	กระบวนการจัดการผู้ให้บริการภายนอก (Third Party Management Procedure)	**รหัสเอกสาร**	**KSC MOPH-Identify-05**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	1 ธ.ค. 68
		ชั้นความลับของเอกสาร	ใช้ภายในเท่านั้น

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นางสาวศิรดา สว่างสุข	นายชัพ ธิราขันธ์	นายภูจิตต์ ตรีบำเพ็ญ
ตำแหน่ง	นักสาธารณสุขปฏิบัติการ	นักจัดการงานทั่วไปชำนาญการ	ผู้อำนวยการโรงพยาบาลเกาะสีชัง
วันเดือนปี	24 พฤศจิกายน 2568	28 พฤศจิกายน 2568	28 พฤศจิกายน 2568

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	1 ธ.ค. 68	จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์

	กระบวนการจัดการผู้ให้บริการภายนอก (Third Party Management Procedure)	รหัสเอกสาร	KSC MOPH-Identify-05
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ธ.ค. 68
		ชั้นความลับของเอกสาร	ใช้ภายในเท่านั้น

สารบัญ

กระบวนการจัดการผู้ให้บริการภายนอก (Third Party Management Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 21.4.1, ข้อ 21.4.2, ข้อ 21.4.3, ข้อ 21.4.4]

1. วัตถุประสงค์

เพื่อให้แน่ใจว่าผู้ให้บริการภายนอกที่เข้ามาเกี่ยวข้องกับบริการที่สำคัญของหน่วยงานสามารถปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด และเพื่อป้องกันหรือลดความเสี่ยงที่อาจเกิดขึ้นจากการใช้ผู้ให้บริการภายนอก

2. ขอบเขต

กระบวนการนี้ครอบคลุมถึงการกำหนด ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในการจัดทำข้อตกลงและสัญญากับผู้ให้บริการภายนอก รวมถึงการตรวจสอบผู้ให้บริการภายนอกว่าได้ดำเนินการถูกต้องและเป็นไปตามข้อกำหนดเหล่านั้น

3. คำจำกัดความ/นิยามศัพท์เฉพาะ

ลำดับ	คำศัพท์	คำจำกัดความ
1	หน่วยงานผู้ว่าจ้างผู้ให้บริการภายนอก	หน่วยงานต่าง ๆ ของ โรงพยาบาลเกาะสีชังที่เป็นผู้ว่าจ้าง ผู้ให้บริการภายนอก ให้บริการ หรือ ติดตั้งระบบ หรือ พัฒนาโปรแกรม
2	ผู้ดูแลระบบ	เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลระบบสารสนเทศ หรือ ระบบคอมพิวเตอร์และเครือข่าย
3	ISM	หัวหน้าคณะทำงานระบบบริหารการรักษาความมั่นปลอดภัยสารสนเทศขององค์กร

4. หน้าที่และความรับผิดชอบ

ลำดับ	ผู้รับผิดชอบ	ความรับผิดชอบ
1	Top Management / ISM	• ดำเนินการอนุมัติกรณีมีการขอใช้ระบบของผู้ให้บริการภายนอก รวมถึงอนุมัติข้อตกลงและสัญญาที่ เกี่ยวข้อง • กำกับดูแลและตรวจสอบให้แน่ใจว่ามีการจัดการผู้ให้บริการภายนอกอย่างเหมาะสมและปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ
2	ผู้ดูแลระบบ	• กำหนดระยะเวลาของสิทธิ์ในการใช้งาน • ทำการบันทึกสิทธิ์ในการเข้าถึงระบบต่าง ๆ • ตรวจสอบการใช้งานของผู้ให้บริการภายนอก • ดำเนินการเพิกถอนสิทธิ์ในการเข้าระบบต่าง ๆ
3	คณะกรรมการตรวจรับ	• ตรวจสอบความเรียบร้อยสมบูรณ์
4	หน่วยงานผู้ว่าจ้างผู้ให้บริการภายนอก	• รับผิดชอบในการดำเนินการตามกระบวนการทั้งหมดที่เกี่ยวข้องกับผู้ให้บริการภายนอก รวมถึงการกำหนดข้อกำหนด การตรวจสอบ และการเจรจาต่อรองสัญญา • คัดเลือก ตรวจสอบคุณสมบัติ และประเมินความสามารถ • ควบคุมดูแลให้มีการส่งคืนทรัพย์สินต่าง ๆ
5	ผู้ให้บริการภายนอก	• มีหน้าที่ในการปฏิบัติตามข้อกำหนดด้านความมั่นคง ปลอดภัยไซเบอร์ที่ระบุไว้ในสัญญาหรือข้อตกลงกับองค์กร • ลงนามเอกสารข้อตกลงไม่เปิดเผยข้อมูล • ดำเนินการขออนุมัติ

5. ขั้นตอนปฏิบัติ

5.1 การกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Requirements)

1) การกำหนดข้อกำหนดในข้อตกลงระดับการให้บริการ (SLA) หรือสัญญากับผู้ให้บริการภายนอก

ขั้นตอน: กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในข้อตกลงระดับการให้บริการ (SLA) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก เพื่อป้องกันและลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยต้องมีการระบุข้อกำหนดที่ชัดเจนเกี่ยวกับการป้องกันข้อมูลที่สำคัญ เช่น การเข้ารหัสข้อมูล และการควบคุมการเข้าถึง รวมถึงพิจารณาใบรับรองที่ผู้ให้การบริการภายนอกควรต้องมี เช่น ISO, NIST Cybersecurity จากหน่วยงานที่รับรอง โดยให้สอดคล้องกับวัตถุประสงค์ของโครงการที่จะดำเนินการ

2) ประเภทของผู้ให้บริการภายนอก

ขั้นตอน: ระบุประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญของหน่วยงาน โดยพิจารณาความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ด้วยเนื่องจากอาจมีการเข้าถึงข้อมูลที่มีความสำคัญสูง/ข้อมูลอ่อนไหว/ข้อมูลที่เป็นความลับ ของหน่วยงาน

3) ภาระหน้าที่ของผู้ให้บริการภายนอก

ขั้นตอน: ระบุภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของหน่วยงาน จากภัยคุกคามทางไซเบอร์ เช่น ผู้ให้บริการภายนอกต้องมีตรวจสอบระบบความปลอดภัยอย่างสม่ำเสมอ หรือ ดำเนินการอัปเดตระบบรักษาความปลอดภัยทุกครั้งที่มีการเปลี่ยนแปลงเทคโนโลยี

4) การจัดการความเสี่ยงในห่วงโซ่อุปทาน (Supply Chain Risk Management)

ขั้นตอน: ระบุความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานของผลิตภัณฑ์ และกำหนดมาตรการในการควบคุมความเสี่ยงเหล่านี้ โดยการการตรวจสอบแหล่งที่มาของการบริการในผลิตภัณฑ์ที่ผู้ให้บริการภายนอกจัดหามาให้เพื่อป้องกันการใช้ส่วนประกอบหรือส่วนที่เกี่ยวข้องที่ไม่ได้มาตรฐานหรือมีความเสี่ยง

5) สิทธิ์ในการตรวจสอบ (Audit Rights)

ขั้นตอน: ระบุสิทธิ์ขององค์กรในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าผู้ให้บริการปฏิบัติตามข้อกำหนดที่ระบุไว้ในสัญญา

5.2 การตรวจสอบความถูกต้องและความสอดคล้อง (Verification and Compliance)

1) การตรวจสอบความถูกต้องของผู้ให้บริการภายนอก

ขั้นตอน: พิจารณาดำเนินการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา เช่น การตรวจสอบโดยบุคคลที่สาม (Site reference) และการตรวจสอบมาตรฐานของผลิตภัณฑ์

2) การเจรจาต่อรองเงื่อนไขของสัญญาจ้าง

ขั้นตอน: พิจารณาเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับข้อกำหนดทางกฎหมาย ปัจจุบันหรือข้อบังคับใหม่ที่อาจเกิดขึ้นในอนาคต เช่น มีการประกาศใช้กฎหมายใหม่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

5.3 การติดตามและปรับปรุงกระบวนการ (Monitoring and Process Improvement)

ขั้นตอน: ดำเนินการติดตามผลการปฏิบัติงานของผู้ให้บริการภายนอกอย่างสม่ำเสมอ และปรับปรุงกระบวนการจัดการผู้ให้บริการตามความเหมาะสม เพื่อให้มั่นใจว่าการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ โดยต้องมีการจัดทำรายงานผลการตรวจสอบกับ ผู้ให้บริการภายนอกเป็นรายไตรมาส

5.4 การควบคุมกำกับดูแลให้มีการลงนามเอกสารข้อตกลงไม่เปิดเผยข้อมูล (Non - Disclosure Agreement)

ขั้นตอน: ดำเนินการให้ผู้ให้บริการภายนอกจะต้องลงนามเอกสารข้อตกลงไม่เปิดเผยข้อมูล (Non -Disclosure Agreement) และต้องปฏิบัติตามนโยบายกฎระเบียบ ขั้นตอนการปฏิบัติงาน และวิธีปฏิบัติงานของหน่วยงานอย่างเคร่งครัด

5.5 การควบคุมกำกับดูแลให้มีการลงนามในเอกสารข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

ขั้นตอน: ในกรณีที่ผู้ให้บริการภายนอกมีการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของหน่วยงาน หน่วยงานจะต้องดำเนินการให้ผู้ให้บริการภายนอกลงในนามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) และต้องปฏิบัติตามนโยบายกฎระเบียบ ขั้นตอนการปฏิบัติงานและวิธีปฏิบัติงานของหน่วยงานอย่างเคร่งครัด

5.6 การควบคุมกำกับดูแลผู้ให้บริการภายนอกที่ต้องการใช้ระบบเทคโนโลยีสารสนเทศของหน่วยงาน

ขั้นตอน: 1. ในกรณีที่ผู้ให้บริการภายนอกต้องการใช้ระบบเทคโนโลยีสารสนเทศของหน่วยงานผู้ให้บริการภายนอกต้องดำเนินการขออนุมัติจาก Top Management / ISM

2. ผู้ดูแลระบบ ดำเนินการกำหนดระยะเวลาของสิทธิ์ในการใช้งาน/เข้าใช้งาน ทำการบันทึกสิทธิ์ในการเข้าถึงระบบต่าง ๆ และตรวจสอบการใช้งานของผู้ให้บริการภายนอก

3. ผู้ดูแลระบบ ดำเนินการเพิกถอนสิทธิ์ในการเข้าระบบต่าง ๆ ของผู้ให้บริการภายนอก เมื่อหมดความจำเป็นตามวัตถุประสงค์ที่ได้ขออนุมัติไว้

6. การทบทวนกระบวนการดำเนินการ

กระบวนการดำเนินการนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

7. เอกสารที่เกี่ยวข้อง

ลำดับ	หมายเลขเอกสาร	ชื่อเอกสาร	สถานที่เก็บ	ระยะเวลาเก็บ
1		สัญญาเก็บรักษาข้อมูลที่เป็นความลับ (Non-Disclosure Agreement)	หน่วยงานผู้ว่าจ้างผู้ให้บริการภายนอก	ไม่น้อยกว่า 1 ปี / ตามนโยบายกฎระเบียบขั้นตอนการปฏิบัติงาน หรือวิธีปฏิบัติงานของหน่วยงาน

8. เอกสารอ้างอิง

ลำดับ	ชื่อเอกสาร
1	ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 - กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - การระบุความเสี่ยงที่อาจจะเกิดขึ้น (Identify) - การจัดการผู้ให้บริการภายนอก (Third-Party Management)
2	ข้อตกลงระดับการให้บริการ (SLA)
3	เงื่อนไขของสัญญากับผู้ให้บริการภายนอก
4	หลักฐานการทำการประเมินความเสี่ยงไซเบอร์ที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์
5	ใบรับรองตามมาตรฐานสากลต่างๆ เช่น ISO/IEC 27001 (ISMS), ISO/IEC 29110 (Software Engineer), ISO 9001 (Quality), ISO 14001 (Environment), ISO 45001 (Safety)
6	หลักฐานการทำการตรวจสอบระบบความมั่นคงปลอดภัยทางไซเบอร์ของผู้ให้บริการภายนอก

โรงพยาบาลเกาะสีชัง

จัดทำโดย : นายชัพ ธิราขันธ์
ผู้อนุมัติ : นายภูจิตต์ ตรีบำเพ็ญ
จัดทำเมื่อ : 24 / พฤศจิกายน / 2568
มีผลบังคับใช้ : 1 / ธันวาคม/ 2568

ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ให้บริการภายนอก (Cybersecurity Requirements for Third-Party Providers)

1. การเข้าถึงข้อมูล (Data Access)

- **ข้อกำหนด**
  - ผู้ให้บริการภายนอกต้องจำกัดการเข้าถึงข้อมูลสำคัญเฉพาะบุคคลที่มีความจำเป็นต้องใช้เท่านั้น (Need-to-Know Basis)
  - ต้องมีการยืนยันตัวตน (Authentication) และการตรวจสอบสิทธิ์ (Authorization) สำหรับการเข้าถึงข้อมูลทุกครั้ง
  - ระบบการเข้าถึงต้องใช้การยืนยันตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication - MFA)

2. การจัดเก็บข้อมูล (Data Storage)

- **ข้อกำหนด**
  - ข้อมูลสำคัญทั้งหมดต้องถูกเข้ารหัสทั้งในระหว่างการจัดเก็บ (Data-at-Rest) และการส่งผ่าน (Data-in-Transit)
  - ผู้ให้บริการภายนอกต้องจัดให้มีการสำรองข้อมูล (Data Backup) อย่างสม่ำเสมอและจัดเก็บในสถานที่ที่ปลอดภัย
  - ต้องมีมาตรการป้องกันการเข้าถึงข้อมูลสำรองที่ไม่ได้รับอนุญาต

3. การสื่อสารข้อมูล (Data Communication)

- **ข้อกำหนด**
  - การสื่อสารข้อมูลระหว่างหน่วยงานและผู้ให้บริการภายนอกต้องใช้การเข้ารหัสที่มีมาตรฐานสากล เช่น TLS/SSL
  - ผู้ให้บริการต้องใช้ VPN ที่ปลอดภัยสำหรับการสื่อสารข้อมูลที่มีความสำคัญกับองค์กรหรือหน่วยงาน
  - ห้ามใช้โปรโตคอลหรือวิธีการสื่อสารที่ไม่ได้รับการอนุมัติจากฝ่ายความมั่นคงปลอดภัยไซเบอร์ขององค์กรหรือหน่วยงาน

4. **การจัดการความปลอดภัย** (Security Management)
   - **ข้อกำหนด**
     - ผู้ให้บริการภายนอกต้องดำเนินการตามแนวปฏิบัติที่ดีที่สุดในด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การใช้การอัปเดตซอฟต์แวร์และแพตช์ความปลอดภัยอย่างสม่ำเสมอ
     - ต้องมีการตรวจสอบและบันทึกการเข้าถึงข้อมูลและระบบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
     - ผู้ให้บริการต้องมีการตรวจสอบภายในและการทดสอบความปลอดภัย (Security Testing) เป็นระยะ ๆ
5. **การจัดการเหตุการณ์ความปลอดภัย** (Incident Management)
   - **ข้อกำหนด**
     - ผู้ให้บริการภายนอกต้องรายงานเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นทันทีแก่องค์กรหรือหน่วยงาน (ไม่เกิน 6 ชั่วโมง)
     - ต้องมีแผนการตอบสนองต่อเหตุการณ์ (Incident Response Plan) ที่สอดคล้องกับนโยบายขององค์กรหรือหน่วยงาน
     - ผู้ให้บริการต้องร่วมมือกับองค์กรหรือหน่วยงานในการตรวจสอบและแก้ไขปัญหาที่เกิดขึ้นจากเหตุการณ์ความไม่ปลอดภัยทางไซเบอร์
6. **การตรวจสอบและการปฏิบัติตามข้อกำหนด** (Audit and Compliance)
   - **ข้อกำหนด**
     - ผู้ให้บริการต้องยอมรับการตรวจสอบความมั่นคงปลอดภัยจากองค์กรหรือหน่วยงานหรือบุคคลที่สามตามที่องค์กรหรือหน่วยงานกำหนด
     - ผู้ให้บริการต้องจัดให้มีการตรวจสอบภายในและการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างสม่ำเสมอ
     - องค์กรหรือหน่วยงานมีสิทธิ์ในการตรวจสอบและประเมินความมั่นคงปลอดภัยทางไซเบอร์ของผู้ให้บริการตลอดระยะเวลาของสัญญา

Logo ชื่อหน่วยงาน

สัญญาการเก็บรักษาข้อมูลที่เป็นความลับ

สัญญาฉบับนี้ทำขึ้น ณ เลขที่ xxx หมู่ที่ x ถนน xxx ตำบล/แขวง xxx อำเภอ/เขต xxx จังหวัด xxx เมื่อวันที่ x เดือน xxxx พ.ศ. 25xx

ระหว่าง นาย xxx อยู่เลขที่ xxx หมู่ที่ xx ถนน xxx ตำบล/แขวง xxx อำเภอ/เขต xxx จังหวัด xxx เลขที่บัตรประชาชน : xxxx เป็นผู้มีอำนาจลงนามในสัญญานี้ ซึ่งต่อไปในสัญญานี้เรียกว่า **"ผู้เก็บข้อมูล"** ฝ่ายหนึ่ง กับ

บริษัท xxx จำกัด ซึ่งจดทะเบียนเป็นนิติบุคคล มีสำนักงานใหญ่อยู่เลขที่ xxx ถนน xxx แขวง xxx เขต xxx กรุงเทพฯ 10xxx โดย นาย xxxx เป็นผู้มีอำนาจลงนามผูกพันนิติบุคคล ซึ่งต่อไปในสัญญานี้เรียกว่า **"ผู้ให้ข้อมูล"** อีกฝ่ายหนึ่ง

โดยที่ผู้ให้ข้อมูลเป็นเจ้าของข้อมูลเกี่ยวกับข้อมูลที่เกี่ยวข้องกับธุรกิจ รวมถึงข้อมูลต่างๆ ซึ่งต่อไปนี้จะเรียกว่า **"ข้อมูล"** มีความประสงค์ที่จะเปิดเผยข้อมูลดังกล่าวให้แก่ผู้รับข้อมูลเพื่อนำไปใช้ประโยชน์ในการทำระบบ ISO 29110 เท่านั้น และผู้รับข้อมูลมีความต้องการที่จะใช้ข้อมูลของผู้ให้ข้อมูลเพื่อที่จะใช้ในการทำระบบ ISO 29110 เท่านั้น เพื่อให้สอดคล้องกับความต้องการของผู้ให้ข้อมูล ซึ่งผู้ให้ข้อมูลประสงค์ที่คุ้มครองเรื่องดังกล่าวไว้เป็นข้อมูลที่เป็นความลับ

ทั้งสองฝ่ายจึงตกลงทำสัญญานี้ขึ้น โดยมีเงื่อนไขดังต่อไปนี้

1. ในสัญญานี้

"ข้อมูลที่เป็นความลับ" หมายความถึง ข้อมูลใดๆ รวมทั้งข้อมูลของบุคคลภายนอกที่ฝ่ายผู้ให้ข้อมูลได้เปิดเผยแก่ฝ่ายผู้รับข้อมูล และฝ่ายผู้ให้ข้อมูลประสงค์ให้ฝ่ายผู้รับข้อมูลเก็บรักษาข้อมูลดังกล่าวไว้เป็นความลับและ/หรือความลับทางการค้าของฝ่ายผู้ให้ข้อมูล

2. การรักษาข้อมูลที่เป็นความลับ

2.1 ฝ่ายผู้รับข้อมูลตกลงว่าจะเก็บรักษาข้อมูลที่เป็นความลับที่ฝ่ายผู้ให้ข้อมูลได้เปิดเผยให้แก่ฝ่ายผู้รับข้อมูลภายใต้สัญญาฉบับนี้ โดยฝ่ายผู้รับข้อมูลตกลงที่จะดำเนินการเก็บรักษาข้อมูลที่เป็นความลับที่ได้รับจากฝ่ายผู้ให้ข้อมูลไว้เป็นความลับอย่างเคร่งครัด และไม่เปิดเผยข้อมูลที่เป็นความลับไม่ว่าทั้งหมดหรือแต่บางส่วนให้แก่บุคคลใดหรือองค์กรใดทราบ เว้นแต่จะเป็นการเปิดเผยข้อมูลที่เป็นความลับให้แก่ลูกจ้างหรือพนักงานของฝ่ายผู้รับข้อมูลและปฏิบัติตามเงื่อนไขในการรักษาข้อมูลที่เป็นความลับอย่างเคร่งครัดด้วย

2.2 การรักษาความลับตามสัญญานี้ ให้รักษาความลับตลอดระยะเวลาที่สัญญานี้มีผลบังคับใช้และมีผลตลอดไป ถึงแม้ว่าทั้งสองผู้ให้ข้อมูลและผู้เก็บข้อมูลจะไม่ได้ทำธุรกิจต่อกันก็ตาม

2.3 ผู้รับข้อมูลตกลงใช้ข้อมูลที่เป็นความลับเพียงเพื่อให้บรรลุตามวัตถุประสงค์ที่กำหนดไว้ในสัญญานี้เท่านั้น

3. การชดใช้ค่าเสียหาย

กรณีที่ผู้รับข้อมูลฝ่าฝืนข้อกำหนดตามสัญญานี้ และก่อให้เกิดความเสียหายแก่ผู้ให้ข้อมูล ผู้รับข้อมูลจะต้องชดใช้ค่าเสียหายให้แก่ผู้ให้ข้อมูลและ/หรือบุคคลที่ได้รับความเสียหายสำหรับความเสียหายเช่นว่านั้น

4. สัญญานี้มีผลใช้บังคับตั้งแต่วันที่ทั้งสองฝ่ายลงนามเป็นต้นไป และมีกำหนดระยะเวลานับแต่วันที่ลงนามในสัญญานี้ เมื่อสัญญานี้ได้สิ้นสุดลงไม่ว่ากรณีใดๆ ให้ข้อผูกพันในการเก็บความลับตามสัญญาฉบับนี้ยังคงมีผลใช้บังคับอยู่ต่อไป

5. สัญญาฉบับนี้ให้อยู่ใต้บังคับของกฎหมายประเทศไทย ให้ศาลของประเทศไทยมีอำนาจในกรณีที่มีข้อพิพาทใดๆ อันเกิดขึ้นจากสัญญานี้

สัญญานี้ทำขึ้นสองฉบับมีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความในสัญญานี้ละเอียดโดยตลอดแล้ว จึงได้ลงลายมือชื่อและประทับตราไว้ (หากมี) ไว้เป็นสำคัญต่อหน้าพยานและคู่สัญญาต่างเก็บไว้ฝ่ายละฉบับ

ลงชื่อ.....ผู้ให้ข้อมูล ลงชื่อ.....ผู้เก็บข้อมูล

(นาย xxx) (นาย xxx)

ลงชื่อ.....ผู้ให้ข้อมูล ลงชื่อ.....พยาน

(นาย xxx) (.....)

โรงพยาบาลเกาะสีชัง

จัดทำโดย : นายชัพ ธิราขันธ์
ผู้อนุมัติ : นายภูจิตต์ ตรีบำเพ็ญ
จัดทำเมื่อ : 24 / พฤศจิกายน / 2568
มีผลบังคับใช้ : 1 /ธันวาคม/ 2568

ข้อตกลงระดับการให้บริการ (Service Level Agreement - SLA)

1. บทนำ (Introduction)

ข้อตกลงระดับการให้บริการฉบับนี้จัดทำขึ้นระหว่าง **โรงพยาบาลเกาะสีชัง** ("ลูกค้า") และ **บริษัท** .....("ผู้ให้บริการ") เพื่อกำหนดข้อกำหนดและมาตรฐานการให้บริการ รวมถึงความคาดหวังในด้านคุณภาพของบริการ ความมั่นคงปลอดภัย และการจัดการเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับการให้บริการ **ระบบจัดการฐานข้อมูลลูกค้า** (Customer Database Management System)

2. ขอบเขตของบริการ (Scope of Services)

- ผู้ให้บริการจะให้บริการ **การจัดการและดูแลรักษาระบบฐานข้อมูลลูกค้า** ของ**โรงพยาบาลเกาะสีชัง** ซึ่งรวมถึง
    - การตรวจสอบและบำรุงรักษาฐานข้อมูลอย่างสม่ำเสมอ
    - การสำรองข้อมูล (Data Backup) เป็นประจำทุกวัน
    - การให้การสนับสนุนและการแก้ไขปัญหาฐานข้อมูลตามที่กำหนดในข้อตกลงนี้

3. **ระดับการให้บริการ** (Service Levels)

- **เวลาการให้บริการ** (Service Availability)
  - ผู้ให้บริการต้องรับประกันความพร้อมใช้งานของระบบฐานข้อมูลอย่างน้อย **99.5%** ต่อเดือน
  - กำหนดเวลาที่ให้บริการ: **24 ชั่วโมงต่อวัน, 7 วันต่อสัปดาห์**
- **เวลาตอบสนอง** (Response Time)
  - ผู้ให้บริการต้องตอบสนองต่อคำขอการสนับสนุนภายใน **1 ชั่วโมง** นับจากเวลาที่ได้รับแจ้งปัญหา
  - กำหนดเวลาการแก้ไขปัญหา:
    - ปัญหาระดับวิกฤติ (Critical): ภายใน **4 ชั่วโมง**
    - ปัญหาระดับสำคัญ (Major): ภายใน **8 ชั่วโมง**
    - ปัญหาระดับปานกลาง (Minor): ภายใน **24 ชั่วโมง**
- **การจัดการเหตุการณ์** (Incident Management)
  - ผู้ให้บริการต้องรายงานเหตุการณ์ทางไซเบอร์หรือการหยุดชะงักของบริการภายใน **30 นาที** นับจากเวลาที่เกิดเหตุการณ์
  - ต้องดำเนินการแก้ไขและป้องกันการเกิดซ้ำของเหตุการณ์ที่เกิดขึ้นโดยเร็วที่สุด

4. **ข้อกำหนดด้านความมั่นคงปลอดภัย** (Security Requirements)

- **การเข้าถึงข้อมูล** (Data Access)
  - ผู้ให้บริการต้องใช้การยืนยันตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication - MFA) ในการเข้าถึงระบบฐานข้อมูลของลูกค้า
  - การเข้าถึงข้อมูลจะต้องได้รับการจำกัดให้เฉพาะพนักงานของผู้ให้บริการที่มีความจำเป็นต้องใช้เท่านั้น
- **การจัดเก็บและการสื่อสารข้อมูล** (Data Storage and Communication)
  - ข้อมูลที่จัดเก็บในฐานข้อมูลและส่งผ่านต้องถูกเข้ารหัสด้วยมาตรฐาน AES-256 และ TLS/SSL ตามลำดับ
  - การสื่อสารข้อมูลทั้งหมดระหว่างผู้ให้บริการและลูกค้าจะต้องดำเนินการผ่าน VPN ที่ปลอดภัย
- **การตรวจสอบและการปฏิบัติตามข้อกำหนด** (Audit and Compliance)
  - ผู้ให้บริการต้องยอมรับการตรวจสอบความมั่นคงปลอดภัยโดยลูกค้าหรือบุคคลที่สามที่ลูกค้าแต่งตั้ง อย่างน้อยปีละหนึ่งครั้ง
  - ผู้ให้บริการต้องปฏิบัติตาม พรบ ไซเบอร์ 2562 ในการจัดการความมั่นคงปลอดภัยทางไซเบอร์

5. **การตรวจสอบประสิทธิภาพ** (Performance Monitoring)

- ผู้ให้บริการต้องจัดทำรายงานการตรวจสอบประสิทธิภาพการให้บริการและความมั่นคงปลอดภัยเป็นประจำทุกเดือน รายงานต้องครอบคลุมถึง
    - ระดับการให้บริการที่เป็นไปตาม SLA (เช่น ความพร้อมใช้งานของระบบ)
    - เหตุการณ์ที่เกิดขึ้นและวิธีการแก้ไข
    - การอัปเดตและการปรับปรุงที่ดำเนินการในเดือนนั้น ๆ
    - การพบเจอเหตุการณ์หรือภัยคุกคามทางไซเบอร์

6. **บทลงโทษและการชดเชย** (Penalties and Compensation)

- หากผู้ให้บริการไม่สามารถปฏิบัติตามระดับการให้บริการที่กำหนดไว้ใน SLA ลูกค้ามีสิทธิ์ในการเรียกร้องการชดเชย เช่น
    - ส่วนลดค่าบริการรายเดือน **10%** หากความพร้อมใช้งานของระบบต่ำกว่า 99.5% แต่ไม่ต่ำกว่า 98%
    - ยกเว้นค่าบริการในเดือนนั้นหากความพร้อมใช้งานของระบบต่ำกว่า 98%

7. **การแก้ไขและการทบทวนข้อตกลง** (Amendments and Review)

- ข้อตกลงนี้สามารถแก้ไขได้ตามความจำเป็น โดยต้องได้รับการเห็นชอบจากทั้งสองฝ่าย การแก้ไขต้องถูกบันทึกและแนบไว้เป็นภาคผนวกของข้อตกลงนี้
- ข้อตกลงนี้จะได้รับการทบทวนเป็นประจำทุกปีเพื่อให้มั่นใจว่าสอดคล้องกับความต้องการของลูกค้าและข้อกำหนดทางกฎหมาย

8. **เงื่อนไขและระยะเวลาของสัญญา** (Terms and Duration)

- ข้อตกลงนี้มีผลบังคับใช้ตั้งแต่วันที่ ..... ถึงวันที่ ..... หรือจนกว่าจะมีการยกเลิกหรือแก้ไขตามข้อตกลง
- การยกเลิกข้อตกลงต้องแจ้งล่วงหน้าอย่างน้อย **30 วัน** เป็นลายลักษณ์อักษรเท่านั้น

9. **ลายเซ็นต์** (Signatures)

- **บริษัท** .....

  ชื่อ: .....

  (.....)

  ตำแหน่ง: ผู้อำนวยการฝ่าย IT

  วันที่: .....

- **บริษัท** .....

  ชื่อ: .....

  (.....)

  ตำแหน่ง: ผู้จัดการฝ่ายบริการลูกค้า

  วันที่: .....