WINNERGY MEDICAL PUBLIC COMPANY LIMITED

Risk Management Policy on

Personal Data Protection

Issue No. 00

16 / 12 / 2022

For Internal Use Only

Version Control for Risk Management Policy on Personal Data Protection

Issue No.	Edit No.	Page	Item No.	Date and Modification Details
00	-	-	-	16/12/2022: Manual commencement

Content

1. Introduction

Risk Management Policy on Personal Data Protection

Winnergy Medical Public Company Limited and its subsidiaries (referred to as the "**Company**") are aware of the risks of personal data protection that affect the rights and freedoms of individuals and must provide security and safety measures that are appropriate. Therefore, conducting a risk assessment of personal data protection impacts is one of the processes that the Company must provide for high-risk processing to comply with the Personal Data Protection Act (PDPA).

The effective protection of personal information will help the Company to better regulate the compliance of the rules on personal data protection. Moreover, it also creates more confidence and trust among the owners of personal information and the public, helping reduce the risk of inappropriate processing of personal data, and reducing the risk of impacts on the Company's reputation. Therefore, the Company has established a Risk Management Policy on Personal Data Protection as follows:

1. Risk assessment to ensure that the processing of personal data is necessary and proportionate to the use of information appropriately.

2. Assessment of risks that may affect privacy rights and freedoms of the subjects of personal data.

3. Guidelines for dealing with potential risks including appropriate data security measures to ensure that the Company provides the protection of rights, liberties, and moral interests of the data subject or other individuals who are at risk. If the Company considers that the level of risk is higher than the Company can provide measures to reduce such risks, the Company should consider not processing personal data or consult the Personal Data Protection Committee.

This policy has been reviewed and approved for additional amendments from the Board of Directors' Meeting No. 6/2022 held on 16 December 2022 and is effective from 16 December 2022 onwards.

(Asst. Prof. Dr. Terdsak Rojsurakitti)
Chairman, Board of Directors
Winnergy Medical Public Company Limited

2. Risk Assessment Criteria – Likelihood

Risk Assessment Criteria – Likelihood		
Likelihood	**Probability**	**Frequency**
(1) Low occurrence	≤ 25%	May occur once a year or not at all
(2) Moderate occurrence	26 – 50%	May occur 2-3 times a year
(3) High occurrence	51 – 75%	May occur once in a trimester or a month
(4) Very High occurrence	≥ 75%	May occur every day or every week

3. Potential Financial Impact

Degree of Risk	Color	Amount Worth (unit: million Baht)
Low	L	0-1 million Baht
Moderate	M	> 1 ≤3 (over 1 million Baht, but below 3 million Baht)
High	H	> 3 ≤5 (over 3 million Baht, but below 5 million Baht))
Crisis	C	> 5 (over 5 million Baht)

4. Potential Impact

Security	Low	Moderate	High
"Confidentiality" refers to the limitation of access and disclosure of information including how to protect privacy and data rights.	Unauthorized disclosure where limited negative impacts on the operation of the organization, property of the organization, or individual may be expected.	Unauthorized disclosure where high negative impacts on the operation of the organization, property of the organization, or individual may be expected.	Unauthorized disclosure where serious negative impacts on the operation of the organization, property of the organization, or individual may be expected.
"Integrity" refers to data security from improper modification or destruction including ensuring that information is accurate.	Unauthorized alterations or destruction of the data where limited negative impact on the operation of the organization, property of the organization, or individual may be expected.	Unauthorized alterations or destruction of the data where high negative impact on the operation of the organization, property of the organization, or individual may be expected.	Unauthorized alterations or destruction of the data where serious negative impact on the operation of the organization, property of the organization, or individual may be expected.
"Availability" refers to the assurance that the information can be accessed and used in a timely and reliable manner.	Interruption of access to or use of data or information systems where limited negative impact on the operation of the organization, property of the organization, or individual may be expected.	Interruption of access to or use of data or information systems where high negative impact on the operation of the organization, property of the organization, or individual may be expected.	Interruption of access to or use of data or information systems where serious negative impact on the operation of the organization, property of the organization, or individual may be expected.

5. Impact Assessment Criteria

Sl. No.	Impact Assessment Criteria	Degree of Impact			
		(1) Low	(2) Moderate	(3) High	(4) Crisis
1	**Corporate Impact**				
1.1	**Corporate Strategy**	Affects the Company, causing the management and related departments to change their strategies *within four (4) months*. *Ref: Risk Assessment Criteria – Likelihood*	Affects the Company, causing the management and related departments to change their strategies *within three (3) months*. *Ref: Risk Assessment Criteria – Likelihood*	Affects the Company, causing the management and related departments to change their strategies *within two (2) months*. *Ref: Risk Assessment Criteria – Likelihood*	Affects the Company, causing the management and related departments to change their strategies *within one (1) month*. *Ref: Risk Assessment Criteria – Likelihood*
1.2	**Credibility and Customer Trust**	There was negative news through the media within the country and the problem has been successfully solved.	There is negative news through the media within the country and the problem is being solved.	There is negative news through both domestic and international media and the problem is being solved.	There is negative news through both domestic and international media and there is no clear solution to the problem.
2	**Information Technology System**				
2.1	**System Interruption (Availability)**	System interruption period < 6 hours	System interruption period ≥ 6 - 12 hours (over 6-12 hours)	System interruption period ≥ 12 - 24 hours (over 12-24 hours)	System interruption period > 24 hours (over 24 hours)
2.2	**Data Corruption (Integrity)**	1. Database is partially corrupted, invalid, not current. 2. Data recovery > 75% (over 75%) of the complete database / insignificant permanent data corruption	1. Database is partially corrupted, invalid, not current. 2. Data recovery > 50% ≤ 75% (over 50% below or equals to 75%) of the complete database.	Critical database corruption over 50%. (over 50%)	All databases are permanently corrupted/damaged.

Sl. No.	Impact Assessment Criteria	Degree of Impact			
		(1) Low	(2) Moderate	(3) High	(4) Crisis
2.3	**Loss of Confidentiality**	Leakage of General Personal Data ≤ 25% (below or equals to 25%)	Leakage of General Personal Data > 25 % ≤ 50% (over 25% but below or equals to 50%)	Leakage of General Personal Data > 50 % ≤ 75 % (over 50% but below or equals to 75%)	1. Leakage or Loss of Sensitive Information 2. Leakage of General Personal Data > 75 % (over 75%)
3. Laws, Rules, Regulations					
3.1	**Legal Penalties and Fines**	Cases/Lawsuits that *may cause the Company to be subjected to civil penalties and pay fines* ranging from 0 – 1 million Baht.	Cases/Lawsuits that *may cause the Company to be subjected to civil penalties and pay fines of* > 1 ≤ 3 million Baht (*over 1 million Baht, but below or equals to 3 million Baht).*	Cases/Lawsuits that *may cause the Company to be subjected to civil penalties and pay fines of* > 3 ≤ 5 million Baht (*over 3 million Baht, but below or equals to 5 million Baht).*	1. Cases/Lawsuits that *cause the Company to be subjected to civil penalties and pay fines* over 5 million Baht (*over 5 million Baht).* 2. Cases/Lawsuits that cause the Company to be subjected to criminal penalties and administrative penalties.
4	**Data Storage/Destruction*** *Remark:* Based on ROPA of each department.	1. Storage of personal data complies with the purpose > 75% (over 75%) 2. Storage period complies to the purpose > 75% (over 75%) 3. Compliance with regulations > 75% (over 75%)	1. Storage of personal data complies with the purpose > 50% ≤ 75% (over 50% but below or equals to 75%) 2. Storage period complies to the purpose > 50% ≤ 75% (over 50% but below or equals to 75%) 3. Compliance with regulations > 50 ≤ 75% (over 50% but below or equals to 75%)	1. Storage of personal data complies with the purpose > 25%≤ 50% (over 25% but below or equals to 50%) 2. Storage period complies to the purpose > 25 ≤ 50% (over 25% but below or equals to 50%) 3. Compliance with regulations > 25% ≤ 50% (over 25% but below or equals to 50%)	1. Storage of personal data complies with the purpose ≤ 25% (below or equals to 25%) 2. Storage period complies to the purpose ≤ 25% (below or equals to 25%) 3. Compliance with regulations ≤ 25% (below or equals to 25%)

Sl. No.	Impact Assessment Criteria	Degree of Impact			
		(1) Low	(2) Moderate	(3) High	(4) Crisis
5	**Data Subject Right**	The data subjects may feel slight uncomfortable or annoyance for them to receive services or results without problems* (e.g., time for re-entering, disturbance) *(*Considering the complaints received by the DPO)*	The data subjects experience significant inconvenience, but can still get the services or results even with more difficulty* (e.g., additional costs, denial of access to business services, fear, lack of understanding, stress) *(*Considering the complaints received by the DPO)*	The data subjects encounter highly significant difficulty or damage, or feel that the services or results are not worthwhile in relation to the difficulty* *(*Considering the complaints received by the DPO)*	The data subjects encounter highly significant difficulty or damage, or feel that the services or results are not worthwhile in relation to the substantial difficulty* (*Considering the complaints received by the DPO)

6. Degree of Risk Determination Criteria

Risk Map				
Impact	Likelihood			
	(1) Low Occurrence	(2) Moderate Occurrence	(3) High Occurrence	(4) Very High Occurrence
(1) Low	L	L	M	M
(2) Moderate	L	M	H	H
(3) High	M	H	H	C
(4) Crisis	C	C	C	C

7. Degree of Risk

Degree of Risk				
Impact	**Likelihood**			
	(1) Low Occurrence	**(2) Moderate Occurrence**	**(3) High Occurrence**	**(4) Very High Occurrence**
(1) Low	1	2	3	4
(2) Moderate	2	4	6	8
(3) High	3	6	9	12
(4) Crisis	4	8	12	16

8. Table of Risk Management Guidelines

Risk Management by Prioritization			
Degree of Risk	**Score**	**Color**	**Risk Response**
Low	1-2	**L**	Acceptable level, but must be cautious
Moderate	3-4	**M**	Relevant departments can manage the risk by **following the procedures**
High	5-9	**H**	The management and relevant departments must take action to control and manage the risks **immediately and control not to elevate to the critical level**.
Crisis	10-16	**C**	The management and relevant departments must **urgently and immediately act on risk management**.