นโยบายความเป็นส่วนตัวและความปลอดภัยของข้อมูล
(Data Privacy & Security Policy)

บริษัท ซีพี ออลล์ จำกัด (มหาชน) และบริษัทย่อย (ซึ่งต่อไปจะใช้คำว่า “บริษัท”) มีความมุ่งมั่นในการดำเนินธุรกิจอย่างยั่งยืนบนพื้นฐานของความรับผิดชอบต่อการบริหารจัดการด้านการรักษาข้อมูลความเป็นส่วนตัว และปฏิบัติตามกฎระเบียบต่างๆ รวมถึงการควบคุมดูแลอย่างเข้มงวด เพื่อรักษาความปลอดภัยข้อมูลสารสนเทศของลูกค้า

1) ข้อมูลส่วนบุคคล

บริษัทยึดมั่นที่จะให้บริการความสะดวกกับทุกชุมชนสร้างผลกระทบเชิงบวกต่อชีวิตของลูกค้าและผู้คนโดยรอบโดยมีเป้าหมายหลักด้วยการสร้างสรรค์สินค้าและบริการที่เพิ่มคุณค่าให้กับลูกค้าครบวงจรเพื่อตอบสนองความต้องการของทุกกลุ่มลูกค้าด้วยเหตุนี้ บริษัทจึงต้องรวบรวมข้อมูลลูกค้าให้รับรู้และเข้าใจผู้บริโภคให้ดีขึ้นและสามารถนำข้อมูลดังกล่าวไปใช้ในการดำเนินงาน

อย่างไรก็ดีบริษัทตระหนักดีว่าการปกป้องข้อมูลส่วนบุคคลของลูกค้าเป็นเรื่องสำคัญและบริษัทก็เคารพความเป็นส่วนตัวของลูกค้าเช่นกันจึงได้กำหนดเป้าหมายในการบริหารจัดการข้อมูลลูกค้าด้วยความโปร่งใส

นโยบายด้านการรักษาข้อมูลและด้านความปลอดภัยของข้อมูลจะครอบคลุมตั้งแต่ช่องทางการจัดเก็บข้อมูลรูปแบบของข้อมูลที่จัดเก็บวัตถุประสงค์ที่บริษัทนำข้อมูลไปใช้การเปิดเผยข้อมูลแก่บุคคลที่สามตลอดจนวิธีการที่บริษัทดำเนินการปกป้องข้อมูลลูกค้าทั้งนี้ขอบเขตของนโยบายนี้มีผลบังคับใช้กับบริษัทในกลุ่มซีพี ออลล์และบริษัทคู่สัญญาทุกบริษัทของกลุ่มซีพี ออลล์

ช่องทางการจัดเก็บข้อมูล
ข้อมูลส่วนบุคคลของลูกค้าที่บริษัทจัดเก็บมีดังนี้

- ☐ เมื่อลูกค้าสมัครใช้บริการของกลุ่มซีพี ออลล์
- ☐ เมื่อลูกค้าใช้บริการของกลุ่มซีพี ออลล์
- ☐ เมื่อลูกค้าติดต่อกับศูนย์บริการลูกค้าของกลุ่มซีพี ออลล์
- ☐ เมื่อลูกค้าตอบรับคำร้องขอของกลุ่มซีพี ออลล์
- ☐ เมื่อลูกค้าเข้าร่วมโครงการและกิจกรรมต่างๆของกลุ่มซีพี ออลล์
- ☐ เมื่อลูกค้าใช้สิทธิประโยชน์ตามโครงการความจงรักภักดีต่อกลุ่มซีพี ออลล์ อาทิ7Eleven Card, 7Eleven Member point

รูปแบบของข้อมูลที่จัดเก็บ

ข้อมูลที่บริษัทจัดเก็บจากลูกค้าสามารถแบ่งออกได้เป็นดังนี้

- ข้อมูลส่วนบุคคลเช่นชื่อวันเกิด เลขที่บัตรประชาชนที่อยู่และข้อมูล การเข้าถึงเว็บไซต์ และ เว็บคุ๊กกี้ วิธีการใช้ข้อมูลของท่าน
- ข้อมูลการใช้บริการเช่นข้อมูลเกี่ยวกับการสั่งซื้อ และการออกใบเสร็จ / ใบกำกับภาษีเป็นต้น
- ข้อมูลการใช้บริการและเลขหมายที่ใช้ติดต่อกับบริษัทผ่านช่องทางติดต่อต่างๆเช่นศูนย์บริการทางโทรศัพท์และอีเมล์รวมถึงคำถามหรือบริการที่ลูกค้าร้องขอ
- ข้อมูลสิทธิประโยชน์สำหรับลูกค้าเช่นการใช้สิทธิประโยชน์ในโครงการความจงรักภักดีสินค้าและบริการราคาพิเศษและช่องทางพิเศษในการติดต่อสอบถามกับบริษัท

การนำข้อมูลไปใช้งาน

- เพื่อการประมวลข้อมูลภายในองค์กร ในการดำเนินการเช่นสร้างออเดอร์ลูกค้าและชำระเงินการส่งมอบและการให้บริการสินค้า
- การค้นคว้าวิจัยทางการตลาดเพื่อทำความเข้าใจความต้องการของลูกค้าเพื่อที่จะนำไปออกแบบสินค้าและบริการให้ตรงกับความต้องการของลูกค้า
- นำเสนอสินค้ารางวัลและสิทธิประโยชน์ใหม่ๆในรูปแบบที่ลูกค้าสนใจและเป็นสิ่งที่เกี่ยวข้องกับลูกค้า

การเปิดเผยข้อมูลแก่บุคคลที่สาม

บริษัทไม่มีการให้ข้อมูลของท่านแก่ บริษัท องค์กร และ บุคคล อื่นๆ ภายนอกบริษัท ยกเว้นในกรณีต่างๆ ดังต่อไปนี้

- ได้รับการอนุญาตจากท่าน
- สำหรับการประมวลผลภายนอก และบริษัทคู่ค้าทางธุรกิจซึ่งให้บริการแก่ท่าน
- สำหรับเหตุผลทางกฎหมาย

การปกป้องข้อมูล

บริษัทยึดมั่นในเรื่องการปกป้องความปลอดภัยของข้อมูลอย่างสูงสุดและมีการนำมาตรฐานต่างๆมาใช้อย่างมีประสิทธิภาพดังนี้

- นำระบบดูแลรักษาความปลอดภัยทางเทคนิคที่เข้มงวดเข้ามาปกป้องการนำข้อมูลไปใช้ในทางที่ผิด
- จำกัดสิทธิการเข้าถึงระบบข้อมูลที่เข้มงวดและกำหนดขั้นตอนการขออนุมัติสิทธิในการเข้าถึงข้อมูลของกับพนักงานอย่างเคร่งครัด

- จัดให้มีการลงนามรักษาความลับทุกครั้งก่อนอนุมัติให้สิทธิในการเข้าถึงข้อมูลลูกค้า
- สร้างความตระหนักด้านความปลอดภัยข้อมูลให้กับบุคลากรทุกระดับ และกำหนดบุคลากรที่ดูแลด้านระบบข้อมูลโดยเฉพาะ

บริษัทมุ่งมั่นในการบริหารจัดการด้านการปกป้องข้อมูลลูกค้าสูงสุดจึงได้นำมาตรฐานในการพัฒนาและรักษามาตรการด้านความปลอดภัยของข้อมูลลูกค้ามาใช้และปฏิบัติตามแนวทางมาตรฐานดังกล่าวโดยบริษัทได้รับการรับรองมาตรฐานด้านการให้บริการไอทีอย่างมีคุณภาพ (ISO/IEC 20000), ได้รับการรับรองมาตรฐานด้านระบบการบริหารความปลอดภัยของข้อมูล และศูนย์คอมพิวเตอร์(ISO/IEC 27001)และได้รับการรับรองมาตรฐานด้านความปลอดภัยของข้อมูลบัตรชำระเงิน (PCI DSS) โดยทั้งสามมาตรฐานดังกล่าวมีการตรวจสอบทั้งภายในและภายนอกเป็นประจำเพื่อให้ลูกค้ามั่นใจในระบบที่มีประสิทธิภาพของบริษัทและเชื่อมั่นได้ว่าข้อมูลของลูกค้าจะได้รับการดูแลปกป้องจากกลุ่มซีพี ออลล์

การเคารพความเป็นส่วนตัวของลูกค้า

บริษัทให้ความสำคัญอย่างมากกับการเคารพความเป็นส่วนตัวของลูกค้าโดยลูกค้าสามารถเลือกที่จะไม่รับบริการข้อมูลทางการตลาดได้ทุกช่องทางการติดต่อและเมื่อปฏิเสธการรับข้อมูลดังกล่าวลูกค้าจะยังคงได้รับข้อมูลที่เกี่ยวเนื่องกับบริการเช่นการแจ้งเตือนเรื่องการบริการเช่นเดิม

2) ความปลอดภัยของข้อมูล

บริษัทยึดมั่นเรื่องระบบคุณภาพที่ใช้ในการบริหารความมั่นคงปลอดภัยสำหรับสารสนเทศ (InformationSecurity Management: ISM) โดยปฏิบัติตามมาตรฐาน ISO/IEC 27001, ISO/IEC20000, PCIDSSอย่างเคร่งครัดภายใต้การกำกับดูแลของคณะกรรมการบริหารความเสี่ยงองค์กร(Risk Management Steering Committee)โดยมีประธาน และคณะกรรมการบริหารความเสี่ยงองค์กรซึ่งประกอบด้วยผู้บริหารที่ดูแลด้านInformation Technology Operations และผู้บริหารด้าน Information Technology Security

บริษัทมีนโยบายด้านความปลอดภัยของข้อมูลที่ช่วยให้การดำเนินธุรกิจและการให้บริการลูกค้าของบริษัทเป็นไปอย่างมีเสถียรภาพซึ่งมีนโยบายหลักด้วยกัน 10นโยบายครอบคลุมลูกค้าผู้รับเหมาคู่ค้าธุรกิจผู้ให้บริการและบริษัทในเครือดังนี้

1. โครงสร้างการจัดการความมั่นคงปลอดภัยของข้อมูล มีหน่วยงานผู้รับผิดชอบในการบริหารและดูแลด้านความมั่นคงปลอดภัยของข้อมูลซึ่งทำหน้าที่ กำหนดมาตรการส่งเสริมความมั่นคงปลอดภัยของข้อมูลสำหรับทั้งกลุ่มบริษัทฯ

2. จัดการทรัพย์สินทางข้อมูลกำหนดจัดระเบียบและแบ่งประเภททรัพย์สินทางข้อมูลที่ควรคุ้มครอง ตรวจสอบระดับความสำคัญของแต่ละทรัพย์สิน และจัดการอย่างเหมาะสมตามรูปแบบการบันทึกทรัพย์สินทางข้อมูลนั้น ๆ
3. การจัดการระบบข้อมูลดำเนินมาตรการต่อไปนี้ต่อระบบข้อมูลทั้งหมดที่ใช้งานทรัพย์สินทางข้อมูล เพื่อให้การใช้งานอุปกรณ์ประมวลผลข้อมูลที่ใช้จัดการทรัพย์สินทางข้อมูลมีความถูกต้องแม่นยำ และทำงานโดยรักษาไว้ซึ่งความปลอดภัย
    (1) การจัดการเครือข่าย
    (2) การจัดการระบบ
    (3) การจัดการข้อมูล
    (4) การจัดการข้อบกพร่อง
    (5) การจัดการการเปลี่ยนแปลง
    (6) การจัดการประวัติข้อมูลการใช้งาน (log)
4. การจัดการสิ่งแวดล้อมทางกายภาพบริษัทมีการจัดเก็บข้อมูลในศูนย์คอมพิวเตอร์ที่เป็นเจ้าของ ซึ่งมีการบริหารพื้นที่ และจัดประเภทของพื้นที่ตามระดับความสำคัญ เพื่อให้แน่ใจว่าสินทรัพย์ข้อมูลอยู่ภายใต้การควบคุมที่เหมาะสม
5. การจัดการทรัพยากรมนุษย์กำหนดมาตรการจัดการการฝึกอบรม เรียนรู้และใช้งานระบบข้อมูล และปฏิบัติตามระเบียบเกี่ยวกับทรัพย์สินทางข้อมูลและความมั่นคงปลอดภัยของข้อมูล รวมถึงนโยบายนี้อย่างเคร่งครัด เพื่อให้แน่ใจว่าผู้บริหาร พนักงาน พนักงานชั่วคราว และทุกคนที่ใช้งานทรัพย์สินทางข้อมูลของบริษัทฯ ปฏิบัติงานโดยมีความเข้าใจในกฎการใช้งานและตระหนักถึงความรับผิดชอบในการใช้งานความมั่นคงปลอดภัยของข้อมูล ตั้งแต่ก่อนจ้างตลอดจนสิ้นสุดการจ้าง และส่งเสริมพัฒนาบุคลากรที่ดูแลระบบไอทีให้มีความเชี่ยวชาญ และทันต่อภัยคุกคามทางไซเบอร์ใหม่ๆ
6. การจัดการการจ้างบริษัทภายนอก (เอาท์ซอร์สซิ่ง)ในการว่าจ้างบริษัทภายนอกให้ปฏิบัติงานซึ่งมีความเกี่ยวข้องกับการใช้งานทรัพย์สินทางข้อมูล ให้ควบคุมจัดการโดยทำสัญญาว่าด้วยการรักษาความลับ และกำหนดขอบเขตความรับผิดชอบที่บริษัทภายนอกผู้รับจ้างควรปฏิบัติตามอย่างเคร่งครัดให้ชัดเจน เพื่อให้สามารถคุ้มครองทรัพย์สินทางข้อมูลของบริษัท
7. การจัดการการปฏิบัติตามกฎ (คอมไพลแอนซ์)บริษัทกำหนดมาตรการด้านการใช้ทรัพย์สินทางข้อมูลที่ถูกต้องตามลิขสิทธิ์ และปฏิบัติตามกฎหมายของแต่ละประเทศอย่างเคร่งครัด เพื่อเลี่ยงการกระทำผิดเงื่อนไขใด ๆ ด้านความมั่นคงปลอดภัย รวมถึงการกระทำผิดหน้าที่ตามสัญญาและกฎระเบียบทางกฎหมายเกี่ยวกับความมั่นคงปลอดภัยของข้อมูล
8. การจัดการภัยคุกคามทางไซเบอร์กำหนดแผนและวางโครงสร้างการรับมือภัยคุกคามทางไซเบอร์ เพื่อให้สามารถดำเนินการจัดการภัยคุกคามทางไซเบอร์ที่อาจกระทบต่อความมั่นคงปลอดภัยของ

ข้อมูล รวมถึงการแจ้งเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยทั้งหมด อาทิ ข้อมูลรั่วไหลเนื่องจากติดไวรัส การหลอกล่วงเข้าถึงข้อมูล การโจมตีจากภัยคุกคามต่างๆ ได้อย่างมีประสิทธิภาพและสม่ำเสมอ

9. การจัดการความต่อเนื่องทางธุรกิจกำหนดมาตราการรองรับการทำงานที่ต่อเนื่อง ทั้งการสำรองข้อมูล การออกแบบระบบให้พร้อมต่อการใช้งาน และให้บริการลูกค้า จัดทำแผน การฝึกซ้อมและโครงสร้างการรายงานเกี่ยวกับความต่อเนื่องทางธุรกิจเพื่อรองรับกรณีภัยพิบัติต่างๆ ให้ระบบสามารถพร้อมให้บริการ และดำเนินกิจกรรมทางธุรกิจรวมถึงกระบวนการทำงานที่สำคัญได้โดยเร็ว
10. การประเมินผลและตรวจสอบบริษัทมีการประเมินผลหรือตรวจสอบเป็นระยะ ทั้งจากผู้ตรวจสอบภายในและภายนอก เพื่อประเมินสถานะและความมั่นคงปลอดภัยของข้อมูลว่ายังคงเหมาะสมหรือต้องปรับเพิ่มเพื่อลดความเสี่ยง และวางแผนการพัฒนาและรักษาไว้ซึ่งการจัดการความมั่นคงปลอดภัยของข้อมูลต่อไป

การรักษาความปลอดภัยของข้อมูลส่วนบุคคลของลูกค้าเป็นเรื่องที่พนักงานทุกคนให้ความสำคัญโดยการรักษาเป็นความลับและไม่นำข้อมูลไปแจกจ่ายโดยพลการหากพนักงานคนใดไม่ปฏิบัติตามจะมีมาตรการลงโทษตามข้อกำหนดที่ระบุไว้ในระเบียบข้อบังคับในการทำงาน