คณะกรรมการคุ้มครองข้อมูลเครดิต

29 ธันวาคม 2546

เรียน ผู้จัดการ

บริษัทข้อมูลเครดิตทุกบริษัท

ที่ กคค.(ว) 6 /2546 เรื่อง แนวทางการรักษาความปลอดภัยการให้บริการข้อมูลเครดิตและแนวทางการให้คำแนะนำแก่สมาชิกหรือผู้ใช้บริการ

ตามที่คณะกรรมการคุ้มครองข้อมูลเครดิตได้ออกประกาศตามมาตรา 17 แห่งพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการจัดระบบและข้อกำหนดเพื่อประมวลผลข้อมูล ลงวันที่ 26 ธันวาคม 2546 แล้ว นั้น

เนื่องจากปัจจุบันการประกอบธุรกิจของบริษัทข้อมูลเครดิตเกี่ยวข้องกับการให้บริการผ่านเครือข่ายสาธารณะ (Public Network) เช่น เครือข่ายอินเตอร์เน็ต ซึ่งต้องมีการเชื่อมต่อกับเครือข่ายภายในของบริษัทข้อมูลเครดิต สมาชิก และผู้ใช้บริการ จึงมีความเสี่ยงสูงที่จะเกิดภัยคุกคามในรูปแบบต่าง ๆ โดยเฉพาะจากผู้บุกรุก (Hackers) ซึ่งสามารถสร้างความเสียหายต่อเจ้าของข้อมูล สมาชิก หรือผู้ใช้บริการ คณะกรรมการคุ้มครองข้อมูลเครดิตจึงเห็นควรออกแนวทางการรักษาความปลอดภัยการให้บริการข้อมูลเครดิตและแนวทางการให้คำแนะนำแก่สมาชิกและผู้ใช้บริการ โดยมีวัตถุประสงค์เพื่อให้บริษัทข้อมูลเครดิตใช้เป็นแนวทางในการกำหนดกรอบการรักษาความปลอดภัยสำหรับการให้บริการข้อมูลเครดิต และมีแนวทางการให้คำแนะนำที่เป็นประโยชน์แก่สมาชิกหรือผู้ใช้บริการเพื่อให้เข้าใจและตระหนักถึงความสำคัญของการรักษาความปลอดภัยในการใช้บริการด้วย

จึงขอส่งมาเพื่อให้ท่านทราบและพิจารณาถือปฏิบัติในส่วนที่เกี่ยวข้องกับท่าน และใคร่ขอความร่วมมือท่านโปรดให้คำแนะนำแก่สมาชิกหรือผู้ใช้บริการตามแนวทางการให้คำแนะนำแก่สมาชิกหรือผู้ใช้บริการดังกล่าวด้วย

ขอแสดงความนับถือ

สรสิทธิ์ สุนทรเกศ

(นายสรสิทธิ์ สุนทรเกศ)
เลขานุการ
คณะกรรมการคุ้มครองข้อมูลเครดิต

สิ่งที่ส่งมาด้วย 1. แนวทางการรักษาความปลอดภัยการให้บริการข้อมูลเครดิต
2. แนวทางการให้คำแนะนำแก่สมาชิกหรือผู้ใช้บริการ

เลขานุการคณะกรรมการคุ้มครองข้อมูลเครดิต
โทร. 0-2283-5820
0-2283-5963

แนวทางการรักษาความปลอดภัยการให้บริการข้อมูลเครดิต

วัตถุประสงค์

เพื่อให้บริษัทข้อมูลเครดิตใช้เป็นแนวทางในการกำหนดกรอบการรักษาความปลอดภัยสำหรับการให้บริการข้อมูลเครดิต และเป็นการรักษาผลประโยชน์ของเจ้าของข้อมูลและสมาชิก

หลักการ

แนวทางการรักษาความปลอดภัยการให้บริการข้อมูลเครดิตนี้มุ่งเน้นการรักษาความปลอดภัยของการให้และใช้บริการข้อมูลเครดิตผ่านเครือข่ายสาธารณะ (Public Network) เช่น เครือข่ายอินเตอร์เน็ต ซึ่งต้องมีการเชื่อมต่อกับเครือข่ายภายในของบริษัทข้อมูลเครดิต สมาชิก และผู้ใช้บริการ ที่มีโอกาสสูงที่จะเกิดภัยคุกคามในรูปแบบต่าง ๆ โดยเฉพาะจากผู้บุกรุก (Hackers) ซึ่งสามารถสร้างความเสียหายต่อเจ้าของข้อมูล สมาชิก หรือผู้ใช้บริการได้

เนื้อหาของแนวทางการรักษาความปลอดภัยการให้บริการข้อมูลเครดิต แบ่งเป็น 3 ส่วน ดังนี้

1. นโยบายการรักษาความปลอดภัย

2. กระบวนการหลักในการรักษาความปลอดภัย ได้แก่

    2.1 การควบคุมการเข้าถึงระบบให้บริการและฐานข้อมูล

    2.2 การตรวจสอบตัวตนของสมาชิกหรือผู้ใช้บริการ

    2.3 การรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูล

    2.4 การรักษาความลับของข้อมูล

    2.5 การรักษาความพร้อมใช้ของระบบให้บริการ

    2.6 การติดตามตรวจสอบความผิดปกติและจุดอ่อนของระบบให้บริการ

    2.7 การแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการขัดข้องหรือได้รับความเสียหายจากภัยคุกคาม

3. กระบวนการเสริมการรักษาความปลอดภัยให้มีประสิทธิภาพ ได้แก่

    3.1 การฝึกอบรมและให้ความรู้แก่พนักงานของบริษัทข้อมูลเครดิต

    3.2 การให้ข้อมูลและคำแนะนำแก่สมาชิกหรือผู้ใช้บริการ

    3.3 การควบคุมภายใน

รายละเอียดของแนวทางการรักษาความปลอดภัยการให้บริการข้อมูลเครดิต

1. <u>นโยบายการรักษาความปลอดภัย</u>

1.1 บริษัทข้อมูลเครดิตควรกำหนดนโยบายและกระบวนการรักษาความปลอดภัยของการให้บริการข้อมูลเครดิตที่ชัดเจน โดยพิจารณาถึงความเสียหายที่อาจเกิดขึ้นต่อระบบให้บริการ เจ้าของข้อมูล สมาชิก และผู้ใช้บริการ อันเนื่องมาจากพฤติกรรมที่ไม่พึงประสงค์ รวมทั้งคำนึงถึงการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็วด้วย

1.2 บริษัทข้อมูลเครดิตควรกำหนดให้มีผู้บริหารและพนักงานที่รับผิดชอบในการดำเนินการ มีการสื่อสารให้พนักงานได้รับทราบอย่างทั่วถึง มีการติดตามดูแลให้พนักงานและผู้ที่เกี่ยวข้องกับระบบให้บริการปฏิบัติตามนโยบายและกระบวนการรักษาความปลอดภัยอย่างเคร่งครัด รวมทั้งมีการตรวจสอบการปฏิบัติตามอย่างเหมาะสม

1.3 บริษัทข้อมูลเครดิตควรจัดให้มีการประเมินประสิทธิภาพของกระบวนการรักษาความปลอดภัยอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบต่อการรักษาความปลอดภัย เช่น การเปลี่ยนแปลงเทคโนโลยีที่ใช้ หรือการลักลอบเข้าถึงระบบให้บริการ (Hacking Incidents) ทั้งนี้ การประเมินควรกระทำโดยผู้เชี่ยวชาญจากภายนอกที่ไม่เป็นผู้พัฒนาหรือปฏิบัติการระบบ นอกจากนั้น บริษัทข้อมูลเครดิตควรมีการติดตามความก้าวหน้าทางเทคโนโลยีอย่างใกล้ชิดเพื่อนำมาพัฒนานโยบายและกระบวนการรักษาความปลอดภัยให้มีประสิทธิภาพมากขึ้น

2. <u>กระบวนการหลักในการรักษาความปลอดภัย</u>

การให้บริการข้อมูลเครดิตแก่สมาชิกหรือผู้ใช้บริการจะต้องมีระบบป้องกันภัยคุกคามจากผู้บุกรุกในรูปแบบต่าง ๆ ที่สามารถสร้างความเสียหายต่อระบบให้บริการ เจ้าของข้อมูล สมาชิก และผู้ใช้บริการได้ เช่น การลักลอบเข้าถึงเครือข่ายภายใน การโจมตีระบบให้บริการโดยมีเป้าหมายเพื่อให้ระบบทำงานไม่ได้หรือให้เปิดเผยข้อมูลที่สำคัญ การปลอมแปลงข้อมูล หรือการโจมตีระบบให้บริการโดยไวรัสคอมพิวเตอร์ เป็นต้น

บริษัทข้อมูลเครดิตต้องมีกระบวนการรักษาความปลอดภัยที่ดีและเลือกใช้เทคโนโลยีสำหรับการรักษาความปลอดภัยที่มีประสิทธิภาพและเป็นที่ยอมรับตามมาตรฐานที่เกี่ยวข้อง เพื่อป้องกันภัยคุกคามต่าง ๆ และเมื่อเกิดภัยคุกคามก็สามารถควบคุมความเสียหายและแก้ไขปัญหาที่เกิดขึ้นได้อย่างรวดเร็ว ทั้งนี้ กระบวนการหลักในการรักษาความปลอดภัยดังกล่าวควรประกอบด้วย

2.1 การควบคุมการเข้าถึงระบบให้บริการและฐานข้อมูล

กระบวนการและเทคโนโลยีที่ใช้ควบคุมการเข้าถึงระบบให้บริการและฐานข้อมูลต้องสามารถป้องกันการลักลอบเข้าถึงโดยผู้ที่ไม่มีสิทธิทั้งจากภายในและภายนอกองค์กร โดยมีการควบคุมการเข้าถึงสถานที่ตั้งของระบบให้บริการและอุปกรณ์สำคัญ และมีการควบคุมการเข้าถึงระบบให้บริการและข้อมูลด้วยวิธีการทางคอมพิวเตอร์ ทั้งนี้ กระบวนการดังกล่าวควรครอบคลุมถึง

1) การกำหนดสิทธิการเข้าถึงระบบให้บริการให้เหมาะสมกับการเข้าใช้บริการของสมาชิกหรือผู้ใช้บริการ และสิทธิหน้าที่ของพนักงานในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

2) การกำหนดให้ผู้มีอำนาจเท่านั้นที่สามารถเข้าแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงต่างๆ ได้

3) การบันทึกรายละเอียดการเข้าถึงระบบให้บริการและฐานข้อมูล การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบให้บริการไว้ เพื่อเป็นหลักฐานการตรวจสอบในกรณีเกิดปัญหา

2.2 การตรวจสอบตัวตนของสมาชิกหรือผู้ใช้บริการ

บริษัทข้อมูลเครดิตควรจัดให้มีระบบการตรวจสอบตัวตนของสมาชิกหรือผู้ใช้บริการ เพื่อป้องกันการเข้าถึงระบบให้บริการและฐานข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้ กระบวนการดังกล่าวควรครอบคลุมถึง

1) วิธีการตรวจสอบตัวตนและสิทธิในการใช้บริการของสมาชิกหรือผู้ใช้บริการก่อนเข้าถึงระบบให้บริการหรือฐานข้อมูล

2) การควบคุมการเข้าถึงและการแก้ไขเปลี่ยนแปลงข้อมูลในฐานข้อมูลที่ใช้ในการตรวจสอบตัวตน

3) การตรวจสอบตัวตนสมาชิกหรือผู้ใช้บริการต้องกระทำอย่างต่อเนื่อง หากมีการหยุดชะงักควรเริ่มตรวจสอบตัวตนสมาชิกหรือผู้ใช้บริการใหม่

4) การบันทึกรายละเอียดการเข้าถึงข้อมูลของสมาชิกหรือผู้ใช้บริการ เพื่อใช้เป็นหลักฐานการตรวจสอบ รวมทั้งมีการจัดเก็บบันทึกดังกล่าวอย่างปลอดภัย

5) การจัดให้มีการทบทวนวิธีการตรวจสอบตัวตนอย่างสม่ำเสมอ โดยคำนึงถึงพัฒนาการทางเทคโนโลยีที่เปลี่ยนแปลงไป

ตัวอย่างเทคโนโลยีที่ใช้ในการตรวจสอบตัวตน อาทิ รหัสผู้ใช้งาน (User ID) รหัสผ่านเพื่อการใช้งาน (Password) เทคโนโลยีการเข้ารหัสลับ (Encryption Technology) ข้อมูลที่ใช้

ตรวจสอบตัวตนสมาชิกหรือผู้ใช้บริการ และการใช้ช่องทางที่มีความปลอดภัยสูงในการรับส่งข้อมูลการตรวจสอบตัวตน เช่น Secure Sockets Layer (SSL) เป็นต้น

2.3 <u>การรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูล</u>

กระบวนการที่ใช้ในการรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูล ควรครอบคลุมถึง

1) การออกแบบระบบให้บริการและการเลือกใช้เทคโนโลยีที่มีประสิทธิภาพ

2) การทดสอบระบบให้บริการให้ทำงานได้อย่างถูกต้องก่อนเริ่มใช้งานหรือทุกครั้งที่มีการเปลี่ยนแปลง

3) การควบคุมการทำงานของระบบให้บริการในขั้นตอนที่สำคัญ เช่น ขั้นตอนการประมวลผล การรับส่ง และการจัดเก็บข้อมูล เพื่อให้สามารถป้องกันและตรวจสอบการลักลอบเข้าถึงระบบให้บริการได้

4) การควบคุมการแก้ไขเปลี่ยนแปลงระบบให้บริการและข้อมูลอย่างรัดกุม

2.4 <u>การรักษาความลับของข้อมูลเครดิต</u>

กระบวนการและเทคโนโลยีที่ใช้ในการรักษาความลับของข้อมูลเครดิต โดยเฉพาะข้อมูลเครดิตที่อยู่ระหว่างการรับส่ง การประมวลผล และการจัดเก็บ ควรครอบคลุมถึง

1) วิธีการรับส่ง ประมวลผล และจัดเก็บข้อมูลในลักษณะที่ปลอดภัยตามระดับความสำคัญของข้อมูล เพื่อป้องกันการเข้าถึงและแก้ไขเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

2) การควบคุมเพื่อให้ผู้ที่มีสิทธิและได้รับการตรวจสอบตัวตนแล้วเท่านั้นที่จะเข้าถึงหรือเปลี่ยนแปลงข้อมูลได้

2.5 <u>การรักษาความพร้อมใช้ของระบบให้บริการ</u>

กระบวนการที่ใช้รักษาความพร้อมใช้ของระบบให้บริการควรครอบคลุมถึงการดำเนินการให้ระบบให้บริการมีประสิทธิภาพและมีความพร้อมในการให้บริการตามช่วงเวลาที่ได้ตกลงไว้กับสมาชิกหรือผู้ใช้บริการ สามารถรองรับการใช้บริการได้อย่างพอเพียง ทั้งในช่วงเวลาปกติและช่วงเวลาที่มีการใช้บริการอย่างหนาแน่น รวมทั้งมีระบบสำรองข้อมูลและระบบการเรียกคืนข้อมูลอย่างทันท่วงทีในกรณีที่เกิดความเสียหายหรือขัดข้อง

ในการเตรียมการรองรับเหตุการณ์ความเสียหายที่อาจเกิดขึ้นโดยไม่ได้คาดหมาย บริษัทข้อมูลเครดิตควรจัดให้มีแผนฉุกเฉินในการรักษาความพร้อมใช้ของการให้บริการ โดยให้คำนึงถึงปัญหาขัดข้องที่เกิดจากระบบขององค์กรภายนอกที่บริษัทข้อมูลเครดิตพึ่งพาหรือเชื่อมต่อด้วย

2.6 <u>การติดตามตรวจสอบความผิดปกติและจุดอ่อนของระบบให้บริการ</u>

กระบวนการและเทคโนโลยีที่ใช้ในการติดตามตรวจสอบความผิดปกติและจุดอ่อนของระบบให้บริการควรครอบคลุมถึง

1) การตรวจสอบความผิดปกติของระบบให้บริการอย่างสม่ำเสมอ โดยอาจตรวจสอบจากหลักฐานที่บันทึกไว้ เช่น การเข้าถึงระบบให้บริการของสมาชิกหรือผู้ใช้บริการ การเข้าถึงฐานข้อมูล การตรวจสอบตัวตน และการปฏิบัติงานของพนักงาน เป็นต้น

2) การตรวจสอบจุดอ่อนของระบบให้บริการอย่างต่อเนื่อง โดยเฉพาะในส่วนของระบบเครือข่าย โปรแกรมระบบงาน และฐานข้อมูล เนื่องจากผู้บุกรุกสามารถใช้ข้อบกพร่องดังกล่าวเป็นช่องทางในการโจมตีหรือลักลอบเข้าถึง

3) การทดสอบเจาะระบบ (Penetration Test) เพื่อทดสอบประสิทธิภาพของเทคโนโลยีการรักษาความปลอดภัย

ตัวอย่างเทคโนโลยีที่เกี่ยวข้องกับการตรวจสอบความผิดปกติและความเปราะบาง อาทิ ระบบตรวจจับการบุกรุก (Intrusion Detection System - IDS) เทคโนโลยีที่ใช้ในการตรวจสอบโปรแกรมหรือข้อมูลที่แปลกปลอมเข้ามาในระบบให้บริการ เช่น Network Scanner, Network Analyzer, Security Alert ต่าง ๆ และโปรแกรมตรวจสอบและป้องกันไวรัสคอมพิวเตอร์ (Anti-virus Software) เป็นต้น

2.7 <u>การแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการขัดข้องหรือได้รับความเสียหายจากภัยคุกคาม</u>

กระบวนการแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการขัดข้องหรือได้รับความเสียหายจากภัยคุกคามหรือการลักลอบเข้าถึง ควรครอบคลุมถึง

1) การวิเคราะห์วิธีการคุกคามและลักลอบเข้าถึงข้อมูลที่อาจเกิดขึ้น รวมทั้งประเมินความเสียหายและผลกระทบจากเหตุการณ์ดังกล่าว

2) เมื่อตรวจพบปัญหาหรือความผิดปกติ ต้องรายงานผู้บริหารหรือผู้รับผิดชอบทันที

3) กำหนดผู้รับผิดชอบในการแก้ไขปัญหาหรือความผิดปกติ ซึ่งควรได้รับการฝึกฝนทั้งในด้านทักษะและความสามารถในการจัดการปัญหาต่าง ๆ ที่เกิดขึ้น

4) การจัดเตรียมข้อมูลและขั้นตอนการขอความช่วยเหลือในกรณีฉุกเฉินจากผู้เชี่ยวชาญทั้งจากภายในและภายนอกองค์กร โดยเฉพาะความช่วยเหลือทางเทคนิค

5) การสื่อสาร ชี้แจง และทำความเข้าใจกับพนักงาน สื่อมวลชน สมาชิก และผู้ใช้บริการอย่างรวดเร็วเกี่ยวกับปัญหาที่เกิดขึ้นและการแก้ไข เพื่อรักษาภาพพจน์และชื่อเสียงของบริษัทข้อมูลเครดิต รวมทั้งสร้างความเชื่อมั่นแก่เจ้าของข้อมูล สมาชิก และผู้ใช้บริการ

6) การรวบรวมหลักฐานต่าง ๆ ที่เป็นประโยชน์ในการดำเนินคดีกับผู้บุกรุก เช่น หลักฐานที่บันทึกการเข้าถึงข้อมูลและส่วนต่าง ๆ ของระบบให้บริการ เครื่องคอมพิวเตอร์ที่ผู้บุกรุกใช้เป็นเครื่องมือติดต่อสื่อสาร ข้อมูลที่แสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วัน เวลา และอื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสาร เป็นต้น

7) การจัดทำรายงานที่เป็นลายลักษณ์อักษร เพื่อเสนอต่อคณะกรรมการบริษัทข้อมูลเครดิต ทั้งนี้ คณะกรรมการบริษัทข้อมูลเครดิตอาจมอบหมายให้ผู้บริหารหรือทีมที่รับผิดชอบพิจารณารายงานดังกล่าวและดำเนินการต่อไป

รายงานที่จัดทำเป็นลายลักษณ์อักษรควรมีสาระสำคัญดังนี้

7.1) วัน เวลา และสถานที่ที่ระบบให้บริการได้รับความเสียหายจากภัยคุกคามหรือการลักลอบเข้าถึง

7.2) ลักษณะ วิธีการที่ใช้ในการลักลอบเข้าถึง และผู้บุกรุก (กรณีทราบ)

7.3) สาเหตุและลักษณะความเสียหายที่เกิดขึ้น โดยระบุถึงข้อมูลหรือระบบการให้บริการที่ได้รับความเสียหาย

7.4) การประเมินความเสียหายที่เกิดขึ้น

7.5) การแก้ไขปัญหาที่ได้ดำเนินการแล้วและแนวทางที่จะดำเนินการต่อไป

3. <u>กระบวนการเสริมการรักษาความปลอดภัยให้มีประสิทธิภาพ</u>

3.1 <u>การฝึกอบรมและให้ความรู้แก่พนักงาน</u>

บริษัทข้อมูลเครดิตควรจัดให้มีการพัฒนา ฝึกอบรมและให้ความรู้แก่ผู้บริหารและพนักงานทุกระดับที่เกี่ยวข้องกับการให้บริการอย่างต่อเนื่อง เพื่อให้ตระหนักถึงความปลอดภัยในการให้บริการและสามารถปฏิบัติตามนโยบายและกระบวนการรักษาความปลอดภัยได้อย่างมีประสิทธิภาพ นอกจากนี้ ผู้บริหารและพนักงานที่เกี่ยวข้องควรมีการติดตามพัฒนาการทางเทคโนโลยีและภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้นอย่างใกล้ชิด รวมทั้งเผยแพร่ข้อมูลที่เป็นประโยชน์แก่พนักงานอื่นในองค์กรด้วย

3.2 <u>การให้คำแนะนำแก่สมาชิกหรือผู้ใช้บริการ</u>

บริษัทข้อมูลเครดิตควรให้ข้อมูลและคำแนะนำที่เป็นประโยชน์แก่สมาชิกหรือผู้ใช้บริการ เช่น วิธีการใช้บริการอย่างปลอดภัย ข้อมูลทางเทคนิคหรือวิธีการรักษาความปลอดภัยเครื่องคอมพิวเตอร์และอุปกรณ์ที่สมาชิกหรือผู้ใช้บริการใช้ในการเข้าถึงข้อมูล คำแนะนำควรรวมถึง

การให้สมาชิกหรือผู้ใช้บริการระมัดระวังการใช้หรือดาวน์โหลดซอฟท์แวร์จากแหล่งที่ไม่เป็นที่รู้จักหรือน่าสงสัย เนื่องจากอาจมีโปรแกรมของผู้บุกรุกแฝงมาด้วย (โปรดดูรายละเอียดเพิ่มเติมในเรื่องแนวทางการให้คำแนะนำแก่สมาชิกหรือผู้ใช้บริการ)

การให้ข้อมูลและคำแนะนำดังกล่าวควรใช้ภาษาที่เข้าใจง่ายและเปิดเผยไว้บน Website ของบริษัทข้อมูลเครดิตโดยให้สมาชิกหรือผู้ใช้บริการสามารถเรียกดูได้โดยสะดวก และเพื่ออำนวยความสะดวกให้แก่สมาชิกหรือผู้ใช้บริการ บริษัทข้อมูลเครดิตอาจจัดให้มี Help Desk เพื่อทำหน้าที่ตอบปัญหาและให้คำแนะนำต่าง ๆ แก่สมาชิกหรือผู้ใช้บริการในการใช้บริการข้อมูลเครดิตด้วย นอกจากนี้ บริษัทข้อมูลเครดิตอาจจัดให้มีการฝึกอบรมสมาชิกหรือผู้ใช้บริการเพื่อสร้างความรู้ความเข้าใจเกี่ยวกับวิธีการรักษาความปลอดภัยในส่วนที่เกี่ยวข้องกับสมาชิกหรือผู้ใช้บริการ รวมทั้งระบบการรักษาความปลอดภัยของบริษัทข้อมูลเครดิตที่สมาชิกหรือผู้ใช้บริการควรทราบ ซึ่งเป็นการให้ความรู้และความมั่นใจในการใช้บริการข้อมูลเครดิตได้อีกทางหนึ่ง

3.3 <u>การควบคุมภายใน</u>

บริษัทข้อมูลเครดิตควรจัดให้มีกระบวนการควบคุมภายในที่เหมาะสมกับการให้บริการข้อมูลเครดิต อาทิ ระมัดระวังไม่ให้การให้บริการข้อมูลเครดิตขัดต่อกฎหมาย ทั้งในเรื่องของวิธีการดำเนินงานและเทคโนโลยีที่ใช้ มีการกำหนดขั้นตอน วิธีการปฏิบัติงาน การแบ่งแยกหน้าที่ และการควบคุมการปฏิบัติงานของพนักงานที่ชัดเจนและเหมาะสม รวมทั้งมีการบันทึกหลักฐานการปฏิบัติงานของพนักงาน และเก็บรักษาหลักฐานและเอกสารสำคัญเกี่ยวกับการให้บริการไว้อย่างปลอดภัย

แนวทางการให้คำแนะนำแก่สมาชิกหรือผู้ใช้บริการ

บริษัทข้อมูลเครดิตควรให้คำแนะนำที่เป็นประโยชน์แก่สมาชิกหรือผู้ใช้บริการเพื่อให้เข้าใจและตระหนักถึงความสำคัญของการรักษาความปลอดภัยในการใช้บริการ โดยควรรวมถึงคำแนะนำดังต่อไปนี้

1. แนะนำสมาชิกหรือผู้ใช้บริการไม่ให้เปิดเผยข้อมูลรหัสผู้ใช้งานและรหัสผ่านเพื่อการใช้งานให้บุคคลอื่นทราบ ไม่เขียนหรือจดรหัสไว้ในที่ที่เห็นได้ง่าย ทำลายเอกสารที่ใช้แจ้งรหัสผู้ใช้งานและรหัสผ่านเพื่อการใช้งาน รวมทั้งแนะนำสมาชิกหรือผู้ใช้บริการให้ระมัดระวังการถูกแอบอ้างหรือหลอกลวงให้เปิดเผยข้อมูลรหัสผู้ใช้งานและรหัสผ่านเพื่อการใช้งาน

2. แนะนำสมาชิกหรือผู้ใช้บริการเกี่ยวกับวิธีการกำหนดรหัสอย่างปลอดภัย มีการเปลี่ยนรหัสผ่านเพื่อการใช้งานเป็นประจำ และแนะนำให้สมาชิกหรือผู้ใช้บริการทราบถึงช่องทางในการแจ้งให้บริษัทข้อมูลเครดิตทราบทันทีที่พบว่าข้อมูลรหัสผู้ใช้งานและรหัสผ่านเพื่อการใช้งานเกิดปัญหา

3. แนะนำสมาชิกหรือผู้ใช้บริการให้รู้จักการรักษาความปลอดภัยเครื่องคอมพิวเตอร์ของตนเอง เช่น

- ติดตั้งและใช้งานโปรแกรมป้องกันไวรัสที่มีการปรับปรุงฐานข้อมูลไวรัสให้ทันสมัยและใช้บริการกรองไวรัสทางอินเตอร์เน็ตที่เชื่อถือได้
- มีการควบคุมการเข้าถึงข้อมูลส่วนตัว
- มีการเข้าและออกจากระบบให้บริการอย่างถูกต้อง
- ไม่ละทิ้งเครื่องคอมพิวเตอร์หรืออุปกรณ์ในระหว่างการเข้าถึงฐานข้อมูล และออกจากระบบให้บริการอย่างถูกต้องเมื่อเสร็จสิ้นการใช้บริการ
- ใช้เครื่องคอมพิวเตอร์และอุปกรณ์ที่เหมาะสมกับระบบการรักษาความปลอดภัยของบริษัทข้อมูลเครดิต
- หลีกเลี่ยงการใช้เครื่องคอมพิวเตอร์และอุปกรณ์ที่ไม่ได้มาตรฐานหรือมาจากแหล่งที่เชื่อถือไม่ได้
- หลีกเลี่ยงการติดตั้ง ดาวน์โหลด หรือใช้ซอฟท์แวร์จากแหล่งที่ไม่รู้จักหรือไม่สามารถตรวจสอบแหล่งที่มาได้ เนื่องจากระบบของสมาชิกหรือผู้ใช้บริการอาจได้รับโปรแกรมไวรัสหรือโปรแกรมอื่น ๆ ที่ผู้บุกรุกสามารถใช้ในการลักลอบเข้าถึงติดมาด้วย

4. ชี้แจงให้สมาชิกหรือผู้ใช้บริการทราบถึงขอบเขตความรับผิดชอบทั้งในส่วนของบริษัทข้อมูลเครดิตและในส่วนของสมาชิกหรือผู้ใช้บริการ