นโยบายการรักษาข้อมูลความลับ

(Information Security Policy)

การกำหนดตัวตนของผู้ใช้งานในระบบ

1. Password ที่ใช้ เข้าระบบหรือเข้าโปรแกรมที่เก็บข้อมูลลูกค้า ต้องเป็นตามข้อกำหนด ดังนี้
   1.1 ต้องมีการบังคับเปลี่ยน Password อย่างน้อย 1 ครั้ง ทุก 30 วัน
   1.2 Password ต้องมีความยาวอย่างน้อย 6 ตัวอักษร และต้องประกอบไปด้วยตัวอักษรและตัวเลข
2. มีการพยายามเข้าสู่ระบบแต่ไม่สำเร็จ ติดต่อกัน 3 ครั้ง ระบบจะต้องพักการใช้งานใน Password นั้นๆ
3. หาก User ID หยุดการใช้งานเกิน 30 วัน จะถูกระงับการใช้งาน
4. โปรแกรมต้องมีรายงานเพื่อตรวจสอบในข้อดังต่อไปนี้
   4.1 เมื่อมีการเพิ่มหรือลบ User ID ของผู้ใช้โปรแกรม
   4.2 เมื่อมีการพยายามเข้าโปรแกรม โดยผู้ที่ได้รับอนุญาต หรือพยายามเข้าไปใช้งานโปรแกรมในส่วนที่ผู้ใช้คนนั้น ไม่ได้รับอนุญาต
5. ต้องมีการตรวจสอบตัวตนของผู้ใช้งานในระบบ เป็นประจำอย่างน้อยเดือนละ 1 ครั้ง

การรักษาความลับ และความถูกต้องของข้อมูล

1. แฟ้มข้อมูลหรือฐานข้อมูลลูกค้า ต้องมีการเข้ารหัส หรือมีการป้องกันโดย Password เมื่อต้องการที่จะส่งข้อมูล
2. เมื่อต้องการจะส่งข้อมูล จะต้องส่งโดยระบบอิเล็กทรอนิกส์และต้องการทำการเข้ารหัสทุกครั้ง
3. การเข้ารหัสแฟ้มข้อมูลของลูกค้า จะต้องใช้โปรแกรมที่บริษัทอนุญาตเท่านั้น
4. Password สำหรับการถอนรหัสแฟ้มข้อมูล จะต้องถูกส่งโดยแยกกันกับแฟ้มข้อมูลที่เข้ารหัสไว้
5. ไม่อนุญาตให้วางข้อมูลลูกค้าของบริษัท ไว้ในสถานที่ ซึ่งบุคคลทั่วไปสามารถเข้าถึงได้ง่าย
6. เครื่องคอมพิวเตอร์ที่สามารถเข้าระบบหรือโปรแกรมที่เก็บข้อมูลลูกค้า ต้องมีการตั้งค่าเพื่อปิดหน้าจออัตโนมัติ
7. ต้องมีการบันทึกข้อมูลจากระบบติดตามหนี้ เพื่อสำรองไว้กรณีฉุกเฉินเป็นประจำ และต้องเก็บบันทึกข้อมูลสำรองนั้น ไว้นอกสถานที่ โดยมีการลงบันทึกรายละเอียด ดังนี้
   7.1 วันที่ทำการบันทึกข้อมูล
   7.2 ช่วงระยะเวลาที่ทำการบันทึกข้อมูล ในการบันทึกแต่ละครั้ง
   7.3 ผู้ที่เก็บบันทึกข้อมูลสำรอง และสถานที่เก็บโดยมีการลงลายมือชื่อไว้เป็นหลักฐาน
   7.4 วันที่มีการนำบันทึกข้อมูลสำรอง และสถานที่เก็บโดยมีการลงลายมือชื่อไว้เป็นหลักฐาน
   7.5 ต้องทำการบันทึกข้อมูลสำรองไว้ทุกอาทิตย์ และนำข้อมูลไปเก็บไว้ที่ DR Site
8. ระบบหรือโปรแกรมที่เก็บข้อมูลลูกค้าของ บริษัท จะต้องมีความสามารถป้องกันการขโมยข้อมูล ที่ใช้โดยวิธีการบันทึกข้อมูลในแผ่น CD / DVD และ Thumb Drive

9. การทำลายเอกสารข้อมูลลูกค้าต้องมีการขออนุมัติก่อนทำลาย ในกรณีที่จ้างหน่วยงานภายนอกเป็นผู้ทำลายต้องมีเจ้าหน้าที่ของบริษัทควบคุมการทำลายร่วมอยู่ด้วย มีการบันทึกการว่าจ้างเป็นลายลักษณ์อักษร
10. ห้ามบุคคลภายนอกเข้าในสถานที่ทำงาน และถ้ามีต้องมีการลงลายมือชื่อพร้อมกับแลกบัตร Visitor แล้วแจ้งไปยังผู้ที่ขอติดต่อรับทราบอนุญาตก่อนทุกครั้ง
11. ห้ามพนักงานเปิดเผยข้อมูลที่จะทำให้เกิดความเสียหาย แก่บุคคลภายนอก และบุคคลที่ไม่เกี่ยวข้องในงาน
12. ไม่อนุญาตให้เปิดเผย Password และ Share Password กับบุคคลอื่นอย่างเด็ดขาด
13. User และ Password จะต้องถูกกำหนดไว้ 1 User ต่อ 1 คน ยกเว้นพนักงานที่จำเป็นต้องมี User มากกว่า 1 จะต้องมีคำอนุมัติจากผู้มีอำนาจในการถือ User มากกว่า 1 User
14. ต้องมีอบรมเกี่ยวกับการป้องกันความเสียหายของข้อมูล ให้แก่พนักงานเข้าใหม่ และพนักงานทั่วไปอย่างน้อยปีละ 1 ครั้ง
15. Programmer ต้องทำการทดสอบโปรแกรม (UAT Testing) เพื่อลดความเสี่ยงที่จะเกิดความผิดพลาด อยู่เสมอ ต้องทำ Log sheet record ไว้ทุกครั้งว่า Test อะไรบ้าง และ Dump Screen ทุกครั้ง
16. ต้องทำลายเอกสารข้อมูลที่ไม่ใช้แล้ว ด้วยเครื่องย่อยเอกสารเท่านั้น และมิให้นำเอกสารที่มีข้อมูลลูกค้ากลับมาใช้อีก
17. กำหนดให้ IT Manager ถือกุญแจห้อง Server Room แต่เพียงผู้เดียวเท่านั้น และกำหนดรายชื่อผู้มีอำนาจในการเข้าห้อง Server ถ้าหากมีผู้ที่ไม่มีชื่อในการเข้าห้อง Server ต้องการที่จะเข้าไปในห้อง จะต้องมีผู้มีอำนาจอยู่ด้วยทุกครั้ง และผู้ที่ไม่มีอำนาจเข้าห้อง Server จะต้องลงลายมือชื่อในสมุดการเข้าออกห้อง Server ทุกครั้ง
18. (ผู้บริหารระบบข้อมูล) ต้องจัดทำนโยบายเทคโนโลยีสารสนเทศ สำหรับระบบข้อมูลขององค์กร อย่างเป็นลายลักษณ์อักษร และนโยบายนี้ต้องได้รับการอนุมัติจากผู้บริหารขององค์กรในการนำไปใช้
19. (ผู้บริหารองค์กร) ต้องจัดให้มีการเผยแพร่นโยบายเทคโนโลยีสารสนเทศ ให้พนักงานทุกระดับในองค์กรทราบ
20. (ผู้บริหารระบบข้อมูล) ต้องดำเนินการตรวจสอบ และประเมินนโยบายเทคโนโลยีสารสนเทศ ตามระยะเวลาที่กำหนดไว้ 1 ครั้งต่อปี
21. (พนักงาน) ทุกคนที่ใช้งานระบบข้อมูล ต้องลงนามยอมรับ และปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศขององค์กร
22. (ผู้บริหารระบบข้อมูล) ต้องมีการตรวจสอบว่าการปฏิบัติงานของพนักงาน เป็นไปตามข้อกำหนดหรือสอดคล้อง กับนโยบายเทคโนโลยีสารสนเทศ สำหรับระบบข้อมูลขององค์กรหรือไม่ทุก 3 เดือน
23. (ผู้บริหารงานสำนักงาน) ต้องจัดทำบัญชีทรัพย์สินขององค์กร (ซึ่งรวมถึงบัญชีครุภัณฑ์คอมพิวเตอร์และบัญชีข้อมูลที่เก็บไว้ในสื่อต่าง ๆ ทั้งหมด) เพื่อใช้ในการกำหนดมูลค่าทรัพย์สิน ระดับความ สำคัญ

24. (ผู้บริหารงานสำนักงาน) ต้องจัดให้มีการตรวจสอบบัญชีทรัพย์สิน ตามระยะเวลาที่กำหนดไว้ปีละ 1 ครั้ง
25. (ผู้บริหารระบบข้อมูล) ต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของข้อมูล เช่น ลับมาก ลับ ภายในสาธารณะ ทั้งนี้ เพื่อจะได้หาวิธีการป้องกันอย่างเหมาะสม
26. (ผู้บริหารงานสำนักงาน) ต้องจัดให้มีการจัดทำป้ายชื่อสำหรับข้อมูล และทรัพย์สินระบบข้อมูล และต้องมีวิธีการจัดการระบบข้อมูลและทรัพย์สินระบบข้อมูล โดยแยกหมวดหมู่
27. (ผู้บริหารงานบุคคล) ต้องตรวจสอบคุณสมบัติของผู้สมัครโดยละเอียด เช่น ตรวจสอบจากจดหมายรับรองประวัติการทำงาน วุฒิการศึกษา บุคคลหรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น
28. (ผู้บริหารงานบุคคล) ต้องกำหนดเงื่อนไขการจ้างงาน ซึ่งรวมถึงหน้าที่ความรับผิดชอบทางด้านความปลอดภัย ทางด้านระบบข้อมูลขององค์กร
29. (ผู้บริหารงานบุคคล) ต้องจัดให้มีการลงนามในข้อตกลง ระหว่างพนักงานและองค์กรว่า จะไม่เปิดเผยความลับขององค์กร (โดยการลงนามนี้ จะเป็นส่วนหนึ่งของการว่าจ้างพนักงาน)
30. (พนักงาน) เมื่อมีเหตุการณ์ที่ส่อทางละเมิดความมั่นคงปลอดภัย (เช่น ไวรัสคอมพิวเตอร์แพร่กระจาย ระบบถูกบุกรุก เป็นต้น) และระบบทำงานบกพร่อง รวมทั้งเพื่อให้บุคคลากรในองค์กร ได้เรียนรู้จากประสบการณ์ ความเสียหายดังกล่าว พนักงานต้องปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศ
31. (ผู้บริหารระบบข้อมูล) ต้องมีการควบคุมการเข้าออก ในบริเวณพื้นที่ควบคุม โดยให้ผ่านเข้าออกเฉพาะผู้มีสิทธิ์เท่านั้น โดยมี Log sheet สำหรับลงมือชื่อเข้าออก
32. (ผู้บริหารระบบข้อมูล) ต้องจัดให้มีมาตราการในการรักษาความมั่นคงปลอดภัยอื่นๆ ให้กับสำนักงาน ห้องทำงาน และเครื่องมือต่างๆ เช่น คอมพิวเตอร์ หรือระบบที่มีความสำคัญสูง ต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก สำนักงานหรือห้องจะต้องไม่มีป้ายสัญลักษณ์ที่บ่งบอกถึงการมีระบบ สำคัญอยู่ในสถานที่ดังกล่าว ประตูหน้าต่าง หรือห้องต้องถูกล็อคเสมอ
33. (ผู้บริหารงานบุคคล) ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์ เช่น ถังดับเพลิง, Temperature Control, Fire Alarm, Power Supply, CCTV อย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงปีละ 1 ครั้ง
34. (ผู้บริหารระบบข้อมูล) ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์ ซึ่งมีข้อมูลสำคัญเก็บไว้ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ ทั้งนี้ เพื่อป้องกันการรั่วไหล หรือการเปิดเผยข้อมูลดังกล่าว
35. (พนักงาน) ต้องไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลที่สำคัญ ๆ ไว้ในที่ที่สามารถพบเห็นได้ง่าย โดยจัดเก็บไว้ในที่ที่ปลอดภัย ต้องทำการลงบันทึกออกจากคอมพิวเตอร์ (Log off) เมื่อจำเป็นต้องหยุดการใช้งาน คอมพิวเตอร์เป็นระยะเวลาหนึ่ง นอกจากนี้ตู้จ่ายเอกสาร หรือจดหมาย และเครื่องถ่ายเอกสารจะต้องได้รับ การดูแลให้ปลอดภัยด้วย
36. (ผู้บริหารระบบข้อมูล) ต้องมีการติดตั้งและใช้งานซอฟแวร์ป้องกันไวรัส หนอน เพื่อป้องกันความเสียหายของข้อมูล รวมทั้งกลไก เพื่อสร้างความตระหนักให้แก่ผู้ใช้ภายในองค์กร และดูแลมาตราการป้องกันให้ทันสมัยอยู่เสมอ

37. (ผู้ดูแลระบบ) ต้องสำรองข้อมูลที่สำคัญไว้ทุกวัน โดยบันทึกข้อมูลสำรองในสื่อบันทึกข้อมูล
38. (ผู้ดูแลระบบ) ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย
39. (ผู้ดูแลระบบ) ต้องจัดให้มีการเข้ารหัสข้อมูลสำรอง ที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย
40. (ผู้ดูแลระบบ) ต้องกำหนดวิธีการกำจัดสื่อบันทึกข้อมูล ที่ความสำคัญสูง เมื่อไม่ได้มีการใช้งานแล้ว
41. (ผู้บริหารระบบข้อมูล) ต้องกำหนดวิธีการปฏิบัติในการจัดเก็บสื่อบันทึกข้อมูล เพื่อป้องกันไม่ให้ข้อมูลที่สำคัญเกิดการรั่วไหล หรือเปิดเผยออกไป ได้แก่ ต้องมีการติดป้ายชื่อไว้ที่สื่อบันทึกอย่างชัดเจน, กำหนด บุคคลากรที่มีสิทธิ์ในการใช้งาน, ต้องเก็บสื่อบันทึกอย่างชัดเจน, กำหนดบุคคลากรที่มีสิทธิ์ในการใช้งาน, ต้องเก็บสื่อบันทึกไว้สถานที่ปลอดภัย จากการเสียหายที่เกิดขึ้นได้
42. (ผู้บริหารระบบข้อมูล) ต้องจัดทำนโยบาย และความต้องการในการใช้งานระบบข้อมูล เพื่อควบคุมการเข้าถึงให้ทำได้ เฉพาะผู้ที่ได้รับอนุญาต เท่านั้น
43. (ผู้บริหารงานบุคคล) ต้องทำระเบียบปฏิบัติในการลงทะเบียนพนักงานใหม่ เพื่อให้สามารถใช้งานระบบข้อมูล หรือโครงสร้างสนับสนุนระบบข้อมูลอื่นทั้งหมดได้ นอกจากนี้ต้องมีระเบียบปฏิบัติ เพื่อยกเลิกการใช้งานของพนักงานทันที ในกรณีที่มีการลาออกจากงาน
44. (ผู้ดูแลระบบ) ต้องบริหารจัดการรหัสผ่านของพนักงานให้มีความมั่นคงปลอดภัย
45. (ผู้ดูแลระบบ) ต้องทบทวนสิทธิในการเข้าถึงระบบข้อมูลตามระยะเวลาที่กำหนดไว้ 1 ครั้ง ในรอบ 6 เดือน

<u>เริ่มมีผลบังคับใช้</u>

นโยบายนี้ให้เริ่มบังคับใช้ตั้งแต่วันที่ 15 พฤศจิกายน พ.ศ.2560

จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

(คุณรินทร์ลภัส พงษ์วิทยภานุ)	(คุณหฤทัย พงษ์วิทยภานุ)	(คุณทวีศักดิ์ พงษ์วิทยภานุ)
วันที่ 15 / พ.ย. / 60	วันที่ 15 / พ.ย. / 60	วันที่ 15 / พ.ย. / 60
กรรมการบริษัท	**กรรมการบริษัท**	**ประธานบริษัท**