

บริษัท วินเนอร์ยี เมดิคอล จำกัด (มหาชน)

นโยบายความเสี่ยงด้านการคุ้มครอง ข้อมูลส่วนบุคคล

ฉบับ 00

16 / 12 / 2565

ใช้เฉพาะภายในเท่านั้น

ตารางควบคุมการเปลี่ยนแปลงของนโยบาย (Version Control)

ฉบับ ที่	แก้ไข ครั้งที่	หน้าที่	ข้อที่	วันที่ และรายละเอียดการแก้ไข
00	-	-	-	วันที่ 16/12/2565 : เริ่มและประกาศใช้คู่มือ

สารบัญ

	หน้า
1. บทนำ.....	4
2. เกณฑ์ประเมินโอกาสที่จะเกิดความเสี่ยง (LIKELIHOOD).....	5
3. ผลกระทบที่อาจเกิดขึ้นด้านจำนวนเงิน (POTENTIAL FINANCIAL IMPACT).....	6
4. ผลกระทบที่อาจเกิดขึ้น (POTENTIAL IMPACT).....	7
5. เกณฑ์ประเมินด้านผลกระทบ (IMPACT)	8
6. เกณฑ์ในการกำหนดระดับความเสี่ยง.....	11
7. ระดับความเสี่ยง (DEGREE OF RISK).....	12
8. ตารางแนวทางการบริหารจัดการความเสี่ยง.....	13

1. บทนำ

นโยบายการบริหารความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล

บริษัท วินเนอร์ยี่ เมดิคอล จำกัด (มหาชน) และบริษัทย่อย (เรียกว่า “บริษัท”) ได้ตระหนักถึงความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล และจะต้องจัดให้มีมาตรการในการรักษาความมั่นคงและปลอดภัยที่เหมาะสมกับความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล ดังนั้นการจัดทำการประเมินความเสี่ยงของผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลนั้นเป็นหนึ่งในกระบวนการที่บริษัทฯ ต้องจัดให้มีสำหรับการประมวลผลที่มีความเสี่ยงสูง เพื่อเป็นการปฏิบัติตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

การจัดทำด้านการคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพนั้นจะช่วยให้บริษัทฯ สามารถกำกับกับการปฏิบัติตามกฎหมายในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลได้ดียิ่งขึ้น อีกทั้งยังเป็นการสร้างความเชื่อมั่นและความไว้วางใจให้กับเจ้าของข้อมูลส่วนบุคคลและส่วนรวมมากขึ้น ช่วยลดความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลที่ไม่เหมาะสม ลดความเสี่ยงที่จะเกิดผลกระทบต่อชื่อเสียงของบริษัทฯ ทางบริษัทฯ จึงกำหนดนโยบายการบริหารความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล ดังต่อไปนี้

1. การประเมินความเสี่ยงเพื่อให้การประมวลผลข้อมูลส่วนบุคคลมีเท่าที่จำเป็น และได้สัดส่วนในการใช้ข้อมูลอย่างเหมาะสม
2. การประเมินความเสี่ยงที่อาจเกิดผลกระทบกับความเป็นส่วนตัว สิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
3. แนวทางในการจัดการกับความเสี่ยงที่อาจเกิดขึ้น รวมถึงมาตรการในการรักษาความปลอดภัยของข้อมูลที่เหมาะสมเพื่อให้แน่ใจว่าบริษัทฯ มีการคุ้มครองสิทธิเสรีภาพและประโยชน์อันของธรรมชาติของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่นที่มีความเสี่ยงที่จะได้รับผลกระทบ หากบริษัทฯ พิจารณาแล้วว่าจะระดับของความเสี่ยงนั้นสูงเกินกว่าที่บริษัทฯ สามารถจัดให้มีมาตรการในการลดความเสี่ยงนั้นได้ บริษัทฯ ควรพิจารณาไม่กระทำการประมวลผลข้อมูลส่วนบุคคลหรือปรึกษาคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

นโยบายฉบับนี้ ได้รับการทบทวนและได้รับการอนุมัติให้แก้ไขเพิ่มเติมจากที่ประชุมคณะกรรมการ ครั้งที่ 6/2565 เมื่อวันที่ 16 ธันวาคม 2565 และให้มีผลบังคับใช้ตั้งแต่วันที่ 16 ธันวาคม 2565 เป็นต้นไป



(ผศ.ดร.นพ.เทอดศักดิ์ ไรจน์สุรจิตติ)

ประธานกรรมการบริษัท

บริษัท วินเนอร์ยี่ เมดิคอล จำกัด (มหาชน)

2. เกณฑ์ประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood)

การวัดระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood)		
โอกาสที่จะเกิดความเสี่ยง	ความน่าจะเป็น	ความถี่ของรายการ
(1) เกิดขึ้นน้อย	น้อยกว่าร้อยละ 25	มีโอกาสดังกล่าวเกิดขึ้นหนึ่งครั้งต่อปี หรือไม่เกิดขึ้นเลย
(2) เกิดขึ้นบ้าง	มากกว่าร้อยละ 25 แต่ไม่เกินร้อยละ 50	มีโอกาสดังกล่าวเกิดขึ้น 2-3 ครั้งต่อปี
(3) เกิดขึ้นบ่อย	มากกว่าร้อยละ 50 แต่ไม่เกินร้อยละ 75	มีโอกาสดังกล่าวเกิดขึ้น 1 ครั้งต่อไตรมาส หรือเดือน
(4) เกิดประจำ	มากกว่าร้อยละ 75	มีโอกาสดังกล่าวเกิดขึ้น ทุกวัน หรือทุกอาทิตย์

3. ผลกระทบที่อาจเกิดขึ้นด้านจำนวนเงิน (Potential Financial Impact)

ระดับความเสี่ยง	แทนด้วยสี	มูลค่าจำนวนเงิน (หน่วยเป็น: ล้านบาท)
ต่ำ (Low)	L	0-1 ล้านบาท
ปานกลาง (Moderate)	M	> 1 ≤ 3 (มากกว่า 1 ล้านบาท แต่ไม่เกิน 3 ล้านบาท)
สูง (High)	H	> 3 ≤ 5 (มากกว่า 3 ล้านบาท แต่ไม่เกิน 5 ล้านบาท)
วิกฤติ (Crisis)	C	> 5 (มากกว่า 5 ล้านบาท)

4. ผลกระทบที่อาจเกิดขึ้น (Potential Impact)

<u>Security</u>	<u>Low</u>	<u>Moderate</u>	<u>High</u>
“Confidentiality” การจำกัดการเข้าถึงและการเปิดเผยข้อมูล รวมถึงวิธีการปกป้องความเป็นส่วนตัวและสิทธิในข้อมูล	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต คาดว่าอาจจะมีผลกระทบในทางลบอย่างจำกัด ต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กร หรือบุคคล	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต คาดว่าอาจจะมีผลกระทบในทางลบอย่างมาก ต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กร หรือบุคคล	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต คาดว่าอาจจะมีผลกระทบในทางลบอย่างร้ายแรงต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กร หรือ บุคคล
“Integrity” การรักษาความปลอดภัยของข้อมูล จากการดัดแปลงหรือถูกทำลายโดยไม่เหมาะสม รวมถึงการทำให้มั่นใจว่าข้อมูลมีความถูกต้อง	การดัดแปลงหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตคาดว่าจะมีผลกระทบอย่างจำกัด ต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กร หรือบุคคล	การดัดแปลงหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตคาดว่าจะมีผลกระทบอย่างมาก ต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กร หรือบุคคล	การดัดแปลงหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตคาดว่าจะมีผลกระทบอย่างร้ายแรง ต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กรหรือบุคคล
“Availability” การทำให้มั่นใจว่า สามารถเข้าถึงข้อมูลและใช้งานได้อย่างทันเวลาและเชื่อถือได้	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบสารสนเทศของข้อมูล คาดว่า <u>อาจมีผลกระทบอย่างจำกัด</u> ต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กรหรือบุคคล	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบสารสนเทศของข้อมูล คาดว่า <u>อาจมีผลกระทบอย่างมาก</u> ต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กรหรือบุคคล	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบสารสนเทศของข้อมูล คาดว่า <u>อาจมีผลกระทบอย่างร้ายแรง</u> ต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กรหรือบุคคล

5. เกณฑ์ประเมินด้านผลกระทบ (Impact)

ลำดับ	การวัดระดับความรุนแรงของผลกระทบ (Impact)	ระดับของผลกระทบ			
		(1) น้อย	(2) ปานกลาง	(3) รุนแรง	(4) วิกฤติ
ผลกระทบต่อองค์กร					
1.1	กลยุทธ์องค์กร	มีผลกระทบต่อบริษัท ส่งผลให้ฝ่ายบริหาร และหน่วยงานที่เกี่ยวข้องต้องเปลี่ยนแปลงกลยุทธ์ภายใน 4 เดือน <u>อ้างอิง</u> การวัดระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood)	มีผลกระทบต่อบริษัท ส่งผลให้ฝ่ายบริหาร และหน่วยงานที่เกี่ยวข้องต้องดำเนินการเปลี่ยนแปลงกลยุทธ์ภายใน 3 เดือน <u>อ้างอิง</u> การวัดระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood)	มีผลกระทบต่อบริษัทอย่างมีนัยสำคัญอย่างมาก ส่งผลให้ฝ่ายบริหาร และหน่วยงานที่เกี่ยวข้องต้องเร่งดำเนินการเปลี่ยนแปลงกลยุทธ์อย่างเร่งด่วนภายใน 2 เดือน <u>อ้างอิง</u> การวัดระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood)	มีผลกระทบต่อบริษัทอย่างมีนัยสำคัญสูงสุด ส่งผลให้ฝ่ายบริหาร และหน่วยงานที่เกี่ยวข้องต้องเร่งดำเนินการเปลี่ยนแปลงกลยุทธ์อย่างเร่งด่วนภายใน 1 เดือน <u>อ้างอิง</u> การวัดระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood)
1.2	ความน่าเชื่อถือ และความไว้วางใจของลูกค้า	มีข่าวเชิงลบ ผ่านสื่อทั้งภายในประเทศและดำเนินการแก้ไขปัญหาเรียบร้อยแล้ว	มีข่าวเชิงลบ ผ่านสื่อทั้งภายในประเทศและอยู่ระหว่างการแก้ไขปัญหา	มีข่าวเชิงลบ ผ่านสื่อทั้งภายในประเทศและต่างประเทศ และอยู่ระหว่างการแก้ไขปัญหา	มีข่าวเชิงลบ ผ่านสื่อทั้งภายในประเทศและต่างประเทศ และยังไม่มีความเห็นว่าการแก้ไขปัญหาที่ชัดเจน
2	ระบบเทคโนโลยีสารสนเทศ				
2.1	การหยุดชะงักของระบบ (Availability)	ระยะเวลาการหยุดชะงักของระบบ < 6 ชั่วโมง	ระยะเวลาการหยุดชะงักของระบบ ≥ 6 - 12 ชั่วโมง (มากกว่า 6-12 ชั่วโมง)	ระยะเวลาการหยุดชะงักของระบบ ≥ 12 - 24 ชั่วโมง (มากกว่า 12-24 ชั่วโมง)	ระยะเวลาการหยุดชะงักของระบบ > 24 ชั่วโมง (มากกว่า 24 ชั่วโมง)

ลำดับ	การวัดระดับความรุนแรงของผลกระทบ (Impact)	ระดับของผลกระทบ			
		(1) น้อย	(2) ปานกลาง	(3) รุนแรง	(4) วิกฤติ
2.2	ความเสียหายของข้อมูล (Integrity)	1. ฐานข้อมูลเสียหายบางส่วนไม่ถูกต้อง ไม่เป็นปัจจุบัน 2. กู้ข้อมูลกลับมาได้ > 75% (มากกว่า 75%) ของฐานข้อมูลบางส่วน / ข้อมูลเสียหายถาวรอย่างไม่มีนัยสำคัญ	1. ฐานข้อมูลเสียหายบางส่วนไม่ถูกต้อง ไม่เป็นปัจจุบัน 2. กู้ข้อมูลกลับมาได้ > 50% ≤ 75% (มากกว่า 50% แต่ไม่น้อยกว่า 75%) ของฐานข้อมูลที่สมบูรณ์	ฐานข้อมูลที่สำคัญเสียหายตั้งแต่ 50% เป็นต้นไป (มากกว่า 50%)	ฐานข้อมูลทั้งหมดเสียหายถาวร
2.3	การสูญเสียการเป็นความลับ (Confidentiality)	ข้อมูลบุคคลทั่วไป (General Personal Data) รั่วไหล ≤ 25% (น้อยกว่าหรือเท่ากับ 25%)	ข้อมูลบุคคลทั่วไป (General Personal Data) รั่วไหล > 25 % ≤ 50% (มากกว่า 25% แต่ไม่น้อยกว่าหรือเท่ากับ 50%)	ข้อมูลบุคคลทั่วไป (General Personal Data) รั่วไหล > 50 % ≤ 75 % (มากกว่า 50% แต่ไม่น้อยกว่าหรือเท่ากับ 75%)	1. ชนิดของข้อมูลอ่อนไหวสูญหาย รั่วไหล 2. ข้อมูลบุคคลทั่วไป (General Personal Data) รั่วไหล > 75 % (มากกว่า 75%)
3. กฎหมาย กฎเกณฑ์ ระเบียบต่าง ๆ					
3.1	โทษทางกฎหมายและค่าปรับ	กรณี/คดีความ ทำให้บริษัทอาจต้องโทษทางแพ่ง และเสียค่าปรับตั้งแต่ 0 – 1 ล้านบาท	กรณี/คดีความ ทำให้บริษัทอาจต้องโทษทางแพ่ง และเสียค่าปรับ > 1 ≤ 3 ล้านบาท (มากกว่า 1 ล้านบาท แต่ไม่เกิน 3 ล้านบาท)	กรณี/คดีความ ทำให้บริษัทอาจต้องโทษทางแพ่ง และเสียค่าปรับ > 3 ≤ 5 ล้านบาท (มากกว่า 3 ล้านบาท แต่ไม่เกิน 5 ล้านบาท)	1. กรณี/คดีความ ทำให้บริษัทต้องโทษทางแพ่งและเสียค่าปรับ > 5 (มากกว่า 5 ล้านบาท) 2. กรณี/คดีความ ทำให้บริษัทอาจต้องโทษทางอาญา และโทษทางปกครอง

ลำดับ	การวัดระดับความรุนแรงของผลกระทบ (Impact)	ระดับของผลกระทบ			
		(1) น้อย	(2) ปานกลาง	(3) รุนแรง	(4) วิกฤติ
4	การจัดเก็บ/ทำลายข้อมูล* <i>Remark:</i> บนพื้นฐานของ ROPA ของแต่ละแผนก	1. การจัดเก็บข้อมูลส่วนบุคคลให้สอดคล้องกับวัตถุประสงค์ > 75% (มากกว่า 75%) 2. ระยะเวลาการเก็บรักษาตามวัตถุประสงค์ > 75% (มากกว่า 75%) 3. ปฏิบัติตามกฎหมายระเบียบที่วางไว้ > 75% (มากกว่า 75%)	1. มีจัดเก็บข้อมูลส่วนบุคคลให้สอดคล้องกับวัตถุประสงค์ > 50% ≤ 75% (มากกว่า 50% แต่ไม่เกิน 75%) 2. ระยะเวลาการเก็บรักษาตามวัตถุประสงค์ > 50% ≤ 75% (มากกว่า 50% แต่ไม่เกิน 75%) 3. ปฏิบัติตามกฎหมายระเบียบที่วางไว้ > 50 ≤ 75% (มากกว่า 50% แต่ไม่เกิน 75%)	1. มีจัดเก็บข้อมูลส่วนบุคคลให้สอดคล้องกับวัตถุประสงค์ > 25% ≤ 50% (มากกว่า 25% แต่ไม่เกิน 50%) 2. ระยะเวลาการเก็บรักษาตามวัตถุประสงค์ > 25 ≤ 50% (มากกว่า 25% แต่ไม่เกิน 50%) 3. ปฏิบัติตามกฎหมายระเบียบที่วางไว้ > 25% ≤ 50% (มากกว่า 25% แต่ไม่เกิน 50%)	1. การจัดเก็บข้อมูลส่วนบุคคลให้สอดคล้องกับวัตถุประสงค์ ≤ 25% (น้อยกว่าหรือเท่ากับ 25%) 2. ระยะเวลาการเก็บรักษาตามวัตถุประสงค์ ≤ 25% (น้อยกว่าหรือเท่ากับ 25%) 3. ปฏิบัติตามกฎหมายระเบียบที่วางไว้ ≤ 25% (น้อยกว่าหรือเท่ากับ 25%)
5	สิทธิของเจ้าของข้อมูล	เจ้าของข้อมูลอาจมีความรู้สึกไม่สะดวก หรือรำคาญเพิ่มขึ้นเล็กน้อยในการที่เขาจะได้รับบริการหรือผลลัพธ์โดยปราศจากปัญหา* (เช่น ระยะเวลาในการกรอกข้อมูลใหม่ การถูกรบกวน)* *พิจารณาจากข้อร้องเรียน ที่ทาง DPO ได้รับจากข้อร้องเรียน)	เจ้าของข้อมูลมีความรู้สึกไม่สะดวกอย่างมีนัยสำคัญ โดยยังสามารถได้รับการบริการหรือผลลัพธ์ถึงแม้จะมีความยากลำบากมากขึ้น* (เช่น มีค่าใช้จ่ายเพิ่มเติม การปฏิเสธให้ได้รับการเข้าถึงการใช้บริการทางธุรกิจ ความกลัว ขาดความเข้าใจความเครียด) (*พิจารณาจากข้อร้องเรียน ที่ทาง DPO ได้รับจากข้อร้องเรียน)	เจ้าของข้อมูลพบความยากลำบาก หรือเสียหายมากอย่างมีนัยสำคัญ หรือรู้สึกที่ไม่คุ้มค่าในการรับบริการหรือผลลัพธ์เมื่อเทียบกับความยากลำบาก* (*พิจารณาจากข้อร้องเรียน ที่ทาง DPO ได้รับจากข้อร้องเรียน)	เจ้าของข้อมูลพบความยากลำบาก หรือเสียหายมากอย่างมีนัยสำคัญ หรือ ไม่คุ้มค่าในการรับบริการหรือผลลัพธ์เมื่อเทียบกับความยากลำบากอย่างมาก* (*พิจารณาจากข้อร้องเรียน ที่ทาง DPO ได้รับจากข้อร้องเรียน)

6. เกณฑ์ในการกำหนดระดับความเสี่ยง

ตารางการจัดระดับความเสี่ยง (Risk Map)				
ผลกระทบ (Impact)	โอกาสที่จะเกิด(Likelihood)			
	(1) เกิดขึ้นน้อย	(2) เกิดขึ้นบ้าง	(3) เกิดขึ้นบ่อย	(4) เกิดประจำ
(1) น้อย	L	L	M	M
(2) ปานกลาง	L	M	H	H
(3) รุนแรง	M	H	H	C
(4) วิกฤติ	C	C	C	C

7. ระดับความเสี่ยง (Degree of Risk)

ระดับความเสี่ยง (Degree of Risk)				
ผลกระทบ (Impact)	โอกาสที่จะเกิด(Likelihood)			
	(1) เกิดขึ้นน้อย	(2) เกิดขึ้นบ้าง	(3) เกิดขึ้นบ่อย	(4) เกิดประจำ
(1) น้อย	1	2	3	4
(2) ปานกลาง	2	4	6	8
(3) รุนแรง	3	6	9	12
(4) วิกฤติ	4	8	12	16

8. ตารางแนวทางการบริหารจัดการความเสี่ยง

การจัดการความเสี่ยงตามลำดับความสำคัญ			
ระดับความเสี่ยง	ระดับคะแนน	แทนด้วยสี	การตอบสนองความเสี่ยง
ต่ำ (Low)	1-2	L	ระดับที่ยอมรับได้ แต่ต้องเฝ้าระวัง
ปานกลาง (Moderate)	3-4	M	หน่วยงานที่เกี่ยวข้อง สามารถจัดการความเสี่ยงได้โดย <u>ปฏิบัติตามกระบวนการ</u>
สูง (High)	5-9	H	ฝ่ายบริหาร และหน่วยงานที่เกี่ยวข้องต้องดำเนินการควบคุมและจัดการความเสี่ยง <u>ทันที และควบคุมไม่ให้เคลื่อนย้ายไประดับวิกฤติ</u>
วิกฤติ (Crisis)	10-16	C	ฝ่ายบริหาร และหน่วยงานที่เกี่ยวข้องต้องเร่งดำเนินการจัดการความเสี่ยง <u>ทันทีอย่างเร่งด่วน</u>