☑ รพ.พญาไทศรีราชา ☑ รพ.พญาไทศรีราชา 2 ☑ คลินิกเวชกรรมพญาไทบางพระ ☑ คลินิกเวชกรรมพญาไทบ่อวิน ☑ สหคลินิกพญาไทสะพานสี่

QP-ISC-008

นโยบายและวัตถุประสงค์ด้านความปลอดภัยของสารสนเทศ

ผู้ทบทวน ..... (รักษาการผู้จัดการส่วนบริการพยาบาล 3/
(พว.นุจรินทร์ เกิดแดง) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO))

ผู้ทบทวน..... (ผู้จัดการแผนกสนับสนุนเทคโนโลยีสารสนเทศ/
(ปรีดี กมลพจน์) เลขานุการคณะกรรมการความปลอดภัย
สารสนเทศ (ISC))

ผู้รับรอง ..... (ผู้อำนวยการโรงพยาบาล/ ISMR /
(นพ.ชาญชัย ลิ้สมประสงค์) ประธานคณะกรรมการความปลอดภัย
สารสนเทศ (ISC))

ผู้อนุมัติ ..... (ผู้อำนวยการโรงพยาบาล/ ISMR /
(นพ.ชาญชัย ลิ้สมประสงค์) ประธานคณะกรรมการความปลอดภัย
สารสนเทศ (ISC))

แก้ไขครั้งที่ : 01

ระดับเอกสาร : C

วันที่มีผลบังคับใช้ : 30 ต.ค. 2567

☑ รพ.พญาไทศรีราชา ☑ รพ.พญาไทศรีราชา 2 ☑ คลินิกเวชกรรมพญาไทบางพระ ☑ คลินิกเวชกรรมพญาไทบ่อวิน ☑ สหคลินิกพญาไทสะพานสี่

ชื่อเอกสาร : QP-ISC-008 นโยบายและวัตถุประสงค์ด้านความปลอดภัยของสารสนเทศ			
ผู้ทบทวน : พว.นุจรินทร์ เกิดแดง		ตำแหน่ง : รักษาการผู้จัดการส่วนบริการพยาบาล 3/ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	
ผู้ทบทวน : ปรีดี กมลพจน์		ตำแหน่ง : ผู้จัดการแผนกสนับสนุนเทคโนโลยีสารสนเทศ / เลขานุการคณะกรรมการความปลอดภัยสารสนเทศ (ISC)	
ผู้รับรอง : นพ.ชาญชัย ลิ้สมประสงค์		ตำแหน่ง : ผู้อำนวยการโรงพยาบาล/ ISMR/ ประธานคณะกรรมการความปลอดภัยสารสนเทศ (ISC)	
ผู้อนุมัติ : นพ.ชาญชัย ลิ้สมประสงค์		ตำแหน่ง : ผู้อำนวยการโรงพยาบาล/ ISMR/ ประธานคณะกรรมการความปลอดภัยสารสนเทศ (ISC)	
แก้ไขครั้งที่ : 01	ระดับเอกสาร : C	วันที่บังคับใช้ : 30 ต.ค. 67	วันที่ครบกำหนดทบทวน : 30 ต.ค. 70

ประวัติการแก้ไขเอกสาร

หน้าที่	แก้ไขครั้งที่	วันที่บังคับใช้ส่วนที่แก้ไข	รายละเอียดการแก้ไข	เลขที่ใบแจ้งขอแก้ไข
ทั้งฉบับ	1	30 ต.ค. 67	ทบทวนนโยบายและวัตถุประสงค์ด้านความปลอดภัยของสารสนเทศหลัง Gap Analysis ISO27001:2022	L140/67

นโยบายและวัตถุประสงค์ด้านความปลอดภัยของสารสนเทศ

โรงพยาบาลฯ มีความมุ่งมั่นที่จะรักษาความมั่นคงปลอดภัยข้อมูลและคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานสากลตามข้อกำหนด ISO/IEC 27001 : 2022 และคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีวัตถุประสงค์ต่อการรักษาความปลอดภัยข้อมูลและการคุ้มครองข้อมูลส่วนบุคคลคือการธำรงไว้ซึ่ง การรักษาความลับของข้อมูล ความถูกต้องครบถ้วน และความสมบูรณ์พร้อมใช้ ดังนี้

1. การรักษาความลับ (Confidentiality) หมายถึง การป้องกันไม่ให้ข้อมูลสารสนเทศสามารถถูกเข้าถึงได้จากผู้ไม่มีสิทธิ โดยการเข้าถึงยังรวมถึงการถูกเปิดเผยและการจำแนกแจกจ่ายซึ่งข้อมูลสารสนเทสและสินทรัพย์สารสนเทศนั้นด้วย
2. ความถูกต้องครบถ้วน (Integrity) หมายถึง การป้องกันไม่ให้ข้อมูลสารสนเทศถูกเปลี่ยนแปลงแก้ไขทั้งที่มีเจตนาหรือไม่ก็ตามจากผู้ไม่มีสิทธิที่จะแก้ไขสิข้อมูลสารสนเทศเหล่านั้น
3. ความสมบูรณ์พร้อมใช้ (Availability) หมายถึง การที่ผู้มีสิทธิสามารถเข้าใช้งานข้อมูลสารสนเทศนั้นได้เมื่อยามต้องการใช้งาน ครอบคลุมทั้งในทางกายภาพและทางเทคโนโลยี

กำหนด <u>นโยบายด้านความปลอดภัยของสารสนเทศ</u> ดังนี้

1. มีการวางแผน จัดการ ดูแล และควบคุม เรื่องความปลอดภัยของสารสนเทศระบบโครงข่าย เครื่องมืออุปกรณ์ ให้อยู่ในระบบมาตรฐาน เป็นที่ยอมรับมีความน่าเชื่อถือ และสามารถตรวจสอบได้ และมีการทบทวนนโยบายด้านความปลอดภัยของสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ
2. มีการประเมินความเสี่ยงด้านความปลอดภัยสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยการประเมินความเสี่ยงดังกล่าวพิจารณาถึงบริบทภายใน (Internal Context) บริบทภายนอก (External Context) ผู้ที่มีส่วนได้ส่วนเสีย (Interested Party) วิสัยทัศน์ พันธกิจ การเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ มีการกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้ และความเสี่ยงที่ยอมรับไม่ได้ เพื่อใช้เป็นแนวทางในการบริหารจัดการความเสี่ยงที่เกิดขึ้นในการประเมินความเสี่ยงที่เกิดขึ้น

3. จัดให้มีทรัพยากร ด้านงบประมาณ ทรัพยากรบุคคล การบริหารจัดการเทคโนโลยีที่เพียงพอต่อการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ
4. กำหนดมาตรการเกี่ยวกับระบบการจัดการความปลอดภัยสารสนเทศ โดยถือเป็นหน้าที่ที่พนักงานทุกคนในโรงพยาบาลฯ จะต้องปฏิบัติตาม และหากมีการฝ่าฝืน ให้ถือว่าเป็นการกระทำผิดวินัยอย่างร้ายแรง
5. บุคลากรที่ปฏิบัติหน้าที่ในโรงพยาบาลทุกระดับ ต้องได้รับการสื่อสาร รับทราบนโยบายด้านความปลอดภัยสารสนเทศ และนโยบายที่เกี่ยวข้อง ผ่านช่องทางการสื่อสารและการรับรู้ที่องค์กรกำหนดตลอดจนการปฏิบัติตามนโยบาย
6. บุคลากรที่ปฏิบัติหน้าที่ในโรงพยาบาลทุกระดับ ต้องมีความรู้ในการรักษาความปลอดภัยสารสนเทศในการปฏิบัติหน้าที่ การสื่อสาร การใช้เครื่องมือสารสนเทศ ตลอดจนการปฏิบัติใดๆที่เกี่ยวข้องกับข้อมูลสารสนเทศ เช่น การใช้สื่อ Social, การละเมิดสิทธิ, การเข้าถึงข้อมูล, กฎหมายด้านสารสนเทศ โดยเน้นพรบ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) เป็นต้น และได้รับการสื่อสาร การรับการอบรมอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงหรือความจำเป็นที่ต้อวได้รับการสื่อสารและเรียนรู้อย่างมีนัยสำคัญ
7. มาตรการเกี่ยวกับผู้ให้บริการจากภายนอก (Outsource) คู่ค้า คู่ความร่วมมือ ต้องครอบคลุมถึงวิธีการคัดเลือกและพิจารณาคุณสมบัติของผู้ให้บริการ มีข้อกำหนดเกี่ยวกับการใช้บริการเพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศอย่างไม่เหมาะสม รวมถึงข้อกำหนดเกี่ยวกับการรักษาความลับของข้อมูล และไม่เปิดเผยข้อมูลที่มีความสำคัญ ต้องปฏิบัติอย่างเคร่งครัด และโรงพยาบาลฯ จะแจ้งซ้ำเมื่อข้อกำหนดเกิดการเปลี่ยนแปลง
8. มาตรการเกี่ยวกับผู้ให้บริการจากภายนอก กรณีผู้ให้บริการระบบ Cloud service และอื่นๆ ต้องครอบคลุมถึงวิธีการคัดเลือกและพิจารณาคุณสมบัติของผู้ให้บริการ ผู้ให้บริการจะต้องมีการจัดให้มีนโยบาย แนวทางปฏิบัติ มาตรการ หรือมาตรฐานที่สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล และมีคุณสมบัติด้านมาตรการรักษาความปลอดภัยข้อมูลที่ได้รับการยอมรับ

9. โรงพยาบาลฯ จะดำเนินการปรับปรุงระบบการจัดการความปลอดภัยของสารสนเทศอย่างต่อเนื่อง เพื่อให้สอดคล้องกับการดำเนินธุรกิจ สภาพแวดล้อม และพัฒนาเชิงระบบเพื่อให้มีระบบการป้องกันและแผนรองรับภัยคุกคามทางไซเบอร์ ภัยโจรกรรมข้อมูลให้สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงอย่างต่อเนื่อง
10. มีการประเมินประสิทธิภาพของการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยหน่วยงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ (IT Audit / Internal Audit) หรือผู้ตรวจสอบภายนอก (External Audit) มีความพร้อมในการตอบสนองภาวะฉุกเฉิน มีการฝึกซ้อมแผนรองรับกรณีระบบคอมพิวเตอร์ของโรงพยาบาล (HIS) ใช้งานไม่ได้ อย่างน้อยปีละ 1 ครั้ง เพื่อปรับปรุงแก้ไขข้อบกพร่องของการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศของโรงพยาบาลเพื่อให้บรรลุถึงนโยบายในการจัดการเกี่ยวกับความปลอดภัยของสารสนเทศให้ได้คุณภาพจึงได้มีการกำหนด
11. มีการประเมินผลสัมฤทธิ์ของนโยบายที่ประกาศใช้ เพื่อนำมาปรับปรุงนโยบาย แผนกลยุทธ์ให้สอดคล้องกับภัยคุกคามในปัจจุบัน และที่อาจเกิดขึ้น

แนวปฏิบัติที่สอดคล้องกับนโยบาย ดังนี้

1. จะต้องไม่มีการรั่วไหล หรือการสูญหายของข้อมูลของผู้ใช้บริการ โดยโรงพยาบาลฯ มีหน้าที่ในการจัดเก็บและรักษาข้อมูลของผู้ใช้บริการภายใต้กรอบแห่งกฎหมาย ข้อกำหนด และกฎเกณฑ์ต่างๆ ที่เกี่ยวข้องตามแบบและวิธีการที่ได้ทำความตกลงร่วมกันไว้ ระหว่างโรงพยาบาลฯ กับผู้ใช้บริการ รวมทั้งการไม่เปิดเผยข้อมูลใดๆ ที่มิได้รับความยินยอมจากผู้ใช้บริการสู่สาธารณชน หรือบุคคลภายนอก
2. มาตรฐานการจัดการความปลอดภัยของสารสนเทศของโรงพยาบาลฯ โรงพยาบาลฯ จะต้องมีการตรวจสอบขั้นตอน หรือวิธีการปฏิบัติอันเกี่ยวกับการจัดการความปลอดภัยของสารสนเทศอยู่ตลอดเวลา และมีการบันทึกไว้เป็นลายลักษณ์อักษร
3. โรงพยาบาลฯ จะต้องจัดทำเอกสารที่ระบุไว้อย่างชัดเจนว่า พนักงานจะไม่นำข้อมูลของโรงพยาบาลฯ หรือข้อมูลของผู้ใช้บริการไปเปิดเผยแก่บุคคลภายนอกหรือที่ใดๆ หากไม่ได้รับความยินยอมจากโรงพยาบาลฯ หรือผู้ใช้บริการเป็นลายลักษณ์อักษร

4. ต้องให้ความรู้แก่พนักงาน และแจ้งให้ทราบถึงความสำคัญของการรักษาความปลอดภัยสารสนเทศ รวมทั้งการแก้ไขหรือเปลี่ยนแปลงใดๆ ที่เกี่ยวข้องกับด้านสารสนเทศ เพื่อให้ผู้ปฏิบัติงานเข้าใจและถือปฏิบัติภายใต้กฎหมาย ข้อกำหนด มาตรการ และกฎเกณฑ์ต่างๆ ที่ออกมาควบคุมและส่งเสริมการรับรู้ด้านความปลอดภัยข้อมูล ภัยคุกคามที่เกิดขึ้นในสังคมและการหาแนวทางการป้องกันความเสี่ยง
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
9. การคัดเลือกผู้ให้บริการด้านสารสนเทศทุกรูปแบบ ได้รับการกำกับ ตรวจสอบ ติดตาม ให้มีมาตรการรักษาความปลอดภัยข้อมูล ป้องกันการเข้าถึงข้อมูลโดยมิชอบ และ ป้องกันข้อมูลรั่วไหล

การประเมินสัมฤทธิ์ของนโยบาย :

วัตถุประสงค์นโยบาย	KPI / การวัดผล	นโยบายที่เกี่ยวข้อง
การรักษาความลับ (Confidentiality)	1. อุบัติการณ์การละเมิดข้อมูลสารสนเทศ 1.1 ข้อมูลถูกเปิดเผยโดยไม่ได้รับอนุญาต 1.2 ข้อมูลถูกเข้าถึงโดยผู้ไม่มีสิทธิการเข้าถึง 1.3 ข้อร้องเรียนจากเหตุละเมิดข้อมูลส่วนบุคคล 1.4 ความถูกต้องของการจัดเก็บและทำลายข้อมูล 2. ความเสี่ยงการละเมิดข้อมูลสารสนเทศ 2.1 การใช้อุปกรณ์ เครื่องมือ ทรัพย์สินสารสนเทศ ไม่ถูกต้อง 2.2 อุปกรณ์ เครื่องมือ ทรัพย์สินสารสนเทศ ไม่ได้รับปกป้องทางเทคนิค	(นโยบาย ข้อ 1) (นโยบาย ข้อ 8) (นโยบาย ข้อ 9)
ความถูกต้องครบถ้วน (Integrity)	1. อุบัติการณ์/ อัตราการบันทึกข้อมูลผิดพลาด 1.1 ความผิดพลาดของระบุตัวตนเจ้าของข้อมูลผิดพลาด 1.2 ความถูกต้องของการบันทึกข้อมูลตามข้อกำหนด กฎหมาย หรือ มาตรฐานการปฏิบัติ 1.3 อัตราการสำรองข้อมูลในระบบ	(นโยบาย ข้อ 1)
ความสมบูรณ์พร้อมใช้ (Availability)	1. อุบัติการณ์ความไม่พร้อมใช้ อุปกรณ์ เครื่องมือ ทรัพย์สินสารสนเทศ ข้อมูลสารสนเทศ 1.1 ระยะเวลาที่เครื่องคอมพิวเตอร์แม่ข่ายใช้งานไม่ได้ (Server Downtime) 1.2 ระยะเวลาสะสมที่ระบบเครือข่ายในโรงพยาบาลหยุดการทำงาน (Network Downtime) 1.3 อุบัติการณ์ระบบคอมพิวเตอร์ใช้งานไม่ได้ 1.4 ความพร้อมใช้ของเครื่องคอมพิวเตอร์ ตอบสนองตามความต้องการที่มีการร้องขอตามระบบที่ถูกต้อง	(นโยบาย ข้อ 1) (นโยบาย ข้อ 3) (นโยบาย ข้อ 9) (นโยบาย ข้อ 10)

วัตถุประสงค์นโยบาย	KPI / การวัดผล	นโยบายที่เกี่ยวข้อง
	2. อัตราความพร้อมใช้ อุปกรณ์ เครื่องมือ ทรัพย์สินสารสนเทศ ข้อมูลสารสนเทศ 2.1 อัตราการสำรองข้อมูลในระบบ 2.2 เปอร์เซ็นต์ความพร้อมในการตอบสนองภาวะฉุกเฉิน	
มาตรการความปลอดภัยเชิงองค์กร มาตรการความปลอดภัยเชิงบุคลากร มาตรการความปลอดภัยเชิงเทคนิค	1. บุคคลากรได้รับการสื่อสารนโยบายรักษาความปลอดภัยข้อมูลสารสนเทศ และนโยบายที่เกี่ยวข้อง 2. บุคลากรได้รับการสื่อสาร และอบรมความรู้ในการรักษาความปลอดภัยข้อมูล และกฎหมายที่เกี่ยวข้อง 3. บุคลากรได้รับการสื่อสาร และอบรมการใช้งาน อุปกรณ์ เครื่องมือ ทรัพย์สินสารสนเทศให้เกิดความปลอดภัย 4. บุคลากรภายนอก, ผู้ให้บริการจากภายนอก (Outsource) คู่ค้าได้รับการสื่อสารและอบรมด้านความรักษาความปลอดภัยข้อมูล	(นโยบาย ข้อ 4) (นโยบาย ข้อ 5) (นโยบาย ข้อ 6) (นโยบาย ข้อ 7) (นโยบาย ข้อ 8) (นโยบาย ข้อ 10)

เอกสารที่เกี่ยวข้อง : -

หน่วยงานที่เกี่ยวข้อง : ทุกหน่วยงาน

เอกสารแนบ : -

IR NO. ที่เกี่ยวข้อง : -