พญาไท PHYATHAI
ศรีราชา • SRIRACHA

QP – PTS – 003
นโยบายและวัตถุประสงค์ด้านความปลอดภัยของสารสนเทศ

ผู้ทบทวน ..... (ผู้จัดการแผนกสนับสนุนเทคโนโลยีสารสนเทศ / เลขานุการคณะกรรมการความปลอดภัยสารสนเทศ (ISC))
(ปรีดี กมลพจน์)
19 ต.ค. 2565

ผู้รับรอง ..... (ผู้จัดการส่วนบริหารคุณภาพ)
(พว.เยาวลักษณ์ บัณฑิตจีน)
19 ต.ค. 2565

ผู้อนุมัติ ..... (ผู้อำนวยการโรงพยาบาล /ประธานคณะกรรมการความปลอดภัยสารสนเทศ ISC / ISMR)
(นพ.ชาญชัย ลี้สมประสงค์)
19 ต.ค. 2565

แก้ไขครั้งที่ : 6

วันที่บังคับใช้ : 19 ต.ค. 2565

ประวัติการแก้ไขเอกสาร

เลขที่ ผอ.	แก้ไขครั้งที่	วันที่บังคับใช้ส่วนที่แก้ไข	รายละเอียดการแก้ไข	เลขที่ใบแจ้งขอแก้ไข
008/2562	1	1 เม.ย. 62	เพิ่มเติมนโยบายด้านความปลอดภัยสารสนเทศ	T026/62
030/2562	2	1 ส.ค. 62	เพิ่มเติมนโยบายด้านความปลอดภัยสารสนเทศ	T092/62
004/2563	3	30 ม.ค. 63	ทบทวนนโยบายและวัตถุประสงค์ด้านความปลอดภัยสารสนเทศ ตามมติที่ประชุมคณะกรรมการ ISC ครั้งที่ 1 / 2563	T005/63
037/2563	4	1 ธ.ค. 63	ทบทวนนโยบายและวัตถุประสงค์ด้านความปลอดภัยสารสนเทศ ตามมติที่ประชุมคณะกรรมการ ISC เมื่อวันที่ 24 พฤศจิกายน 2563	T065/63
044/2564	5	28 ต.ค. 64	ทบทวนนโยบายและวัตถุประสงค์ด้านความปลอดภัยสารสนเทศ ตามมติที่ประชุมคณะกรรมการ ISC เมื่อวันที่ 22 ตุลาคม 2564	T056/64
121/2565	6	19 ต.ค. 2565	ทบทวนนโยบายและวัตถุประสงค์ด้านความปลอดภัยสารสนเทศ	T134/65

พญาไท PHYATHAI
ศรีราชา • SRIRACHA

คำสั่งที่ ผอ.121/2565

นโยบายและวัตถุประสงค์ด้านความปลอดภัยของสารสนเทศ

ตามที่ผู้อำนวยการโรงพยาบาล ซึ่งเป็นผู้บริหารสูงสุดของโรงพยาบาลฯ มีความมุ่งมั่นที่จะนำโรงพยาบาลเข้าสู่ระบบมาตรฐานสากลตามข้อกำหนด ISO/IEC 27001 : 2013 ซึ่งมีองค์ประกอบครอบคลุม C I A คือ

- การรักษาความลับ (Confidentiality)
- ความถูกต้อง ครบถ้วน สมบูรณ์ (Integrity)
- ความพร้อมใช้เสมอ (Availability)

โรงพยาบาลฯ จึงได้กำหนด**นโยบายด้านความปลอดภัยของสารสนเทศ** ดังนี้

1. โรงพยาบาลฯ จะวางแผน จัดการ ดูแล และควบคุม เรื่องความปลอดภัยของสารสนเทศ ระบบโครงข่าย เครื่องมือ อุปกรณ์ ให้อยู่ในระบบมาตรฐาน เป็นที่ยอมรับมีความน่าเชื่อถือ และสามารถตรวจสอบได้
2. การเก็บรักษาความปลอดภัยของสารสนเทศ จะต้องระบุไว้เป็นส่วนหนึ่งในสัญญาบริการที่โรงพยาบาลฯ ทำกับผู้ใช้บริการ ไม่ว่าจะเป็นการบริการประเภทใด ซึ่งโรงพยาบาลฯ จะต้องถือปฏิบัติโดยเคร่งครัด ภายใต้กรอบแห่งกฎหมาย ข้อกำหนด และกฎเกณฑ์ต่างๆ ที่เกี่ยวข้อง
3. โรงพยาบาลฯ กำหนดมาตรการเกี่ยวกับระบบการจัดการความปลอดภัยสารสนเทศ โดยถือเป็นหน้าที่ที่พนักงานทุกคนในโรงพยาบาลฯ จะต้องปฏิบัติตาม และหากมีการฝ่าฝืน ให้ถือว่าเป็นการกระทำผิดวินัยอย่างร้ายแรง
4. โรงพยาบาลฯ ถือเป็นหน้าที่ที่จะต้องให้ความรู้แก่พนักงาน และแจ้งให้ทราบถึงความสำคัญของการรักษาความปลอดภัยสารสนเทศ เช่น การใช้สื่อ Social, การละเมิดสิทธิ, การเข้าถึงข้อมูล, กฎหมายด้านสารสนเทศ โดยเน้นพรบ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) เป็นต้น อย่างน้อยปีละ 1 ครั้ง รวมทั้งเมื่อมีการแก้ไขหรือเปลี่ยนแปลงใดๆ ที่เกี่ยวข้องกับกฎหมาย ข้อกำหนด มาตรการ และกฎเกณฑ์ต่างๆ ด้านสารสนเทศ โรงพยาบาลฯ จะต้องแจ้งแก่พนักงานทราบ
5. มาตรการเกี่ยวกับผู้ให้บริการจากภายนอก (Outsource) คู่ค้า คู่ความร่วมมือ ต้องครอบคลุมถึงวิธีการคัดเลือกและพิจารณาคุณสมบัติของผู้ให้บริการ มีข้อกำหนดเกี่ยวกับการใช้บริการเพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศอย่างไม่เหมาะสม รวมถึงข้อกำหนดเกี่ยวกับการรักษาความลับของข้อมูล และไม่เปิดเผยข้อมูลที่มีความสำคัญ ต้องปฏิบัติอย่างเคร่งครัด และโรงพยาบาลฯ จะแจ้งซ้ำเมื่อข้อกำหนดเกิดการเปลี่ยนแปลง
6. โรงพยาบาลฯ จะดำเนินการปรับปรุงระบบการจัดการความปลอดภัยของสารสนเทศอย่างต่อเนื่อง เพื่อให้สอดคล้องกับการดำเนินธุรกิจ สภาพแวดล้อม และพัฒนาเชิงระบบเพื่อให้มีระบบการป้องกันและแผนรองรับภัยคุกคามทางไซเบอร์ ภัยโจรกรรมข้อมูลให้สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงอย่างต่อเนื่อง
7. โรงพยาบาลฯ ต้องจัดให้มีการประเมินประสิทธิภาพของการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยหน่วยงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศของโรงพยาบาล (IT Audit / Internal Audit) หรือผู้ตรวจสอบภายนอก (External Audit) และฝึกซ้อมแผนรองรับกรณีระบบคอมพิวเตอร์ของโรงพยาบาล (HIS) ใช้งานไม่ได้ อย่างน้อยปีละ 1 ครั้ง เพื่อปรับปรุงแก้ไขข้อบกพร่องของการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

เพื่อให้บรรลุถึงนโยบายในการจัดการเกี่ยวกับความปลอดภัยของสารสนเทศให้ได้คุณภาพจึงได้มีการกำหนด

วัตถุประสงค์ด้านความปลอดภัยของสารสนเทศ ไว้ดังนี้

1. จะต้องไม่มีการรั่วไหล หรือการสูญหายของข้อมูลของผู้ใช้บริการ โดยโรงพยาบาลฯ มีหน้าที่ในการจัดเก็บและรักษาข้อมูลของผู้ใช้บริการภายใต้กรอบแห่งกฎหมาย ข้อกำหนด และกฎเกณฑ์ต่างๆ ที่เกี่ยวข้องตามแบบและวิธีการที่ได้ทำความตกลงร่วมกันไว้ ระหว่างโรงพยาบาลฯ กับผู้ใช้บริการ รวมทั้งการไม่เปิดเผยข้อมูลใดๆ ที่มิได้รับความยินยอมจากผู้ใช้บริการสู่สาธารณชนหรือบุคคลภายนอก
2. เรื่องมาตรฐานการจัดการความปลอดภัยของสารสนเทศของโรงพยาบาลฯ โรงพยาบาลฯ จะต้องมีการตรวจสอบขั้นตอน หรือวิธีการปฏิบัติอันเกี่ยวกับการจัดการความปลอดภัยของสารสนเทศอยู่ตลอดเวลา และมีการบันทึกไว้เป็นลายลักษณ์อักษร
3. โรงพยาบาลฯ จะต้องจัดทำเอกสารที่ระบุไว้อย่างชัดเจนว่า พนักงานจะไม่นำข้อมูลของโรงพยาบาลฯ หรือข้อมูลของผู้ใช้บริการไปเปิดเผยแก่บุคคลภายนอกหรือที่ใดๆ หากไม่ได้รับความยินยอมจากโรงพยาบาลฯ หรือผู้ใช้บริการเป็นลายลักษณ์อักษร
4. ต้องให้ความรู้แก่พนักงาน และแจ้งให้ทราบถึงความสำคัญของการรักษาความปลอดภัยสารสนเทศ รวมทั้งการแก้ไขหรือเปลี่ยนแปลงใดๆ ที่เกี่ยวข้องกับด้านสารสนเทศ เพื่อให้ผู้ปฏิบัติงานเข้าใจและถือปฏิบัติภายใต้กฎหมาย ข้อกำหนด มาตรการและกฎเกณฑ์ต่างๆ ที่ออกมาควบคุม
5. กำหนดให้ผู้มีสิทธิเท่านั้นที่จะเข้าถึงข้อมูลได้ทุกเมื่อที่ต้องการ ต้องมีการควบคุมไม่ให้ระบบล้มเหลว มีการสำรองข้อมูลเพื่อให้ระบบมีสมรรถภาพทำงานได้อย่างต่อเนื่อง
6. ระบบสารสนเทศได้รับการดูแล ให้มีความถูกต้อง ครบถ้วน สมบูรณ์ และควบคุมไม่ให้มีการเปลี่ยนแปลงแก้ไขโดยผู้ไม่มีอำนาจ คุณภาพและความเชื่อมั่นของการให้บริการของโรงพยาบาลฯ เป็นความรับผิดชอบของเจ้าหน้าที่ หรือบุคลากรทุกคน
7. ต้องประเมินประสิทธิภาพ ติดตามตรวจสอบความผิดปกติและช่องโหว่ ฝึกซ้อมแผนรองรับกรณีระบบคอมพิวเตอร์ของโรงพยาบาล (HIS) ใช้งานไม่ได้ และทบทวนประเด็นที่ต้องปรับปรุงแก้ไขข้อบกพร่องของการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศของโรงพยาบาล อย่างต่อเนื่องและสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง
8. ต้องจัดทำแนวทางปฏิบัติสำหรับรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ (Information Technology Risk Management) และความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cyber security) และทบทวนอย่างน้อยปีละ 1 ครั้ง รวมทั้งศึกษา ถอดบทเรียนจากเหตุการณ์ที่เกิดขึ้นจริง เรียนรู้ และพัฒนาเชิงระบบอย่างต่อเนื่อง

จึงประกาศมาเพื่อทราบโดยทั่วกัน

ทั้งนี้ ตั้งแต่วันที่ 19 ตุลาคม 2565 เป็นต้นไป

(นพ.ชาญชัย ลี้สมประสงค์)
ผู้อำนวยการโรงพยาบาลพญาไทศรีราชา / ISMR
ประธานคณะกรรมการความปลอดภัยสารสนเทศ (ISC)

พญาไท PHYATHAI
ศรีราชา • SRIRACHA

QP – PTS – 003(E)

Information Security Policy and Objectives

Reviewer..... (Manager of Information Technology Support
(Predee Kamonpoj) Department / Secretary of the Information
Security Committee (ISC))
19 ต.ค. 2565

Certifier..... (Quality Management Division Manager)
(Yaowalak Banditjean) 19 ต.ค. 2565

Approver..... (Director of Phyathai Sriracha Hospital/ ISMR
(Dr.Chanchai Leesomprasong) Secretary of the Information Security Commit
(ISC))
19 ต.ค. 2565

Edit No. : 6

Effective date : 19 ต.ค. 2565

Document revision history

No.	Edit No.	Effective date	Correction details	notification number for correction
008/2562	1	1 Apr 2019	Additional Information Security Policy	T026/62
030/2562	2	1 Aug 2019	Additional Information Security Policy	T092/62
004/2563	3	30 Jan 2020	Review information security policies and objectives, according to the resolution of the Board of Directors' meeting ISC No. 1 / 2563	T005/63
037/2563	4	1 Dec 2020	Review information security policies and objectives, according to the resolution of the Board of Directors' meeting ISC date 24 November 2563	T065/63
044/2564	5	28 Oct 2021	Review information security policies and objectives. according to the resolution of the Board of Directors' meeting ISC date 22 October 2564	T056/64
121/2565	6	19 ต.ค. 2565	Review information security policies and objectives.	T134/65

พญาไท PHYATHAI
ศรีราชา • SRIRACHA

Order no.121/2565

Information Security Policy and Objectives

According to the hospital director who is the chief executive of the hospital with the objective to bring the hospital into the system of international standards according to ISO/IEC ISO27001: 2013 requirements, which gives the information system the characteristics of C I A, which are:

- Confidentiality
- Integrity
- Availability

The hospital therefore has established a **policy on information security** as follows:

1. 1. The hospital will plan, manage, supervise and control information security, network system, tools and equipment following a standard system. This is acknowledged to be reliable and can be tracked.
2. Information Security Preservation must be specified as part of the service contract at the hospital with service users, regardless of any type of service. Which the hospital must be strictly adhered to within the framework of laws, regulations and rules related.
3. The hospital determines and finalizes the measures related to the information security management system. This is a responsibility that all staff in the hospital must comply to and if there is a violation then should be regarded as a serious breach of discipline.
4. The hospital is a duty to educate employees. and inform them of the importance of information security such as the use of social media, rights violations, access to information, information laws By emphasizing the Personal Data Protection Act (PDPA), etc., at least once a year, including when there is any amendment or change. related to laws, regulations, measures and rules regarding information, the hospital must inform its employees.
5. Measures relating to outsourced service providers, partners and cooperation partners. Must cover how to select and consider the qualifications of service providers. There are provisions in place regarding the use of services to reduce the risk of improper access to information assets including data confidentiality requirements which does not disclose sensitive information and must be strictly adhered to and the hospital will notify again when the terms change.
6. The hospital will continually improve its information security management system to be in line with business operations, environmental and systematic development in order to have a protection system and a plan to support cyber threats and to identity theft in line with constantly changing technology.
7. The hospital must provide an assessment of the effectiveness of the security of the information technology system. By the Hospital's Information Technology Internal Audit Unit (IT Audit / Internal Audit) or external auditors and practice plans to support the hospital's computer system (HIS) failure at least annually 1 time to improve and fix the security flaws of the hospital's information technology system. In order to achieve the quality of information security management policies.

Information security objectives are as follows:

1. There must be no leakage or loss of user data by the hospital. It is responsible for collecting and maintaining user data within the framework of laws, regulations and rules related according to the forms and methods that have been mutually agreed upon between the hospital with service users including non-disclosure of any information without the consent of the user to the public or outsiders.
2. Regarding the hospital's information security management standards, the hospital must have a review process or practices relating to information security management at all times and record in writing.
3. The hospital must provide a document that clearly states that employees will not use the hospital's information or information of service users to disclose to third parties or any others without the consent of the hospital or service users in writing.
4. Employees must be informed of the importance of information security including any amendments or changes related to information to enable operators to understand and comply with laws, regulations, measures and rules.
5. Assign only those who have the right to access information. There must be some control to prevent system failures and to have a backup in order for the system to be able to work continuously.
6. Information systems are maintained to be accurate and complete to control that changes are not made by those without authority. The quality and confidence of the hospital's services is the responsibility of the officer or all personnel.
7. Must evaluate the efficiency monitoring anomalies and vulnerabilities rehearsal plans to support the hospital's computer system failure (HIS) and review issues that need to be improved and corrected in the hospital's information technology system security at least once a year.
8. Must establish guidelines for the security and risk control of information technology systems and cyber-threat risks and review at least once a year. Including studying and taking lessons from actual incidents, learning of and continually developing systems.

Please be informed accordingly

Starting from 19 October 2022 onwards

(Dr. Chanchai Leesomprasong)

Director of Phyathai Sriracha Hospital / ISMR

Secretary of the Information Security Committee (ISC)