มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
บริษัท ทีบีเคเค (ประเทศไทย) จำกัด

มาตรการฉบับนี้กำหนดรายละเอียดเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่อยู่ในความรับผิดชอบของบริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เพื่อให้ข้อมูลส่วนบุคคลมีความปลอดภัยบนพื้นฐานของการธำรงไว้ซึ่งความลับ (**Confidentiality)** ความถูกต้องครบถ้วน (**Integrity**) และสภาพพร้อมใช้งาน (**Availability**) ตามข้อกำหนดและสอดคล้องกับพรบ.คุ้มครองข้อมูลส่วนบุคคล ดังนี้

1. มาตรการเชิงองค์กร (Organizational measures)

1. บริษัทฯ จะกำกับ ตรวจสอบ มอบหมาย ติดตามการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของกฎหมาย และรักษาความปลอดภัยของข้อมูลส่วนบุคคลในแง่ของความลับ ความถูกต้องและความพร้อมใช้งานของข้อมูลส่วนบุคคล
2. บริษัทฯ จะแจ้งนโยบาย แนวปฏิบัติ และมาตรการคุ้มครองข้อมูลส่วนบุคคลให้พนักงานรับทราบและปฏิบัติ
3. บริษัทฯ จะฝึกอบรมและให้ความรู้พนักงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นประจำปีทุกปี
4. บริษัทฯ จะกำหนดสิทธิการเข้าถึงและจัดทำสัญญารักษาความลับกับบุคคลที่จำเป็นต้องทราบข้อมูลส่วนบุคคล
5. บริษัทฯ จะดำเนินการทบทวนความสอดคล้องของมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลอย่างสม่ำเสมอเมื่อมีความจำเป็นหรือการเปลี่ยนแปลงของเทคโนโลยี ตามมาตรฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคล
6. บริษัทฯ จะดำเนินการให้ผู้ประมวลผลข้อมูลส่วนบุคคลที่บริษัทฯ มอบหมายมีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลตามมาตรฐานขั้นต่ำตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

2. มาตรการเชิงเทคนิค (Technical measures)

เพื่อความปลอดภัยของข้อมูลส่วนบุคคลที่อยู่ในระบบสารสนเทศหรือรูปแบบอิเล็กทรอนิกส์ ได้แก่ ความปลอดภัยของระบบและอุปกรณ์จัดเก็บข้อมูลส่วนบุคคล ความปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ความปลอดภัยของเครื่องคอมพิวเตอร์ลูกข่าย (Clients) และอุปกรณ์ต่าง ๆ ที่ใช้ ความปลอดภัยของระบบเครือข่าย ความปลอดภัยของซอฟแวร์และแอปพลิเคชั่น บริษัทฯ จึงกำหนดมาตรการแนวปฏิบัติดังนี้

1. ข้อมูลส่วนบุคคลจะต้องได้รับการจัดเก็บไว้ในอุปกรณ์บันทึกข้อมูลที่มีความปลอดภัยและมีการเข้ารหัส (**Encryption)**

2. บริษัทฯ ไม่อนุญาตให้ใช้อุปกรณ์บันทึกข้อมูล เช่น **Hard disk, External drive, Thumb Drive** จัดเก็บข้อมูลส่วนบุคคล ยกเว้นอุปกรณ์นั้นจะได้รับการตรวจสอบและอนุญาตจากฝ่ายบริหารทั่วไป โดยหากอุปกรณ์บันทึกข้อมูลนั้นจัดเก็บข้อมูลส่วนบุคคลจะต้องได้รับการเข้ารหัส
3. พนักงานที่ใช้งานเครื่องคอมพิวเตอร์แบบพกพา หรืออุปกรณ์ที่สามารถเคลื่อนย้ายได้จะต้องไม่วางอุปกรณ์เหล่านี้ทิ้งไว้โดยไม่ได้รับการดูแล นอกเสียจากว่า อุปกรณ์เหล่านี้จะได้รับการผูกติดอยู่กับสิ่งที่เคลื่อนไหวได้ยาก เช่น โต๊ะทำงาน หรือเก็บไว้ในตู้หรือลิ้นชักที่ได้รับการล็อค
4. บริษัทฯ ไม่อนุญาตให้พนักงานใช้งานอุปกรณ์บันทึกข้อมูล เว้นแต่อุปกรณ์นั้นจะได้รับอนุญาตจากฝ่ายบริหารทั่วไป และเมื่อใดก็ตามที่ข้อมูลส่วนบุคคลถูกจัดเก็บอยู่ใน **External Hard Disk, Thumb Drive** อุปกรณ์บันทึกข้อมูลเลหล่านี้จะต้องถูกจัดเก็บอย่างปลอดภัยและถูกล็อคไว้ในที่เก็บเอกสารที่มีระบบการล็อค
5. พนักงานจะต้องระมัดระวังไม่ให้ข้อมูลส่วนบุคคลถูกเปิดเผยโดยไม่เจตนาต่อบุคคลที่ไม่มีความจำเป็นที่จะต้องใช้ข้อมูลนั้น ๆ พนักงานทุกคนต้องจัดเก็บข้อมูลสำคัญไว้ในบริเวณที่ทำงานซึ่งไม่มีบุคคลภายนอกหรือบุคคลที่ไม่ได้รับอนุญาตอยู่ในบริเวณนั้น ในกรณีที่บุคคลที่ไม่ได้รับอนุญาตอยู่ในบริเวณที่สามารถเห็นหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์แสดงผลได้ ผู้ใช้ข้อมูลจะต้องใช้ **Screen Saver, Log-off** หรือดำเนินการใด ๆ ที่เกิดผลแบบเดียวกัน และเครื่องคอมพิวเตอร์ที่จัดเก็บข้อมูลสำคัญจะต้องมีการกำหนดพาสเวิร์ด (**Password)** เพื่อใช้ในการเข้าถึงข้อมูล
6. สำหรับสิทธิในการเข้าถึงข้อมูลส่วนบุคคลจากภายนอก เช่น การทำงานจากที่บ้าน จะต้องได้รับการพิจารณาจากผู้จัดการฝ่ายบริหารทั่วไปก่อนที่พนักงานจะสามารถเริ่มการใช้งานข้อมูลจากภายนอกได้ และในการทำงานนอกสถานที่ พนักงานจะต้องใช้ความระมัดระวังเพื่อป้องกันทรัพย์สินต่าง ๆ ของบริษัทฯ ทั้ง **Hardware** และ **Software** จากการถูกขโมย การสูญหาย เป็นต้น รวมถึงต้องใช้อุปกรณ์ที่ได้รับอนุญาตจากบริษัทฯ เท่านั้น
7. ห้ามพนักงานนำอุปกรณ์คอมพิวเตอร์ส่วนตัวหรืออุปกรณ์ที่ไม่ใช่ทรัพย์สินของบริษัทฯ มาใช้ทำงานที่บริษัทฯ เว้นแต่ได้รับอนุมัติจากบริษัทฯ
8. ห้ามพนักงานนำ **Email** ส่วนตัว เช่น **GMAIL** หรือ **Outlook** มาใช้งานแทน **Email** ของบริษัทฯ รับ-ส่งข้อมูลในการทำงานของบริษัทฯ หรือใช้สื่อสารภายในและบุคคลภายนอกบริษัทฯ
9. ห้ามพนักงานเปิดเผย **Password** ให้แก่บุคคลอื่นทั้งภายในและภายนอกบริษัทฯ และพนักงานจะต้องเปลี่ยน **Password** ทุก ๆ **3** เดือนตามระเบียบของบริษัทฯ
10. การเข้าถึงระบบต่าง ๆ จะต้องใช้ **User-IDs** และ **Password** ที่สามารถระบุตัวตนได้ เพื่อป้องกันบริษัทจากการใช้งานที่ไม่ได้รับอนุญาต และห้ามพนักงานทำงาน **Share Password** ของตนเองให้กับผู้อื่น
11. ในกรณีที่พนักงานไม่ได้ใช้เครื่อง **Computer** จะต้องทำการ **Enable Password Protection** จะมี **Screen Saver** ขึ้นมาบนหน้าจอ ซึ่งจะทำให้ผู้ที่ไม่ได้รับอนุญาต ไม่สามารถเห็นข้อมูลที่อยู่บนจอได้

12. หลังการพิมพ์แล้วข้อมูลส่วนบุคคลจะต้องไม่ถูกทิ้งไว้ที่เครื่อง **Printer**

13. การพยายามเข้าถึงระบบ โดยไม่ได้รับอนุญาต (**Hacking)** การพยายามคาดเดา **Password** การพยายามถอดรหัส (**File Decryption)** การลักลอบสำเนาข้อมูล หรือการใด ๆ ที่กระทบต่อความปลอดภัยของระบบจะถือเป็นการกระทำผิดวินัยขั้นร้ายแรง

14. พนักงานที่ต้องการขอ **User IDs** หรือปรับเปลี่ยนสิทธิในการใช้งาน จะต้องส่งเอกสาร/แบบการขอใช้สิทธิเพื่อขออนุมัติจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (**Data Protection Officer : DPO)**

15. ผู้ดูแลระบบจะต้องไม่ให้สิทธิในการเข้าถึงแก่พนักงานหรือผู้ใดผู้หนึ่ง หากไม่ขออนุญาตตามขั้นตอน

16. หากมีการโยกย้ายปรับเปลี่ยนตำแหน่งของพนักงาน สิทธิในการเข้าถึงระบบต่าง ๆ จะต้องเปลี่ยนไปตามตำแหน่งงานใหม่ของพนักงานนั้น ๆ และจะต้องมีการตรวจสอบสิทธิ์และการเข้าถึงระบบเป็นประจำทุกเดือนโดยฝ่ายเทคโนโลยีสารสนเทศ**(IT**)

17. ในกรณีที่พนักงานสิ้นสุดสัญญาจ้างแรงงานด้วยเหตุใด ๆ จะต้องคืนทรัพย์สินทุกอย่างของบริษัทฯ และสิทธิในการเข้าถึงระบบต่าง ๆ จะถูกยกเลิกโดยทันที

18. เครื่องคอมพิวเตอร์ของพนักงานจะต้องติดตั้งโปรแกรม **Anti-Virus** และพนักงานจะต้อง **Update** เวอร์ชั่นอย่างสม่ำเสมอตามระเบียบของบริษัทฯ

19. การใช้งานระบบเทคโนโลยีสารสนเทศต่าง ๆ จะต้องได้รับการป้องกันผ่านการใช้ **Firewall** ตลอดเวลาที่มีการเชื่อมต่อบน **Internet** ตามที่บริษัทฯ กำหนด

20. บริษัทฯ กำหนดมาตรการป้องกันเชิงลึกเพื่อความปลอดภัยของข้อมูลส่วนบุคคลด้วยมาตรการป้องกันหลายชั้น (**Multiple layers of security control)** ในกรณีดังต่อไปนี้

i. การค้นหาและจำแนกประเภทของข้อมูล แล้วจัดลำดับความสำคัญ เพื่อให้สามารถกำหนดนโยบายเพื่อควบคุมการเข้าถึงข้อมูลเหล่านั้นได้อย่างถูกต้อง

ii. บริหารจัดการสิทธิ์ในการเข้าถึงข้อมูลประเภทต่างๆ

iii. เฝ้าระวังและติดตามการเข้าถึงข้อมูล ป้องกันการโจมตี การเข้าถึงที่ไม่มีสิทธิ์ และการขโมยข้อมูล

iv. จัดเก็บบันทึกการเข้าถึงข้อมูลสำหรับยืนยันการปฏิบัติตามข้อกำหนดและข้อบังคับขององค์กร

v. ปกป้องข้อมูล เพื่อให้มั่นใจว่าข้อมูลถูกเก็บเป็นความลับ และไม่ถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

vi. เสริมสร้างความตระหนักรู้ถึงความมั่นคงปลอดภัยและความพร้อมในการรับมือกับภัยคุกคาม

21. บุคคลภายนอก (**Visitor)** ที่ได้รับอนุญาตให้เข้าห้องเก็บข้อมูลจะต้องลงทะเบียนตามระบบของบริษัทฯ และจะต้องได้รับการดูแลโดยพนักงานฝ่ายเทคโนโลยีสารสนเทศ**(IT)**ตลอดเวลา

22. ให้หน่วยงานตรวจสอบภายใน**(Internal Audit)** ดำเนินการตรวจสอบอย่างน้อยต้องครอบคลุมที่ระบุในมาตรการข้างต้นอย่างน้อยปีละครั้ง

3. มาตรการเชิงกายภาพ (Physical measures)

3.1 มาตรการการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบหรือเปิดเผยข้อมูล

3.1.1 การควบคุมการเข้าถึง (Access control)

i. ให้ผู้จัดการ/หัวหน้างานกำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคลตามหลักเท่าที่จำเป็น (need-to-know basis) และหลักให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (principle of least privilege) ตามแนวปฏิบัติเกี่ยวกับมาตรการดำเนินการตามระดับความเสี่ยง

ii. การเข้าถึงข้อมูลส่วนบุคคลที่จัดเก็บในระบบสารสนเทศ จะต้องกำหนดวิธีการพิสูจน์และยืนยันตัวตนเพื่อป้องกันการสวมสิทธิ เช่น การกำหนด password โดยเฉพาะการเข้าถึงข้อมูลจากทางไกล (remote)

3.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

i. การลงทะเบียนผู้ใช้งานระบบสารสนเทศของบริษัท ให้ดำเนินการดังนี้

- ต้องเป็นเครื่องคอมพิวเตอร์ ที่ได้รับการลงทะเบียนกับทางบริษัทเท่านั้น
- ในการเข้าถึงข้อมูลจะต้องมีการกำหนดสิทธิ์เพื่ออนุญาตในการเข้าถึงเท่านั้น
- หากลืมรหัสผ่านหรือ ต้องการเปลี่ยนสิทธิ์การเข้าถึง ต้องร้องขอมายังหน่วยงานที่ดูแลเท่านั้น

ii. ให้หน่วยงานเทคโนโลยีสารสนเทศ ถอนสิทธิผู้ใช้งานตามระเบียบบริษัทฯ หรือเข้าเงื่อนไขใดเงื่อนไขหนึ่งดังต่อไปนี้

- หากมีการเปลี่ยนแปลงโอนย้ายหน้าที่ หรือหน่วยงาน
- หากผู้ใช้งานนั้นได้พ้นสภาพการเป็นพนักงานไปแล้ว

iii. ข้อมูลส่วนบุคคลที่เป็นความลับหรือมีความเสี่ยงหรือเสี่ยงสูง จะต้องกำหนดระบบพิสูจน์ตัวตนผู้ใช้งานอย่างเข้มงวดตามแนวปฏิบัติเกี่ยวกับมาตรการดำเนินการตามระดับความเสี่ยง

iv. ให้หน่วยงานเทคโนโลยีสารสนเทศ (IT) ทบทวนสิทธิของผู้ใช้งานระบบสารสนเทศ ในกรณีดังต่อไปนี้

- มีการร้องขอเปลี่ยนรหัสผ่าน
- มีการเปลี่ยนแปลงโอนย้ายหน้าที่หรือหน่วยงาน
- หากหัวหน้าหน่วยงานหรือผู้มีอำนวจร้องขอให้ดำเนินการใด ๆ กับ ผู้ใช้งานนั้น ๆ

3.1.3 มาตรการเชิงปฏิบัติสำหรับผู้ใช้ข้อมูลส่วนบุคคล

บุคคลผู้ที่มีสิทธิเข้าถึง ใช้ แก้ไข เปลี่ยนแปลง เปิดเผย ข้อมูลส่วนบุคคล โดยมีขอบเขตการใช้ข้อมูลตามตำแหน่งหน้าที่หรือข้อกำหนดในสัญญาและภายใต้การอนุญาตของบริษัทฯ เช่น พนักงานประจำ พนักงานชั่วคราว ผู้รับจ้าง ฯลฯ ผู้ใช้ข้อมูลส่วนบุคคลมีหน้าที่รักษาความมั่นคงปลอดภัยข้อมูลจากการเข้าถึง แก้ไขเปลี่ยนแปลง เปิดเผย หรือทำลายข้อมูลโดยมิชอบหรือโดยปราศจากอำนาจ โดยให้ถือปฏิบัติดังนี้

1. สามารถเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล ตามหน้าที่และความรับผิดชอบหรือตามที่ได้รับมอบหมายจากบริษัทฯ เท่านั้น

2. เข้าถึง ใช้ เปิดเผย ข้อมูลส่วนบุคคล ตามที่บริษัทฯ หรือผู้ดูแลระบบกำหนดไว้เท่านั้น
3. ปฏิบัติหน้าที่ของตนโดยดำเนินการต่าง ๆ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปิดเผย แก้ไข เปลี่ยนแปลง ข้อมูลส่วนบุคคลโดยมิชอบหรือโดยปราศจากอำนาจ
4. เมื่อไม่ได้ใช้งานหรือไม่ได้นำมาใช้งานอย่างต่อเนื่อง ข้อมูลส่วนบุคคลจะต้องได้รับการจัดเก็บอย่างปลอดภัย เช่น การล็อกลิ้นชัก โต๊ะทำงาน หรือล็อคห้อง เป็นต้น
5. การเข้าถึงโดยมิชอบ การกระทำที่นอกเหนือที่ได้รับมอบหมายหรือการลักลอบทำสำเนา การขโมยอุปกรณ์จัดเก็บ/การประมวลข้อมูลส่วนบุคคล บริษัทฯ จะดำเนินการลงโทษผู้กระทำทางวินัยในการทำงาน และ/หรือการดำเนินคดีทางแพ่งและทางอาญา

3.1.4 การตรวจสอบย้อนหลัง (Audit trails)

สามารถตรวจสอบการเข้าถึงข้อมูลต่างๆ ซึ่งจัดเก็บอยู่ในระบบ แยกตามสถานะ ดังนี้

- Input (อินพุท) การนำเข้าข้อมูล
- Update (อัพเดท) มีการเปลี่ยนแปลงเอกสาร
- Cancel (แคนเซ็ล) ยกเลิกเอกสาร (เอกสารยังคงอยู่ในระบบ แต่ไม่ได้ถูกนำมาใช้งาน)
- Delete (ดิลีท) ลบเอกสารออกจากระบบ (เอกสารถูกลบออกจากระบบ)

หากมีการลบข้อมูลออกจากระบบไป สามารถเรียกดูข้อมูลนั้น ๆ ได้จากระบบ Backup ข้อมูล

3.2 มาตรการการลบทำลายข้อมูลส่วนบุคคล

เมื่อหมดความจำเป็นที่จะต้องเก็บข้อมูลตามระยะเวลาที่ระบุใน **“ประกาศความเป็นส่วนตัว” (Privacy Notice)** ของเจ้าของข้อมูลส่วนบุคคลแต่ละประเภท บริษัทฯ จะลบ หรือทำลายข้อมูลส่วนบุคคลนั้นอย่างถาวร (permanently) หรือทำให้ข้อมูลนั้นไม่อาจระบุตัวบุคคลได้ โดยบริษัทฯ อาจเลือกที่จะดำเนินกระบวนการดังต่อไปนี้

- เอกสารในรูปแบบอิเล็กทรอนิกส์จะต้องถูกลบด้วยวิธีการที่ทำให้ข้อมูลนั้นไม่อาจถูกเข้าถึงได้อีกเลย
- ข้อมูลส่วนบุคคลที่ถูกเก็บอยู่ในอุปกรณ์ที่เก็บข้อมูลหรือวัตถุใด ๆ จะต้องถูกลบออกจากอุปกรณ์ดังกล่าวก่อนที่จะมีการทิ้งอุปกรณ์นั้น
- ในกรณีที่ข้อมูลส่วนบุคคลนั้นไม่สามารถถูกลบจากอุปกรณ์ได้ จะต้องมีการทำลายตัวอุปกรณ์นั้นโดยบุคคลที่มีสิทธิหรือบริษัทที่ได้รับอนุญาตให้ประกอบกิจการทำลาย
- ข้อมูลส่วนบุคคลที่ได้พิมพ์ไว้ในกระดาษจะต้องถูกทำลายโดยเครื่องย่อยเอกสาร
- ให้มีการบันทึกรายละเอียดการลบหรือทำลายข้อมูลส่วนบุคคล เช่น วิธีการทำลาย จำนวนข้อมูลที่ทำลาย การตรวจสอบผลการทำลาย เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลที่ถูกทำลายไปแล้วจะไม่เข้าถึงและสามารถกู้คืนข้อมูลได้