





9.6.1 จัดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) อย่างน้อยปีละ 1 ครั้ง โดยมีผู้ตรวจสอบภายใน หรือ ภายนอกที่มีความรู้ความสามารถ และจัดทำรายงานผลต่อผู้บริหารที่เกี่ยวข้อง

Audit Procedure, Audit Report

	<p style="text-align: center;">แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</p> <p style="text-align: center;">(Cybersecurity Audit Plan Procedure)</p>	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

การอนุมัติเอกสาร

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

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	23 มี.ค. 2569	จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์

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

	<p style="text-align: center;">แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</p> <p style="text-align: center;">(Cybersecurity Audit Plan Procedure)</p>	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

สารบัญ

	หน้า
1. วัตถุประสงค์	3
2. คำจำกัดความ	4
3. คุณสมบัติของผู้ตรวจสอบภายใน	4
4. หน้าที่และความรับผิดชอบของทีมผู้ตรวจสอบภายใน	5
5. ขั้นตอนปฏิบัติการตรวจสอบภายใน	6
6. การปฏิบัติงานที่ไม่เป็นไปตามข้อกำหนด (Non-conformance)	11
7. สรุปผลการตรวจสอบ (Audit Closing)	13
8. การรายงานการแก้ไขและป้องกัน (Corrective and Preventive Action Report)	13
9. การตอบรับการแก้ไขและป้องกัน	14
10. การแก้ไขและการป้องกัน (Corrective and Preventive Action)	155
11. การติดตามผลการแก้ไขและป้องกัน (Corrective and Preventive Action Follow up)	155
12. การตรวจสอบผลการแก้ไขและป้องกัน (Verification of Corrective and Preventive Action) ..	155
13. การทบทวนกระบวนการดำเนินการ	166

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของ โรงพยาบาลปรังกะไม่ให้นำไปเผยแพร่หรือนำไปใช้ในทางที่ผิดโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรังกะ เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	<p style="text-align: center;">แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</p> <p style="text-align: center;">(Cybersecurity Audit Plan Procedure)</p>	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม.44, ม.54), ประมวลและกรอบ [ข้อ 17.1, ข้อ 17.1(ก), ข้อ 17.1(ข), ข้อ 17.1(ค), ข้อ 17.2, ข้อ 17.3, ข้อ 17.4, ข้อ 17.5]

1. วัตถุประสงค์

- 1.1 เพื่ออธิบายถึงหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องกับกระบวนการตรวจสอบภายใน
- 1.2 เพื่ออธิบายขั้นตอนในการดำเนินการตรวจสอบภายใน
- 1.3 เพื่อตรวจสอบความสอดคล้องของการปฏิบัติงานและประสิทธิภาพในการปฏิบัติตามข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๒๕๖๔ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญ รวมถึงกฎหมายหลัก กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับ ข้อบังคับ นโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (๒๕๖๕ – ๒๕๗๐) และเอกสารประกอบการปฏิบัติงานที่เกี่ยวข้อง
- 1.4 เพื่อประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของหน่วยงาน ตามหลักการบริหารความเสี่ยง

ทั้งนี้ ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ สอบภายใน หรือสอบอิสระภายนอก อย่างน้อยปีละ 1 ครั้ง

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

	<p style="text-align: center;">แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</p> <p style="text-align: center;">(Cybersecurity Audit Plan Procedure)</p>	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

2. คำจำกัดความ

ลำดับ	คำศัพท์	คำจำกัดความ
1	Non - Conformance	<p>สิ่งที่ไม่เป็นไปตามข้อกำหนด ซึ่งอาจเป็นได้ทั้งเหตุการณ์/การปฏิบัติงานที่ไม่สอดคล้องหรือไม่มีประสิทธิภาพ ซึ่งอาจเกิดได้จากความบกพร่อง การเปลี่ยนแปลง หรือความเบี่ยงเบนที่เกิดขึ้นในเรื่องต่างๆ ดังต่อไปนี้</p> <ol style="list-style-type: none"> 1. ไม่สอดคล้องตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน 2. ไม่สอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ (Policy) 3. ไม่สอดคล้องตามเอกสารประกอบการปฏิบัติงานที่เกี่ยวข้อง (Process, Procedure, Work) เช่น เอกสารมอบหมายงาน เอกสารข้อตกลง 4. ไม่สอดคล้องตามกฎหมายที่เกี่ยวข้อง (Law and Relevant Legislation) 5. ไม่สอดคล้องตามระเบียบ เช่น ระเบียบข้อบังคับที่เกี่ยวข้องกับอุตสาหกรรม ระเบียบข้อบังคับของกระทรวงสาธารณสุข 6. ไม่สอดคล้องตามสัญญาการให้บริการ (Contract)

3. คุณสมบัติของผู้ตรวจสอบภายใน

กำหนดให้ผู้ตรวจสอบภายใน มีคุณสมบัติ ข้อหนึ่งข้อใด ดังต่อไปนี้

- เป็นผู้ได้รับการฝึกอบรม หลักสูตร Lead Auditor พรบ ไซเบอร์ จากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
- เป็นผู้ได้รับการฝึกอบรม หลักสูตร Lead Auditor พรบ ไซเบอร์ จากสำนักงานปลัดกระทรวงสาธารณสุข จัดขึ้น
- เป็นผู้ที่ได้รับการฝึกอบรม หลักสูตร ISMS Lead Audit โดยหลักสูตรการอบรมดังกล่าวจะต้องได้รับการรับรองจากสถาบันสากลที่มีการยอมรับ เช่น IRCA, PECB, Exemplar Global
- เป็นผู้ที่ได้รับการฝึกอบรมหลักสูตรผู้ตรวจสอบภายใน จากหน่วยงานภายนอกที่เชื่อถือได้
- เป็นผู้ที่มีความรู้ความเข้าใจระบบบริหารความมั่นคงปลอดภัยสารสนเทศ หรือกระบวนการปฏิบัติงานต่าง ๆ ของหน่วยงานที่ถูกตรวจสอบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของ โรงพยาบาลปรังคู้ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรังคู้ เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	<p style="text-align: center;">แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</p> <p style="text-align: center;">(Cybersecurity Audit Plan Procedure)</p>	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

- เป็นผู้ที่ได้รับการแต่งตั้งให้เป็นผู้ตรวจสอบภายในหรือเป็นผู้ทรงคุณวุฒิที่ได้รับเชิญเป็นกรณีพิเศษ

4. หน้าที่และความรับผิดชอบของทีมผู้ตรวจสอบภายใน

ลำดับ	ผู้รับผิดชอบ	ความรับผิดชอบ
1	หัวหน้าทีมผู้ตรวจสอบภายใน (Lead Internal Auditor)	<ul style="list-style-type: none"> - จัดทำโปรแกรมการตรวจสอบภายในประจำปี - จัดทำแผนการตรวจสอบภายในให้สอดคล้องกับโปรแกรมการตรวจสอบภายในประจำปี - ควบคุมให้มีการตรวจสอบตามที่กำหนดไว้ในโปรแกรมการตรวจสอบภายในประจำปี และแผนการตรวจสอบภายใน - ศึกษาและทำความเข้าใจเอกสารและข้อมูลต่างๆ ที่เกี่ยวข้องกับการตรวจสอบ - จัดเตรียมรายการตรวจสอบ - รับผิดชอบในการดำเนินการเปิด - ปิดประชุม - ดำเนินการตรวจสอบภายในตามแผนการตรวจสอบภายใน - บันทึกสิ่งที่เป็นข้อบกพร่อง ข้อสังเกตเป็นลายลักษณ์อักษร - ให้ข้อเสนอแนะเพื่อปรับปรุงประสิทธิภาพการปฏิบัติงาน - จัดทำรายงานผลการตรวจสอบภายใน - ชี้แจงผลการตรวจสอบภายในและข้อเสนอแนะ - จัดทำรายงานการดำเนินการแก้ไขและป้องกัน - ตรวจสอบการดำเนินงานแก้ไขและป้องกันปัญหาและลงนามรับรองผลการดำเนินการในรายงานการดำเนินการแก้ไขและป้องกัน
2	ผู้ตรวจสอบภายใน (Internal Auditor)	<ul style="list-style-type: none"> - ศึกษาทำความเข้าใจเอกสารและข้อมูลต่างๆ ที่เกี่ยวข้องกับการตรวจสอบ - จัดเตรียมรายการตรวจสอบ - ดำเนินการตรวจสอบภายในตามแผนการตรวจสอบภายใน - บันทึกสิ่งที่เป็นข้อบกพร่อง ข้อสังเกตเป็นลายลักษณ์อักษร

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

	แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan Procedure)	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

ลำดับ	ผู้รับผิดชอบ	ความรับผิดชอบ
		<ul style="list-style-type: none"> - ให้ข้อเสนอแนะเพื่อปรับปรุงประสิทธิภาพการปฏิบัติงาน - จัดทำรายงานผลการตรวจสอบภายใน - จัดทำรายงานการดำเนินการแก้ไขและป้องกัน

5. ขั้นตอนปฏิบัติการตรวจสอบภายใน

ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง
1	การทำโปรแกรมการตรวจสอบภายใน หัวหน้าทีมผู้ตรวจสอบภายใน จะต้องจัดเตรียมตาราง การตรวจสอบภายในภายใต้ขอบเขตตามผลการวิเคราะห์จากกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) เป็นประจำทุกปี โดยตารางดังกล่าวจะต้องประกอบไปด้วย <ul style="list-style-type: none"> o ช่วงเวลาในการตรวจสอบ o ขอบเขตในการตรวจสอบ o ผู้ตรวจสอบ <ul style="list-style-type: none"> • โปรแกรมการตรวจสอบภายในประจำปี ต้องได้รับการอนุมัติโดยผู้บริหารหรือคณะกรรมการที่มีอำนาจหน้าที่ • ทุกกระบวนการจะต้องมีการตรวจสอบอย่างน้อยปีละ 1 ครั้ง ทั้งนี้ หัวหน้าทีมผู้ตรวจสอบภายในอาจเพิ่มความถี่ในการตรวจสอบได้ ขึ้นอยู่กับผลของการตรวจสอบในครั้งที่ผ่านมา หรือมีการเปลี่ยนแปลงใดๆ ที่มีความสำคัญต่อการปฏิบัติงานภายใต้ขอบเขต • ข้อกำหนดที่จะปฏิบัติต้องสอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน บริบทองค์กรในแต่ละปี จะต้องได้รับการตรวจสอบอย่างน้อยปีละ 1 ครั้ง • ต้องมีการทบทวนและแก้ไขโปรแกรมการตรวจสอบประจำปี หากมีเหตุการณ์เหล่านี้เกิดขึ้น 	หัวหน้าทีมผู้ตรวจสอบภายใน	โปรแกรมการตรวจสอบภายในประจำปี

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของ โรงพยาบาลปรังค์กูห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรังค์กู เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan Procedure)	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง
	<ul style="list-style-type: none"> o การเปลี่ยนแปลงที่สำคัญขององค์กร (Major organization change) o ข้อบกพร่องหลักที่กระทบกับระบบงาน (Major Non-conformances for a function) o ข้อบกพร่องหลักที่กระทบต่อข้อกำหนดของประมวลแนวทางปฏิบัติและกรอบมาตรฐาน 		
2	การเตรียมการเพื่อวางแผนการตรวจสอบภายใน (Preparation for Audit Plan) 1. ทบทวนผลการตรวจสอบภายในและผลการดำเนินการแก้ไข Finding ที่พบจากการตรวจสอบภายในและการตรวจสอบจากหน่วยงานภายนอก ครั้งที่ผ่านมา (ถ้ามี) 2. ทบทวนรายงานการประชุมทบทวนของผู้บริหาร 3. ทบทวนเหตุการณ์ด้านความมั่นคงปลอดภัยต่างๆ ที่เกิดขึ้น 4. ทบทวนรายงานการประเมินความเสี่ยงของปีที่ผ่านมา 5. ทบทวนประสิทธิภาพการดำเนินงานตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานในปีที่ผ่านมา	ผู้ตรวจสอบ ภายใน	
3	จัดทำแผนการตรวจสอบ (Audit Plan) จัดเตรียมรายละเอียดของแผนการตรวจสอบประจำปี สำหรับการดำเนินงานในแต่ละช่วงลงในแผนการตรวจสอบภายใน (Internal Audit Plan) โดยจะต้องประกอบไปด้วย: <ul style="list-style-type: none"> • วัตถุประสงค์ • มาตรฐานที่ใช้ในการตรวจสอบ • ขอบเขตงาน • กำหนดพื้นที่หรือระบบที่จะตรวจสอบ (ฟังก์ชันงาน หน่วยงานหรือที่ตั้ง) • เอกสารอ้างอิง ถ้ามี • ผู้ตรวจสอบภายใน • ผู้รับการตรวจสอบ 	ทีมผู้ตรวจสอบ ภายใน	แผนการ ตรวจสอบ ภายใน (Internal Audit Plan)

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

	แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan Procedure)	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง
	• วัน เวลา		
4	การเสนอแผนเพื่อขออนุมัติ (Audit Plan Approval) เมื่อจัดทำแผนการตรวจสอบเสร็จแล้ว หัวหน้าทีมผู้ตรวจสอบภายใน เป็นผู้เสนอขออนุมัติแผนการดำเนินงานดังกล่าวไปยัง ผู้บริหารหรือคณะกรรมการที่มีอำนาจหน้าที่ ทั้งนี้แผนการตรวจสอบภายในต้องได้รับความเห็นชอบร่วมกันทั้งผู้ตรวจสอบภายในและผู้รับการตรวจสอบ	หัวหน้าทีมผู้ตรวจสอบภายใน	แผนการตรวจสอบภายใน (Internal Audit Plan)
5	การดำเนินการตรวจสอบ (Audit Execution) <ol style="list-style-type: none"> การจัดเตรียมการตรวจสอบ <ul style="list-style-type: none"> ผู้ตรวจสอบภายในควรทำการศึกษาเอกสารนโยบาย กระบวนการ มาตรฐานและแนวทางอื่นๆ ที่เกี่ยวข้อง จัดทำรายการการตรวจสอบ (Audit Checklist) เพื่อใช้เวลาตรวจสอบจริง และเพื่อใช้อ้างอิงเมื่อถูกตรวจสอบกระบวนการตรวจสอบภายใน การประชุมเพื่อเริ่มการตรวจสอบ (Opening Meeting) <ul style="list-style-type: none"> การประชุมจะดำเนินการร่วมกับผู้รับการตรวจสอบก่อนที่จะเริ่มการตรวจสอบจริง ทีมผู้ตรวจสอบภายในจะต้องอธิบายแผนการตรวจสอบและหารือร่วมกับผู้รับการตรวจสอบเกี่ยวกับกระบวนการที่จะใช้ในการตรวจสอบ ทั้งนี้ผู้รับการตรวจสอบอาจหารือในบางประเด็นร่วมกับผู้ตรวจสอบภายในได้ การจัดเก็บข้อมูลการตรวจสอบ (Recording of Objective Evidence) <ul style="list-style-type: none"> ทีมผู้ตรวจสอบดำเนินการตรวจสอบตามหน้าที่ของผู้ตรวจสอบแต่ละคน และใช้รายการตรวจสอบที่ได้จัดเตรียมขึ้นเป็นแนวทางในการตรวจสอบ โดยใช้เทคนิคในการตรวจสอบ เบื้องต้นดังต่อไปนี้ <ul style="list-style-type: none"> ทำการตรวจเอกสาร (Document) และ “บันทึก” ต่างๆ ที่เกี่ยวข้อง สัมภาษณ์หรือสอบถามข้อมูลจากบุคคลที่เกี่ยวข้องในการปฏิบัติงานในแต่ละจุด 	ผู้ตรวจสอบภายใน/ผู้รับการตรวจสอบ	1. Audit Checklist 2. Internal Audit Report

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

	<p style="text-align: center;">แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</p> <p style="text-align: center;">(Cybersecurity Audit Plan Procedure)</p>	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง
	<ul style="list-style-type: none"> ○ สังเกตการณ์การปฏิบัติงานที่เกิดขึ้นจริง ว่าเป็นไปตามเอกสารและข้อกำหนดหรือไม่ • ผู้ตรวจสอบต้องจดบันทึกสิ่งที่ได้พบจากการเข้าตรวจสอบ อย่างเหมาะสม ตามผลการตรวจสอบที่เกิดขึ้นจริง โดยแยกตามประเด็นที่ตรวจพบได้ ทั้งที่อาจมีอยู่ในรายการตรวจสอบหรือไม่ก็ได้ • ในการดำเนินการตรวจสอบในแต่ละสถานที่ ผู้ตรวจสอบภายในควรจัดเก็บข้อมูลให้เพียงพอต่อการจัดทำรายงานผลการตรวจสอบภายใน (Internal Audit Report) อาทิ เช่น <ul style="list-style-type: none"> ○ วัน - เวลาที่ทำการตรวจสอบ ○ หน่วยงานที่ถูกตรวจสอบ ○ สถานที่ / พื้นที่ที่ถูกตรวจสอบ ○ ข้อมูลบุคคลที่ได้พบ ○ เอกสารอ้างอิงที่พบ เช่น นโยบาย ระเบียบการปฏิบัติ หรือวิธีการปฏิบัติงาน ○ ข้อมูลหลักฐานการตรวจสอบ เช่น รายการสำรองข้อมูลล็อก การดำเนินงาน (operator logs) ซอฟต์แวร์ลิขสิทธิ์ (software licenses) รายการการฝึกอบรม (training records) ○ การดำเนินงานที่ไม่สอดคล้องกับข้อกำหนดในมาตรฐานที่ใช้อ้างอิง • หากเกิดข้อสงสัยต่อเหตุการณ์ที่ไม่เป็นไปตามข้อกำหนด (Non-conformance) ผู้ตรวจสอบภายในควรจัดเก็บข้อมูลโดยการสังเกตจากสถานการณ์จริง และตั้งข้อสังเกตถึงสาเหตุที่ไม่ปฏิบัติตามข้อกำหนด ทั้งนี้ผู้ตรวจสอบต้องตระหนักว่า การรายงานสิ่งที่ไม่เป็นไปตามข้อกำหนด (Non-conformance) ต้องมีหลักฐานที่ชัดเจนและเชื่อถือได้ (Objective Evidence) <p>4. การรายงานผลการตรวจสอบ (Audit Reporting)</p> <ul style="list-style-type: none"> • หัวหน้าผู้ตรวจสอบภายใน (Lead Auditor) และผู้ตรวจสอบภายใน (Auditor) จะต้องจัดทำรายงานผลการตรวจสอบภายใน (Internal Audit Report) ของแต่ละคน พร้อมทั้งจัดส่งรายงานผลการตรวจสอบดังกล่าวให้หัวหน้าผู้ตรวจสอบภายใน (Lead 		

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

	<p style="text-align: center;">แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</p> <p style="text-align: center;">(Cybersecurity Audit Plan Procedure)</p>	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง
	<p>Auditor) เพื่อร่วมกันปรึกษาและหาข้อสรุปที่ได้จากการตรวจสอบ ก่อนให้หัวหน้าผู้ตรวจสอบภายในจัดเก็บบันทึกต่อไป</p> <ul style="list-style-type: none"> • โดยรายละเอียดที่ปรากฏในรายงานผลการตรวจสอบภายใน (Internal Audit Report) จะต้องประกอบไปด้วยข้อมูลดังต่อไปนี้ <ul style="list-style-type: none"> ○ รายงานสรุปสิ่งที่พบในการตรวจสอบ ○ พื้นที่ ที่ได้รับการตรวจสอบ ○ ขอบเขตการตรวจสอบ ○ รายละเอียดและประเภทของข้อบกพร่องหรือสิ่งที่ไม่เป็นไปตามข้อกำหนด ได้แก่ NC ประเภท Major หรือ Minor ○ ข้อสังเกต (Observation) ○ ข้อเสนอแนะ (Opportunity for Improvement) ○ สรุปจำนวนข้อบกพร่อง ข้อสังเกต และข้อเสนอแนะ • หัวหน้าผู้ตรวจสอบภายใน (Lead Auditor) ต้องเป็นผู้แนะนำเสนอรายงานการตรวจสอบแก่คณะกรรมการหรือผู้บริหารที่เกี่ยวข้อง 		

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

	<p style="text-align: center;">แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</p> <p style="text-align: center;">(Cybersecurity Audit Plan Procedure)</p>	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

6. การปฏิบัติงานที่ไม่เป็นไปตามข้อกำหนด (Non-conformance)

ลำดับ	คำศัพท์	ความหมาย
1	การปฏิบัติงานที่ไม่สอดคล้อง หรือไม่มีประสิทธิภาพ	<ul style="list-style-type: none"> o ไม่ปฏิบัติตาม หรือปฏิบัติตามแต่ไม่มีประสิทธิภาพตามผู้บริหารหรือคณะกรรมการที่มีอำนาจหน้าที่ o ไม่ปฏิบัติตาม หรือปฏิบัติตามแต่ไม่มีประสิทธิภาพตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน o ไม่ปฏิบัติตาม หรือปฏิบัติตามแต่ไม่มีประสิทธิภาพตามนโยบายความมั่นคงปลอดภัยสารสนเทศ (Policy) o ไม่ปฏิบัติตาม หรือปฏิบัติตามแต่ไม่มีประสิทธิภาพตามเอกสารประกอบการปฏิบัติงานที่เกี่ยวข้อง (Process, Procedure, Work Instructions etc.) o ไม่ปฏิบัติตาม หรือปฏิบัติตามแต่ไม่มีประสิทธิภาพตามกฎหมายที่เกี่ยวข้อง (Law and relevant legislation) o ไม่ปฏิบัติตาม หรือปฏิบัติตามแต่ไม่มีประสิทธิภาพตามระเบียบข้อบังคับที่เกี่ยวข้องกับอุตสาหกรรม ระเบียบข้อบังคับกระทรวงสาธารณสุข o ไม่ปฏิบัติตาม หรือปฏิบัติตามแต่ไม่มีประสิทธิภาพตามสัญญาการให้บริการ (Contract)
2.	การปฏิบัติงานที่ไม่เป็นไปตามข้อกำหนด (Non-Conformance) จำแนกออกเป็น 2 ประเภท ได้แก่ ‘Minor’ หรือ ‘Major’ โดยเหตุการณ์ที่จะเป็น ‘Major’	<ul style="list-style-type: none"> o เป็นเหตุการณ์ที่ส่งผลกระทบต่อทั้งระบบ ข้อบังคับ กระบวนการหรือขั้นตอนการทำงาน o ขาดเอกสารการดำเนินงานหลักตามที่กำหนดไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน o มีเหตุการณ์ระดับ Minor ตั้งแต่ 5 เหตุการณ์ที่เกี่ยวข้องกับข้อกำหนดเดียวกัน ตามที่กำหนดไว้ในมาตรฐานและเอกสารกระบวนการหรือเอกสารขั้นตอนการทำงาน

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

	<p style="text-align: center;">แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</p> <p style="text-align: center;">(Cybersecurity Audit Plan Procedure)</p>	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

ลำดับ	คำศัพท์	ความหมาย
3.	ข้อสังเกต (Observation)	<ul style="list-style-type: none"> ข้อมูลที่ได้จากการตรวจสอบไม่เพียงพอที่จะสามารถสรุปผลได้ในเวลาที่ดำเนินการตรวจสอบว่าเป็น Non-conformance หรือไม่ ข้อสังเกตทุกประเด็น จะต้องถูกนำไปใส่ไว้ใน รายการตรวจสอบ (Audit Checklist) สำหรับการตรวจสอบครั้งต่อไป
4.	ข้อเสนอแนะ (Opportunity for Improvement)	<ul style="list-style-type: none"> เมื่อเหตุการณ์ที่พบ เป็นไปตามข้อกำหนดแต่ผู้ตรวจสอบภายในมีข้อเสนอแนะเพื่อให้การดำเนินงานดังกล่าวมีประสิทธิภาพมากยิ่งขึ้น ผู้รับตรวจสอบจะปฏิบัติตามข้อเสนอแนะหรือไม่ก็ได้

พิจารณาระยะเวลาการแก้ไขตามความเหมาะสม ดังนี้

ประเภทความไม่สอดคล้อง	ระยะเวลาแก้ไข	การแก้ไข ปัญหาแบบ ชั่วคราว	วิเคราะห์ สาเหตุ	แนวทางการ แก้ไข
ความไม่สอดคล้องหลัก (Major Non-Conformance)	ภายใน 30 วัน	✓	✓	✓
ความไม่สอดคล้องย่อย (Minor Non-Conformance)	ภายใน 60 วัน	✓	✓	✓
ข้อสังเกต (Observation)	ภายใน 365 วัน	-	-	✓
โอกาสในการปรับปรุง (Opportunity for Improvement: OFI)	ภายใน 365 วัน	-	-	✓

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

	แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan Procedure)	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

7. สรุปผลการตรวจสอบ (Audit Closing)

- เมื่อสิ้นสุดการตรวจสอบ ให้ทีมผู้ตรวจสอบภายในประชุมร่วมกับผู้รับการตรวจสอบ เพื่อสรุปผลการตรวจสอบทุกครั้ง
- หัวหน้าผู้ตรวจสอบควรทำการประชุมปิดการตรวจสอบโดยกล่าวสรุปถึงผลการตรวจสอบที่ได้ดำเนินการไป สิ่งที่ต้องตรวจพบทั้งหมด โดยแยกตามประเด็นที่ตรวจพบตามที่ได้กำหนดไว้ และควรกล่าวถึงส่วนที่ดีที่ได้ตรวจพบก่อน ที่จะกล่าวถึงสิ่งที่ไม่เป็นไปตามข้อกำหนด (Non-conformance)
- ทั้ง 2 ฝ่ายต้องทำความเข้าใจและชี้แจงรายละเอียดของสิ่งที่ตรวจพบทั้งหมด และควรอธิบายให้ผู้รับการตรวจสอบยอมรับ ถึงสิ่งที่ไม่เป็นไปตามข้อกำหนด (Non-Conformance)
- หัวหน้าทีมผู้ตรวจสอบภายในจะต้องจัดส่ง รายงานผลการตรวจสอบภายใน (Internal Audit Report) ให้กับผู้รับการตรวจสอบภายใน 15 วัน นับจากวันสรุปผลการตรวจสอบ

8. การรายงานการแก้ไขและป้องกัน (Corrective and Preventive Action Report)

8.1 Internal Audit Finding

- กลุ่มงานหรือเจ้าหน้าที่ที่ได้รับมอบหมายเป็นผู้รายงานการดำเนินการแก้ไขและป้องกัน (Corrective and Preventive Action Report : CAR)
- กรณีที่มีการจ้างบริษัทจากภายนอกเพื่อทำการตรวจสอบภายใน ให้กลุ่มงานหรือเจ้าหน้าที่ที่ได้รับมอบหมายเป็นผู้รายงานการดำเนินการแก้ไขและป้องกัน (Corrective and Preventive Action Report : CAR)

8.2 External Audit Finding

- กลุ่มงานหรือเจ้าหน้าที่ที่ได้รับมอบหมายเป็นผู้รายงานการดำเนินการแก้ไขและป้องกัน (Corrective and Preventive Action Report : CAR)

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของ โรงพยาบาลปรังค์กูห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรังค์กู เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	<p style="text-align: center;">แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</p> <p style="text-align: center;">(Cybersecurity Audit Plan Procedure)</p>	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

9. การตอบรับการแก้ไขและป้องกัน

9.1 Internal Audit Finding

- ผู้ที่ได้รับผู้รายงานการดำเนินการแก้ไขและป้องกัน (Corrective and Preventive Action Report : CAR) ต้องจัดส่งแนวทางหรือวิธีการแก้ไขปัญหาที่พบ ให้แก่ผู้รายงานการดำเนินการแก้ไขและป้องกัน ตามระยะเวลาและขั้นตอนที่ระบุไว้ในเอกสารระเบียบการปฏิบัติงาน เรื่อง การแก้ไขและป้องกัน (Corrective and Preventive action Procedure)

9.2 External Audit Finding

- ให้ปฏิบัติตามมมาตรา 54 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยดำเนินการตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ดังนี้
 - กรณี เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อ สกมช. ภายในกำหนด 30 วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา 54 พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย ทั้งนี้ รูปแบบและรายละเอียดผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปตามที่ สกมช. กำหนด
 - ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา 54 ระบุการไม่ปฏิบัติตามข้อ 17.1 ของประมวลแนวทางปฏิบัติและกรอบมาตรฐาน เว้นแต่ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศส่งแผนการดำเนินการแก้ไขไปยัง สกมช. ภายในกำหนด 30 วัน นับแต่จากวันที่ได้รับรายงานการตรวจสอบโดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้
 - (ก) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และ
 - (ข) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ 17.3 (ก) ของประมวลแนวทางปฏิบัติและกรอบมาตรฐาน
 - ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการ

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

	แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan Procedure)	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

ปรับปรุงแล้วไปยังสภมช. ภายในระยะเวลาที่ กกม. กำหนด พร้อมส่งทั้งสำเนาให้หน่วยงาน
ควบคุมหรือกำกับดูแลด้วย

- เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม. หน่วยงานโครงสร้างพื้นฐาน
สำคัญทางสารสนเทศจะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการ
แก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การ
พิจารณาของ กกม.

10. การแก้ไขและการป้องกัน (Corrective and Preventive Action)

- ผู้ที่ได้รับมอบหมายให้ตรวจสอบผลการแก้ไขและป้องกัน ต้องดำเนินการตรวจสอบตามระเบียบการ
ปฏิบัติงาน เรื่อง การแก้ไขและป้องกัน (Corrective and Preventive action Procedure)
- ผู้ที่ได้รับมอบหมายให้ตรวจสอบฯ ต้องตรวจสอบจากข้อเท็จจริง หรือหลักฐานที่ปรากฏให้เชื่อถือได้ว่า
ผู้ที่ได้รับมอบหมาย ได้ดำเนินการแล้วเสร็จอย่างมีประสิทธิภาพ

11. การติดตามผลการแก้ไขและป้องกัน (Corrective and Preventive Action Follow up)

11.1 Internal Audit Finding

- กลุ่มงานหรือเจ้าหน้าที่ที่ได้รับมอบหมายมีหน้าที่ในการติดตามสถานะการดำเนินงานการแก้ไขและ
ป้องกัน

11.2 External Audit Finding 1

- กลุ่มงานหรือเจ้าหน้าที่ที่ได้รับมอบหมายมีหน้าที่ในการติดตามสถานะการดำเนินงานการแก้ไขและ
ป้องกัน

12. การตรวจสอบผลการแก้ไขและป้องกัน (Verification of Corrective and Preventive Action)

- ผู้ที่ได้รับมอบหมายให้ตรวจสอบผลการแก้ไขและป้องกัน ต้องดำเนินการตรวจสอบตามระเบียบการ
ปฏิบัติงาน เรื่อง การแก้ไขและป้องกัน (Corrective and Preventive action Procedure)
- ผู้ที่ได้รับมอบหมายให้ตรวจสอบฯ ต้องตรวจสอบจากข้อเท็จจริง หรือหลักฐานที่ปรากฏให้เชื่อถือได้ว่า
ผู้ที่ได้รับมอบหมาย ได้ดำเนินการแล้วเสร็จอย่างมีประสิทธิภาพ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น
กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของ โรงพยาบาลปรังกะบุรีห้ามแจกจ่ายไปยัง
บุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลปรังกะบุรี เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น
ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	<p style="text-align: center;">แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</p> <p style="text-align: center;">(Cybersecurity Audit Plan Procedure)</p>	รหัสเอกสาร	PKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

การทบทวนกระบวนการดำเนินการ

แนวทางดำเนินการนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. แผนงานการตรวจสอบ (Audit Programme / Audit Plan)
2. รายงานการตรวจสอบ (Audit Reporting)
3. ผลการดำเนินการแก้ไข และรายงานผลการแก้ไข (Corrective Action Report)
4. แผนการตรวจสอบระยะเวลา 1 ปี (Annual Audit Plan) หรือ เกินกว่า 1 ปี (Multi-Year Audit Plan)
5. รายงานหรือเอกสารแสดงการจัดทำ BIA

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



โรงพยาบาลปรังคู้

รายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (Audit Report)

ชื่อหน่วยงานที่รับการตรวจประเมิน : โรงพยาบาลปรังคู้

ประเภทของหน่วยงาน : CII | Regulator | Gov

วันที่ประเมิน: วันที่ 1 – 2 เมษายน 2569

ชื่อผู้ตรวจสอบ: 1. นายวิทยา แหวนหล่อ (Lead Auditor), 2. นางสุปราณี ศรีหะโคตร์ (Auditor)

Audit Objective : เพื่อแน่ใจว่าหน่วยงาน โรงพยาบาลปรังคู้ ได้ปฏิบัติตาม พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และกฎหมายลำดับรอง 15 ฉบับ

Audit Scope : โรงพยาบาลปรังคู้

Audit Criteria : พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และกฎหมายลำดับรอง 15 ฉบับ

ผลการประเมินก่อนหน้า: - ไม่มีการตรวจประเมิน , อ้างอิงถึงเอกสาร - ไม่มี

สรุปผลการประเมินโดยภาพรวม (Executive Summary)

1. ผ่านการประเมินโดยรวม
2. คะแนนรวมที่ได้จากการประเมิน : 98 % - คิดตามสัดส่วน (จำนวนข้อที่สอดคล้อง / จำนวนข้อทั้งหมด)
เช่น $(96 / 98) * 100 = 97.95 \%$
3. จำนวนตัวควบคุมทั้งหมดที่ใช้ในการตรวจประเมิน = 98 ตัวควบคุม
4. จำนวนตัวควบคุมที่ไม่ผ่านการประเมิน = 2 ตัวควบคุม

	รายการการตรวจประเมิน	จำนวนตัวควบคุม/ คะแนนเต็ม	ผลการประเมิน	% Score ที่ ได้รับ
1	พรบ.ความมั่นคงปลอดภัยไซเบอร์ 2562	12	S	12
2	นโยบายฯ ไซเบอร์แห่งชาติ (2565-2570)	13	S	13
3	ประมวลแนวทางปฏิบัติและกรอบ มาตรฐาน	73	2 NC	71
3.1	ประมวลแนวทางปฏิบัติ			
3.1.1	แผนการตรวจสอบ		O (1)	
3.1.2	การประเมินความเสี่ยง		S	
3.1.3	แผนการรับมือภัยคุกคามทางไซเบอร์		S	
3.2	กรอบมาตรฐาน			
3.2.1	Govern		S	
3.2.2	Identify		S	
3.2.3	Protect		S	
3.2.4	Detect		S	
3.2.5	Respond		S	
3.2.6	Recover		O (1)	
	ผลรวม	98		96

S – Satisfied = Conformity

O – Non-Satisfied = NC (Non-Conformity)

N/A - Not Applicable

รายละเอียดการตรวจสอบ

ข้อดี (Strong Point) :

1. หน่วยงานดังกล่าวได้มีการจัดทำเอกสารต่างๆ โดยรวมได้เป็นอย่างดี ตรงตามที่ พรบ ไซเบอร์ ได้กำหนดไว้
2. โดยส่วนมาก บุคลากรที่ได้รับการสัมภาษณ์มีความรู้ในส่วนที่เกี่ยวข้องได้ดี

ข้อที่ควรทำการแก้ไข (Weak Point) :

1. ตัวควบคุม: Domain 3 : ประมวลและกรอบฯ | แผนการตรวจสอบ | ข้อ 17.1

วัตถุประสงค์: ต้องมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศทั้งโดยผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 ครั้ง

วิธีการประเมิน:

1. Interview : สัมภาษณ์ผู้ตรวจสอบภายใน
2. Review Document : ร้องขอเอกสารรายงานการตรวจสอบ

อธิบายการดำเนินการของผู้ตรวจ :

ทางผู้ตรวจสอบ ได้ดำเนินการตรวจสอบเอกสารและบันทึกการรายงานต่างๆ รวมถึงการสัมภาษณ์ผู้ที่เกี่ยวข้อง ตามหลักการ ISO 19011 พบว่าไม่มีหลักฐานในการทำการตรวจสอบภายใน ภายในปี ตามที่ระบุไว้ ผลการประเมิน:

ไม่ผ่านการประเมิน (O) : พบว่า ไม่มีการทำการตรวจสอบภายใน ภายในปี ตามที่ระบุไว้

ความคิดเห็นของผู้ประเมิน: เนื่องจากการตรวจสอบภายในมีความสำคัญเป็นอย่างยิ่ง ในการปรับปรุงพัฒนาอย่างต่อเนื่องของระบบ ดังนั้น จึงถือว่าข้อนี้ ไม่สอดคล้องตามเกณฑ์ของ พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์

คำแนะนำ: ผู้รับการตรวจสอบ กระทำตามที่กำหนดไว้

ส่วนของผู้รับการตรวจ

ทำการวิเคราะห์หาสาเหตุ (Root Cause Analyst) : พบว่าทางเจ้าหน้าที่ที่เกี่ยวข้องละเอียดไม่ได้จัดทำ การตรวจสอบ เนื่องจากเจ้าหน้าที่ยังขาดองค์ความรู้ในการตรวจสอบ และโรงพยาบาลปรังค์กูเพิ่งเริ่มต้นการขึ้นระบบ ตาม พรบ.ไซเบอร์ เมื่อเดือน มีนาคม พ.ศ.2569

วิธีการแก้ไขเพื่อไม่ให้ปัญหาเกิดขึ้นอีก (Corrective Action) : ทางหน่วยงานได้มีการทบทวนแผนการ ตรวจสอบใหม่ทั้งหมด และมอบหมายให้ผู้บังคับบัญชาโดยตรง รับผิดชอบในการควบคุมหรือตรวจตรา ตามเวลาที่ กำหนด โดยมี Timeline ดังต่อไปนี้

1. ทบทวนแผนการตรวจสอบใหม่ทั้งหมด | วันที่ดำเนินการคือ 19 เมษายน 2569, ผู้รับผิดชอบ คือ นาย วิทยา แหวนหล่อ

2. ตัวควบคุม: Domain 3 : ประมวลและกรอบฯ | Recover - Cybersecurity Resilience and Recovery | ข้อ 25.1.1

วัตถุประสงค์: ต้องมีการจัดทำแผนความต่อเนื่องทางธุรกิจ Business Continuity Plan : BCP) และมีการซ้อมแผนเพื่อให้หน่วยงานสามารถกลับมาดำเนินการได้อย่างต่อเนื่อง

วิธีการประเมิน:

1. Review Document : ตรวจสอบเอกสารที่ได้จัดทำในส่วนที่เป็นกรอบมาตรฐาน (Recover > Cybersecurity Resilience and Recovery)
2. Interview : สัมภาษณ์ผู้ดูแลระบบ (พรบ.ไซเบอร์ 2562)
3. Observation : จากการสังเกตการณ์ ไม่พบหลักฐานถึงการทำแผนความต่อเนื่องทางธุรกิจ

อธิบายการดำเนินการของผู้ตรวจ :

ทางผู้ตรวจสอบ ได้ดำเนินการตรวจสอบเอกสารและบันทึกการรายงานต่างๆ รวมถึงการสัมภาษณ์ผู้ที่เกี่ยวข้อง และการสังเกตการณ์ ตามหลักการ ISO 19011 พบว่ามีหลักฐานในการจัดทำแผนความต่อเนื่องทางธุรกิจ Business Continuity Plan : BCP) ตามที่ระบุไว้

ผลการประเมิน:

ไม่ผ่านการประเมิน (O): พบที่มีการจัดทำแผนความต่อเนื่องทางธุรกิจ Business Continuity Plan แต่ไม่มีการฝึกซ้อมตามแผน

ความคิดเห็นของผู้ประเมิน: ทางหน่วยงานดังกล่าวได้มีการจัดทำเอกสารที่เป็นขั้นตอนการปฏิบัติงาน (Procedure) ได้เป็นอย่างดี ตรงตามที่ พรบ ไซเบอร์ ได้กำหนด แต่จากการตรวจสอบเอกสารโดยละเอียดแล้ว รวมถึงหาหลักฐานประกอบ พบว่า ทางหน่วยงาน มีการจัดทำแผนความต่อเนื่อง ซึ่งแผนดังกล่าว มีความสำคัญต่อผู้บริหารหรือหน่วยควบคุมการกำกับดูแล

คำแนะนำ: ควรต้องมีการฝึกซ้อมแผน BCP ด้วย

.....
ส่วนของผู้รับการตรวจ

ทำการวิเคราะห์หาสาเหตุ (Root Cause Analyst) : พบว่าทางเจ้าหน้าที่ที่เกี่ยวข้องไม่ได้จัดทำแผนความต่อเนื่อง ในปีดังกล่าว เนื่องจากเป็นเจ้าหน้าที่ใหม่ ซึ่งไม่ทราบว่าต้องมีการจัดทำ

วิธีการแก้ไขเพื่อไม่ให้ปัญหาเกิดขึ้นอีก (Corrective Action) : ทางหน่วยงานได้มีการทบทวนแผนการอบรม พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์ ให้กับพนักงานที่เกี่ยวข้องให้รับทราบ โดยมี Timeline ดังต่อไปนี้

1. ทำการอบรมเจ้าหน้าที่ที่เกี่ยวข้อง ทั้งหมด พร้อม Post test หลังการอบรม โดยเน้นในส่วนของการจัดทำแผนความต่อเนื่องทางธุรกิจ | วันที่ดำเนินการคือ เมษายน 2569, ผู้รับผิดชอบ คือ นายสันต์ สิงห์ไกร Lead Implementor

ผู้ตรวจสอบ



(นายวิทยา แหวนหล่อ) (Lead Auditor)



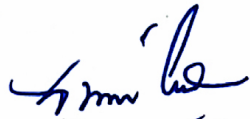
(นางสุปราณี ศรีหะโคตร) (Auditor)

ผู้รับการตรวจ



(นายสันต์ สิงห์ไกร) (Lead Implementor)

รับทราบ



(นายแพทย์อัครเดช บุญเย็น)

ผู้อำนวยการโรงพยาบาลปรางค์กู่ (CISO)