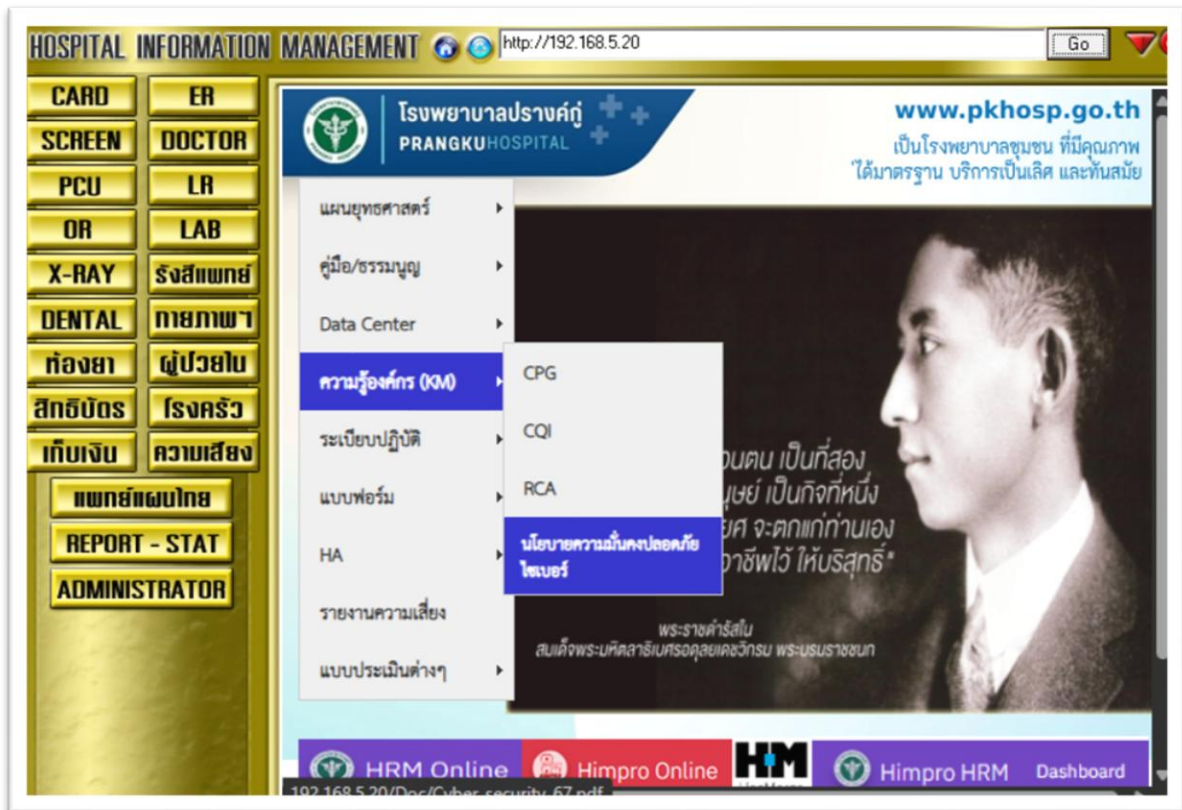




9.3.3 มีการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) อย่างสม่ำเสมอ

Cybersecurity Awareness Procedure

เผยแพร่ประชาสัมพันธ์ในระบบอินทราเน็ตของโรงพยาบาล



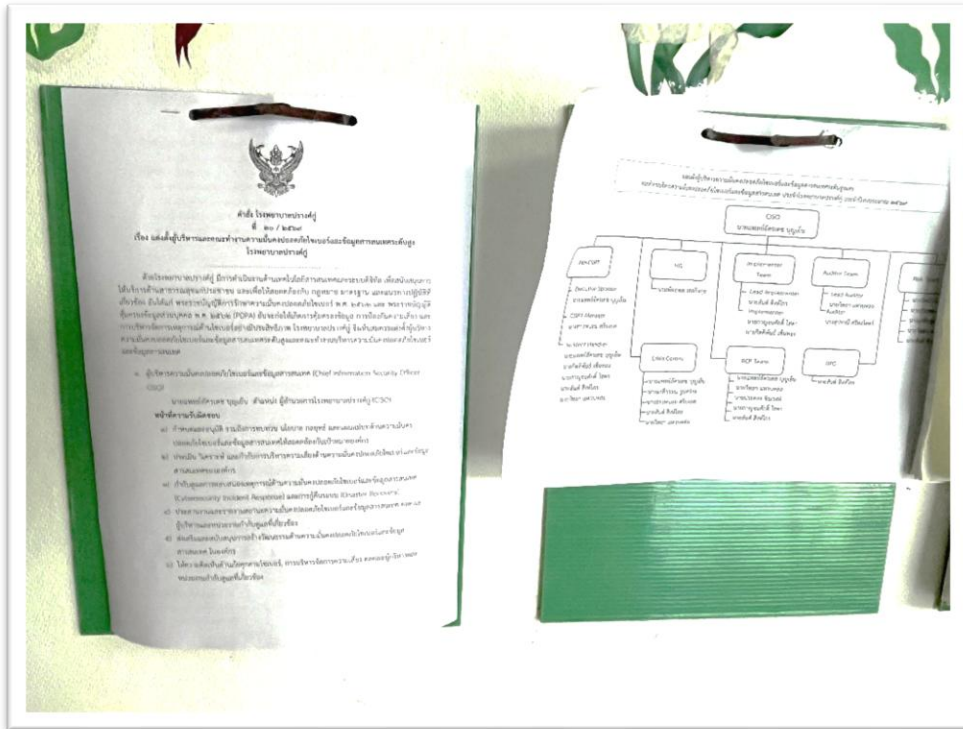
เผยแพร่ประชาสัมพันธ์ผ่านเว็บไซต์โรงพยาบาล



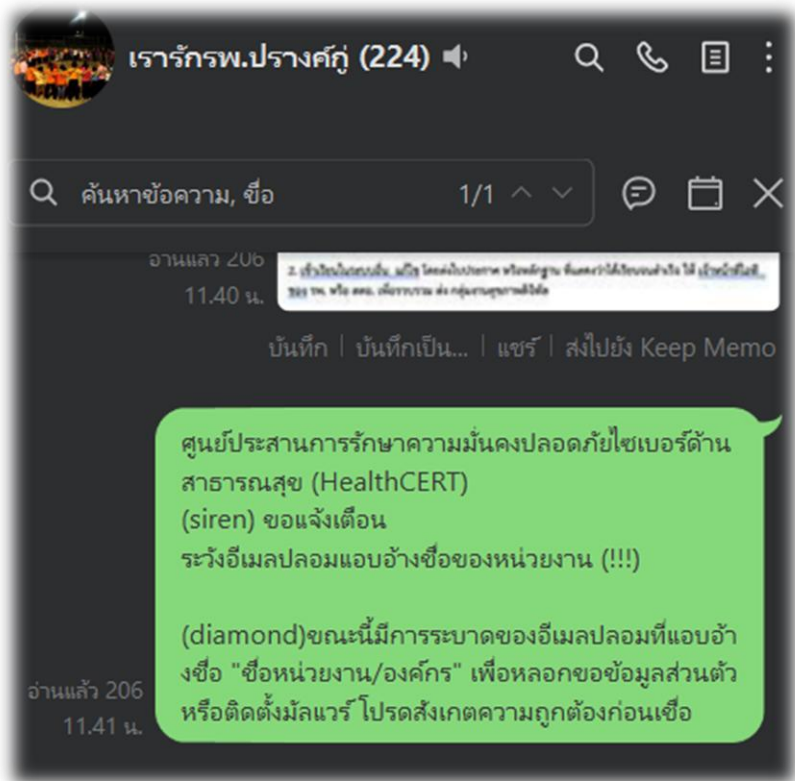
ประกาศรับสมัครงาน ประกาศจัดซื้อจัดจ้าง ข่าวประชาสัมพันธ์ การคุ้มครองข้อมูลส่วนบุคคล PDPA นโยบาย

- นโยบายสุขภาพศึกษา [Click](#)
- นโยบายความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Management Policy) [Click](#)

ป้ายประชาสัมพันธ์




การแจ้งเตือนภัยคุกคามผ่านกลุ่มไลน์เรารักโรงพยาบาลปราจีนบุรี



การอบรมปฐมนิเทศเจ้าหน้าที่ใหม่ (เอกสารแนบท้าย)
หนังสือเวียน (เอกสารแนบท้าย)

	กระบวนการสร้างความตระหนักรู้ด้าน ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Procedure)	รหัสเอกสาร	PKH MOPH Protect -05
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับ ของเอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็น			
ชื่อ-สกุล	นายกาญจนศักดิ์ โสตา	นายสันต์ สิงห์ไกร	นายแพทย์อัครเดช บุญเย็น
ตำแหน่ง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	เจ้าพนักงานเวชสถิติชำนาญงาน (Lead Implementer)	ผู้อำนวยการโรงพยาบาลปรางค์กู่ (CISO)
วันเดือนปี	16 มีนาคม 2569	20 มีนาคม 2569	23 มีนาคม 2569

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	23 มีนาคม 2569	จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลปรางค์กู่ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรางค์กู่ เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	กระบวนการสร้างความตระหนักรู้ด้าน ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Procedure)	รหัสเอกสาร	PKH MOPH
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับ ของเอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

สารบัญ

1. วัตถุประสงค์	3
2. ขอบเขต.....	3
3. คำจำกัดความ/นิยามศัพท์เฉพาะ	3
4. หน้าที่และความรับผิดชอบ	4
5. ขั้นตอนปฏิบัติ.....	5
6. เอกสารที่เกี่ยวข้อง	6
7. เอกสารอ้างอิง.....	7

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลปรังคู้ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรังคู้ เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	กระบวนการสร้างความตระหนักรู้ด้าน ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Procedure)	รหัสเอกสาร	PKH MOPH Protect -05
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับ ของเอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

กระบวนการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 22.5.1, ข้อ 22.5.2]

1. วัตถุประสงค์

กระบวนการนี้จัดทำขึ้นเพื่อส่งเสริมและสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่เจ้าหน้าที่ พนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศของหน่วยงาน เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

2. ขอบเขต

กระบวนการนี้ครอบคลุมถึงการจัดทำแผนงาน การเผยแพร่ และการทบทวนกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรที่เกี่ยวข้องในหน่วยงาน

3. คำจำกัดความ/นิยามศัพท์เฉพาะ

ลำดับ	คำศัพท์	คำจำกัดความ
1	พนักงาน	เจ้าหน้าที่ของหน่วยงานต่าง ๆ ของโรงพยาบาลปรางค์กู่
2	ผู้ให้บริการภายนอก	เจ้าหน้าที่/พนักงาน ของบริษัทหรือองค์กรภายนอกที่มาดำเนินงานตามคำสั่งหรือสัญญาของโรงพยาบาลปรางค์กู่
3	Cybersecurity Awareness Team	เจ้าหน้าที่ผู้ได้รับมอบหมายให้ทำหน้าที่สร้างการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลปรางค์กู่ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรางค์กู่ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	กระบวนการสร้างความตระหนักรู้ด้าน ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Procedure)	รหัสเอกสาร	PKH MOPH
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับ ของเอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

4	ISM	หัวหน้าคณะทำงานระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร
---	-----	---------------------------------------------------------------------

4. หน้าที่และความรับผิดชอบ

ลำดับ	ผู้รับผิดชอบ	ความรับผิดชอบ
1	Top Management / ISM	รับผิดชอบในการสนับสนุนและกำกับดูแลการดำเนินการตามแผนงาน การสร้างความรู้ด้านความมั่นคงปลอดภัยไซเบอร์
2	ทีมสร้างความตระหนักรู้ เรื่องการรักษาความ มั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Team)	รับผิดชอบในการพัฒนาและดำเนินการตามแผนงานการสร้างความรู้ ด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงการจัดกิจกรรมและ การเผยแพร่ข้อมูล
3	พนักงานและผู้ให้บริการ ภายนอก (Employees and External Service Providers)	มีหน้าที่เข้าร่วม กิจกรรมและปฏิบัติตามนโยบายและแนวทางที่ได้รับ การอบรมหรือเผยแพร่

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลปรังคู้ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรังคู้ เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	กระบวนการสร้างความตระหนักรู้ด้าน ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Procedure)	รหัสเอกสาร	PKH MOPH Protect -05
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับ ของเอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

5. ขั้นตอนปฏิบัติ

5.1 การจัดทำแผนงานการสร้างความตระหนักรู้ (Development of Cybersecurity Awareness Plan)

1) กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท

ขั้นตอน: จัดทำกิจกรรมให้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรทุกกลุ่ม รวมถึง พนักงานใหม่ ผู้ใช้ และผู้บริหาร เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญ และผู้ขายหรือผู้รับเหมา โดย การจัดอบรมความมั่นคงปลอดภัยไซเบอร์สำหรับพนักงานใหม่เมื่อเริ่มงาน และ การจัดสัมมนาเชิงปฏิบัติการ สำหรับเจ้าหน้าที่ IT เพื่อเรียนรู้เกี่ยวกับภัยคุกคามใหม่ ๆ

2) การเผยแพร่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์

ขั้นตอน: เผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคง ปลอดภัยไซเบอร์ของบริการที่สำคัญ โดยใช้ช่องทางต่าง ๆ เช่น อีเมล บอร์ดประกาศ เว็บไซต์ของหน่วยงาน และ การประชุม

3) การตระหนักรู้กฎหมายและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

ขั้นตอน: จัดทำและเผยแพร่ข้อมูลเกี่ยวกับกฎหมาย กฎ ระเบียบ นโยบาย และแนวปฏิบัติที่ เกี่ยวข้องกับการใช้งานและการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อให้บุคลากรทุกคนตระหนักถึง ข้อกำหนดที่ต้องปฏิบัติตาม มีการจัดทำคู่มือหรืออินโฟการปฏิบัติตามนโยบายความมั่นคงปลอดภัยไซเบอร์ และ การอบรมเกี่ยวกับกฎหมายความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง

4) การสื่อสารและเผยแพร่ข้อมูลอย่างสม่ำเสมอ

ขั้นตอน: สื่อสารข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามใหม่ ๆ อย่างสม่ำเสมอ และทันท่วงทีผ่านช่องทางที่เหมาะสม เช่น อีเมล บอร์ดข่าวสารภายในองค์กร เว็บไซต์ของหน่วยงาน หรือ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลปรังค์กู ห้ามแจกจ่ายไปยัง บุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรังค์กู เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	กระบวนการสร้างความตระหนักรู้ด้าน ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Procedure)	รหัสเอกสาร	PKH MOPH Protect -05
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับ ของเอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

ระบบการจัดการเรียนรู้ เช่น การส่งข่าวสารเกี่ยวกับภัยคุกคามไซเบอร์ล่าสุดให้กับพนักงานทุกสัปดาห์ และการจัดทำคอร์สออนไลน์เกี่ยวกับภัยคุกคามทางไซเบอร์

5.2 การทบทวนแผนงานและการปรับปรุง (Review and Improvement of Awareness Plan)

1) การทบทวนแผนงานประจำปี

ขั้นตอน: ทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีความเกี่ยวข้องกับ สถานการณ์ปัจจุบัน

2) การปรับปรุงเนื้อหาและกิจกรรมตามผลการทบทวน

ขั้นตอน: ปรับปรุงเนื้อหาและกิจกรรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ตามผลการทบทวน เพื่อเพิ่มประสิทธิภาพในการตระหนักรู้และป้องกันภัยคุกคาม เช่น การเพิ่มโมดูลการอบรมเกี่ยวกับการป้องกันการโจมตีในรูปแบบต่าง ๆ

6. การทบทวนกระบวนการดำเนินการ

กระบวนการดำเนินการนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

7. เอกสารที่เกี่ยวข้อง

ลำดับ	หมายเลขเอกสาร	ชื่อเอกสาร
1		

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลปรังคู้ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรังคู้ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	กระบวนการสร้างความตระหนักรู้ด้าน ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Procedure)	รหัสเอกสาร	PKH MOPH Protect -05
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับ ของเอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

8. เอกสารอ้างอิง

ลำดับ	ชื่อเอกสาร
1	ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวล แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 - กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect) - การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
2	แผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์
3	หลักฐานหรือเอกสาร การจัดทำกิจกรรมให้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ แก่บุคลากร

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลปรังคู้ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรังคู้ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



โรงพยาบาลปรังคู้

จัดทำโดย : นายสันต์ สิงห์ไกร

ผู้อนุมัติ : นายแพทย์อัครเดช บุญเย็น

จัดทำเมื่อ : 19 มีนาคม 2569

มีผลบังคับใช้ : 23 มีนาคม 2569

แผนงานการสร้างความรู้ในองค์กร (Cybersecurity Awareness Plan)

1. พนักงานใหม่ (New Employees)

1.1 การฝึกอบรมเบื้องต้นด้านความมั่นคงปลอดภัยไซเบอร์และกฎหมายอื่นที่เกี่ยวข้อง

1. การฝึกอบรมในห้องเรียน (In-person Training)

- **เนื้อหาหลัก:** การใช้รหัสผ่านที่ปลอดภัย, การระบุและป้องกันอีเมลฟิชซิง, การรายงานเหตุการณ์ และบทบาทและความรับผิดชอบตามกฎหมายความมั่นคงปลอดภัยไซเบอร์
- **ระยะเวลา:** 2 ชั่วโมง
- **การวัดผล:** ทดสอบความเข้าใจหลังการฝึกอบรม

2. การฝึกอบรมออนไลน์ (E-learning)

- **เนื้อหาหลัก:** วิดีโอสอนเกี่ยวกับข้อกำหนดสำคัญ, การใช้รหัสผ่าน, การป้องกันภัยคุกคาม, และแบบทดสอบในแต่ละบท
- **ระยะเวลา:** 1-2 ชั่วโมง
- **การวัดผล:** คะแนนจากแบบทดสอบออนไลน์

3. คู่มือการปฏิบัติตามกฎหมายและการใช้งานที่ปลอดภัย (Legal Compliance and Security Handbook)

- **เนื้อหาหลัก:** สรุปข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์และแนวทางปฏิบัติที่ปลอดภัย

- การแจกจ่าย: แจกคู่มือในวันแรกของการทำงาน
 - การวัดผล: ไม่มีการทดสอบ
4. การประชุมแนะนำกฎหมายและความมั่นคงปลอดภัยไซเบอร์ (Orientation Meeting)
- เนื้อหาหลัก: แนะนำพนักงานใหม่เกี่ยวกับกฎหมายและแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
 - ระยะเวลา: 1 ชั่วโมง
 - การวัดผล: การตอบคำถามและทบทวนความเข้าใจ
5. การฝึกอบรมเชิงปฏิบัติ (Practical Compliance Training)
- เนื้อหาหลัก: ฝึกอบรมการปฏิบัติตามกฎหมายในสถานการณ์จริง เช่น การจัดการข้อมูลส่วนบุคคล, การปฏิบัติเมื่อพบเหตุการณ์ทางไซเบอร์
 - ระยะเวลา: 1.5 ชั่วโมง
 - การวัดผล: การปฏิบัติจริงในสถานการณ์จำลอง

2. ผู้ใช้และระดับบริหาร (Users and Management)

2.1 การฝึกอบรมประจำปีด้านความมั่นคงปลอดภัยไซเบอร์และกฎหมาย

1. สัมมนาออนไลน์ (Webinar)
- เนื้อหาหลัก: การจัดการการเข้าถึงข้อมูล, การป้องกันการโจมตีไซเบอร์, การอัปเดตกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
 - ระยะเวลา: 2 ชั่วโมง
 - การวัดผล: แบบทดสอบหลังสัมมนา
2. การฝึกอบรมเชิงลึกด้านกฎหมายและความมั่นคงปลอดภัยไซเบอร์ (In-depth Legal and Cybersecurity Training)
- เนื้อหาหลัก: การวิเคราะห์และจัดการความเสี่ยงทางกฎหมายที่เกี่ยวข้องกับไซเบอร์, การตอบสนองต่อเหตุการณ์, การปฏิบัติตามข้อกำหนดทางกฎหมาย
 - ระยะเวลา: 3 ชั่วโมง
 - การวัดผล: การประเมินจากสถานการณ์จำลอง

3. การแจ้งเตือนภัยคุกคามและการเปลี่ยนแปลงกฎหมาย (Threat and Legal Updates Alerts)

- **เนื้อหาหลัก:** การแจ้งเตือนเกี่ยวกับภัยคุกคามใหม่ ๆ และการเปลี่ยนแปลงของกฎหมายที่อาจส่งผลกระทบต่อการทำงาน
- **ระยะเวลา:** ส่งแจ้งเตือนเป็นระยะตามความจำเป็น
- **การวัดผล:** การตรวจสอบการปรับปรุงการปฏิบัติตามข้อกำหนดใหม่

4. การฝึกอบรมเฉพาะทาง (Specialized Training)

- **เนื้อหาหลัก:** การป้องกันและตอบสนองต่อการโจมตีขั้นสูง, ความรับผิดชอบทางกฎหมายในการปกป้องข้อมูลและระบบสารสนเทศ
- **ระยะเวลา:** 4 ชั่วโมง
- **การวัดผล:** การประเมินความเข้าใจและการทดสอบกรณีศึกษา

5. การประชุมทบทวนกฎหมายและความมั่นคงปลอดภัยไซเบอร์ (Legal and Cybersecurity Review Meetings)

- **เนื้อหาหลัก:** ทบทวนการปฏิบัติตามกฎหมายและนโยบายความมั่นคงปลอดภัยในปีที่ผ่านมา และวางแผนการปรับปรุง
- **ระยะเวลา:** 5 ชั่วโมง
- **การวัดผล:** การวางแผนและดำเนินการตามแผนการปรับปรุงที่ระบุ

3. เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Support Staff)

3.1 การฝึกอบรมเชิงลึกด้านกฎหมายความมั่นคงปลอดภัยไซเบอร์สำหรับ IT และ ICS

1. การฝึกอบรมเชิงปฏิบัติการและกฎหมาย (Hands-on and Legal Training)

- **เนื้อหาหลัก:** การจัดการความปลอดภัยของระบบอุปกรณ์เครื่องมือแพทย์, การควบคุมการเข้าถึงเครือข่าย, การปฏิบัติตามข้อกำหนดทางกฎหมายที่เกี่ยวข้อง
- **ระยะเวลา:** 5 ชั่วโมง
- **การวัดผล:** ทดสอบการปฏิบัติจริง

2. การทดสอบจำลองสถานการณ์และความรู้ด้านกฎหมาย (Simulation Exercises and Legal Knowledge Test)

- **เนื้อหาหลัก:** การตอบสนองต่อเหตุการณ์ที่จำลองขึ้น, ทดสอบความรู้ด้านกฎหมายที่เกี่ยวข้องกับการปฏิบัติงานในระบบ IT และ ICS
- **ระยะเวลา:** 3 ชั่วโมง
- **การวัดผล:** การประเมินความรวดเร็วและประสิทธิภาพในการตอบสนอง

3. การสัมมนากฎหมายและความเสี่ยง (Legal and Risk Seminar)

- **เนื้อหาหลัก:** วิเคราะห์ความเสี่ยงทางกฎหมายที่เกี่ยวข้องกับการจัดการระบบโครงสร้างพื้นฐาน, การป้องกันการโจมตีทางไซเบอร์
- **ระยะเวลา:** 4 ชั่วโมง
- **การวัดผล:** การประเมินความเข้าใจและการจัดทำแผนการจัดการความเสี่ยง

4. การฝึกอบรมการปฏิบัติตามกฎหมายเชิงลึก (In-depth Compliance Training)

- **เนื้อหาหลัก:** ฝึกอบรมการปฏิบัติตามกฎหมายในรายละเอียดที่เกี่ยวข้องกับการจัดการระบบสารสนเทศ, การป้องกันการโจมตีที่มีประสิทธิภาพ
- **ระยะเวลา:** 3 ชั่วโมง
- **การวัดผล:** การประเมินผลการปฏิบัติในสถานการณ์จริง

5. การประชุมทบทวนกฎหมายที่เกี่ยวข้องกับ ICS (ICS Legal Review Meetings)

- **เนื้อหาหลัก:** ทบทวนข้อกำหนดทางกฎหมายที่เกี่ยวข้องกับระบบควบคุมอุตสาหกรรมและปรับปรุงกระบวนการปฏิบัติตาม
- **ระยะเวลา:** 2 ชั่วโมง
- **การวัดผล:** การวางแผนและดำเนินการตามข้อเสนอแนะ

4. ผู้ขาย ผู้รับเหมา และผู้ให้บริการภายนอก (Vendors, Contractors, and Service Providers)

4.1 การประชุมและฝึกอบรมด้านกฎหมายและความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ให้บริการภายนอก

- 1. การฝึกอบรมกฎหมายและข้อกำหนด (Legal and Compliance Training)**
 - **เนื้อหาหลัก:** ความรับผิดชอบทางกฎหมายในการจัดการข้อมูลและการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับองค์กร, การป้องกันการรั่วไหลของข้อมูล
 - **ระยะเวลา:** 3 ชั่วโมง
 - **การวัดผล:** การลงนามในข้อตกลงการปฏิบัติตามข้อกำหนด
- 2. การสัมมนาออนไลน์ด้านกฎหมายและความมั่นคงปลอดภัยไซเบอร์ (Online Legal and Cybersecurity Webinars)**
 - **เนื้อหาหลัก:** สรุปข้อกฎหมายที่เกี่ยวข้องกับการให้บริการภายนอก, การคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยไซเบอร์
 - **ระยะเวลา:** 2 ชั่วโมง
 - **การวัดผล:** การตอบแบบสอบถามหลังสัมมนา
- 3. การประชุมเชิงปฏิบัติการด้านกฎหมายและความมั่นคงปลอดภัยไซเบอร์ (Legal and Cybersecurity Workshops)**
 - **เนื้อหาหลัก:** ฝึกอบรมและแลกเปลี่ยนความคิดเห็นเกี่ยวกับข้อกำหนดทางกฎหมายในการทำงานร่วมกับองค์กร, การรักษาความปลอดภัยของข้อมูลลูกค้า
 - **ระยะเวลา:** 4 ชั่วโมง
 - **การวัดผล:** การทดสอบความเข้าใจและการประเมินผลการฝึกอบรม
- 4. การประชุมรายไตรมาสเกี่ยวกับการปฏิบัติตามกฎหมายและความมั่นคงปลอดภัยไซเบอร์ (Quarterly Compliance and Cybersecurity Meetings)**
 - **เนื้อหาหลัก:** ทบทวนและปรับปรุงการปฏิบัติตามข้อกำหนดทางกฎหมายสำหรับผู้ให้บริการภายนอก, การประเมินความเสี่ยงและการปรับปรุงมาตรการป้องกัน
 - **ระยะเวลา:** 2 ชั่วโมง
 - **การวัดผล:** การติดตามการปรับปรุงที่เกิดขึ้นจริง

5. การแจ้งเตือนภัยคุกคามและการเปลี่ยนแปลงกฎหมาย (Threat Alerts and Legal Change Notifications)

- **เนื้อหาหลัก:** การแจ้งเตือนเกี่ยวกับภัยคุกคามที่อาจเกิดขึ้นและการเปลี่ยนแปลงของกฎหมายที่ส่งผลกระทบต่อให้บริการ, คำแนะนำในการป้องกัน
- **ระยะเวลา:** ส่งแจ้งเตือนเป็นระยะตามความจำเป็น
- **การวัดผล:** การตอบสนองต่อภัยคุกคามและการปรับปรุงกระบวนการตามกฎหมายที่เปลี่ยนแปลง



บันทึกข้อความ

ส่วนราชการ...โรงพยาบาลปรางค์กู่ กลุ่มงานสุขภาพดิจิทัล โทร.๐ ๔๕๖๙ ๗๑๖๗ ต่อ.๑๕๘.....

ที่ ศก ๐๐๓๓.๓๑๔/ ๑๐๐๕ วันที่ ๑ เมษายน ๒๕๖๙.....

เรื่อง ขอแจ้งเวียนแผนการรับมือภัยคุกคามทางไซเบอร์ นโยบาย ระเบียบปฏิบัติต่างๆ ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

เรียน หัวหน้ากลุ่มงาน/หัวหน้างาน และผู้ที่เกี่ยวข้อง

ด้วยโรงพยาบาลปรางค์กู่ ได้มีคำสั่งแต่งตั้งผู้บริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศระดับสูงและคณะทำงานประจำโรงพยาบาลปรางค์กู่ ให้เป็นไปตามกฎหมาย มาตรฐาน และแนวทางปฏิบัติที่เกี่ยวข้อง อันได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) ทั้งนี้เพื่อยกระดับด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศให้สามารถ ป้องกัน รับมือ ลดความเสี่ยงภัยคุกคามทางด้านไซเบอร์

ในการนี้โรงพยาบาลปรางค์กู่ จึงขอแจ้งเวียนแผนการรับมือภัยคุกคามทางไซเบอร์ นโยบาย ระเบียบปฏิบัติต่างๆ ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล ซึ่งโรงพยาบาลปรางค์กู่ได้ปรับปรุงขึ้น รายละเอียดตามเอกสารที่แนบมาพร้อมหนังสือนี้

จึงเรียนมาเพื่อโปรดทราบและแจ้งให้ผู้มีส่วนเกี่ยวข้องทราบโดยทั่วกันถือปฏิบัติ

(นายอัครเดช บุญเย็น)

นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน) รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลปรางค์กู่



เอกสารแนบ

กลุ่มงาน/งาน	รับทราบ	กลุ่มงาน/งาน	รับทราบ
๑. กลุ่มงานการแพทย์		๘. กลุ่มงานทันตสาธารณสุข	
๒. กลุ่มงานการพยาบาล		๙. กลุ่มงานบริการด้านปฐมภูมิ	
๓. กลุ่มงานบริหารทั่วไป		๑๐. กลุ่มงานโภชนศาสตร์	
๔. กลุ่มงานเภสัชกรรมฯ		๑๑. กลุ่มงานประกันสุขภาพฯ	
๕. กลุ่มงานเทคนิคการแพทย์		๑๒. กลุ่มงานจิตเวชและยาเสพติด	
๖. กลุ่มงานรังสีการแพทย์		๑๓. กลุ่มงานแพทย์แผนไทย	
๗. กลุ่มงานเวชกรรมฟื้นฟู		๑๔. กลุ่มงานสุขภาพดิจิทัล	