 <u>การบริหารทั่วไป</u>

(1) การจัดองค์กร ให้บริษัทจัดให้มีฝ่ายงานที่รับผิดชอบระบบการประมวลผลข้อมูลด้วยคอมพิวเตอร์เป็นเอกเทศจากฝ่ายอื่นๆ และมีการแบ่งแยกหน้าที่ความรับผิดชอบภายในฝ่ายงานอย่างชัดเจน

(2) การวางแผน ให้บริษัทกำหนดนโยบายและจัดทำแผนงานเกี่ยวกับการจัดหาเครื่องคอมพิวเตอร์ โปรแกรมระบบเครื่อง โปรแกรมระบบงาน และบุคลากรที่จะรองรับความต้องการภายในองค์กรและการบริการลูกค้าในระยะสั้นและระยะยาว ตลอดจนควบคุมดูแลให้มีการปฏิบัติงานเป็นไปตามแผนงานที่วางไว้

(3) ระเบียบปฏิบัติงาน ให้บริษัทกำหนดระเบียบปฏิบัติงานสำหรับหน่วยงานในฝ่ายประมวลผลข้อมูล ฯ เพื่อเป็นแนวทางปฏิบัติและใช้ฝึกอบรมพนักงานใหม่

(4) การรายงานผลการปฏิบัติงาน ให้บริษัทจัดทำรายงานผลการปฏิบัติงานเป็นระยะตามความเหมาะสม โดยมีเนื้อหาครอบคลุมถึงการปฏิบัติงานประมวลผล การพัฒนาระบบงาน การพัฒนาและเรื่องทั่ว ๆ ไป

4.1.2 <u>การพัฒนาระบบงานและโปรแกรม</u> บริษัทอาจกระทำการพัฒนาระบบงานด้วยตนเอง หรือว่าจ้างให้บุคคลภายนอกเป็นผู้พัฒนาหรือจัดหาโปรแกรมระบบงานสำเร็จให้

(1) ในการพัฒนาระบบงานด้วยตนเอง ให้บริษัทกำหนดมาตรฐานและวิธีการปฏิบัติ โดยมีสาระสำคัญดังนี้

(1.1) การศึกษาเบื้องต้นเกี่ยวกับความเป็นไปได้ทางเทคนิคและความคุ้มค่าของระบบงาน เพื่อพิจารณาความเหมาะสมที่จะดำเนินการพัฒนาในขั้นรายละเอียดต่อไปหรือไม่ (Feasibility study)

(1.2) การวิเคราะห์และกำหนดลักษณะระบบงานที่ผู้ใช้งานต้องการเพื่อจัดทำรายละเอียด ระบบงาน และโปรแกรมต่อไป (System requirements)

(1.3) การกำหนดรายละเอียดของระบบงานเพื่อจัดทำโปรแกรมคำสั่งงาน ทดสอบ และนำระบบงานออกใช้ (system design)

(1.4) การจัดทำโปรแกรมระบบงาน (Programming) ในแต่ละโปรแกรมระบบงานควรมีคำสั่งงานที่เกี่ยวกับการเช็คสอบความครบถ้วนของจำนวนข้อมูล (Control totals techniques) การเช็คสอบความถูกต้องของข้อมูล (Data input editing) และ การเช็คสอบความถูกต้องของแฟ้มข้อมูลที่ใช้ในการประมวลผล (File label checking)

(1.5) การทดสอบโปรแกรมระบบงาน (System testing) เพื่อพิสูจน์ว่าการออกแบบและจัดทำโปรแกรมระบบงานถูกต้องตรงตามความต้องการของผู้ใช้ก่อนที่จะนำไปติดตั้งใช้งานต่อไป

(1.6) การนำระบบออกใช้งาน (System implementation) ให้มีการสอบทานเพื่อให้มั่นใจว่าอยู่ในสภาพพร้อมใช้งาน

(1.7) การประเมินผลปฏิบัติงาน (System evaluation) ให้มีการประเมินผลการปฏิบัติงานระบบใหม่ รวมทั้งค่าใช้จ่ายที่เกิดขึ้นจริงกับที่ประมาณการ และปัญหาในการปฏิบัติงานภายหลังได้มีการปฏิบัติงานไปแล้วระยะหนึ่ง

(1.8) การปรับปรุงแก้ไขโปรแกรมระบบงาน (System maintenance) ทุกครั้งที่จะปรับปรุงแก้ไขโปรแกรมระบบงาน ให้มีการควบคุมขั้นตอนการปฏิบัติงานอย่างเข้มงวด เช่นเดียวกับการพัฒนาระบบงานใหม่ เพื่อป้องกันความผิดพลาดและการกระทำทุจริต

(2) การว่าจ้างให้บุคคลภายนอกเป็นผู้พัฒนาหรือจัดซื้อโปรแกรมระบบงานสำเร็จ รวมทั้งการควบคุมความถูกต้องและความปลอดภัยของข้อมูลและโปรแกรมระบบงาน

(2.1) กำหนดคุณสมบัติและลักษณะความต้องการเกี่ยวกับข้อมูลนำเข้า การรายงาน รวมทั้งการควบคุมความถูกต้องและความปลอดภัยของข้อมูลและโปรแกรมระบบงาน

(2.2) วิเคราะห์ผลประโยชน์กับค่าใช้จ่ายระหว่างการว่าจ้างหรือจัดซื้อโปรแกรมระบบงานภายนอก

(2.3) วิเคราะห์ฐานะการเงิน ชื่อเสียง และความพร้อมทางเทคนิคของผู้ผลิตหรือผู้ขาย ที่จะให้การสนับสนุนภายหลังการขายเมื่อมีปัญหา

(2.4) วิเคราะห์ความเพียงพอและความสมบูรณ์ของเอกสารประกอบการใช้โปรแกรมระบบงาน

(2.5) วิเคราะห์แผนการฝึกอบรมของผู้ผลิตหรือผู้ขาย

4.1.3 <u>เอกสารสนับสนุนการปฏิบัติงานระบบประมวลผลข้อมูล</u> ให้บริษัทจัดให้มีเอกสารสนับสนุนการปฏิบัติงานด้านคอมพิวเตอร์และควบคุมดูแลให้มีการจัดเอกสารตามมาตรฐานที่กำหนด โดยมีรายละเอียดดังนี้

(1) เอกสารสนับสนุนการปฏิบัติงาน

(1.1) มาตรฐานและระเบียบปฏิบัติงานประมวลผลข้อมูล เป็นแนวปฏิบัติทั่ว ๆ ไปเกี่ยวกับการออกแบบรายงาน การจัดทำโปรแกรมระบบงาน การใช้เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ การเตรียมข้อมูลและป้อนข้อมูลเข้าเครื่อง การประมวลผลข้อมูล การรวบรวมและตรวจสอบความถูกต้องของรายงานผลลัพธ์จากการประมวลผล

(1.2) เอกสารสนับสนุนระบบงาน เพื่อเป็นคู่มือใช้ประกอบการทำงาน เพื่อให้การประมวลผลข้อมูลเป็นไปด้วยความถูกต้องและลดปัญหาในการปฏิบัติงาน เอกสารที่ควรประกอบอยู่ในคู่มือระบบงาน ได้แก่

(1.2.1) รายละเอียดเกี่ยวกับระบบงาน (System documentation) ซึ่งประกอบด้วย คำอธิบายลักษณะงาน (System narrative) ผังระบบงาน (System flowchart) ผังข้อมูล (Record layout) ลักษณะแฟ้มข้อมูล (File description) ลักษณะรายงาน (Print layout) การควบคุมในระบบ (Control function) รหัสประเภทรายการ บัญชี และอื่นๆ

(1.2.2) รายละเอียดเกี่ยวกับโปรแกรมระบบงาน (Program documentation) ซึ่งประกอบด้วย คำอธิบายลักษณะของโปรแกรม (Program description) ผังขั้นตอนการทำงานของโปรแกรม (Program flowchart) สำเนาโปรแกรมชุดปัจจุบัน (Source code) และการควบคุมในโปรแกรม (Programmed controls)

(1.2.3) รายละเอียดวิธีการปฏิบัติสำหรับพนักงานเครื่องคอมพิวเตอร์ (Operation documentation) ซึ่งอธิบายวัตถุประสงค์ของโปรแกรมระบบงาน แฟ้มข้อมูลที่ใช้ในการประมวลผล รูปแบบของข้อมูลนำเข้าและผลลัพธ์ (Input form & output formats) ชุดคำสั่งงานประมวลผล (Job command language) วิธีปฏิบัติเมื่อโปรแกรมทำงานผิดพลาดและเครื่องหยุดทำงานโดยกระทันหัน (Program error & Halts) รวมทั้งวิธีปฏิบัติงานเมื่อเกิดกรณีฉุกเฉิน

(1.2.4) รายละเอียดวิธีการปฏิบัติงานสำหรับผู้ใช้ข้อมูล (User documentation) ซึ่งควรอธิบายถึงลักษณะของข้อมูลที่ต้องนำเข้าเครื่อง (Input) ลักษณะและจำนวนรายงานที่ได้จากการประมวลผล (Output) วิธีปฏิบัติในการควบคุมและการตรวจสอบความถูกต้องของข้อมูลนำเข้าและรายงาน และวิธีปฏิบัติเมื่อพบข้อผิดพลาด

(2) การควบคุมดูแลเอกสารสนับสนุนการปฏิบัติงาน จัดให้มีสถานที่เก็บโดยเฉพาะ โดยอาจรวมไว้ในที่เดียวกับแฟ้มข้อมูลและโปรแกรม และมีระบบการควบคุมดูแลการนำออกใช้งานหรือการปรับปรุงเอกสารให้ถูกต้องทันสมัยอยู่เสมอ รวมทั้งจัดทำสำเนาไว้อย่างน้อย 1 ชุดและเก็บรักษาไว้ในที่ปลอดภัยแยกจากสถานที่ทำการเพื่อว่าเมื่อเกิดกรณีฉุกเฉินสามารถนำมาใช้ในการปฏิบัติงานทดแทนได้

4.1.4 <u>การปฏิบัติการประมวลผล</u> ให้บริษัทกำหนดระเบียบปฏิบัติทั่วไปเกี่ยวกับการใช้เครื่อง ดังนี้

(1) การรักษาความสะอาดเรียบร้อยภายในสถานที่ทำงาน เพื่อป้องกันฝุ่นละอองและการเกิดเพลิงไหม้

(2) การบำรุงรักษาเครื่องคอมพิวเตอร์ เพื่อป้องกันมิให้เครื่องคอมพิวเตอร์เสื่อมสภาพเร็วกว่าเวลาอันสมควร

(3) การแบ่งแยกและสับเปลี่ยนหน้าที่ เพื่อป้องกันการทุจริตและลดความผิดพลาด และยังเป็นการสร้างระบบการสอบยันความถูกต้องในการปฏิบัติงานโดยมิให้พนักงานผู้หนึ่งผู้ใด ปฏิบัติงานหลายอย่าง สำหรับในหน่วยงานประมวลผลข้อมูลขนาดเล็กไม่สามารถแบ่งแยกหน้าที่ได้อย่างสมบูรณ์และจำเป็นต้องมอบหมายให้พนักงานปฏิบัติมากกว่า 1 อย่าง ควรกำหนดให้มีการหมุนเวียนสับเปลี่ยนหน้าที่ และติดตามดูแลการปฏิบัติงานอย่างใกล้ชิด

(4) การควบคุมการใช้เครื่องคอมพิวเตอร์ประมวลผล กำหนดให้พนักงานถือปฏิบัติตามคู่มือของบริษัทผู้ผลิต คู่มือระบบงาน และตารางปฏิบัติงานโดยเคร่งครัด

(5) การจัดทำตารางปฏิบัติงานประมวลผล จัดทำตารางกำหนดการใช้เครื่องประมวลผลข้อมูล ประจำวัน ประจำสัปดาห์ และประจำเดือน เพื่อช่วยควบคุมให้การใช้เครื่องเป็นไปด้วยความมีประสิทธิภาพและงานเสร็จทันเวลาที่กำหนด

(6) การควบคุมการปฏิบัติงานของพนักงานประมวลผลข้อมูล เพื่อกำหนดขอบเขตการปฏิบัติงานของพนักงานประมวลผลมิให้ปฏิบัติงานที่อาจเกิดความเสียหายต่อเครื่องคอมพิวเตอร์ โปรแกรม และข้อมูล

(7) การควบคุมการใช้แฟ้มข้อมูล โปรแกรม และคู่มือปฏิบัติงาน เพื่อป้องกันการใช้โดยไม่ได้รับอนุญาต หรือเกิดการสูญหาย จึงควรมีการควบคุมการจัดเก็บ ดังนี้

(7.1) เอกสารคู่มือปฏิบัติงาน ควรแยกเก็บไว้ในสถานที่ซึ่งปลอดภัย และมีการควบคุมการนำออกไปใช้

(7.2) แฟ้มข้อมูลและโปรแกรมที่เก็บอยู่ในเครื่องคอมพิวเตอร์ ควรใช้โปรแกรมพิเศษควบคุมการใช้งาน

4.1.5 <u>การประมวลผลในระบบสื่อสาร</u> ให้บริษัทที่มีการนำระบบสื่อสารมาใช้ในการประมวลผล จัดให้มีการควบคุม ดังนี้

(1) การควบคุมความปลอดภัยเครื่องเทอร์มินัล (Terminal security) ให้ทำทั้งที่ตัวเครื่อง ฯ และการใช้โปรแกรมควบคุมการใช้เครื่อง เพื่อป้องกันมิให้ผู้ที่ไม่มีสิทธิและบุคคลภายนอกเข้าไปใช้ได้ และจำกัดสิทธิของผู้ใช้เครื่อง ฯ ให้อยู่ภายในขอบเขตที่ได้รับมอบหมาย

(2) การควบคุมการรับส่งข้อมูล (Transmission controls) การป้องกันมิให้ข้อมูลผิดพลาดหรือคลาดเคลื่อนจากการสื่อสารข้อมูล ดังนี้

(2.1) การควบคุมเอกสารที่เกี่ยวกับระบบสื่อสาร และแผนแสดงที่ตั้งเครื่องมือสื่อสารและสายสื่อสาร มิให้ผู้ที่ไม่มีหน้าที่เกี่ยวข้องนำไปใช้งานได้และไม่ควรให้สายโทรศัพท์ที่ใช้งานระบบออนไลน์ปรากฏแก่สายตาบุคคลทั่วไปหรือมีเครื่องหมายพิเศษ

(2.2) แปลงรหัสประจำตัวผู้มีสิทธิเข้าถึงข้อมูล และตัวข้อมูลสำคัญในระบบให้อยู่ในรูปแบบซึ่งหากมีการรั่วไหลแล้วบุคคลภายนอกไม่สามารถนำไปใช้ประโยชน์ได้

(2.3) มีการพิสูจน์ความถูกต้องของแหล่งที่มาของข้อมูลนำเข้าเพื่อให้มั่นใจได้ว่าข้อมูลที่ได้รับนั้นถูกต้อง เช่น เติมรหัสต่อท้ายข้อมูล เป็นต้น

(2.4) มีการให้ลำดับเลขหมายกำกับข้อมูล วันที่และเวลาที่ได้รับข้อมูลแต่ละรายการจากเทอร์มินัลแต่ละเครื่อง เพื่อให้สามารถตรวจสอบการสูญหายหรือการซ้ำซ้อนของข้อมูลในระบบสื่อสารได้

(2.5) กำหนดให้ระบบคอมพิวเตอร์สามารถหยุดการติดต่อกับเทอร์มินัลได้โดยอัตโนมัติ ในกรณีที่ขาดการติดต่อกับระบบคอมพิวเตอร์เป็นระยะเวลานาน เพื่อป้องกันมิให้บุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้องสวมรอยเข้าใช้งาน

(2.6) มีการควบคุมการใช้เครื่องเทอร์มินัลให้อยู่ภายในกำหนดเวลา

(3) การเตรียมการเมื่อระบบสื่อสารขัดข้อง ในกรณีใช้ระบบสื่อสารข้อมูลทางโทรศัพท์ บริษัทควรพิจารณากำหนดอุปกรณ์สื่อสารและระบบสำรองไว้ใช้งานในกรณีฉุกเฉิน วิธีปฏิบัติในการใช้ระบบสื่อสารชุดสำรอง และมีการทดสอบเป็นครั้งคราว เพื่อให้แน่ใจว่าสามารถปฏิบัติได้เมื่อเกิดกรณีฉุกเฉิน

4.1.6 <u>การควบคุมความถูกต้องและน่าเชื่อถือของข้อมูล</u> ให้บริษัทจัดให้มีการควบคุมเพื่อให้ข้อมูลถูกต้องและน่าเชื่อถือได้ ดังนี้

(1) การควบคุมการนำข้อมูลเข้าเครื่อง (Data entry controls)

(1.1) มีการสะสมยอดรวมจำนวนข้อมูลทั้งหมดก่อนหน้าและหลังจากการป้อนรายการเข้าระบบคอมพิวเตอร์ เพื่อใช้ในการสอบทานความครบถ้วนของข้อมูล

(1.2) มีการตรวจเช็คความถูกต้องของข้อมูลแต่ละรายการในขณะที่ทำการป้อนข้อมูล เพื่อป้องกันมิให้ข้อมูลผิดพลาดหรือแปลกปลอมเข้าไปในเครื่องคอมพิวเตอร์ ซึ่งยากต่อการค้นหาและแก้ไขในภายหลัง

(1.3) มีรายงานคอมพิวเตอร์แสดงรายละเอียดข้อมูลทุกรายการที่เข้าไปในเครื่องคอมพิวเตอร์เพื่อใช้เช็คสอบความถูกต้องกับเอกสารหลักฐานเบื้องต้นที่ใช้ในการบันทึกรายการเช่นเดียวกับการบันทึกรายการในสมุดรายวันทั่วไป

(2) การควบคุมการออกข้อมูลผลลัพธ์และรายงาน (Output controls)

(2.1) มีการสอบทานความเรียบร้อยและความถูกต้องของข้อมูลผลลัพธ์และรายงาน โดยการตรวจสอบและกระทบกับยอดรวมของข้อมูลที่นำเข้าเครื่องเทอร์มินัล ยอดรวมข้อมูลที่นำเข้าเครื่องคอมพิวเตอร์ ยอดรวมในบัญชีแยกประเภททั่วไป และยอดคงเหลือในงบทดลอง

(2.2) มีการควบคุมการจัดส่งข้อมูลผลลัพธ์และรายงานให้ถึงมือผู้ใช้อย่างถูกต้องและครบถ้วน โดยจัดทำทะเบียนบันทึกรายงานที่ได้รับจากการประมวลผลรายวัน รายสัปดาห์ และรายเดือน ผู้รับหรือผู้ใช้งาน ลายมือชื่อและวันที่ที่รับรายงาน เพื่อป้องกันมิให้เกิดการสูญหายหรือถูกนำไปใช้ในทางทุจริต

(3) การควบคุมอุปกรณ์ที่ใช้บันทึกข้อมูล (Data file media controls) การป้องกันมิให้เกิดความเสียหายกับอุปกรณ์ที่ใช้บันทึกข้อมูลคอมพิวเตอร์ประเภทจานแม่เหล็กและเทปแม่เหล็กกระทำได้ดังนี้

(3.1) เก็บรักษาไว้ในสถานที่ปลอดภัย มีการควบคุมอุณหภูมิความชื้น ฝุ่นละออง การป้องกันเพลิงไหม้ อุปกรณ์ดับเพลิง และจัดให้มีเจ้าหน้าที่เฉพาะควบคุมดูแลการนำออกไปใช้งานและมีการตรวจนับจำนวนคงเหลือเป็นครั้งคราว

(3.2) จัดทำป้ายชื่อติดกำกับภายนอกอุปกรณ์บันทึกข้อมูล รวมทั้งบันทึกข้อมูลเกี่ยวกับชื่อแฟ้มข้อมูล วันที่ และจำนวนรายการข้อมูลทั้งหมดที่บรรจุอยู่ในแฟ้มข้อมูลไว้ที่บริเวณหัวและท้ายแฟ้มข้อมูลนั้นด้วย

(3.3) มีอุปกรณ์บันทึกข้อมูลชุดสำเนา (Backup file) แยกเก็บไว้ในที่ปลอดภัยห่างจากอาคารที่ทำการประมวลผลข้อมูล

4.1.7 <u>การรักษาความปลอดภัย</u> ให้บริษัทจัดมาตรการรักษาความปลอดภัย เพื่อมิให้การประมวลผลข้อมูลหยุดชะงักและเพื่อคุ้มครองป้องกันความเสียหายที่อาจเกิดขึ้นกับเครื่องคอมพิวเตอร์ โปรแกรมและข้อมูลจากเหตุการณ์ที่เกิดขึ้นโดยไม่สามารถคาดการณ์ได้ล่วงหน้าหรือโดยการกระทำอย่างจงใจของบุคคลภายในหรือภายนอกบริษัท ดังนี้

(1) แผนรักษาความปลอดภัย ซึ่งประกอบด้วย การป้องกันความเสียหายที่จะมีต่อเครื่องคอมพิวเตอร์ โปรแกรม ข้อมูล และพนักงานปฏิบัติการคอมพิวเตอร์ รวมทั้งการปฏิบัติงานขณะที่เกิดความเสียหายและการปฏิบัติการเพื่อย้ายการประมวลผลข้อมูลไป ณ ที่แห่งใหม่ที่ได้จัดเตรียมไว้

(2) การป้องกันความเสียหายจากภัยพิบัติและสาเหตุอื่นๆ ภัยที่จะก่อให้เกิดความเสียหายต่อการประมวลผลข้อมูลด้วยคอมพิวเตอร์โดยทั่วไป ได้แก่ อุทกภัย อัคคีภัย การก่อวินาศกรรม กระแสไฟฟ้าดับหรือแรงดันตก การโจรกรรมและเครื่องคอมพิวเตอร์ขัดข้องใช้การไม่ได้เป็นเวลานาน บริษัทจึงควรกำหนดมาตรการการป้องกันความเสียหายจากสาเหตุดังกล่าว

(3) การจัดเตรียมระบบประมวลผลสำรอง จัดเตรียมระบบประมวลผลสำรองไว้ปฏิบัติในยามฉุกเฉิน ทั้งนี้ระบบประมวลผลสำรองของบริษัทที่ประมวลผลข้อมูลด้วยคอมพิวเตอร์ขนาดเล็กอาจจะเป็นระบบที่ปฏิบัติงานโดยบุคคล (Manual system) หรือระบบคอมพิวเตอร์ (Computer system) ก็ได้

(3.1) ระบบประมวลผลด้วยระบบคอมพิวเตอร์สำรอง ควรประกอบด้วย เครื่องคอมพิวเตอร์ โปรแกรม และแฟ้มข้อมูลที่เตรียมไว้อีกอย่างน้อง 1 ชุด สำหรับปฏิบัติในกรณีฉุกเฉิน ทั้งนี้ในการจัดหาเครื่องคอมพิวเตอร์สำรอง บริษัทอาจทำข้อตกลงกับบริษัทอื่นที่มีเครื่องคอมพิวเตอร์ซึ่งสามารถใช้ร่วมกันได้หรือกับบริษัทผู้ผลิตหรือผู้ขาย

(3.2) โปรแกรมและเอกสารสนับสนุนการปฏิบัติงานประมวลผล มีชุดสำรองเก็บไว้อย่างปลอดภัยนอกสถานที่ทำการ เพื่อป้องกันมิให้เสียหายไปพร้อมกับชุดที่ใช้งานประจำ

(3.3) แฟ้มข้อมูลชุดสำรอง มีให้เพียงพอสำหรับการสร้างข้อมูลให้เป็นปัจจุบัน และควรเก็บรักษาไว้นอกสถานที่ทำการเช่นดียวกับโปรแกรมและเอกสารสนับสนุนการปฏิบัติงาน

(4) การประกันภัย จัดให้มีการประกันภัย เพื่อคุ้มครองความเสียหายที่อาจเกิดขึ้น โดยเฉพาะความเสียหายที่มีมูลค่าจำนวนเงินสูง เช่น เครื่องคอมพิวเตอร์ และอุปกรณ์ที่

จำเป็นในการประมวลผลข้อมูล และค่าใช้จ่ายพิเศษที่เกิดจากการประมวลผลข้อมูลด้วยคอมพิวเตอร์สำรอง เป็นต้น

4.1.8 <u>การตรวจสอบงานคอมพิวเตอร์</u> ให้บริษัทจัดให้มีการตรวจสอบการปฏิบัติงานด้านคอมพิวเตอร์ของบริษัทเพื่อให้มั่นใจว่าการปฏิบัติงานประมวลผลข้อมูลเป็นไปตามนโยบาย มาตรฐานและระเบียบปฏิบัติงานที่บริษัทกำหนด รวมทั้งเครื่องคอมพิวเตอร์ โปรแกรม และแฟ้มข้อมูลได้รับการปฏิบัติอย่างถูกต้องและปลอดภัย ข้อมูลผลลัพธ์และรายงานที่ได้รับจากการประมวลผลมีความถูกต้อง เชื่อถือได้

(1) มอบหมายให้ผู้ตรวจสอบภายในหรือว่าจ้างให้ผู้สอบบัญชีภายนอกหรือร่วมกันตรวจสอบการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ของบริษัท และให้รายงานผลการตรวจสอบโดยตรงต่อคณะกรรมการของบริษัท เพื่อให้มีความเป็นอิสระในการปฏิบัติงาน

(2) กำหนดบทบาท มาตรฐาน และวิธีปฏิบัติงานตรวจสอบด้านคอมพิวเตอร์โดยละเอียดไว้ในคู่มือการตรวจสอบ เพื่อให้ผู้ตรวจสอบภายในถือปฏิบัติและเพื่อใช้ประโยชน์ในการฝึกอบรมพนักงานใหม่

(3) การตรวจสอบด้านคอมพิวเตอร์ ให้มีขอบเขตการตรวจสอบที่ครอบคลุมถึงการพัฒนาระบบงานและโปรแกรม (System development & programming) การปฏิบัติงานประมวลผลข้อมูล (Computer operations) การรักษาความปลอดภัย การนำข้อมูลเข้า (Data entry) และการสอบทานความถูกต้องของข้อมูลผลลัพธ์และรายงานที่ได้จากการประมวลผล (Data output & report)

(4) การปฏิบัติงานตรวจสอบในแต่ละเรื่อง ให้มีขั้นตอนการตรวจสอบอย่างน้อย 3 ขั้นตอน คือ

(4.1) การสอบทานและวิเคราะห์ความเพียงพอเบื้องต้นของการควบคุมภายใน

(4.2) การทดสอบการปฏิบัติงานเพื่อประเมินประสิทธิภาพของการควบคุม

(4.3) การทดสอบความถูกต้องของข้อมูล ในกรณีที่เห็นว่าการควบคุมภายในที่ถือปฏิบัติไม่เพียงพอหรือไม่มีประสิทธิภาพ

ในการทดสอบการควบคุมและทดสอบความถูกต้องของข้อมูล ผู้ตรวจสอบอาจใช้คอมพิวเตอร์ช่วยในการตรวจสอบก็ได้ ซึ่งจะทำให้สามารถขยายขอบเขตการทดสอบ และสามารถตรวจสอบการทำงานของโปรแกรมระบบงานและข้อมูลในเครื่องได้โดยตรงแทนที่จะถูกจำกัดให้ตรวจสอบได้เพียงข้อมูลนำเข้าและข้อมูลผลลัพธ์

(5) การจัดทำรายงานผลการตรวจสอบ รายงานสรุปผลการตรวจสอบ ประกอบด้วยหัวข้อ ดังนี้

(5.1) เรื่องที่ตรวจสอบ

(5.2) วันที่เริ่มตรวจสอบและวันที่ตรวจสอบเสร็จ

(5.3) รายชื่อผู้ตรวจสอบ

(5.4) ขอบเขตและวัตถุประสงค์ในการตรวจสอบ

(5.5) ข้อสังเกตและข้อเสนอแนะ

(5.6) รายละเอียดเอกสารประกอบผลการตรวจสอบ

(6) การจัดทำกระดาษทำการ กำหนดมาตรฐานของการจัดทำกระดาษทำการ ประกอบด้วย

(6.1) แผนการตรวจสอบ

(6.2) ขอบเขตและวัตถุประสงค์ของการตรวจสอบ

(6.3) การบรรยายสรุปวิธีการปฏิบัติงานและการควบคุมภายใน

(6.4) แบบสอบถาม และวิธีการอื่นๆที่ใช้ในการตรวจสอบ

(6.5) บันทึกสรุปข้อสังเกตและปัญหาที่พบระหว่างการตรวจสอบ

(7) การติดตามผลการตรวจสอบ กำหนดให้ส่วนงานที่ถูกตรวจสอบตอบชี้แจงการปรับปรุงแก้ไขตามข้อเสนอแนะของผู้ตรวจสอบ และให้ฝ่ายตรวจสอบติดตามผลการดำเนินการแก้ไขดังกล่าวเสนอคณะกรรมการของบริษัทต่อไป

4.2 การควบคุมการประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์

4.2.1 <u>การรักษาความปลอดภัยเครื่องไมโครคอมพิวเตอร์</u> ให้บริษัทติดตั้งไมโครคอมพิวเตอร์ไว้ในสถานที่ที่สามารถควบคุมการเข้าออก เพื่อป้องกันการโจรกรรมตัวเครื่อง และมิให้บุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปใช้เครื่อง และมอบหมายให้หน่วยงานเจ้าของเครื่องเป็นผู้รับผิดชอบการใช้งานและดูแลรักษาเครื่อง

4.2.2 <u>การควบคุมความปลอดภัยของแฟ้มข้อมูลและโปรแกรม</u> ให้บริษัทควบคุมแฟ้มข้อมูลและโปรแกรมเพื่อป้องกันมิให้เกิดความสูญหาย เนื่องจากการสูญหาย ถูกทำลาย ถูกแก้ไขหรือถูกถ่ายสำเนา โดยไม่ได้รับอนุญาต ดังนี้

(1) แฟ้มข้อมูลและโปรแกรมต่าง ๆ ขณะที่ยังไม่ได้ใช้งานควรเก็บไว้ในสถานที่ปลอดภัย สามารถควบคุมและป้องกันมิให้ผู้ที่ไม่มีสิทธินำออกไปใช้งานได้และปิดสลากภายนอกแฟ้มข้อมูลและโปรแกรมทุกแผ่นเพื่อป้องกันการนำไปใช้ผิดพลาด

(2) แฟ้มข้อมูลและโปรแกรมที่อยู่ในเครื่อง (Hard disks) ขณะที่ยังไม่ได้ใช้งาน ให้ปิดเครื่อง เพื่อป้องกันมิให้ผู้ไม่มีสิทธิไปใช้เครื่องและข้อมูลในเครื่อง กรณีเป็นไมโครคอมพิวเตอร์ที่ใช้ร่วมกันหลายงานและหลายคน ให้กำหนดรหัสประจำตัวผู้มีสิทธิเข้าถึงแฟ้มข้อมูลและโปรแกรม (Identification code) และรหัสการใช้งาน (Password) ซึ่งระบุขอบเขตของการใช้งานแฟ้มข้อมูลและโปรแกรมดังกล่าว

(3) จัดทำสำเนาแฟ้มข้อมูลและโปรแกรมที่สำคัญ ๆ ไว้ใช้ทดแทนในกรณีที่แฟ้มข้อมูลและโปรแกรมที่ใช้อยู่ปัจจุบันสูญหาย หรือเสียหายจนใช้การไม่ได้ เพื่อป้องกันมิให้การประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์หยุดชะงัก

(4) มีเอกสารประกอบระบบงานที่ใช้ไมโครคอมพิวเตอร์ อาทิ เช่น ลักษณะของงาน ลักษณะของแฟ้มข้อมูล ขั้นตอนการเตรียมข้อมูลนำเข้า การประมวลผลข้อมูล ลักษณะของผลลัพธ์หรือรายงานที่ได้ และการตรวจสอบความถูกต้องของข้อมูลและรายงาน เป็นต้น

4.2.3 <u>การตรวจสอบการประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์</u> ให้บริษัทมอบหมายให้ผู้ตรวจสอบภายในหรือหน่วยงานที่ไม่เกี่ยวข้องกับการประมวลผลข้อมูล ตรวจสอบการรักษาความปลอดภัยไมโครคอมพิวเตอร์ แฟ้มข้อมูลและโปรแกรมการจัดทำสำเนาแฟ้มข้อมูลและโปรแกรม และตรวจสอบความถูกต้องของข้อมูลและรายงานที่ได้จากการประมวลผล

เอกสารแนบ 6

แนวทางการป้องกันการทุจริตผ่านเครือข่ายอินเทอร์เน็ตด้วยวิธี Phishing

---

เพื่อให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ตระหนักถึงปัญหาการทุจริตที่เกิดขึ้นในปัจจุบัน เพิ่มความระมัดระวังในการให้บริการ รวมทั้งจัดให้มีมาตรการป้องกันและแจ้งเตือนลูกค้าเกี่ยวกับการทุจริตที่อาจเกิดขึ้น เพื่อให้การให้บริการมีความปลอดภัยต่อลูกค้า ลดผลกระทบและความเสียหายต่อธุรกิจของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ และเป็นการรักษาความเชื่อมั่นของลูกค้าในการใช้บริการของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์

เนื้อหา

"Phishing" คือ การโจมตีในรูปแบบของการปลอมแปลง E-mail (E-mail Spoofing) และสร้าง Website ปลอม เพื่อทำการหลอกลวงให้เหยื่อผู้รับ E-mail เปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนบุคคลอื่น ๆ อาทิ หมายเลขบัตรเครดิต ชื่อบัญชีผู้ใช้บริการ (Username) และรหัสผ่าน (Password) หมายเลขบัตรประจำตัวประชาชน หรือข้อมูลส่วนบุคคลอื่น ๆ

1. ปัญหาการทุจริต

ปัจจุบันปัญหาการทุจริตด้วยวิธี Phishing มีการแพร่ระบาดในหลายประเทศ และได้เริ่มแพร่ระบาดในกลุ่มผู้ใช้ E-mail ในประเทศไทย โดยมีแนวโน้มที่จะเพิ่มมากขึ้น เนื่องจากการทุจริตด้วยวิธีดังกล่าวสามารถกระทำได้ง่ายและอาศัยความรู้เท่าไม่ถึงการณ์ของลูกค้าในการกระทำทุจริต ซึ่งจะสร้างความเสียหายทางการเงินต่อลูกค้า และบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ รวมทั้งส่งผลกระทบต่อความเชื่อมั่นของลูกค้าในการใช้บริการการเงินทางอิเล็กทรอนิกส์โดยรวมด้วย

วิธีการกระทำทุจริตที่พบในปัจจุบัน ได้แก่ การส่ง E-mail หลอกลวงไปยังลูกค้าเพื่อให้หลงเชื่อว่าเป็น E-mail มาจากบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ โดยมักใช้หัวข้อและข้อความที่มีความน่าเชื่อถือ เช่น การร้องขอให้ลูกค้าแจ้งยืนยันข้อมูลทางการเงินเพื่อให้เป็นไปตามมาตรการการรักษาความปลอดภัยของบัญชีลูกค้า หรือ การแจ้งลูกค้าว่าถึงรอบระยะเวลาที่จะต้องตรวจสอบข้อมูลของลูกค้า หรือ การแจ้งว่าบัญชีของลูกค้าได้ถูกอายัดไว้ชั่วคราว จึงขอให้ลูกค้ายืนยันข้อมูล เพื่อให้การทำธุรกรรมทางการเงินของลูกค้าสามารถดำเนินการได้ต่อไป เป็นต้น พร้อมทั้งแนบลิงค์การเชื่อมโยง (Hyperlink) Website ของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์

ปลอมที่ทำขึ้นโดยการขโมยหรือนำเครื่องหมายหรือสัญลักษณ์ตลอดจนรูปลักษณ์ของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ที่มีชื่อเสียง หรือแนบแบบฟอร์มการสอบถามข้อมูล เพื่อให้ลูกค้ากรอกข้อมูลส่วนบุคคล เช่น หมายเลขบัตรเครดิต เลขที่บัญชีเงินฝาก ชื่อบัญชีผู้ใช้บริการ (Username) และรหัสผ่าน (Password) เป็นต้น หลังจากที่ลูกค้าได้กรอกข้อมูลลงใน Website ปลอม หรือ แบบฟอร์มการสอบถามนั้นแล้ว ผู้กระทำการทุจริตจะนำข้อมูลเหล่านั้นไปใช้ประโยชน์ในทางมิชอบได้หลายช่องทาง เช่น การโอนเงินหรือการชำระเงินให้บุคคลที่สามผ่านการให้บริการ Internet Banking หรือ Tele Banking หรือ Mobile Banking หรือ การซื้อสินค้าและบริการทางอินเทอร์เน็ตโดยใช้บัตรเครดิต เป็นต้น

2. แนวทางการป้องกัน

2.1 การเพิ่มความระมัดระวัง

บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ควรเพิ่มความระมัดระวังและจัดให้มีมาตรการรักษาความปลอดภัย ดังนี้

2.1.1 ในกรณีที่บริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์มีการให้บริการส่ง E-mail ไปยังลูกค้า บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ต้องไม่แนบลิงค์เพื่อเชื่อมโยง Website ของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ หรือแบบฟอร์มการสอบถามข้อมูลส่วนบุคคลไปให้ลูกค้า

2.1.2 การจัดให้มีกระบวนการประเมินความเสี่ยง เพื่อพิจารณาการให้บริการที่มีความเสี่ยงสูง และจัดให้มีมาตรการเพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้น เช่น ในกรณีที่บริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์มีการให้บริการโอนเงินจากบัญชีเงินฝากของลูกค้าไปยังบุคคลที่สามผ่านเครือข่ายอินเทอร์เน็ต โดยลูกค้าไม่ต้องแจ้งบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์เป็นลายลักษณ์อักษรก่อนการใช้บริการ บริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ควรพิจารณากำหนดวงเงินสูงสุดในการโอนเงินที่เหมาะสม หรือการพิจารณาใช้วิธีการตรวจสอบตัวตนแบบ Two-Factor Authentication[1] ในการให้บริการผ่านเครือข่ายอินเทอร์เน็ตที่มีความเสี่ยงสูง เป็นต้น

---

[1] เป็นวิธีการตรวจสอบตัวตนที่จะเพิ่มความปลอดภัยในการให้บริการผ่านเครือข่ายอินเทอร์เน็ต ซึ่งประกอบด้วยการพิสูจน์ตัวตน 2 ขั้นตอน ดังนี้
1. การใช้ชื่อบัญชีผู้ใช้บริการ (Username) และรหัสผ่าน (Password)
2. การใช้อุปกรณ์เสริมเข้ามาใช้ในการพิสูจน์ตัวตน เช่น การใช้ Token เพื่อสร้างรหัสผ่านใหม่ทุกครั้งเมื่อจะเข้าใช้บริการ หรือการใช้กุญแจส่วนตัว (Private key) ที่เก็บอยู่ใน Smart card ของลูกค้า หรืออุปกรณ์อื่น ๆ ที่ลูกค้าเป็นเจ้าของ เป็นต้น

2.1.3 การจัดให้มีกระบวนการติดตามข้อมูลการทำรายการของลูกค้าผ่านช่องทางอิเล็กทรอนิกส์ต่าง ๆ อย่างต่อเนื่อง ซึ่งจะช่วยให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ทราบถึงรูปแบบการทำธุรกรรมที่ผิดปกติ และโอกาสที่จะเกิดการกระทำทุจริตได้อย่างรวดเร็ว

2.1.4 การติดตามความก้าวหน้าทางเทคโนโลยีที่เกี่ยวข้องกับการให้บริการรวมทั้งรูปแบบการทุจริตผ่านเครือข่ายอินเทอร์เน็ต[2] และช่องทางอิเล็กทรอนิกส์อื่นอย่างต่อเนื่อง เพื่อนำมาปรับปรุงมาตรการการรักษาความปลอดภัยได้อย่างเหมาะสม และเลือกใช้เทคโนโลยีที่มีประสิทธิภาพในการป้องกันการกระทำทุจริต

2.1.5 การแจ้งเตือนให้ลูกค้าทราบถึงพฤติกรรมการหลอกลวงด้วยวิธี Phishing โดยแสดงข้อความเตือนบนหน้าจอภาพหลักของ Website ของบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ และการแจ้งให้ลูกค้าทราบทางจดหมาย นอกจากนี้ บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ควรมีกระบวนการแจ้งให้ลูกค้ารายใหม่ได้ทราบด้วย

2.1.6 การจัดให้มีกระบวนการแก้ไขปัญหา มีการกำหนดทีมผู้รับผิดชอบที่ได้รับการฝึกฝนให้วิเคราะห์และจัดการแก้ปัญหาได้อย่างรวดเร็ว รวมทั้งการจัดให้มีการรายงานต่อผู้บริหารของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ถึงปัญหาที่เกิดขึ้น

2.2 ข้อแนะนำแก่ลูกค้า

บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ควรให้ข้อมูลและคำแนะนำที่เป็นประโยชน์แก่ลูกค้า โดยจัดทำเป็นลายลักษณ์อักษรและดำเนินการแจ้งให้ลูกค้าทราบ เพื่อให้ลูกค้าสามารถใช้บริการการเงินทางอิเล็กทรอนิกส์ได้อย่างปลอดภัย ซึ่งเป็นการลดโอกาสที่จะเกิดความเสียหายทั้งต่อลูกค้าและบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ ทั้งนี้ คำแนะนำที่ให้แก่ลูกค้าควรครอบคลุมถึง

2.2.1 การแจ้งให้ลูกค้าทราบว่าบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ไม่มีนโยบายในการให้บริการแก่ลูกค้า ดังนี้

(1) ส่ง E-mail พร้อมลิงค์การเชื่อมโยง Website ของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ให้กับลูกค้าผู้ใช้บริการ

---

[2] ศึกษาข้อมูลเพิ่มเติมได้ที่

- ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (Thai Computer Emergency Response Team: ThaiCERT) http://www.thaicert.nectec.or.th

- สมาคม Anti-Phishing Working Group ของสหรัฐอเมริกา http://www.antiphishing.org

(2) สอบถามข้อมูลส่วนบุคคลและข้อมูลสำคัญทางการเงิน เช่น ชื่อบัญชีผู้ใช้บริการ (Username) และรหัสผ่าน (Password) หมายเลขบัตรเครดิต เป็นต้น ผ่านทาง E-mail รวมถึงช่องทางอื่น ๆ เช่น ทางโทรศัพท์ ทางจดหมาย เป็นต้น

2.2.2 แนะนำให้ลูกค้าพิมพ์ Address ของ Website (URL) ของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ด้วยตนเองเมื่อต้องการเข้าใช้บริการผ่านเครือข่ายอินเทอร์เน็ตของบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ ไม่ควรใช้ลิงค์การเชื่อมโยงที่แนบมากับ E-mail

2.2.3 แนะนำให้ลูกค้าตรวจสอบความถูกต้องของรายการธุรกรรม เช่น จำนวนเงิน วันที่ทำรายการ เลขที่บัญชี และตรวจสอบยอดเงินในบัญชีอย่างสม่ำเสมอ เพื่อป้องกันรายการผิดปกติที่อาจเกิดขึ้น

2.2.4 แนะนำลูกค้าไม่ให้ส่งข้อมูลส่วนบุคคลหรือข้อมูลสำคัญทางการเงินไปกับ E-mail ที่มีข้อความน่าสงสัยว่ามีการแอบอ้างมาจากบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์ รวมทั้งแนะนำให้ลูกค้ารีบติดต่อบริษัทเงินทุนหรือบริษัทเครดิตฟองซิเอร์โดยเร็ว

3. กระบวนการรับข้อร้องเรียน

บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ควรจัดให้มีช่องทางในการรับแจ้งปัญหาและข้อร้องเรียนจากลูกค้า และแจ้งให้ลูกค้าทราบถึงช่องทางดังกล่าว โดยอย่างน้อยบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ควรจัดให้มีหมายเลขโทรศัพท์ที่ลูกค้าสามารถติดต่อได้ ในกรณีที่พบเหตุการณ์หรือรายการผิดปกติต่าง ๆ ทั้งนี้ บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ควรมีการฝึกอบรมเจ้าหน้าที่ผู้รับเรื่องร้องเรียนดังกล่าว ให้มีความรู้และสามารถแนะนำลูกค้าในการใช้บริการการเงินทางอิเล็กทรอนิกส์ได้อย่างถูกต้องและปลอดภัย

เอกสารแนบ 7

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

พระราชบัญญัติ
ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
พ.ศ. ๒๕๔๔

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๒ ธันวาคม พ.ศ. ๒๕๔๔

เป็นปีที่ ๕๖ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรให้มีกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๙ ประกอบกับมาตรา ๕๐ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของรัฐสภาดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ พระราชบัญญัตินี้ให้ใช้บังคับแก่ธุรกรรมในทางแพ่งและพาณิชย์ที่ดำเนินการโดยใช้ข้อมูลอิเล็กทรอนิกส์ เว้นแต่ธุรกรรมที่มีพระราชกฤษฎีกากำหนดมิให้นำพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับ

ความในวรรคหนึ่งไม่มีผลกระทบกระเทือนถึงกฎหมายหรือกฎใดที่กำหนดขึ้นเพื่อคุ้มครองผู้บริโภค

พระราชบัญญัตินี้ใช้บังคับแก่ธุรกรรมในการดำเนินงานของรัฐตามที่กำหนดในหมวด ๔

มาตรา ๔ ในพระราชบัญญัตินี้

“ธุรกรรม” หมายความว่า การกระทำใด ๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์หรือในการดำเนินงานของรัฐตามที่กำหนดในหมวด ๔

“อิเล็กทรอนิกส์” หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ เช่นว่านั้น

“ธุรกรรมทางอิเล็กทรอนิกส์” หมายความว่า ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน

“ข้อความ” หมายความว่า เรื่องราว หรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ

“ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

“ลายมือชื่ออิเล็กทรอนิกส์” หมายความว่า อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

“ระบบข้อมูล” หมายความว่า กระบวนการประมวลผลด้วยเครื่องมืออิเล็กทรอนิกส์สำหรับสร้าง ส่ง รับ เก็บรักษา หรือประมวลผลข้อมูลอิเล็กทรอนิกส์

“การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์” หมายความว่า การส่งหรือรับข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์โดยใช้มาตรฐานที่กำหนดไว้ล่วงหน้า

“ผู้ส่งข้อมูล” หมายความว่า บุคคลซึ่งเป็นผู้ส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ก่อนจะมีการเก็บรักษาข้อมูลเพื่อส่งไปตามวิธีการที่ผู้นั้นกำหนด โดยบุคคลนั้นอาจจะส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง หรือมีการส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนบุคคลนั้นก็ได้ ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

“ผู้รับข้อมูล” หมายความว่า บุคคลซึ่งผู้ส่งข้อมูลประสงค์จะส่งข้อมูลอิเล็กทรอนิกส์ให้และได้รับข้อมูลอิเล็กทรอนิกส์นั้น ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

“บุคคลที่เป็นสื่อกลาง” หมายความว่า บุคคลซึ่งกระทำการในนามผู้อื่นในการส่ง รับ หรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์อันใดอันหนึ่งโดยเฉพาะ รวมถึงให้บริการอื่นที่เกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้น

“ใบรับรอง” หมายความว่า ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใด ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์

“เจ้าของลายมือชื่อ” หมายความว่า ผู้ซึ่งถือข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์และสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นในนามตนเองหรือแทนบุคคลอื่น

“คู่กรณีที่เกี่ยวข้อง” หมายความว่า ผู้ซึ่งอาจกระทำการใด ๆ โดยขึ้นอยู่กับใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์

“หน่วยงานของรัฐ” หมายความว่า กระทรวง ทบวง กรม ส่วนราชการที่เรียกชื่ออย่างอื่นและมีฐานะเป็นกรม ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจที่ตั้งขึ้นโดยพระราชบัญญัติหรือพระราชกฤษฎีกา และให้หมายความรวมถึงนิติบุคคล คณะบุคคล หรือบุคคลซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่าในการใด ๆ

“คณะกรรมการ” หมายความว่า คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๕ บทบัญญัติมาตรา ๑๓ ถึงมาตรา ๒๔ และบทบัญญัติมาตรา ๒๖ ถึงมาตรา ๓๑ จะตกลงกันเป็นอย่างอื่นก็ได้

มาตรา ๖ ให้นายกรัฐมนตรีรักษาการตามพระราชบัญญัตินี้

หมวด ๑
ธุรกรรมทางอิเล็กทรอนิกส์

มาตรา ๗ ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใดเพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

มาตรา ๘ ภายใต้บังคับบทบัญญัติแห่งมาตรา ๙ ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว

มาตรา ๙ ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า

(๑) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ

(๒) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

มาตรา ๑๐ ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว

(๑) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และ

(๒) สามารถแสดงข้อความนั้นในภายหลังได้

ความถูกต้องของข้อความตาม (๑) ให้พิจารณาถึงความครบถ้วนและไม่มีการเปลี่ยนแปลงใดของข้อความ เว้นแต่การรับรองหรือบันทึกเพิ่มเติม หรือการเปลี่ยนแปลงใด ๆ ที่อาจจะเกิดขึ้นได้ตามปกติในการติดต่อสื่อสาร การเก็บรักษา หรือการแสดงข้อความซึ่งไม่มีผลต่อความถูกต้องของข้อความนั้น

ในการวินิจฉัยความน่าเชื่อถือของวิธีการรักษาความถูกต้องของข้อความตาม (๑) ให้พิเคราะห์ถึงพฤติการณ์ที่เกี่ยวข้องทั้งปวง รวมทั้งวัตถุประสงค์ของการสร้างข้อความนั้น

มาตรา ๑๑ ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายเพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะหรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง

มาตรา ๑๒ ภายใต้บังคับบทบัญญัติมาตรา ๑๐ ในกรณีที่กฎหมายกำหนดให้เก็บรักษาเอกสารหรือข้อความใด ถ้าได้เก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการเก็บรักษาเอกสารหรือข้อความตามที่กฎหมายต้องการแล้ว

(๑) ข้อมูลอิเล็กทรอนิกส์นั้นสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง

(๒) ได้เก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นให้อยู่ในรูปแบบที่เป็นอยู่ในขณะที่สร้าง ส่ง หรือได้รับข้อมูลอิเล็กทรอนิกส์นั้น หรืออยู่ในรูปแบบที่สามารถแสดงข้อความที่สร้าง ส่ง หรือได้รับให้ปรากฏอย่างถูกต้องได้ และ

(๓) ได้เก็บรักษาข้อความส่วนที่ระบุถึงแหล่งกำเนิด ต้นทาง และปลายทางของข้อมูลอิเล็กทรอนิกส์ ตลอดจนวันและเวลาที่ส่งหรือได้รับข้อความดังกล่าว ถ้ามี

ความในวรรคหนึ่ง มิให้ใช้บังคับกับข้อความที่ใช้เพียงเพื่อวัตถุประสงค์ในการส่งหรือรับข้อมูลอิเล็กทรอนิกส์

หน่วยงานของรัฐที่รับผิดชอบในการเก็บรักษาเอกสารหรือข้อความใด อาจกำหนดหลักเกณฑ์รายละเอียดเพิ่มเติมเกี่ยวกับการเก็บรักษาเอกสารหรือข้อความนั้นได้ เท่าที่ไม่ขัดหรือแย้งกับบทบัญญัติในมาตรานี้

มาตรา ๑๓ คำเสนอหรือคำสนองในการทำสัญญาอาจทำเป็นข้อมูลอิเล็กทรอนิกส์ก็ได้ และห้ามมิให้ปฏิเสธการมีผลทางกฎหมายของสัญญาเพียงเพราะเหตุที่สัญญานั้นได้ทำคำเสนอหรือคำสนองเป็นข้อมูลอิเล็กทรอนิกส์

มาตรา ๑๔ ในระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล การแสดงเจตนาหรือคำบอกกล่าวอาจทำเป็นข้อมูลอิเล็กทรอนิกส์ก็ได้

มาตรา ๑๕ บุคคลใดเป็นผู้ส่งข้อมูลไม่ว่าจะเป็นการส่งโดยวิธีใด ให้ถือว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้นั้น

ในระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล ให้ถือว่าเป็นข้อมูลอิเล็กทรอนิกส์ของผู้ส่งข้อมูลหากข้อมูลอิเล็กทรอนิกส์นั้นได้ส่งโดย

(๑) บุคคลผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูลเกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้น หรือ

(๒) ระบบข้อมูลที่ผู้ส่งข้อมูลหรือบุคคลผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูลได้กำหนดไว้ล่วงหน้าให้สามารถทำงานได้โดยอัตโนมัติ

มาตรา ๑๖ ผู้รับข้อมูลชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้ส่งข้อมูลและชอบที่จะดำเนินการไปตามข้อมูลอิเล็กทรอนิกส์นั้นได้ ถ้า

(๑) ผู้รับข้อมูลได้ตรวจสอบโดยสมควรตามวิธีการที่ได้ตกลงกับผู้ส่งข้อมูลว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้ส่งข้อมูล หรือ

(๒) ข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นเกิดจากการกระทำของบุคคลซึ่งใช้วิธีการที่ผู้ส่งข้อมูลใช้ในการแสดงว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นของผู้ส่งข้อมูล ซึ่งบุคคลนั้นได้ล่วงรู้โดยอาศัยความสัมพันธ์ระหว่างบุคคลนั้นกับผู้ส่งข้อมูลหรือผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูล

ความในวรรคหนึ่งมิให้ใช้บังคับ ถ้า

(๑) ในขณะนั้นผู้รับข้อมูลได้รับแจ้งจากผู้ส่งข้อมูลว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นมิใช่ของผู้ส่งข้อมูล และในขณะเดียวกันผู้รับข้อมูลมีเวลาพอสมควรที่จะตรวจสอบข้อเท็จจริงตามที่ได้รับแจ้งนั้น หรือ

(๒) กรณีตามวรรคหนึ่ง (๒) เมื่อผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอนิกส์นั้นไม่ใช่ของผู้ส่งข้อมูล หากผู้รับข้อมูลได้ใช้ความระมัดระวังตามสมควร หรือดำเนินการตามวิธีการที่ได้ตกลงกันไว้ก่อนแล้ว

มาตรา ๑๗ ในกรณีตามมาตรา ๑๕ หรือมาตรา ๑๖ วรรคหนึ่ง ในระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล ผู้รับข้อมูลมีสิทธิถือว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับนั้นถูกต้องตามเจตนาของผู้ส่งข้อมูลและสามารถดำเนินการไปตามข้อมูลอิเล็กทรอนิกส์นั้นได้ เว้นแต่ผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับนั้นมีข้อผิดพลาดอันเกิดจากการส่ง หากผู้รับข้อมูลได้ใช้ความระมัดระวังตามสมควรหรือดำเนินการตามวิธีการที่ได้ตกลงกันไว้ก่อนแล้ว

มาตรา ๑๘ ผู้รับข้อมูลชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับแต่ละชุดเป็นข้อมูลที่แยกจากกัน และสามารถดำเนินการไปตามข้อมูลอิเล็กทรอนิกส์แต่ละชุดนั้นได้ เว้นแต่ข้อมูลอิเล็กทรอนิกส์ชุดนั้นจะซ้ำกับข้อมูลอิเล็กทรอนิกส์อีกชุดหนึ่ง และผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นข้อมูลอิเล็กทรอนิกส์ซ้ำ หากผู้รับข้อมูลได้ใช้ความระมัดระวังตามสมควรหรือดำเนินการตามวิธีการที่ได้ตกลงกันไว้ก่อนแล้ว

มาตรา ๑๙ ในกรณีที่ต้องมีการตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์ ไม่ว่าผู้ส่งข้อมูลได้ร้องขอหรือตกลงกับผู้รับข้อมูลไว้ก่อนหรือขณะที่ส่งข้อมูลอิเล็กทรอนิกส์หรือปรากฏในข้อมูลอิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(๑) ในกรณีที่ผู้ส่งข้อมูลมิได้ตกลงให้ตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์ในรูปแบบหรือวิธีการใดโดยเฉพาะ การตอบแจ้งการรับอาจทำได้ด้วยการติดต่อสื่อสารจากผู้รับข้อมูล ไม่ว่าโดยระบบข้อมูลที่ทำงานโดยอัตโนมัติหรือโดยวิธีอื่นใด หรือด้วยการกระทำใด ๆ ของผู้รับข้อมูลซึ่งเพียงพอจะแสดงต่อผู้ส่งข้อมูลว่าผู้รับข้อมูลได้รับข้อมูลอิเล็กทรอนิกส์นั้นแล้ว

(๒) ในกรณีที่ผู้ส่งข้อมูลกำหนดเงื่อนไขว่าจะถือว่ามีการส่งข้อมูลอิเล็กทรอนิกส์ต่อเมื่อได้รับการตอบแจ้งการรับจากผู้รับข้อมูล ให้ถือว่ายังไม่มีการส่งข้อมูลอิเล็กทรอนิกส์จนกว่าผู้ส่งข้อมูลจะได้รับการตอบแจ้งการรับแล้ว

(๓) ในกรณีที่ผู้ส่งข้อมูลมิได้กำหนดเงื่อนไขตามความใน (๒) และผู้ส่งข้อมูลมิได้รับการตอบแจ้งการรับนั้นภายในเวลาที่กำหนดหรือตกลงกัน หรือภายในระยะเวลาอันสมควรในกรณีที่มิได้กำหนดหรือตกลงเวลาไว้

(ก) ผู้ส่งข้อมูลอาจส่งคำบอกกล่าวไปยังผู้รับข้อมูลว่าตนยังไม่ได้รับการตอบแจ้งการรับ และกำหนดระยะเวลาอันสมควรให้ผู้รับข้อมูลตอบแจ้งการรับ และ

(ข) หากผู้ส่งข้อมูลมิได้รับการตอบแจ้งการรับภายในระยะเวลาตาม (ก) เมื่อผู้ส่งข้อมูลบอกกล่าวแก่ผู้รับข้อมูลแล้ว ผู้ส่งข้อมูลชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมิได้มีการส่งเลย หรือผู้ส่งข้อมูลอาจใช้สิทธิอื่นใดที่ผู้ส่งข้อมูลมีอยู่ได้

มาตรา ๒๐ ในกรณีที่ผู้ส่งข้อมูลได้รับการตอบแจ้งการรับจากผู้รับข้อมูล ให้สันนิษฐานว่าผู้รับข้อมูลได้รับข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องแล้ว แต่ข้อสันนิษฐานดังกล่าวมิให้ถือว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นถูกต้องตรงกันกับข้อมูลอิเล็กทรอนิกส์ที่ผู้ส่งข้อมูลได้ส่งมา

มาตรา ๒๑ ในกรณีที่ปรากฏในการตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์นั้นเองว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับเป็นไปตามข้อกำหนดทางเทคนิคที่ผู้ส่งข้อมูลและผู้รับข้อมูลได้ตกลงหรือระบุไว้ในมาตรฐานซึ่งใช้บังคับอยู่ ให้สันนิษฐานว่าข้อมูลอิเล็กทรอนิกส์ที่ส่งไปนั้นได้เป็นไปตามข้อกำหนดทางเทคนิคทั้งหมดแล้ว

มาตรา ๒๒ การส่งข้อมูลอิเล็กทรอนิกส์ให้ถือว่าได้มีการส่งเมื่อข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลที่อยู่นอกเหนือการควบคุมของผู้ส่งข้อมูล

มาตรา ๒๓ การรับข้อมูลอิเล็กทรอนิกส์ให้ถือว่ามีผลนับแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลของผู้รับข้อมูล

หากผู้รับข้อมูลได้กำหนดระบุข้อมูลที่ประสงค์จะในการรับข้อมูลอิเล็กทรอนิกส์ไว้โดยเฉพาะให้ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนับแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลที่ผู้รับข้อมูลได้กำหนดไว้นั้น แต่ถ้าข้อมูลอิเล็กทรอนิกส์ดังกล่าวได้ส่งยังระบบข้อมูลอื่นของผู้รับข้อมูลซึ่งมิใช่ระบบข้อมูลที่ผู้รับข้อมูลกำหนดไว้ ให้ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนับแต่เวลาที่ได้เรียกข้อมูลอิเล็กทรอนิกส์จากระบบข้อมูลนั้น

ความในมาตรานี้ให้ใช้บังคับแม้ระบบข้อมูลของผู้รับข้อมูลตั้งอยู่ในสถานที่อีกแห่งหนึ่งต่างหากจากสถานที่ที่ถือว่าผู้รับข้อมูลได้รับข้อมูลอิเล็กทรอนิกส์ตามมาตรา ๒๔

มาตรา ๒๔ การส่งหรือการรับข้อมูลอิเล็กทรอนิกส์ ให้ถือว่าได้ส่ง ณ ที่ทำการงานของผู้ส่งข้อมูล หรือได้รับ ณ ที่ทำการงานของผู้รับข้อมูล แล้วแต่กรณี

ในกรณีที่ผู้ส่งข้อมูลหรือผู้รับข้อมูลมีที่ทำการงานหลายแห่ง ให้ถือเอาที่ทำการงานที่เกี่ยวข้องมากที่สุดกับธุรกรรมนั้นเป็นที่ทำการงานเพื่อประโยชน์ตามวรรคหนึ่ง แต่ถ้าไม่สามารถกำหนดได้ว่าธุรกรรมนั้นเกี่ยวข้องกับที่ทำการงานแห่งใดมากที่สุด ให้ถือเอาสำนักงานใหญ่เป็นสถานที่ที่ได้รับหรือส่งข้อมูลอิเล็กทรอนิกส์นั้น

ในกรณีที่ไม่ปรากฏที่ทำการงานของผู้ส่งข้อมูลหรือผู้รับข้อมูล ให้ถือเอาถิ่นที่อยู่ปกติเป็นสถานที่ที่ส่งหรือได้รับข้อมูลอิเล็กทรอนิกส์

ความในมาตรานี้มิให้ใช้บังคับการส่งและการรับข้อมูลอิเล็กทรอนิกส์โดยวิธีการทางโทรเลขและโทรพิมพ์ หรือวิธีการสื่อสารอื่นตามที่กำหนดในพระราชกฤษฎีกา

มาตรา ๒๕ ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกา ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้

หมวด ๒
ลายมือชื่ออิเล็กทรอนิกส์

_____

มาตรา ๒๖ ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

(๑) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นได้เชื่อมโยงไปยังเจ้าของลายมือชื่อโดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้

(๒) ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(๓) การเปลี่ยนแปลงใด ๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้ และ

(๔) ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่ออิเล็กทรอนิกส์เป็นไปเพื่อรับรองความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์

บทบัญญัติในวรรคหนึ่ง ไม่เป็นการจำกัดว่าไม่มีวิธีการอื่นใดที่แสดงได้ว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ หรือการแสดงพยานหลักฐานใดเกี่ยวกับความไม่น่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์

มาตรา ๒๗ ในกรณีมีการใช้ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์เพื่อสร้างลายมือชื่ออิเล็กทรอนิกส์ที่จะมีผลตามกฎหมายเจ้าของลายมือชื่อต้องดำเนินการดังต่อไปนี้

(๑) ใช้ความระมัดระวังตามสมควรเพื่อมิให้มีการใช้ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

(๒) แจ้งให้บุคคลที่คาดหมายได้โดยมีเหตุอันควรเชื่อว่าจะกระทำการใดโดยขึ้นอยู่กับลายมือชื่ออิเล็กทรอนิกส์หรือให้บริการเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ ทราบโดยมิชักช้า เมื่อ

(ก) เจ้าของลายมือชื่อรู้หรือควรได้รู้ว่าข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นสูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(ข) เจ้าของลายมือชื่อรู้จากสภาพการณ์ที่ปรากฏว่ากรณีมีความเสี่ยงมากพอที่ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ สูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(๓) ในกรณีมีการออกใบรับรองสนับสนุนการใช้ลายมือชื่ออิเล็กทรอนิกส์ จะต้องใช้ความระมัดระวังตามสมควรให้แน่ใจในความถูกต้องและสมบูรณ์ของการแสดงสาระสำคัญทั้งหมดซึ่งกระทำโดยเจ้าของลายมือชื่อเกี่ยวกับใบรับรองนั้นตลอดอายุใบรับรอง หรือตามที่มีการกำหนดในใบรับรอง

มาตรา ๒๘ ในกรณีมีการให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ให้มีผลทางกฎหมายเสมือนหนึ่งลงลายมือชื่อผู้ให้บริการออกใบรับรองต้องดำเนินการ ดังต่อไปนี้

(๑) ปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ตนได้แสดงไว้

(๒) ใช้ความระมัดระวังตามสมควรให้แน่ใจในความถูกต้องและความสมบูรณ์ของการแสดงสาระสำคัญทั้งหมดที่ตนได้กระทำเกี่ยวกับใบรับรองนั้นตลอดอายุใบรับรอง หรือตามที่มีการกำหนดในใบรับรอง

(๓) จัดให้มีวิธีการในการเข้าถึงโดยสมควร ให้คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบข้อเท็จจริงในการแสดงสาระสำคัญทั้งหมดจากใบรับรองได้ ในเรื่องดังต่อไปนี้

(ก) การระบุผู้ให้บริการออกใบรับรอง

(ข) เจ้าของลายมือชื่อซึ่งระบุในใบรับรองได้ควบคุมข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ในขณะมีการออกใบรับรอง

(ค) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์มีผลใช้ได้ในขณะหรือก่อนที่มีการออกใบรับรอง

(๔) จัดให้มีวิธีการเข้าถึงโดยสมควร ให้คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบกรณีดังต่อไปนี้จากใบรับรองหรือจากวิธีอื่น

(ก) วิธีการที่ใช้ในการระบุตัวเจ้าของลายมือชื่อ

(ข) ข้อจำกัดเกี่ยวกับวัตถุประสงค์และคุณค่าที่มีการนำข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์หรือใบรับรอง

(ค) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์มีผลสมบูรณ์ใช้ได้และไม่สูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบหรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(ง) ข้อจำกัดเกี่ยวกับขอบเขตความรับผิดที่ผู้ให้บริการออกใบรับรองได้ระบุไว้

(จ) การมีวิธีการให้เจ้าของลายมือชื่อส่งคำบอกกล่าวเมื่อมีเหตุตามมาตรา ๒๗ (๒)

(ฉ) การมีบริการเกี่ยวกับการเพิกถอนใบรับรองที่ทันการ

(๕) ในกรณีที่มีบริการตาม (๔) (จ) บริการนั้นต้องมีวิธีการที่ให้เจ้าของลายมือชื่อสามารถแจ้งได้ตามหลักเกณฑ์ที่กำหนดตามมาตรา ๒๗ (๒) และในกรณีที่มีบริการตาม (๔) (ฉ) บริการนั้นต้องสามารถเพิกถอนใบรับรองได้ทันการ

(๖) ใช้ระบบ วิธีการ และบุคลากรที่เชื่อถือได้ในการให้บริการ

มาตรา ๒๙ ในการพิจารณาความเชื่อถือได้ของระบบ วิธีการ และบุคลากรตามมาตรา ๒๘ (๖) ให้คำนึงถึงกรณีดังต่อไปนี้

(๑) สถานภาพทางการเงิน บุคลากร และสินทรัพย์ที่มีอยู่

(๒) คุณภาพของระบบฮาร์ดแวร์และซอฟต์แวร์

(๓) วิธีการออกใบรับรอง การขอใบรับรอง และการเก็บรักษาข้อมูลการให้บริการนั้น

(๔) การจัดให้มีข้อมูลข่าวสารเกี่ยวกับเจ้าของลายมือชื่อ ที่ระบุในใบรับรองและผู้ที่อาจคาดหมายได้ว่าจะเป็นคู่กรณีที่เกี่ยวข้อง

(๕) ความสม่ำเสมอและขอบเขตในการตรวจสอบโดยผู้ตรวจสอบอิสระ

(๖) องค์กรที่ให้การรับรองหรือให้บริการออกใบรับรองเกี่ยวกับการปฏิบัติหรือการมีอยู่ของสิ่งที่กล่าวมาใน (๑) ถึง (๕)

(๗) กรณีใด ๆ ที่คณะกรรมการประกาศกำหนด

มาตรา ๓๐ คู่กรณีที่เกี่ยวข้องต้องดำเนินการ ดังต่อไปนี้

(๑) ดำเนินการตามสมควรในการตรวจสอบความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์

(๒) ในกรณีลายมือชื่ออิเล็กทรอนิกส์มีใบรับรอง ต้องมีการดำเนินการตามสมควร ดังนี้

(ก) ตรวจสอบความสมบูรณ์ของใบรับรอง การพักใช้ หรือการเพิกถอนใบรับรอง และ

(ข) ปฏิบัติตามข้อจำกัดใด ๆ ที่เกี่ยวกับใบรับรอง

มาตรา ๓๑ ใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ให้ถือว่ามีผลทางกฎหมายโดยไม่ต้องคำนึงถึง

(๑) สถานที่ออกใบรับรองหรือสถานที่สร้างหรือใช้ลายมือชื่ออิเล็กทรอนิกส์ หรือ

(๒) สถานที่ทำการงานของผู้ออกใบรับรองหรือเจ้าของลายมือชื่ออิเล็กทรอนิกส์

ใบรับรองที่ออกในต่างประเทศให้มีผลตามกฎหมายในประเทศเช่นเดียวกับใบรับรองที่ออกในประเทศ หากการออกใบรับรองดังกล่าวได้ใช้ระบบที่เชื่อถือได้ไม่น้อยกว่าระบบที่เชื่อถือได้ตามพระราชบัญญัตินี้

ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างหรือใช้ในต่างประเทศให้ถือว่ามีผลตามกฎหมายในประเทศเช่นเดียวกับลายมือชื่ออิเล็กทรอนิกส์ที่สร้างหรือใช้ในประเทศ หากการสร้างหรือใช้ลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวได้ใช้ระบบที่เชื่อถือได้ไม่น้อยกว่าระบบที่เชื่อถือได้ตามพระราชบัญญัตินี้

ในการพิจารณาว่าใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ใดมีความเชื่อถือได้ตามวรรคสองหรือวรรคสาม ให้คำนึงถึงมาตรฐานระหว่างประเทศและปัจจัยอื่น ๆ ที่เกี่ยวข้องประกอบด้วย

หมวด ๓
ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

มาตรา ๓๒ บุคคลย่อมมีสิทธิประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ แต่ในกรณีที่จำเป็นเพื่อรักษาความมั่นคงทางการเงินและการพาณิชย์ หรือเพื่อประโยชน์ในการเสริมสร้างความเชื่อถือและยอมรับในระบบข้อมูลอิเล็กทรอนิกส์ หรือเพื่อป้องกันความเสียหายต่อสาธารณชนให้มีการตราพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ใดเป็นกิจการที่ต้องแจ้งให้ทราบต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาตก่อนก็ได้

ในการกำหนดให้กรณีใดต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาตตามวรรคหนึ่ง ให้กำหนดโดยพิจารณาจากความเหมาะสมในการป้องกันความเสียหายตามระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นจากการประกอบธุรกิจนั้น

ในการนี้ จะกำหนดให้หน่วยงานของรัฐแห่งหนึ่งแห่งใดเป็นผู้รับผิดชอบในการควบคุมดูแลในพระราชกฤษฎีกาดังกล่าวก็ได้

ก่อนเสนอให้ตราพระราชกฤษฎีกาตามวรรคหนึ่ง ต้องจัดให้มีการรับฟังความคิดเห็นของประชาชนตามความเหมาะสม และนำข้อมูลที่ได้รับมาประกอบการพิจารณา

มาตรา ๓๓ ในกรณีที่มีพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ใดเป็นกิจการที่ต้องแจ้งให้ทราบ หรือต้องขึ้นทะเบียน ให้ผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวต้องแจ้งหรือขึ้นทะเบียนต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาก่อนเริ่มประกอบธุรกิจนั้น

หลักเกณฑ์และวิธีการแจ้งหรือขึ้นทะเบียนตามวรรคหนึ่ง ให้เป็นไปตามที่กำหนดในพระราชกฤษฎีกา และเมื่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาได้รับแจ้งหรือรับขึ้นทะเบียนให้ออกใบรับแจ้งหรือใบรับขึ้นทะเบียนเพื่อเป็นหลักฐานการแจ้งหรือการขึ้นทะเบียนในวันที่ได้รับแจ้งหรือรับขึ้นทะเบียน และให้ผู้แจ้งหรือผู้ขึ้นทะเบียนประกอบธุรกิจนั้นได้ตั้งแต่วันที่ได้รับแจ้งหรือรับขึ้นทะเบียน แต่ถ้าพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาตรวจพบในภายหลังว่าการแจ้งหรือขึ้นทะเบียนไม่ถูกต้องหรือไม่ครบถ้วน ให้มีอำนาจสั่งผู้แจ้งหรือผู้ขึ้นทะเบียนแก้ไขให้ถูกต้องหรือครบถ้วนภายในเจ็ดวันนับแต่วันที่ได้รับคำสั่งดังกล่าว

ในการประกอบธุรกิจ ผู้แจ้งหรือผู้ขึ้นทะเบียนตามวรรคหนึ่งต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในพระราชกฤษฎีกาและตามที่คณะกรรมการประกาศกำหนด

ถ้าผู้แจ้งหรือผู้ขึ้นทะเบียนตามวรรคหนึ่งไม่แก้ไขการแจ้งหรือขึ้นทะเบียนให้ถูกต้องหรือครบถ้วนตามวรรคสอง หรือฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์การประกอบธุรกิจตามวรรคสาม ให้คณะกรรมการพิจารณามีคำสั่งลงโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท โดยคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด และในกรณีที่เห็นสมควรคณะกรรมการอาจมีคำสั่งให้ผู้นั้นดำเนินการใด ๆ เพื่อแก้ไขให้ถูกต้องหรือเหมาะสมได้

หลักเกณฑ์ในการพิจารณาลงโทษปรับทางปกครองให้เป็นไปตามที่คณะกรรมการกำหนดและถ้าผู้ถูกลงโทษปรับทางปกครองไม่ยอมชำระค่าปรับทางปกครอง ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม และในกรณีไม่มีเจ้าหน้าที่ดำเนินการบังคับตามคำสั่ง ให้คณะกรรมการมีอำนาจฟ้องคดีต่อศาลปกครองเพื่อบังคับชำระค่าปรับ ในการนี้ ถ้าศาลปกครองเห็นว่าคำสั่งให้ชำระค่าปรับนั้นชอบด้วยกฎหมายก็ให้ศาลปกครองมีอำนาจพิจารณาพิพากษาและบังคับให้มีการยึดหรืออายัดทรัพย์สินขายทอดตลาดเพื่อชำระค่าปรับได้

ในกรณีผู้กระทำผิดตามวรรคสี่ไม่ดำเนินการแก้ไขตามคำสั่งของคณะกรรมการหรือกระทำความผิดซ้ำอีก ให้คณะกรรมการมีอำนาจออกคำสั่งห้ามมิให้ผู้นั้นประกอบธุรกิจตามที่ได้แจ้งหรือขึ้นทะเบียนอีกต่อไป

มาตรา ๓๔ ในกรณีที่มีพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์กรณีใดเป็นกิจการที่ต้องได้รับใบอนุญาต ให้ผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวยื่นคำขอรับใบอนุญาตต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกา

คุณสมบัติของผู้ขอรับใบอนุญาต หลักเกณฑ์และวิธีการขออนุญาต การออกใบอนุญาต การต่ออายุใบอนุญาต การคืนใบอนุญาต และการสั่งพักใช้หรือเพิกถอนใบอนุญาต ให้เป็นไปตามหลักเกณฑ์ที่กำหนดในพระราชกฤษฎีกา

ในการประกอบธุรกิจ ผู้ได้รับใบอนุญาตตามวรรคหนึ่ง ต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในพระราชกฤษฎีกา ประกาศที่คณะกรรมการกำหนดหรือเงื่อนไขในใบอนุญาต

ในกรณีที่ผู้ได้รับใบอนุญาตฝ่าฝืนหรือปฏิบัติไม่ถูกต้องตามหลักเกณฑ์การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ตามวรรคสาม ให้คณะกรรมการพิจารณามีคำสั่งลงโทษปรับทางปกครองไม่เกินสองล้านบาท โดยคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด และในกรณีที่เห็นสมควรคณะกรรมการอาจมีคำสั่งให้ผู้นั้นดำเนินการใด ๆ เพื่อแก้ไขให้ถูกต้องหรือเหมาะสมได้ ทั้งนี้ ให้นำความในมาตรา ๓๓ วรรคห้า มาใช้บังคับโดยอนุโลม

ถ้าผู้กระทำความผิดตามวรรคสี่ไม่ดำเนินการแก้ไขตามคำสั่งของคณะกรรมการหรือกระทำความผิดซ้ำอีก ให้คณะกรรมการมีอำนาจออกคำสั่งเพิกถอนใบอนุญาต

หมวด ๔
ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

มาตรา ๓๕ คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศหรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกาให้นำพระราชบัญญัตินี้มาใช้บังคับและให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด ทั้งนี้ ในพระราชกฤษฎีกาอาจกำหนดให้บุคคลที่เกี่ยวข้องต้องกระทำหรืองดเว้นกระทำการใด ๆ หรือให้หน่วยงานของรัฐออกระเบียบเพื่อกำหนดรายละเอียดในบางกรณีด้วยก็ได้

ในการออกพระราชกฤษฎีกาตามวรรคหนึ่ง พระราชกฤษฎีกาดังกล่าวอาจกำหนดให้ผู้ประกอบธุรกิจบริการเกี่ยวกับธุรกิจทางอิเล็กทรอนิกส์ต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาต แล้วแต่กรณี ก่อนประกอบกิจการก็ได้ ในกรณีนี้ ให้นำบทบัญญัติในหมวด ๓ และบทกำหนดโทษที่เกี่ยวข้องมาใช้บังคับโดยอนุโลม

หมวด ๕
คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

มาตรา ๓๖ ให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วยรัฐมนตรีว่าการกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อมเป็นประธานกรรมการ และกรรมการซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้ทรงคุณวุฒิ ที่ได้รับการสรรหาอีกจำนวนสิบสองคน โดยในจำนวนนี้เป็นผู้ทรงคุณวุฒิในด้านดังต่อไปนี้ด้านละสองคน

(๑) การเงิน

(๒) การพาณิชย์อิเล็กทรอนิกส์

(๓) นิติศาสตร์

(๔) วิทยาการคอมพิวเตอร์

(๕) วิทยาศาสตร์หรือวิศวกรรมศาสตร์

(๖) สังคมศาสตร์

ทั้งนี้ ผู้ทรงคุณวุฒิคนหนึ่งของแต่ละด้านต้องมาจากภาคเอกชน และให้ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติเป็นกรรมการและเลขานุการ

หลักเกณฑ์และวิธีการสรรหาและการเสนอชื่อบุคคลที่เห็นสมควรต่อคณะรัฐมนตรีเพื่อพิจารณาแต่งตั้งเป็นคณะกรรมการตามวรรคหนึ่ง ให้เป็นไปตามระเบียบที่รัฐมนตรีประกาศกำหนด

ให้เลขานุการแต่งตั้งผู้ช่วยเลขานุการอีกไม่เกินสองคน

มาตรา ๓๗ ให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ มีอำนาจหน้าที่ดังต่อไปนี้

(๑) เสนอแนะต่อคณะรัฐมนตรีเพื่อวางนโยบายการส่งเสริมและพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ตลอดจนการแก้ไขปัญหาและอุปสรรคที่เกี่ยวข้อง

(๒) ติดตามดูแลการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

(๓) เสนอแนะหรือให้คำปรึกษาต่อรัฐมนตรีเพื่อการตราพระราชกฤษฎีกาตามพระราชบัญญัตินี้

(๔) ออกระเบียบหรือประกาศเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์เพื่อให้เป็นไปตามพระราชบัญญัตินี้ หรือตามพระราชกฤษฎีกาที่ออกตามพระราชบัญญัตินี้

(๕) ปฏิบัติการอื่นใดเพื่อให้เป็นไปตามพระราชบัญญัตินี้ หรือกฎหมายอื่น

ในการปฏิบัติการตามพระราชบัญญัตินี้ให้คณะกรรมการเป็นเจ้าพนักงานตามประมวลกฎหมายอาญา

มาตรา ๓๘ กรรมการผู้ทรงคุณวุฒิมีวาระการดำรงตำแหน่งสามปี

กรรมการซึ่งพ้นจากตำแหน่งอาจได้รับแต่งตั้งอีกได้ แต่ไม่เกินสองวาระติดต่อกัน

มาตรา ๓๙ นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา ๓๘ กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่ง เมื่อ

(๑) ตาย

(๒) ลาออก

(๓) คณะรัฐมนตรีให้ออกเพราะมีความประพฤติเสื่อมเสีย บกพร่อง หรือไม่สุจริตต่อหน้าที่ หรือหย่อนความสามารถ

(๔) เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๕) ได้รับโทษจำคุกโดยต้องคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

มาตรา ๔๐ ในกรณีที่กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งตามมาตรา ๓๙ ให้ถือว่าคณะกรรมการประกอบด้วยกรรมการเท่าที่เหลืออยู่และให้ดำเนินการแต่งตั้งกรรมการใหม่แทนภายในหกสิบวันนับแต่วันที่กรรมการพ้นจากตำแหน่ง

ให้กรรมการซึ่งได้รับแต่งตั้งแทนอยู่ในตำแหน่งเท่ากับวาระที่เหลืออยู่ของผู้ซึ่งตนแทน

มาตรา ๔๑ การประชุมของคณะกรรมการต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการทั้งหมดจึงเป็นองค์ประชุม

ถ้าประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้คณะกรรมการเลือกกรรมการคนหนึ่งทำหน้าที่ประธานในที่ประชุม

การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากันให้ประธานออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

มาตรา ๔๒ คณะกรรมการมีอำนาจแต่งตั้งคณะอนุกรรมการเพื่อพิจารณาหรือปฏิบัติการอย่างหนึ่งอย่างใดแทนคณะกรรมการก็ได้

ให้นำความในมาตรา ๔๑ มาใช้บังคับแก่การประชุมของคณะอนุกรรมการโดยอนุโลม

มาตรา ๔๓ ให้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ทำหน้าที่เป็นหน่วยงานธุรการของคณะกรรมการ

หมวด ๖
บทกำหนดโทษ

มาตรา ๔๔ ผู้ใดประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่แจ้งหรือขึ้นทะเบียนต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาตามมาตรา ๓๓ วรรคหนึ่ง หรือโดยฝ่าฝืนคำสั่งห้ามการประกอบธุรกิจของคณะกรรมการตามมาตรา ๓๓ วรรคหก ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๔๕ ผู้ใดประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่ได้รับใบอนุญาตตามมาตรา ๓๔ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสองแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๔๖ บรรดาความผิดตามพระราชบัญญัตินี้ที่กระทำโดยนิติบุคคล ผู้จัดการหรือผู้แทนนิติบุคคลหรือผู้ซึ่งมีส่วนร่วมในการดำเนินงานของนิติบุคคลต้องรับผิดในความผิดนั้นด้วย เว้นแต่พิสูจน์ได้ว่าตนมิได้รู้เห็นหรือมีส่วนร่วมในการกระทำความผิดนั้น

ผู้รับสนองพระบรมราชโองการ
พันตำรวจโท ทักษิณ ชินวัตร
นายกรัฐมนตรี

<u>หมายเหตุ</u> :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่การทำธุรกรรมในปัจจุบันมีแนวโน้มที่จะปรับเปลี่ยนวิธีการในการติดต่อสื่อสารที่อาศัยการพัฒนาการเทคโนโลยีทางอิเล็กทรอนิกส์ซึ่งมีความสะดวก รวดเร็ว และมีประสิทธิภาพ แต่เนื่องจากการทำธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวมีความแตกต่างจากวิธีการทำธุรกรรมซึ่งมีกฎหมายรองรับอยู่ในปัจจุบันเป็นอย่างมาก อันส่งผลให้ต้องมีการรองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมอกับการทำเป็นหนังสือ หรือหลักฐานเป็นหนังสือ การรับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์ ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือ และมีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิม ควรกำหนดให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ทำหน้าที่วางนโยบายกำหนดหลักเกณฑ์เพื่อส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ ติดตามดูแลการประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งมีหน้าที่ในการส่งเสริมการพัฒนาการทางเทคโนโลยีเพื่อติดตามความก้าวหน้าของเทคโนโลยี ซึ่งมีการเปลี่ยนแปลงและพัฒนาศักยภาพตลอดเวลาให้มีมาตรฐานน่าเชื่อถือ ตลอดจนเสนอแนะแนวทางแก้ไขปัญหาและอุปสรรคที่เกี่ยวข้อง อันจะเป็นการส่งเสริมการใช้ธุรกรรมทางอิเล็กทรอนิกส์

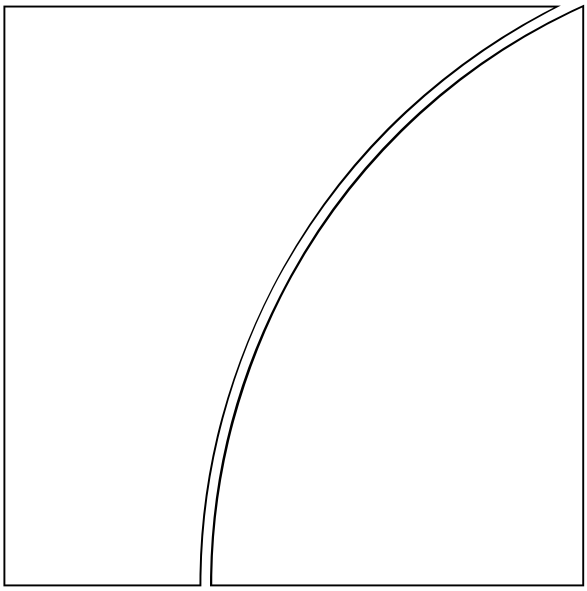
ทั้งภายในประเทศและระหว่างประเทศ ด้วยการมีกฎหมายรองรับในลักษณะที่เป็นเอกรูป และสอดคล้องกับมาตรฐานที่นานาประเทศยอมรับ จึงจำเป็นต้องตราพระราชบัญญัตินี้

เอกสารแนบ 8

Risk Management Principles for Electronic Banking

โดย Bank for International Settlements (BIS)

Basel Committee
on Banking Supervision



Risk Management Principles for Electronic Banking

July 2003

BANK FOR INTERNATIONAL SETTLEMENTS

Table of Contents

Executive Summary 1

I. Introduction 4

A. Risk Management Challenges 5

B. Risk Management Principles 6

II. Risk Management Principles for Electronic Banking 7

A. Board and Management Oversight (Principles 1 to 3) 8

B. Security Controls (Principles 4 to 10) 12

C. Legal and Reputational Risk Management (Principles 11 to 14) 18

Appendix I: Sound Security Control Practices for E-Banking 22

Appendix II: Sound Practices for Managing Outsourced E-Banking Systems and Services 23

Appendix III: Sound Authorisation Practices for E-Banking Applications 26

Appendix IV: Sound Audit Trail Practices for E-Banking Systems 27

Appendix V: Sound Practices to Help Maintain the Privacy of Customer E-Banking Information 28

Appendix VI: Sound Capacity, Business Continuity and Contingency Planning Practices for E-Banking 29

Electronic Banking Group of the Basel Committee on Banking Supervision

Chairman:

Mr John Hawke, Jr - Comptroller of the Currency, Washington DC

Members:

Australian Prudential Regulation Authority, Australia	Mr Graham Johnson
Commission Bancaire et Financière, Belgium	Mr Jos Meuleman Mr Koen Algoet
Office of the Superintendent of Financial Institutions, Canada	Ms Judy Cameron Mr Abilash Bhachech
Commission Bancaire, France	Mr Alain Duchâteau
Deutsche Bundesbank, Germany	Mr Sven Jongebloed
Bundesanstalt für Finanzdienstleistungsaufsicht, Germany	Mr Stefan Czekay
Hong Kong Monetary Authority, Hong Kong SAR	Mr Shu-Pui Li Mr Brian Lee
Banca d'Italia, Italy	Mr Filippo Siracusano Mr Tullio Pra
Bank of Japan, Japan	Mr Toshihiko Mori Mr Hiroaki Kuwahara Ms Tomoko Suzuki
Financial Services Agency, Japan	Mr Koji Hamada Ms Yoko Ota
Commission de Surveillance du Secteur Financier, Luxembourg	Mr David Hagen Mr Claude Bernard
De Nederlandsche Bank N.V., The Netherlands	Mr Erik Smid
Monetary Authority of Singapore, Singapore	Mr Leon Chang Mr Enoch Ch'ng Mr Tony Chew
Banco de España, Spain	Ms Maria Jesús Nieto
Finansinspektionen, Sweden	Ms Christina Westerling
Federal Banking Commission, Switzerland	Mr Daniel Schmid
Financial Services Authority, United Kingdom	Mr Peter MacCormack
Federal Reserve Bank of New York, United States	Mr George Juncker Ms Barbara Yelcich
Office of the Comptroller of the Currency (OCC), United States	Mr Hugh Kelly Mr Clifford Wilke
Board of Governors of the Federal Reserve System, United States	Ms Angela Desmond Mr Jeff Marquardt
Federal Deposit Insurance Corporation, United States	Ms Sandra Thomson

European Central Bank — Mr Christian Fehlker

Secretariat, Basel Committee on Banking Supervision, Bank for International Settlements — Mr Laurent Le Mouël

Risk Management Principles for Electronic Banking

Executive Summary

Continuing technological innovation and competition among existing banking organisations and new entrants have allowed for a much wider array of banking products and services to become accessible and delivered to retail and wholesale customers through an electronic distribution channel collectively referred to as e-banking. However, the rapid development of e-banking capabilities carries risks as well as benefits.

The Basel Committee on Banking Supervision expects such risks to be recognised, addressed and managed by banking institutions in a prudent manner according to the fundamental characteristics and challenges of e-banking services. These characteristics include the unprecedented speed of change related to technological and customer service innovation, the ubiquitous and global nature of open electronic networks, the integration of e-banking applications with legacy computer systems and the increasing dependence of banks on third parties that provide the necessary information technology. While not creating inherently new risks, the Committee noted that these characteristics increased and modified some of the traditional risks associated with banking activities, in particular strategic, operational, legal and reputational risks, thereby influencing the overall risk profile of banking.

Based on these conclusions, the Committee considers that while existing risk management principles remain applicable to e-banking activities, such principles must be tailored, adapted and, in some cases, expanded to address the specific risk management challenges created by the characteristics of e-banking activities. To this end, the Committee believes that it is incumbent upon the Boards of Directors and banks' senior management to take steps to ensure that their institutions have reviewed and modified where necessary their existing risk management policies and processes to cover their current or planned e-banking activities. The Committee also believes that the integration of e-banking applications with legacy systems implies an integrated risk management approach for all banking activities of a banking institution.

To facilitate these developments, the Committee has identified fourteen *Risk Management Principles for Electronic Banking* to help banking institutions expand their existing risk oversight policies and processes to cover their e-banking activities.

These *Risk Management Principles* are not put forth as absolute requirements or even "best practice." The Committee believes that setting detailed risk management requirements in the area of e-banking might be counter-productive, if only because these would be likely to become rapidly outdated because of the speed of change related to technological and customer service innovation. The Committee has therefore preferred to express supervisory expectations and guidance in the form of *Risk Management Principles* in order to promote safety and soundness for e-banking activities, while preserving the necessary flexibility in implementation that derives in part from the speed of change in this area. Further, the Committee recognises that each bank's risk profile is different and requires a tailored risk mitigation approach appropriate for the scale of the e-banking operations, the materiality of the risks present, and the willingness and ability of the institution to manage these risks. This implies that a "one size fits all" approach to e-banking risk management issues may not be appropriate.

For a similar reason, the *Risk Management Principles* issued by the Committee do not attempt to set specific technical solutions or standards relating to e-banking. Technical

solutions are to be addressed by institutions and standard setting bodies as technology evolves. However, this Report contains appendices that list some examples current and widespread risk mitigation practices in the e-banking area that are supportive of the *Risk Management Principles*.

Consequently, the *Risk Management Principles* and sound practices identified in this Report are expected to be used as tools by national supervisors and implemented with adaptations to reflect specific national requirements and individual risk profiles where necessary. In some areas, the Principles have been expressed by the Committee or by national supervisors in previous bank supervisory guidance. However, some issues, such as the management of outsourcing relationships, security controls and legal and reputational risk management, warrant more detailed principles than those expressed to date due to the unique characteristics and implications of the Internet distribution channel.

The *Risk Management Principles* fall into three broad, and often overlapping, categories of issues that are grouped to provide clarity: *Board and Management Oversight; Security Controls; and Legal and Reputational Risk Management*.

Board and Management Oversight

Because the Board of Directors and senior management are responsible for developing the institution's business strategy and establishing an effective management oversight over risks, they are expected to take an explicit, informed and documented strategic decision as to whether and how the bank is to provide e-banking services. The initial decision should include the specific accountabilities, policies and controls to address risks, including those arising in a cross-border context. Effective management oversight is expected to encompass the review and approval of the key aspects of the bank's security control process, such as the development and maintenance of a security control infrastructure that properly safeguards e-banking systems and data from both internal and external threats. It also should include a comprehensive process for managing risks associated with increased complexity of and increasing reliance on outsourcing relationships and third-party dependencies to perform critical e-banking functions.

Security Controls

While the Board of Directors has the responsibility for ensuring that appropriate security control processes are in place for e-banking, the substance of these processes needs special management attention because of the enhanced security challenges posed by e-banking. This should include establishing appropriate authorisation privileges and authentication measures, logical and physical access controls, adequate infrastructure security to maintain appropriate boundaries and restrictions on both internal and external user activities and data integrity of transactions, records and information. In addition, the existence of clear audit trails for all e-banking transactions should be ensured and measures to preserve confidentiality of key e-banking information should be appropriate with the sensitivity of such information.

Although customer protection and privacy regulations vary from jurisdiction to jurisdiction, banks generally have a clear responsibility to provide their customers with a level of comfort regarding information disclosures, protection of customer data and business availability that approaches the level they can expect when using traditional banking distribution channels.

To minimise legal and reputational risk associated with e-banking activities conducted both domestically and cross-border, banks should make adequate disclosure of information on their web sites and take appropriate measures to ensure adherence to customer privacy requirements applicable in the jurisdictions to which the bank is providing e-banking services.

Legal and Reputational Risk Management

To protect banks against business, legal and reputation risk, e-banking services must be delivered on a consistent and timely basis in accordance with high customer expectations for constant and rapid availability and potentially high transaction demand. The bank must have the ability to deliver e-banking services to all end-users and be able to maintain such availability in all circumstances. Effective incident response mechanisms are also critical to minimise operational, legal and reputational risks arising from unexpected events, including internal and external attacks, that may affect the provision of e-banking systems and services. To meet customers' expectations, banks should therefore have effective capacity, business continuity and contingency planning. Banks should also develop appropriate incident response plans, including communication strategies, that ensure business continuity, control reputation risk and limit liability associated with disruptions in their e-banking services.

Risk Management Principles for Electronic Banking

I. Introduction

Banking organisations have been delivering electronic services to consumers and businesses remotely for years. Electronic funds transfer, including small payments and corporate cash management systems, as well as publicly accessible automated machines for currency withdrawal and retail account management, are global fixtures. However, the increased world-wide acceptance of the Internet[1] as a delivery channel for banking products and services provides new business opportunities for banks as well as service benefits for their customers.

Continuing technological innovation and competition among existing banking organisations and new market entrants has allowed for a much wider array of electronic banking[2] products and services for retail and wholesale banking customers. These include traditional activities such as accessing financial information, obtaining loans and opening deposit accounts, as well as relatively new products and services such as electronic bill payment services, personalised financial "portals," account aggregation[3] and business-to-business market places and exchanges.

Notwithstanding the significant benefits of technological innovation, the rapid development of e-banking capabilities carries risks as well as benefits and it is important that these risks are recognised and managed by banking institutions in a prudent manner.[4] These developments led the Basel Committee on Banking Supervision to conduct a preliminary study of the risk management implications of e-banking and e-money in 1998.[5] This early study demonstrated a clear need for more work in the area of e-banking risk management and that mission was entrusted to a working group comprised of bank supervisors and central banks, the Electronic Banking Group (EBG), which was formed in November 1999.

---

1 For the purposes of this Report, the Internet is defined to include all related web enabling technologies and open telecommunications networks ranging from direct dial-up connections, the public World Wide Web, and virtual private networks.

2 For the purpose of this Report, electronic banking, or ***e-banking***, includes the provision of retail and small value banking products and services through electronic channels as well as large value electronic payments and other wholesale banking services delivered electronically.

3 Account aggregation services allow customers to obtain consolidated information about their financial and non-financial accounts in one place. An aggregator essentially acts as agent for customers to provide consolidated information on customers' accounts across several financial institutions. Customers provide the aggregator with the necessary security password or personal identification number to access and consolidate account information primarily through screen scraping, a process that involves culling data from the other institutions' websites, often without their knowledge, or through contractually arranged direct data feeds between financial institutions.

4 Because of rapid changes in information technology, no description of such of risks can be exhaustive. However, the risks facing banks engaged in e-banking are generally not new and they are encompassed by risk categories identified in the Basel Committee's *Core Principles for Effective Banking Supervision*, September 1997. That guidance identified eight risk categories including credit risk, country and transfer risk, market risk, interest rate risk, liquidity risk, operational risk, legal risk and reputational risk. The *Core Principles* are available on the BIS website at http://www.bis.org.

5 *"Risk Management for Electronic Banking and Electronic Money Activities*", March 1998, available on the Bank for International Settlements' website at http://www.bis.org.

The Basel Committee released the EBG's Report on risk management and supervisory issues arising from e-banking developments in October 2000.[6] This Report inventoried and assessed the major risks associated with e-banking, namely strategic risk, reputational risk, operational risk (including security and legal risks),[7] and credit, market, and liquidity risks. The EBG concluded that e-banking activities did not raise risks that were not already identified by the previous work of the Basel Committee. However, it noted that e-banking increase and modifies some of these traditional risks, thereby influencing the overall risk profile of banking. In particular, strategic risk, operational risk, and reputational risk are certainly heightened by the rapid introduction and underlying technological complexity of e-banking activities.

A. Risk management challenges

The EBG noted that the fundamental characteristics of e-banking (and e-commerce more generally) posed a number of risk management challenges:

- The speed of change relating to technological and customer service innovation in e-banking is unprecedented. Historically, new banking applications were implemented over relatively long periods of time and only after in-depth testing. Today, however, banks are experiencing competitive pressure to roll out new business applications in very compressed time frames – often only a few months from concept to production. This competition intensifies the management challenge to ensure that adequate strategic assessment, risk analysis and security reviews are conducted prior to implementing new e-banking applications.

- Transactional e-banking web sites and associated retail and wholesale business applications are typically integrated as much as possible with legacy computer systems to allow more straight-through processing of electronic transactions. Such straight-through automated processing reduces opportunities for human error and fraud inherent in manual processes, but it also increases dependence on sound systems design and architecture as well as system interoperability and operational scalability.

- E-banking increases banks' dependence on information technology, thereby increasing the technical complexity of many operational and security issues and furthering a trend towards more partnerships, alliances and outsourcing arrangements with third parties, many of whom are unregulated. This development has been leading to the creation of new business models involving banks and non-bank entities, such as Internet service providers, telecommunication companies and other technology firms.

- The Internet is ubiquitous and global by nature. It is an open network accessible from anywhere in the world by unknown parties, with routing of messages through unknown locations and via fast evolving wireless devices. Therefore, it significantly

---

[6] *"Electronic Banking Group Initiatives and White Papers"*, October 2000, available on the BIS website at http://www.bis.org.

[7] This Report uses the Basel Committee's definition of operational risk, which includes security risk and legal risk (see Basel Committee on Banking Supervision, *The New Basel Capital Accord*, April 2003, paragraph 607: "risk of loss resulting from inadequate or failed internal processes, people and systems or from external events").

magnifies the importance of security controls, customer authentication techniques, data protection, audit trail procedures, and customer privacy standards.

B. Risk management principles

Based on the early work of the EBG, the Committee concluded that, while traditional banking risk management principles are applicable to e-banking activities, the complex characteristics of the Internet delivery channel dictate that the application of these principles must be tailored to fit many online banking activities and their attendant risk management challenges. To this end, the Committee believes that it is incumbent upon the Boards of Directors and banks' senior management to take steps to ensure that their institutions have reviewed and modified where necessary their existing risk management policies and processes to cover their current or planned e-banking activities. Further, as the Committee believes that banks should adopt an integrated risk management approach for all banking activities, it is critical that the risk management oversight afforded e-banking activities becomes an integral part of the banking institution's overall risk management framework.

To facilitate these developments, the Committee asked the EBG to identify the key risk management principles that would help banking institutions expand their existing risk oversight policies and processes to cover their e-banking activities and, in turn, promote the safe and sound electronic delivery of banking products and services.

These *Risk Management Principles for Electronic Banking*, which are identified in this Report, are not put forth as absolute requirements or even "best practice" but rather as guidance to promote safe and sound e-banking activities. The Committee believes that setting detailed risk management requirements in the area of e-banking might be counter-productive, if only because these would be likely to become rapidly outdated by the speed of change related to technological and product innovation. Therefore the principles included in the present Report express supervisory expectations related to the overall objective of banking supervision to ensure safety and soundness in the financial system rather than stringent regulations.

The Committee is of the view that such supervisory expectations should be tailored and adapted to the e-banking distribution channel but not be fundamentally different to those applied to banking activities delivered through other distribution channels. Consequently, the principles presented below are largely derived and adapted from supervisory principles that have already been expressed by the Committee or national supervisors over a number of years. In some areas, such as the management of outsourcing relationships, security controls and legal and reputational risk management, the characteristics and implications of the Internet distribution channel introduce a need for more detailed principles than those expressed to date.

The Committee recognises that banks will need to develop risk management processes appropriate for their individual risk profile, operational structure and corporate governance culture, as well as in conformance with the specific risk management requirements and policies set forth by the bank supervisors in their particular jurisdiction(s). Further, the numerous e-banking risk management practices identified in this Report, while representative of current industry sound practice, should not be considered to be all-inclusive or definitive, since many security controls and other risk management techniques continue to evolve rapidly to keep pace with new technologies and business applications.

This Report does not attempt to dictate specific technical solutions to address particular risks or set technical standards relating to e-banking. Technical issues will need to be addressed on an on-going basis by both banking institutions and various standards-setting bodies as

technology evolves. Further, as the industry continues to address e-banking technical issues, including security challenges, a variety of innovative and cost efficient risk management solutions are likely to emerge. These solutions are also likely to address issues related to the fact that banks differ in size, complexity and risk management culture and that jurisdictions differ in their legal and regulatory frameworks.

For these reasons, the Committee does not believe that a "one size fits all" approach to e-banking risk management is appropriate, and it encourages the exchange of good practices and standards to address the additional risk dimensions posed by the e-banking delivery channel. In keeping with this supervisory philosophy, the risk management principles and sound practices identified in this Report are expected to be used as tools by national supervisors and implemented with adaptations to reflect specific national requirements where necessary, to help promote safe and secure e-banking activities and operations.

The Committee recognises that each bank's risk profile is different and requires a risk mitigation approach appropriate for the scale of the e-banking operations, the materiality of the risks present, and the willingness and ability of the institution to manage these risks. These differences imply that the risk management principles presented in this Report are intended to be flexible enough to be implemented by all relevant institutions across jurisdictions. National supervisors will assess the materiality of the risks related to e-banking activities present at a given bank and whether, and to what extent, the risk management principles for e-banking have been adequately met by the bank's risk management framework.

II. Risk Management Principles for Electronic Banking

The e-banking risk management principles identified in this Report fall into three broad, and often overlapping, categories of issues. However, these principles are not weighted by order of preference or importance. If only because such weighting might change over time, it is preferable to remain neutral and avoid such prioritisation.

A. Board and Management Oversight[8] (Principles 1 to 3):

1. Effective management oversight of e-banking activities.

2. Establishment of a comprehensive security control process.

3. Comprehensive due diligence and management oversight process for outsourcing relationships and other third-party dependencies.

---

[8] This Report refers to a management structure composed of a board of directors and senior management. The Committee is aware that there are significant differences in legislative and regulatory frameworks across countries as regards the functions of the board of directors and senior management. In some countries, the board has the main, if not exclusive, function of supervising the executive body (senior management, general management) so as to ensure that the latter fulfils its duties. For this reason it is sometimes known as the supervisory board. In such cases, the board has no executive powers. By contrast, in other countries, the board has a broader competence including the definition of the bank's general management framework. Because of these differences, the terms "board of directors" and "senior management" are used in the report to identify two decision-making functions within a bank but not to identify legal constructs.

B. Security Controls (Principles 4 to 10):

4. Authentication of e-banking customers.

5. Non-repudiation and accountability for e-banking transactions.

6. Appropriate measures to ensure segregation of duties.

7. Proper authorisation controls within e-banking systems, databases and applications.

8. Data integrity of e-banking transactions, records, and information.

9. Establishment of clear audit trails for e-banking transactions.

10. Confidentiality of key bank information.

C. Legal and Reputational Risk Management (Principles 11 to 14):

11. Appropriate disclosures for e-banking services.

12. Privacy of customer information.

13. Capacity, business continuity and contingency planning to ensure availability of e-banking systems and services.

14. Incident response planning.

Each of the above issues is discussed more specifically in the following sections, as they relate to e-banking and the underlying risk management principles that should be considered by banks to address these issues. Where appropriate, sound practices that may be considered as effective ways to address these risks are also offered in a referenced appendix.

A. Board and Management Oversight (Principles 1 to 3)

The Board of Directors and senior management are responsible for developing the banking institution’s business strategy. An explicit strategic decision should be made as to whether the Board wishes the bank to provide e-banking transactional services before beginning to offer such services. Specifically, the Board should ensure that e-banking plans are clearly integrated within corporate strategic goals, a risk analysis is performed of the proposed e-banking activities, appropriate risk mitigation and monitoring processes are established for identified risks, and ongoing reviews are conducted to evaluate the results of e-banking activities against the institution’s business plans and objectives.

In addition, the Board and senior management should ensure that the operational and security risk dimensions of the institution's e-banking business strategies are appropriately considered and addressed. The provision of financial services over the Internet may significantly modify and/or even increase traditional banking risks (e.g. strategic, reputational, operational, credit and liquidity risk). Steps should therefore be taken to ensure that the bank's existing risk management processes, security control processes, due diligence and oversight processes for outsourcing relationships are appropriately evaluated and modified to accommodate e-banking services.

Principle 1: The Board of Directors and senior management should establish effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks.

Vigilant management oversight is essential for the provision of effective internal controls over e-banking activities. In addition to the specific characteristics of the Internet distribution channel discussed in the Introduction, the following aspects of e-banking may pose considerable challenge to traditional risk management processes:

- Major elements of the delivery channel (the Internet and related technologies) are outside of the bank's direct control.

- The Internet facilitates delivery of services across multiple national jurisdictions, including those not currently served by the institution through physical locations.

- The complexity of issues that are associated with e-banking and that involve highly technical language and concepts are in many cases outside the traditional experience of the Board and senior management.

In light of the unique characteristics of e-banking, new e-banking projects that may have a significant impact on the bank's risk profile and strategy should be reviewed by the Board of Directors and senior management and undergo appropriate strategic and cost/reward analysis. Without adequate up-front strategic review and ongoing performance to plan assessments, banks are at risk of underestimating the cost and/or overestimating the payback of their e-banking initiatives.

In addition, the Board and senior management should ensure that the bank does not enter into new e-banking businesses or adopt new technologies unless it has the necessary expertise to provide competent risk management oversight. Management and staff expertise should be commensurate with the technical nature and complexity of the bank's e-banking applications and underlying technologies. Adequate expertise is essential regardless of whether the bank's e-banking systems and services are managed in-house or outsourced to third parties. Senior management oversight processes should operate on a dynamic basis in order to effectively intervene and correct any material e-banking systems problems or security breaches that may occur. The increased reputational risk associated with e-banking necessitates vigilant monitoring of systems operability and customer satisfaction as well as appropriate incident reporting to the Board and senior management.

Finally, the Board and senior management should ensure that its risk management processes for its e-banking activities are integrated into the bank's overall risk management approach. The bank's existing risk management policies and processes should be evaluated to ensure that they are robust enough to cover the new risks posed by current or planned e-banking activities. Additional risk management oversight steps that the Board and senior management should consider taking include:

- Clearly establishing the banking organisation's risk appetite in relation to e-banking.

- Establishing key delegations and reporting mechanisms, including the necessary escalation procedures for incidents that impact the bank's safety, soundness or

reputation (e.g. networks penetration, employee security infractions and any serious misuse of computer facilities).[9]

- Addressing any unique risk factors associated with ensuring the security, integrity and availability of e-banking products and services, and requiring that third parties to whom the banks has outsourced key systems or applications take similar measures.

- Ensuring that appropriate due diligence and risk analysis are performed before the bank conducts cross-border e-banking activities.

The Internet greatly facilitates a bank's ability to distribute products and services over virtually unlimited geographic territory, including across national borders. Such cross-border e-banking activity, particularly if conducted without any existing licensed physical presence in the "host country," potentially subjects banks to increased legal, regulatory and country risk due to the substantial differences that may exist between jurisdictions with respect to bank licensing, supervision and customer protection requirements. Because of the need to avoid inadvertent non-compliance with a foreign country's laws or regulations, as well as to manage relevant country risk factors, banks contemplating cross-border e-banking operations need to fully explore these risks before undertaking such operations and effectively manage them.[10]

Depending on the scope and complexity of e-banking activities, the scope and structure of risk management programs will vary across banking organisations. Resources required to oversee e-banking services should be commensurate with the transactional functionality and criticality of systems, the vulnerability of networks and the sensitivity of information being transmitted.

Principle 2: The Board of Directors and senior management should review and approve the key aspects of the bank's security control process.

The Board of Directors and senior management should oversee the development and continued maintenance of a security control infrastructure that properly safeguards e-banking systems and data from both internal and external threats. This should include establishing appropriate authorisation privileges, logical and physical access controls, and adequate infrastructure security to maintain appropriate boundaries and restrictions on both internal and external user activities.

Safeguarding of bank assets is one of the Board's fiduciary duties and one of senior management's fundamental responsibilities. However, it is a challenging task in a rapidly evolving e-banking environment because of the complex security risks associated with operating over the public Internet network and using innovative technology.

To ensure proper security controls for e-banking activities, the Board and senior management need to ascertain whether the bank has a comprehensive security process, including policies and procedures, that addresses potential internal and external security

---

[9] In addition to internal reporting requirements, incident reporting escalation procedures should also set forth the necessary reporting to appropriate supervisory authorities.

[10] For further developments, see Basel Committee on Banking Supervision, *Management and Supervision of Cross-border Electronic Banking Activities*, July 2003.

threats both in terms of incident prevention and response. Key elements of an effective e-banking security process include:

- Assignment of explicit management/staff responsibility for overseeing the establishment and maintenance of corporate security policies.[11]

- Sufficient physical controls to prevent unauthorised physical access to the computing environment.

- Sufficient logical controls and monitoring processes[12] to prevent unauthorised internal[13] and external access to e-banking applications and databases.

- Regular review and testing of security measures and controls, including the continuous tracking of current industry security developments and installation of appropriate software upgrades, service packs and other required measures.[14]

Appendix I contains a number of additional sound practices to help ensure e-banking security.

Principle 3: The Board of Directors and senior management should establish a comprehensive and ongoing due diligence and oversight process for managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking.

Increased reliance upon partners and third party service providers to perform critical e-banking functions lessens bank management's direct control. Accordingly, a comprehensive process for managing the risks associated with outsourcing and other third-party dependencies is necessary. This process should encompass the third-party activities of partners and service providers, including the sub-contracting of outsourced activities that may have a material impact on the bank.

Historically, outsourcing was often limited to a single service provider for a given functionality. However, in recent years, banks' outsourcing relationships have increased in scale and complexity as a direct result of advances in information technology and the emergence of e-banking. Adding to the complexity is the fact that outsourced e-banking services can be sub-contracted to additional service providers and/or conducted in a foreign country. Further, as e-banking applications and services have become more technologically advanced and have grown in strategic importance, certain e-banking functional areas are dependent upon a small number of specialised third-party vendors and service providers. These developments may lead to increased risk concentrations that warrant attention both from an individual bank as well as a systemic industry standpoint.

---

[11] This responsibility should normally not be part of the audit function, which has responsibility for seeing that the security oversight function is carried out effectively.

[12] Including controlled access rights and privileges as well as ongoing monitoring of network intrusion attempts.

[13] Including employees, contractors and those with access rights through outsourced relationships.

[14] Including measures to monitor network activity, log intrusion attempts and report of serious security breaches.

Together, these factors underscore the need for a comprehensive and ongoing evaluation of outsourcing relationships and other external dependencies, including the associated implications for the bank's risk profile and risk management oversight abilities.[15] Board and senior management oversight of outsourcing relationships and third-party dependencies should specifically focus on ensuring that:

- The bank fully understands the risks associated with entering into an outsourcing or partnership arrangement for its e-banking systems or applications.

- An appropriate due diligence review of the competency and financial viability of any third-party service provider or partner is conducted prior to entering into any contract for e-banking services.

- The contractual accountability of all parties to the outsourcing[16] or partnership relationship is clearly defined. For instance, responsibilities for providing information to and receiving information from the service provider should be clearly defined.

- All outsourced e-banking systems and operations are subject to risk management, security and privacy policies that meet the bank's own standards.

- Periodic independent internal and/or external audits are conducted of outsourced operations to at least the same scope required if such operations were conducted in-house.

- Appropriate contingency plans for outsourced e-banking activities exist.

Appendix II lists a number of additional sound practices for managing outsourced e-banking systems and other third-party dependencies.

B. Security Controls (Principles 4 to 10)

While the Board of Directors has the responsibility for ensuring that appropriate security control processes are in place for e-banking, the substance of these processes needs special management attention because of the enhanced security challenges posed by e-banking.[17] The following issues are particularly pertinent:

- Authentication

- Non-repudiation

- Data and transaction integrity

---

[15] Such an evaluation should also take into account the degree of control exercised on the third-party. A major shareholder in a joint venture may, in many cases, exercise more control than in the case of a contractual relationship with a service provider. However, it should not be inferred through such distinctions that shareholder control over a joint venture or a partnership will necessarily be sufficient, especially if the technologies and services necessary to operate the association are provided by the minority shareholder. Such distinctions are mainly useful to assert that evaluations should be made on a case-by-case basis.

[16] This would also include sub-contractors.

[17] For instance, where a Board relies on third-party vendors for e-banking services, it needs to ensure that the vendor has adequately addressed these issues and, at minimum, meets the bank's own standards.

- Segregation of duties
- Authorisation controls
- Maintenance of audit trails
- Confidentiality of key bank information

Principle 4: Banks should take appropriate measures to authenticate[18] the identity and authorisation of customers with whom it conducts business over the Internet.

It is essential in banking to confirm that a particular communication, transaction, or access request is legitimate. Accordingly, banks should use reliable methods for verifying the identity and authorisation of new customers as well as authenticating the identity and authorisation of established customers seeking to initiate electronic transactions.

Customer verification during account origination is important in reducing the risk of identity theft, fraudulent account applications and money laundering. Failure on the part of the bank to adequately authenticate customers could result in unauthorised individuals gaining access to e-banking accounts and ultimately financial loss and reputational damage to the bank through fraud, disclosure of confidential information or inadvertent involvement in criminal activity.

Establishing and authenticating an individual's identity and authorisation to access banking systems in a purely electronic open network environment can be a difficult task. Legitimate user authorisation can be misrepresented through a variety of techniques generally known as "spoofing."[19] Online hackers can also take over the session of a legitimate authorised individual through use of a "sniffer"[20] and carry out activities of a mischievous or criminal nature. Authentication control processes can in addition be circumvented through the alteration of authentication databases.

Accordingly, it is critical that banks have formal policy and procedures identifying appropriate methodology(ies) to ensure that the bank properly authenticates the identity and authorisation of an individual, agent or system[21] by means that are unique and, as far as practical, exclude unauthorised individuals or systems.[22] Banks can us a variety of methods to establish authentication, including PINs, passwords, smart cards, biometrics, and digital

---

[18] *Authentication* as used in this Report refers to the techniques, procedures and processes used to verify the identity and authorisation of prospective and established customers. *Identification* refers to the procedures, techniques and processes used to establish the identity of a customer when opening an account. *Authorisation* refers to the procedures, techniques and processes used to determine that a customer or an employee has legitimate access to the bank account or the authority to conduct associated transactions on that account.

[19] Spoofing is impersonating a legitimate customer through use of his/her account number, password, personal identification number (PIN) and/or email address.

[20] A sniffer is a device that is capable of eavesdropping on telecommunications traffic, capturing passwords and data in transit.

[21] Systems include the institution's own web sites.

[22] Systems must ensure that they are dealing with an authenticated individual, agent or system and with a valid authentication database.

certificates.[23] These methods can be either single factor or multi-factor (e.g. using both a password and biometric technology[24] to authenticate). Multi-factor authentication generally provides stronger assurance.

The bank must determine which authentication methods to use based on management's assessment of the risk posed by the e-banking system as a whole or by the various sub-components. This risk analysis should evaluate the transactional capabilities[25] of the e-banking system (e.g. funds transfer, bill payment, loan origination, account aggregation etc.), the sensitivity and value of the stored e-banking data, and the customer's ease of using the authentication method.

Robust customer identification and authentication processes are particularly important in the cross-border e-banking context given the additional difficulties that may arise from doing business electronically with customers across national borders, including the greater risk of identity impersonation and the greater difficulty in conducting effective credit checks on potential customers.

As authentication methods continue to evolve, banks are encouraged to monitor and adopt industry sound practice in this area such as ensuring that:

- Authentication databases that provide access to e-banking customer accounts or sensitive systems are protected from tampering and corruption. Any such tampering should be detectable and audit trails should be in place to document such attempts.

- Any addition, deletion or change of an individual, agent or system to an authentication database is duly authorised by an authenticated source.[26]

- Appropriate measures are in place to control the e-banking system connection such that unknown third parties cannot displace known customers.

- Authenticated e-banking sessions remain secure throughout the full duration of the session or in the event of a security lapse the session should require re-authentication.

Principle 5: Banks should use transaction authentication methods that promote non-repudiation and establish accountability for e-banking transactions.

Non-repudiation involves creating proof of the origin or delivery of electronic information to protect the sender against false denial by the recipient that the data has been received, or to

---

[23] A bank may issue digital certificates using public key infrastructure (PKI) to a customer in order to secure communications with the bank. Digital certificates and PKI are discussed more fully in Principle 5.

[24] Biometric technology is an automated view of physiological or behavioural characteristics used to identify and/or authenticate a person. Common forms of biometric technology include facial scans, finger scans, iris scans, retina scans, hand scans, signature scans, voice scans and keystroke dynamics. Biometric identification systems provide very strong authentication, but may pose greater implementation complexities than other identification/authentication methods.

[25] Effective authentication measures can also reduce the risk of repudiation, in which an authorised user subsequently denies that he or she authorised a particular transaction (see also Principle 5).

[26] In some cases, the authenticated source may be an electronic source.

protect the recipient against false denial by the sender that the data has been sent. Risk of transaction repudiation is already an issue with conventional transactions such as credit cards or securities transactions. However, e-banking heightens this risk because of the difficulties of positively authenticating the identities and authority of parties initiating transactions, the potential for altering or hijacking electronic transactions, and the potential for e-banking users to claim that transactions were fraudulently altered.

To address these heightened concerns, banks need to make reasonable efforts, commensurate with the materiality and type of the e-banking transaction, to ensure that:

- E-banking systems are designed to reduce the likelihood that authorised users will initiate unintended transactions and that customers fully understand the risks associated with any transactions they initiate.

- All parties to the transaction are positively authenticated and control is maintained over the authenticated channel.

- Financial transaction data are protected from alteration and any alteration is detectable.

Banking organisations have begun to employ various techniques that help establish non-repudiation and ensure confidentiality and integrity of e-banking transactions, such as digital certificates using public key infrastructure (PKI).[27] A bank may issue a digital certificate to a customer or counterparty to allow for their unique identification/authentication and reduce the risk of transaction repudiation. Although in some countries customers' rights to disclaim transactions is provided in specific legal provisions, legislation has been passed in certain national jurisdictions making digital signatures legally enforceable. Wider global legal acceptance of such techniques is likely as technology continues to evolve.

Principle 6: Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.

Segregation of duties is a basic internal control measure designed to reduce the risk of fraud in operational processes and systems and ensure that transactions and company assets are properly authorised, recorded and safeguarded. Segregation of duties is critical to ensuring the accuracy and integrity of data and is used to prevent the perpetration of fraud by an individual. If duties are adequately separated, fraud can only be committed through collusion.

E-banking services may necessitate modifying the ways in which segregation of duties are established and maintained because transactions take place over electronic systems where identities can be more readily masked or faked. In addition, operational and transaction-based functions have in many cases become more compressed and integrated in e-banking

---

[27] In a public key infrastructure (PKI), each party has a private/public key pair. The private key is secret so that only one person should use it. All parties use the public key. The private key generates an electronic signature on the document and the key pairs are designed so that a message encrypted with the private key can only be read by using the other key. A bank may act as its own certification authority (CA) or rely on another trusted third-party to associate a person or entity with the digital certificate. However, if a bank is to rely upon a third-party digital certificate to establish authenticity, it should confirm that the CA, when issuing the certificate, used the same level of authentication that the bank would have used to authenticate the person. The primary drawback of a PKI authentication system is that it is more complicated to implement.

applications. Therefore, the controls traditionally required to maintain segregation of duties need to be reviewed and adapted to ensure an appropriate level of control is maintained. Because access to poorly secured databases can be more easily gained through internal or external networks, strict authorisation and identification procedures, safe and sound architecture of the straight-through processes, and adequate audit trails should be emphasised.

Common practices used to establish and maintain segregation of duties within an e-banking environment include the following:

- Transaction processes and systems should be designed to ensure that no single employee/outsourced service provider could enter, authorise and complete a transaction.

- Segregation should be maintained between those initiating static data (including web page content) and those responsible for verifying its integrity.

- E-banking systems should be tested to ensure that segregation of duties cannot be bypassed.

- Segregation should be maintained between those developing and those administrating e-banking systems.[28]

Principle 7: Banks should ensure that proper authorisation controls and access privileges are in place for e-banking systems, databases and applications.

In order to maintain segregation of duties, banks need to strictly control authorisation and access privileges. Failure to provide adequate authorisation control could allow individuals to alter their authority, circumvent segregation and gain access to e-banking systems, databases or applications to which they are not privileged.

In e-banking systems, the authorisations and access rights can be established in either a centralised or distributed manner within a bank and are generally stored in databases. The protection of those databases from tampering or corruption is therefore essential for effective authorisation control.

Appendix III identifies a number of sound practices to help establish proper control over authorisation and access rights to e-banking systems, databases and applications.

Principle 8: Banks should ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information.

Data integrity refers to the assurance that information that is in-transit or in storage is not altered without authorisation. Failure to maintain the data integrity of transactions, records and information can expose banks to financial losses as well as to substantial legal and reputational risk.

---

[28] Or alternate mitigating controls should be in place.

The inherent nature of straight-through processes for e-banking may make programming errors or fraudulent activities more difficult to detect at an early stage. Therefore, it is important that banks implement straight-through processing in a manner that ensures safety and soundness and data integrity.

As e-banking is transacted over public networks, transactions are exposed to the added threat of data corruption, fraud and the tampering of records. Accordingly, banks should ensure that appropriate measures are in place to ascertain the accuracy, completeness and reliability of e-banking transactions, records and information that is either transmitted over the Internet, resident on internal bank databases, or transmitted/stored by third-party service providers on behalf of the bank.[29] Common practices used to maintain data integrity within an e-banking environment include the following:

- E-banking transactions should be conducted in a manner that makes them highly resistant to tampering throughout the entire process.

- E-banking records should be stored, accessed and modified in a manner that makes them highly resistant to tampering.

- E-banking transaction and record-keeping processes should be designed in a manner as to make it virtually impossible to circumvent detection of unauthorised changes.

- Adequate change control policies, including monitoring and testing procedures, should be in place to protect against any e-banking system changes that may erroneously or unintentionally compromise controls or data reliability.

- Any tampering with e-banking transactions or records should be detected by transaction processing, monitoring and record keeping functions.

Principle 9: Banks should ensure that clear audit trails exist for all e-banking transactions.

Delivery of financial services over the Internet can make it more difficult for banks to apply and enforce internal controls and maintain clear audit trails if these measures are not adapted to an e-banking environment. Banks are not only challenged to ensure that effective internal control can be provided in highly automated environments, but also that the controls can be independently audited, particularly for all critical e-banking events and applications.

A bank's internal control environment may be weakened if it is unable to maintain clear audit trails for its e-banking activities. This is because much, if not all, of its records and evidence supporting e-banking transactions are in an electronic format. In making a determination as to where clear audit trails should be maintained, the following types of e-banking transactions should be considered:

- The opening, modification or closing of a customer’s account.

---

[29] Banks should ensure that record keeping systems are designed and installed in a manner that allows for recovery of records that may have been tampered with or degraded.

- Any transaction with financial consequences.
- Any authorisation granted to a customer to exceed a limit.
- Any granting, modification or revocation of systems access rights or privileges.

Appendix IV identifies several sound practices to help ensure that a clear audit trail exists for e-banking transactions.

Principle 10: Banks should take appropriate measures to preserve the confidentiality of key e-banking information. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the information being transmitted and/or stored in databases.

Confidentiality is the assurance that key information remains private to the bank and is not viewed or used by those unauthorised to do so. Misuse or unauthorised disclosure of data exposes a bank to both reputation and legal risk. The advent of e-banking presents additional security challenges for banks because it increases the exposure that information transmitted over the public network or stored in databases may be accessible by unauthorised or inappropriate parties or used in ways the customer providing the information did not intend. Additionally, increased use of service providers may expose key bank data to other parties.

To meet these challenges concerning the preservation of confidentiality of key e-banking information, banks need to ensure that:

- All confidential bank data and records are only accessible by duly authorised and authenticated individuals, agents or systems.
- All confidential bank data are maintained in a secure manner and protected from unauthorised viewing or modification during transmission over public, private or internal networks.
- The bank's standards and controls for data use and protection must be met when third parties have access to the data through outsourcing relationships.
- All access to restricted data is logged and appropriate efforts are made to ensure that access logs are resistant to tampering.

C. Legal and Reputational Risk Management (Principles 11 to 14)

Specific customer protection and privacy regulations and laws will vary from jurisdiction to jurisdiction. However, banks generally have a clear responsibility to provide their customers with a level of comfort regarding information disclosures, protection of customer data and business availability that approaches the level they would have if transacting business through traditional banking distribution channels.

Principle 11: Banks should ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status of the bank prior to entering into e-banking transactions.

To minimise legal and reputational risk associated with e-banking activities conducted both domestically and cross-border, banks should ensure that adequate information is provided on their websites to allow customers to make informed conclusions about the identity and regulatory status of the bank before they enter into e-banking transactions.

Examples of such information that a bank could provide on its own website include:

- The name of the bank and the location of its head office (and local offices if applicable).
- The identity of the primary bank supervisory authority(ies) responsible for the supervision of the bank's head office.
- How customers can contact the bank's customer service centre regarding service problems, complaints, suspected misuse of accounts, etc.
- How customers can access and use applicable Ombudsman or consumer complaint schemes.
- How customers can obtain access to information on applicable national compensation or deposit insurance coverage and the level of protection that they afford (or links to websites that provide such information).
- Other information that may be appropriate or required by specific jurisdictions.[30]

Principle 12: Banks should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the bank is providing e-banking products and services.

Maintaining a customer's information privacy is a key responsibility for a bank. Misuse or unauthorised disclosure of confidential customer data exposes a bank to both legal and reputation risk. To meet these challenges concerning the preservation of privacy of customer information, banks should make reasonable endeavours to ensure that:

- The bank's customer privacy policies and standards take account of and comply with all privacy regulations and laws applicable to the jurisdictions to which it is providing e-banking products and services.
- Customers are made aware of the bank's privacy policies and relevant privacy issues concerning use of e-banking products and services.
- Customers may decline ("opt out") from permitting the bank to share with a third party for cross-marketing purposes any information about the customer's personal needs, interests, financial position or banking activity.
- Customer data are not used for purposes beyond which they are specifically allowed or for purposes beyond which customers have authorised.[31]

---

[30] For instance, the bank may wish to specify those countries in which the bank intends to provide e-banking services or, conversely, those countries in which it does not intend to provide such services.

- The bank's standards for customer data use must be met when third parties have access to customer data through outsourcing relationships.

Appendix V identifies several sound practices to help maintain the privacy of customer e-banking information.

Principle 13: Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.

To protect banks against business, legal and reputation risk, e-banking services must be delivered on a consistent and timely basis in accordance with customer expectations. To achieve this, the bank must have the ability to deliver e-banking services to end-users from either primary (e.g. internal bank systems and applications) or secondary sources (e.g. systems and applications of service providers). The maintenance of adequate availability is also dependent upon the ability of contingency back-up systems to mitigate denial of service attacks or other events that may potentially cause business disruption.

The challenge to maintain continued availability of e-banking systems and applications can be considerable given the potential for high transaction demand, especially during peak time periods. In addition, high customer expectations regarding short transaction processing cycle times and constant availability (24 X 7) has also increased the importance of sound capacity, business continuity and contingency planning. To provide customers with the continuity of e-banking services that they expect, banks need to ensure that:

- Current e-banking system capacity and future scalability are analysed in light of the overall market dynamics for e-commerce and the projected rate of customer acceptance of e-banking products and services.[32]

- E-banking transaction processing capacity estimates are established, stress tested and periodically reviewed.

- Appropriate business continuity and contingency plans for critical e-banking processing and delivery systems are in place and regularly tested.

Appendix VI identifies several sound capacity, business continuity and contingency planning practices.

Principle 14: Banks should develop appropriate incident response plans to manage, contain and minimise problems arising from unexpected events, including internal

---

[31] In some jurisdictions, laws and regulations may not oblige banks to seek the customer's permission to use customer data for internal purposes. However, they may oblige banks to give the customer the option to decline from permitting the bank to share such information with a third party or an affiliate. In other jurisdictions, customers may have the right to prevent the bank from using their data for either internal or external purposes.

[32] The current and future capacity of critical e-banking delivery systems should be assessed on an ongoing basis.

and external attacks, that may hamper the provision of e-banking systems and services.

Effective incident response mechanisms are critical to minimise operational, legal and reputational risks arising from unexpected events such as internal and external attacks that may affect the provision of e-banking systems and services. Banks should develop appropriate incident response plans, including communication strategies, that ensure business continuity, control reputation risk and limit liability associated with disruptions in their e-banking services, including those originating from outsourced systems and operations.

To ensure effective response to unforeseen incidents, banks should develop:

- Incident response plans to address recovery of e-banking systems and services under various scenarios, businesses and geographic locations. Scenario analysis should include consideration of the likelihood of the risk occurring and its impact on the bank. E-banking systems that are outsourced to third-party service providers should be an integral part of these plans

- Mechanisms to identify an incident or crisis as soon as it occurs, assess its materiality, and control the reputation risk associated with any disruption in service.[33]

- A communication strategy to adequately address external market and media concerns that may arise in the event of security breaches, online attacks and/or failures of e-banking systems.

- A clear process for alerting the appropriate regulatory authorities in the event of material security breaches or disruptive incidents occur.

- Incident response teams with the authority to act in an emergency and sufficiently trained in analysing incident detection/response systems and interpreting the significance of related output.

- A clear chain of command, encompassing both internal as well as outsourced operations, to ensure that prompt action is taken appropriate for the significance of the incident. In addition, escalation and internal communication procedures should be developed and include notification of the Board where appropriate.

- A process to ensure all relevant external parties, including bank customers, counterparties and the media, are informed in a timely and appropriate manner of material e-banking disruptions and business resumption developments.

- A process for collecting and preserving forensic evidence to facilitate appropriate post-mortem reviews of any e-banking incidents as well as to assist in the prosecution of attackers.

---

[33] Monitoring of help desk and customer support activities and regular review of customer complaints may help to identify gaps in information being detected and reported through established security controls versus actual intrusion activities.

Appendix I

Sound Security Control Practices for E-Banking

1. Security profiles should be created and maintained and specific authorisation privileges assigned to all users of e-banking systems and applications, including all customers, internal bank users and outsourced service providers. Logical access controls should also be designed to support proper segregation of duties.[34]

2. E-banking data and systems should be classified according to their sensitivity and importance and protected accordingly. Appropriate mechanisms, such as encryption, access control and data recovery plans should be used to protect all sensitive and high-risk e-banking systems, servers, databases and applications.

3. Storage of sensitive or high-risk data on the organisation's desktop and laptop systems should be minimised and properly protected by encryption, access control and data recovery plans.

4. Sufficient physical controls should be in place to deter unauthorised access[35] to all critical e-banking systems, servers, databases and applications.

5. Appropriate techniques should be employed to mitigate external threats to e-banking systems, including the use of:

   - Virus-scanning software at all critical entry points (e.g. remote access servers, e-mail proxy servers) and on each desktop system.

   - Intrusion detection software and other security assessment tools to periodically probe networks, servers and firewalls for weaknesses and/or violations of security policies and controls.

   - Penetration testing of internal and external networks.

6. A rigorous security review process should be applied to all employees and service providers holding sensitive positions.

---

[34] Definitions of security and quality standards and reliance on certification schemes can be institution specific or standardised (i.e. within a national banking industry in order to enhance and foster the security level of e-banking activities). Banks can also choose to establish access rights in either a centralised or distributed manner. For example, there may be a single authorisation authority responsible for assigning access rights to specific identities, groups or roles within a bank, or there may be a number of authorisation authorities established to address the varying needs within the different business lines.

[35] This should include controls guarding against unauthorised access by external parties such as visitors, contractors or technicians who may have access to the premises although they may not be directly involved in the e-banking service.

Appendix II

Sound Practices for Managing Outsourced E-Banking Systems and Services

1. Banks should adopt appropriate processes for evaluating decisions to outsource e-banking systems or services.

   - Bank management should clearly identify the strategic purposes, benefits and costs associated with entering into outsourcing arrangements for e-banking with third parties.

   - The decision to outsource a key e-banking function or service should be consistent with the bank's business strategies, be based on a clearly defined business need, and recognise the specific risks that outsourcing entails.

   - All affected areas of the bank need to understand how the service provider(s) will support the bank's e-banking strategy and fit into its operating structure.

2. Banks should conduct appropriate risk analysis and due diligence prior to selecting an e-banking service provider and at appropriate intervals thereafter.

   - Banks should consider developing processes for soliciting proposals from several e-banking service providers and criteria for choosing among the various proposals.

   - Once a potential service provider has been identified, the bank should conduct an appropriate due diligence review, including a risk analysis of the service provider's financial strength, reputation, risk management policies and controls, and ability to fulfil its obligations.

   - Thereafter, banks should regularly monitor and, as appropriate,[36] conduct due diligence reviews of the ability of the service provider to fulfil its service and associated risk management obligations throughout the duration of the contract.

   - Banks need to ensure that adequate resources are committed to overseeing outsourcing arrangements supporting e-banking.

   - Responsibilities for overseeing e-banking outsourcing arrangements should be clearly assigned.

---

[36] The extent of ongoing due diligence reviews should be based on the materiality of the outsourced operations and the extent of systems or risk management changes over time, including any subsequent sub-contracting the service provider may engage in.

- An appropriate exit strategy for the bank to manage risks should it need to terminate the outsourcing relationship.

3. Banks should adopt appropriate procedures for ensuring the adequacy of contracts governing e-banking. Contracts governing outsourced e-banking activities should address, for example, the following:[37]

   - The contractual liabilities of the respective parties as well as responsibilities for making decisions, including any sub-contracting of material services are clearly defined.

   - Responsibilities for providing information to and receiving information from the service provider are clearly defined. Information from the service provider should be timely and comprehensive enough to allow the bank to adequately assess service levels and risks. Materiality thresholds and procedures to be used to notify the bank of service disruptions, security breaches and other events that pose a material risk to the bank should be spelled out.

   - Provisions that specifically address insurance coverage, the ownership of the data stored on the service provider's servers or databases, and the right of the bank to recover its data upon expiration or termination of the contract should be clearly defined.

   - Performance expectations, under both normal and contingency circumstances, are defined.

   - Adequate means and guarantees, for instance through audit clauses, are defined to insure that the service provider complies with the bank's policies.

   - Provisions are in place for timely and orderly intervention and rectification in the event of substandard performance by the service provider.

   - For cross-border outsourcing arrangements, determining which country laws and regulations, including those relating to privacy and other customer protections, are applicable.

   - The right of the bank to conduct independent reviews and/or audits of security, internal controls and business continuity and contingency plans is explicitly defined.

4. Banks should ensure that periodic independent internal and/or external audits are conducted of outsourced operations to at least the same scope required if such operations were conducted in-house.[38]

---

[37] As with other legal contracts that a bank may enter to, its legal counsel or legal division should review all terms and conditions in contracts governing e-banking outsourcing arrangements.

[38] Banks that do not have a specific audit function in-house should, at minimum, have staff not involved in management of outsourced relationships reviewing the effectiveness of the oversight of the outsourcing arrangement.

- For outsourced relationships involving critical or technologically complex e-banking services/applications, banks may need to arrange for other periodic reviews to be performed by independent third parties with sufficient technical expertise.

5. Banks should develop appropriate contingency plans for outsourced e-banking activities.

   - Banks need to develop and periodically test their contingency plans for all critical e-banking systems and services that have been outsourced to third parties.

   - Contingency plans should address credible worst-case scenarios for providing continuity of e-banking services in the event of a disruption affecting outsourced operations.

   - Banks should have an identified team that is responsible for managing recovery and assessing the financial impact of a disruption in outsourced e-banking services.

6. Banks that provide e-banking services to third parties should ensure that their operations, responsibilities, and liabilities are sufficiently clear so that serviced institutions can adequately carry out their own effective due diligence reviews and ongoing oversight of the relationship.

   - Banks have a responsibility to provide serviced institutions with information necessary to identify, control and monitor any risks associated with the e-banking service arrangement.

Appendix III

Sound Authorisation Practices for E-Banking Applications

1. Specific authorisation and access privileges should be assigned to all individuals, agents or systems, which conduct e-banking activities.

2. All e-banking systems should be constructed to ensure that they interact with a valid authorisation database.

3. No individual agent or system should have the authority to change his or her own authority or access privileges in an e-banking authorisation database.[39]

4. Any addition of an individual, agent or system or changes to access privileges in an e-banking authorisation database should be duly authorised by an authenticated source empowered with the adequate authority and subject to suitable and timely oversight and audit trails.

5. Appropriate measures should be in place in order to make e-banking authorisation databases reasonably resistant to tampering. Any such tampering should be detectable through ongoing monitoring processes. Sufficient audit trails should exist to document any such tampering.

6. Any e-banking authorisation database that has been tampered with should not be used until replaced with a validated database.

7. Controls should be in place to prevent changes to authorisation levels during e-banking transaction sessions and any attempts to alter authorisation should be logged and brought to the attention of management.

[39] As this might not be feasible for system administrator users, other stringent internal controls and segregation of duties should be put in place to monitor the activities of those user accounts.

Appendix IV

Sound Audit Trail Practices for E-Banking Systems

1. Sufficient logs should be maintained for all e-banking transactions to help establish a clear audit trail and assist in dispute resolution.

2. E-banking systems should be designed and installed to capture and maintain forensic evidence in a manner that maintains control over the evidence, and prevents tampering and the collection of false evidence.

3. In instances where processing systems and related audit trails are the responsibility of a third-party service provider:

    - The bank should ensure that it has access to relevant audit trails maintained by the service provider.

    - Audit trails maintained by the service provider meet the bank's standards.

Appendix V

Sound Practices to Help Maintain the Privacy of Customer E-Banking Information

1. Banks should employ appropriate cryptographic techniques, specific protocols or other security controls to ensure the confidentiality of customer e-banking data.

2. Banks should develop appropriate procedures and controls to periodically assess its customer security infrastructure and protocols for e-banking.

3. Banks should ensure that its third-party service providers have confidentiality and privacy policies that are consistent with their own.

4. Banks should take appropriate steps to inform e-banking customers about the confidentiality and privacy of their information. These steps may include:

    - Informing customers of the bank's privacy policy, possibly on the bank's website. Clear, concise language in such statements is essential to assure that the customer fully understands the privacy policy. Lengthy legal descriptions, while accurate, are likely to go unread by the majority of customers.

    - Instructing customers on the need to protect their passwords, personal identification numbers (PINs) and other banking and/or personal data.

    - Providing customers with information regarding the general security of their personal computer, including the benefits of using virus protection software, physical access controls and personal firewalls for static Internet connections.

Appendix VI

Sound Capacity, Business Continuity and Contingency Planning Practices for E-Banking

1. All e-banking services and applications, including those provided by third-party service providers, should be identified and assessed for criticality.

2. A risk assessment for each critical e-banking service and application, including the potential implications of any business disruption on the bank's credit, market, liquidity, legal, operational and reputation risk should be conducted.

3. Performance criteria for each critical e-banking service and application should be established, and service levels should be monitored against such criteria. Appropriate measures should be taken to ensure that e-banking systems can handle high and low transaction volume and that systems performance and capacity is consistent with the bank's expectations for future growth in e-banking.

4. Consideration should be given to developing processing alternatives for managing demand when e-banking systems appear to be reaching defined capacity checkpoints.

5. E-banking business continuity plans should be formulated to address any reliance on third-party service providers and any other external dependencies required achieving recovery.

6. E-banking contingency plans should set out a process for restoring or replacing e-banking processing capabilities, reconstructing supporting transaction information, and include measures to be taken to resume availability of critical e-banking systems and applications in the event of a business disruption.