

นโยบายการรักษาความมั่นคงและความปลอดภัยของระบบการเก็บข้อมูลส่วนบุคคลด้าน IT

1 ระบุชื่อ ที่เรียกระบบการเก็บข้อมูลลูกค้าและการทำธุรกรรมของลูกค้า

2 ระบุประเภทรูปแบบของข้อมูลลูกค้าและธุรกรรมที่จัดเก็บในระบบข้อ 1

3 ระบุแหล่งเก็บ Back up (แหล่งที่สำรองเก็บข้อมูล)

4 ระบุมาตรฐานของระบบการเก็บข้อมูล ข้อ 1 และ 3 (มีมาตรฐานอะไรรับรองหรือไม่)

5 มีมาตรการป้องกันมิให้บุคคลภายนอก เจาะเข้าระบบเพื่อดึงข้อมูลออกไปโดยไม่ได้รับอนุญาตหรือไม่ และให้ระบุโอกาสที่จะมีบุคคลภายนอก เจาะเข้าระบบเพื่อดึงข้อมูลของลูกค้าออกไป (ระดับที่ 1-5 : โอกาสที่ถูกเจาะข้อมูลได้ง่ายที่สุด คือ ระดับ 1 โอกาสที่ถูกเจาะข้อมูลยากที่สุด 5)

6 ระบุ การแจ้งเตือนของระบบ เมื่อถูก Hacker เจาะเข้าระบบ จะได้รับการแจ้งเตือนจากระบบหรือไม่ และ หากมีการแจ้งเตือน จะทราบภายใน ชั่วโมง หรือ.... วัน

7 กรณีที่ถูกเจาะเข้าระบบโดยไม่ได้รับอนุญาต สามารถระงับหรือแก้ไขจัดการการ Hack เข้าระบบได้ภายในชม. หรือ วัน

8 มีมาตรการด้าน IT ในการแยกข้อมูล ชื่อ หมายเลขประจำตัว ออกจากข้อมูลอื่นๆของลูกค้า เพื่อมิให้ระบุข้อมูลส่วนบุคคลของลูกค้าได้หรือไม่

นโยบายการปฏิบัติหรือการดำเนินการเมื่อข้อมูลส่วนบุคคลถูกเผยแพร่หรือนำไปใช้โดยไม่ได้รับอนุญาตหรือถูกละเมิดจากเหตุต่างๆ

หากข้อมูลของลูกค้า ถูกเจาะและนำออกไปเผยแพร่ มีวิธีการทาง IT ในการแก้ไขหรือดำเนินการอย่างไรในทาง IT เพื่อแก้ไขการละเมิดข้อมูลดังกล่าว

นโยบายในการรักษาความลับ การจัดชั้นความลับในการเข้าถึงข้อมูลส่วนบุคคล

1 มีชั้นความลับในการเข้าถึง (เข้าดู) ข้อมูลลูกค้าและการทำธุรกรรมของลูกค้า หรือไม่ (ถ้ามี อธิบายว่า ใครเข้าถึงได้บ้าง การเข้าถึงต้องใช้รหัสประจำตัวของใครบ้าง)

2 มีชั้นความลับในการแก้ไข เปลี่ยนแปลง ปริ๊นท์ ลบ ข้อมูลของลูกค้าและการทำธุรกรรมของลูกค้าหรือไม่(ถ้ามี อธิบายว่า ใครทำได้บ้าง การแก้ไข เปลี่ยนแปลง ลบหรือปริ๊นท์ ต้องใช้รหัสประจำตัวของใครบ้าง)

3 หากมีบุคลากรตามข้อ 1 และ 2 เข้าถึงหรือดำเนินการกับข้อมูลลูกค้า ระบบมีการแจ้งเตือน หรือ มีการบันทึกไว้หรือไม่ ว่าใครดำเนินการอย่างไรกับข้อมูลของลูกค้าบ้าง และใครเป็นผู้ทราบถึงการแจ้งเตือน

4 มีกฎหรือระเบียบ ห้ามพนักงานดำเนินการกับข้อมูลลูกค้า โดยไม่ได้รับอนุญาต หรือไม่ (บทลงโทษพนักงานที่ละเมิดข้อมูลลูกค้า เป็นต้น)

นโยบายเกี่ยวกับข้อมูลส่วนบุคคลที่อาจเผยแพร่ผ่านโซเชียลเน็ตเวิร์ค

1 คอมพิวเตอร์ของบริษัทฯ สามารถเข้าเครือข่ายโซเชียลได้หรือไม่ (ไม่ได้เลย หรือจำกัดเวลาเข้า)

2 พนักงานสามารถนำคอมพิวเตอร์ของบริษัทฯกลับบ้านได้หรือไม่

3 พนักงานสามารถใช้โทรศัพท์ที่มีแอปพลิเคชัน โซเชียลเน็ตเวิร์ค ระหว่างการปฏิบัติงานหรือไม่

4 มีการตรวจสอบการใช้โซเชียลเน็ตเวิร์คของพนักงานหรือไม่ (เช่น การโพสต์ที่ไม่สุภาพ หรือการนำข้อมูลลูกค้าไปเผยแพร่ บริษัทฯจะมีโอกาสทราบหรือไม่)

5 มีกฎ ระเบียบ เกี่ยวกับขอบเขตการใช้โซเชียลเน็ตเวิร์คสำหรับพนักงานหรือไม่

6 มีกฎ ระเบียบ ห้ามพนักงานนำข้อมูลของลูกค้า ไปเผยแพร่ หรือห้ามนำข้อมูลลูกค้าออกจากคอมพิวเตอร์หรือระบบของบริษัทฯหรือไม่