

	<b>แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</b>  <b>(Cybersecurity Audit Plan Procedure)</b>	รหัสเอกสาร	NKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็น			
ชื่อ-สกุล	นายอิสรภาพ เบ้าน้อย	นางพรณี วรรณรม	นายธนสันตชัย พรหมบุตร
ตำแหน่ง	นักวิชาการคอมพิวเตอร์	พยาบาลวิชาชีพชำนาญการพิเศษ (Lead Implementer)	นายแพทย์ชำนาญการพิเศษ รักษาการใน ตำแหน่งผู้อำนวยการโรงพยาบาลโนนคูณ (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 หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลโนนคูณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคูณ เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	<p style="text-align: center;"><b>แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</b></p> <p style="text-align: center;"><b>(Cybersecurity Audit Plan Procedure)</b></p>	รหัสเอกสาร	NKH 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).....	12
7. สรุปผลการตรวจสอบ (Audit Closing) .....	14
8. การรายงานการแก้ไขและป้องกัน (Corrective and Preventive Action Report) .....	14
9. การตอบรับการแก้ไขและป้องกัน.....	15
10. การแก้ไขและการป้องกัน (Corrective and Preventive Action) .....	16
11. การติดตามผลการแก้ไขและป้องกัน (Corrective and Preventive Action Follow up) .....	17
12. การตรวจสอบผลการแก้ไขและป้องกัน (Verification of Corrective and Preventive Action) ....	17
13. การทบทวนกระบวนการดำเนินการ .....	18

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

	<b>แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan Procedure)</b>	รหัสเอกสาร	NKH 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 โรงพยาบาลโนนคุณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคุณ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	<b>แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</b>  <b>(Cybersecurity Audit Plan Procedure)</b>	รหัสเอกสาร	NKH 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"> <li>1. ไม่สอดคล้องตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน</li> <li>2. ไม่สอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ (Policy)</li> <li>3. ไม่สอดคล้องตามเอกสารประกอบการปฏิบัติงานที่เกี่ยวข้อง (Process, Procedure, Work) เช่น เอกสารมอบหมายงาน เอกสารข้อตกลง</li> <li>4. ไม่สอดคล้องตามกฎหมายที่เกี่ยวข้อง (Law and Relevant Legislation)</li> <li>5. ไม่สอดคล้องตามระเบียบ เช่น ระเบียบข้อบังคับที่เกี่ยวข้องกับอุตสาหกรรม ระเบียบข้อบังคับของกระทรวงสาธารณสุข</li> <li>6. ไม่สอดคล้องตามสัญญาการให้บริการ (Contract)</li> </ol>

## 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

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



**แผนการตรวจสอบด้านการรักษาความ  
มั่นคงปลอดภัยไซเบอร์  
(Cybersecurity Audit Plan  
Procedure)**

รหัสเอกสาร	NKH MOPH Audit Plan -01
แก้ไขครั้งที่	00
วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

- เป็นผู้ที่ได้รับการฝึกอบรมหลักสูตรผู้ตรวจสอบภายใน จากหน่วยงานภายนอกที่เชื่อถือได้
- เป็นผู้ที่มีความรู้ความเข้าใจระบบบริหารความมั่นคงปลอดภัยสารสนเทศ หรือกระบวนการปฏิบัติงานต่าง ๆ ของหน่วยงานที่ถูกตรวจสอบ
- เป็นผู้ที่ได้รับการแต่งตั้งให้เป็นผู้ตรวจสอบภายในหรือเป็นผู้ทรงคุณวุฒิที่ได้รับเชิญเป็นกรณีพิเศษ

**4. หน้าที่และความรับผิดชอบของทีมผู้ตรวจสอบภายใน**

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

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลโนนคูณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคูณ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ครอบครองจะถูกระงับในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	<b>แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</b>  <b>(Cybersecurity Audit Plan Procedure)</b>	รหัสเอกสาร	NKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

		<ul style="list-style-type: none"> <li>- ตรวจสอบการดำเนินงานแก้ไขและป้องกันปัญหาและลงนามรับรองผลการดำเนินการในรายงานการดำเนินการแก้ไขและป้องกัน</li> </ul>
2	ผู้ตรวจสอบภายใน (Internal Auditor)	<ul style="list-style-type: none"> <li>- ศึกษาทำความเข้าใจเอกสารและข้อมูลต่างๆ ที่เกี่ยวข้องกับการตรวจสอบ</li> <li>- จัดเตรียมรายการตรวจสอบ</li> <li>- ดำเนินการตรวจสอบภายในตามแผนการตรวจสอบภายใน</li> <li>- บันทึกสิ่งที่พบข้อบกพร่อง ข้อสังเกตเป็นลายลักษณ์อักษร</li> <li>- ให้ข้อเสนอแนะเพื่อปรับปรุงประสิทธิภาพการปฏิบัติงาน</li> <li>- จัดทำรายงานผลการตรวจสอบภายใน</li> <li>- จัดทำรายงานการดำเนินการแก้ไขและป้องกัน</li> </ul>

### 5. ขั้นตอนปฏิบัติการตรวจสอบภายใน

ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง
1	<b>การทำโปรแกรมการตรวจสอบภายใน</b> หัวหน้าทีมผู้ตรวจสอบภายใน จะต้องจัดเตรียมตาราง การตรวจสอบภายในภายใต้ขอบเขตตามผลการวิเคราะห์จากกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) เป็นประจำทุกปี โดยตารางดังกล่าวจะต้องประกอบไปด้วย <ul style="list-style-type: none"> <li>○ ช่วงเวลาในการตรวจสอบ</li> <li>○ ขอบเขตในการตรวจสอบ</li> <li>○ ผู้ตรวจสอบ</li> </ul>	หัวหน้าทีม ผู้ตรวจสอบ ภายใน	โปรแกรม การ ตรวจสอบ ภายใน ประจำปี

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลโนนคุณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคุณ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



**แผนการตรวจสอบด้านการรักษาความ  
มั่นคงปลอดภัยไซเบอร์  
(Cybersecurity Audit Plan  
Procedure)**

รหัสเอกสาร	NKH 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"> <li>• โปรแกรมการตรวจสอบภายในประจำปี ต้องได้รับการอนุมัติโดยผู้บริหารหรือคณะกรรมการที่มีอำนาจหน้าที่</li> <li>• ทุกกระบวนการจะต้องมีการตรวจสอบอย่างน้อยปีละ 1 ครั้ง ทั้งนี้ หัวหน้าทีมผู้ตรวจสอบภายในอาจเพิ่มความถี่ในการตรวจสอบได้ ขึ้นอยู่กับผลของการตรวจสอบในครั้งที่ผ่านมา หรือมีการเปลี่ยนแปลงใดๆ ที่มีความสำคัญต่อการปฏิบัติงานภายใต้ขอบเขต</li> <li>• ข้อกำหนดที่จะปฏิบัติต้องสอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน บริบทองค์กรในแต่ละปี จะต้องได้รับการตรวจสอบอย่างน้อยปีละ 1 ครั้ง</li> <li>• ต้องมีการทบทวนและแก้ไขโปรแกรมการตรวจสอบประจำปี หากมีเหตุการณ์เหล่านี้เกิดขึ้น               <ul style="list-style-type: none"> <li>o การเปลี่ยนแปลงที่สำคัญขององค์กร (Major organization change)</li> <li>o ข้อบกพร่องหลักที่กระทบกับระบบงาน (Major Non-conformances for a function)</li> <li>o ข้อบกพร่องหลักที่กระทบต่อข้อกำหนดของประมวลแนวทางปฏิบัติและกรอบมาตรฐาน</li> </ul> </li> </ul>		
2	<p><b>การเตรียมการเพื่อวางแผนการตรวจสอบภายใน (Preparation for Audit Plan)</b></p> <ol style="list-style-type: none"> <li>1. ทบทวนผลการตรวจสอบภายในและผลการดำเนินการแก้ไข Finding ที่พบจากการตรวจสอบภายในและการตรวจสอบจากหน่วยงานภายนอก ครั้งที่ผ่านมา (ถ้ามี)</li> <li>2. ทบทวนรายงานการประชุมทบทวนของผู้บริหาร</li> <li>3. ทบทวนเหตุการณ์ด้านความมั่นคงปลอดภัยต่างๆ ที่เกิดขึ้น</li> </ol>	ผู้ตรวจสอบ ภายใน	

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลโนนคูณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคูณ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



แผนการตรวจสอบด้านการรักษาความ  
มั่นคงปลอดภัยไซเบอร์  
(Cybersecurity Audit Plan  
Procedure)

รหัสเอกสาร	NKH MOPH Audit Plan -01
แก้ไขครั้งที่	00
วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง
	4. ทบทวนรายงานการประเมินความเสี่ยงของปีที่ผ่านมา 5. ทบทวนประสิทธิภาพการดำเนินงานตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานในปีที่ผ่านมา		
3	<b>จัดทำแผนการตรวจสอบ (Audit Plan)</b> จัดเตรียมรายละเอียดของแผนการตรวจสอบประจำปี สำหรับการดำเนินงานในแต่ละช่วงลงในแผนการตรวจสอบภายใน (Internal Audit Plan) โดยจะต้องประกอบไปด้วย: <ul style="list-style-type: none"><li>วัตถุประสงค์</li><li>มาตรฐานที่ใช้ในการตรวจสอบ</li><li>ขอบเขตงาน</li><li>กำหนดพื้นที่หรือระบบที่จะตรวจสอบ (ฟังก์ชันงาน หน่วยงานหรือที่ตั้ง)</li><li>เอกสารอ้างอิง ถ้ามี</li><li>ผู้ตรวจสอบภายใน</li><li>ผู้รับการตรวจสอบ</li><li>วัน เวลา</li></ul>	ทีมผู้ตรวจสอบภายใน	แผนการตรวจสอบภายใน (Internal Audit Plan)
4	<b>การเสนอแผนเพื่อขออนุมัติ (Audit Plan Approval)</b> เมื่อจัดทำแผนการตรวจสอบเสร็จแล้ว หัวหน้าทีมผู้ตรวจสอบภายใน เป็นผู้เสนอขออนุมัติแผนการดำเนินงานดังกล่าวไปยัง ผู้บริหารหรือคณะกรรมการที่มีอำนาจหน้าที่ ทั้งนี้แผนการตรวจสอบภายในต้องได้รับความเห็นชอบร่วมกันทั้งผู้ตรวจสอบภายในและผู้รับการตรวจสอบ	หัวหน้าทีมผู้ตรวจสอบภายใน	แผนการตรวจสอบภายใน (Internal Audit Plan)

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลโนนคูณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคูณ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ควบคุมจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



แผนการตรวจสอบด้านการรักษาความ  
มั่นคงปลอดภัยไซเบอร์  
(Cybersecurity Audit Plan  
Procedure)

รหัสเอกสาร

NKH MOPH  
Audit Plan -01

แก้ไขครั้งที่

00

วันที่บังคับใช้  
ชั้นความลับของ  
เอกสาร

23 มี.ค. 2569  
ใช้ภายในเท่านั้น

ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง
5	<p><b>การดำเนินการตรวจสอบ (Audit Execution)</b></p> <p>1. การจัดเตรียมการตรวจสอบ</p> <ul style="list-style-type: none"> <li>ผู้ตรวจสอบภายในควรทำการศึกษาเอกสารนโยบาย กระบวนการ มาตรฐานและแนวทางอื่นๆ ที่เกี่ยวข้อง</li> <li>จัดทำรายการการตรวจสอบ (Audit Checklist) เพื่อใช้เวลาตรวจสอบจริง และเพื่อใช้อ้างอิงเมื่อถูกตรวจสอบกระบวนการตรวจสอบภายใน</li> </ul> <p>2. การประชุมเพื่อเริ่มการตรวจสอบ (Opening Meeting)</p> <ul style="list-style-type: none"> <li>การประชุมจะดำเนินการร่วมกับผู้รับการตรวจสอบก่อนที่จะเริ่มการตรวจสอบจริง</li> <li>ทีมผู้ตรวจสอบภายในจะต้องอธิบายแผนการตรวจสอบและหารือร่วมกับผู้รับการตรวจสอบเกี่ยวกับกระบวนการที่จะใช้ในการตรวจสอบ ทั้งนี้ผู้รับการตรวจสอบอาจหารือในบางประเด็นร่วมกับผู้ตรวจสอบภายในได้</li> </ul> <p>3. การจัดเก็บข้อมูลการตรวจสอบ (Recording of Objective Evidence)</p> <ul style="list-style-type: none"> <li>ทีมผู้ตรวจสอบดำเนินการตรวจสอบตามหน้าที่ของผู้ตรวจสอบแต่ละคน และใช้รายการตรวจสอบที่ได้จัดเตรียมขึ้นเป็นแนวทางในการตรวจสอบ โดยใช้เทคนิคในการตรวจสอบ เบื้องต้นดังต่อไปนี้ <ul style="list-style-type: none"> <li>ทำการตรวจเอกสาร (Document) และ “บันทึก” ต่างๆ ที่เกี่ยวข้อง</li> <li>สัมภาษณ์หรือสอบถามข้อมูลจากบุคคลที่เกี่ยวข้องในการปฏิบัติงานในแต่ละจุด</li> <li>สังเกตการณ์การปฏิบัติงานที่เกิดขึ้นจริง ว่าเป็นไปตามเอกสารและข้อกำหนดหรือไม่</li> </ul> </li> <li>ผู้ตรวจสอบต้องจดบันทึกสิ่งที่ได้พบจากการเข้าตรวจสอบ อย่างเหมาะสม ตามผลการตรวจสอบที่เกิดขึ้นจริง โดยแยกตามประเด็นที่ตรวจพบได้ ทั้งที่อาจมีอยู่ในรายการตรวจสอบหรือไม่ก็ได้</li> </ul>	ผู้ตรวจสอบ ภายใน/ผู้รับ การตรวจสอบ	1. Audit Checklist 2. Internal Audit Report

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของ โรงพยาบาลโนนคุณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคุณ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



แผนการตรวจสอบด้านการรักษาความ  
มั่นคงปลอดภัยไซเบอร์  
(Cybersecurity Audit Plan  
Procedure)

รหัสเอกสาร	NKH 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"> <li>• ในการดำเนินการตรวจสอบในแต่ละสถานที่ ผู้ตรวจสอบภายในควรจัดเก็บข้อมูลให้เพียงพอต่อการจัดทำรายงานผลการตรวจสอบภายใน (Internal Audit Report) อาทิ เช่น               <ul style="list-style-type: none"> <li>o วัน - เวลาที่ทำการตรวจสอบ</li> <li>o หน่วยงานที่ถูกตรวจสอบ</li> <li>o สถานที่ / พื้นที่ที่ถูกตรวจสอบ</li> <li>o ข้อมูลบุคคลที่ได้พบ</li> <li>o เอกสารอ้างอิงที่พบ เช่น นโยบาย ระเบียบการปฏิบัติ หรือวิธีการปฏิบัติงาน</li> <li>o ข้อมูลหลักฐานการตรวจสอบ เช่น รายการสำรองข้อมูลล็อก การดำเนินงาน (operator logs) ซอฟต์แวร์ลิขสิทธิ์ (software licenses) รายการการฝึกอบรม (training records)</li> <li>o การดำเนินงานที่ไม่สอดคล้องกับข้อกำหนดในมาตรฐานที่ใช้อ้างอิง</li> </ul> </li> <li>• หากเกิดข้อสงสัยต่อเหตุการณ์ที่ไม่เป็นไปตามข้อกำหนด (Non-conformance) ผู้ตรวจสอบภายในควรจัดเก็บข้อมูลโดยการสังเกตจากสถานการณ์จริง และตั้งข้อสังเกตถึงสาเหตุที่ไม่ปฏิบัติตามข้อกำหนด ทั้งนี้ผู้ตรวจสอบต้องตระหนักว่า การรายงานสิ่งที่ไม่เป็นไปตามข้อกำหนด (Non-conformance) ต้องมีหลักฐานที่ชัดเจนและเชื่อถือได้ (Objective Evidence)</li> </ul> <p>4. การรายงานผลการตรวจสอบ (Audit Reporting)</p> <ul style="list-style-type: none"> <li>• หัวหน้าผู้ตรวจสอบภายใน (Lead Auditor) และผู้ตรวจสอบภายใน (Auditor) จะต้องจัดทำรายงานผลการตรวจสอบภายใน (Internal Audit Report) ของแต่ละคน พร้อมทั้งจัดส่งรายงานผลการตรวจสอบดังกล่าวให้หัวหน้าผู้ตรวจสอบภายใน (Lead</li> </ul>		

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของ โรงพยาบาลโนนคุณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคุณ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



แผนการตรวจสอบด้านการรักษาความ  
มั่นคงปลอดภัยไซเบอร์  
(Cybersecurity Audit Plan  
Procedure)

รหัสเอกสาร

NKH 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"><li>• โดยรายละเอียดที่ปรากฏในรายงานผลการตรวจสอบภายใน (Internal Audit Report) จะต้องประกอบไปด้วยข้อมูลดังต่อไปนี้<ul style="list-style-type: none"><li>o รายงานสรุปสิ่งที่พบในการตรวจสอบ</li><li>o พื้นที่ ที่ได้รับการตรวจสอบ</li><li>o ขอบเขตการตรวจสอบ</li><li>o รายละเอียดและประเภทของข้อบกพร่องหรือสิ่งที่ไม่เป็นไปตามข้อกำหนด ได้แก่ NC ประเภท Major หรือ Minor</li><li>o ข้อสังเกต (Observation)</li><li>o ข้อเสนอแนะ (Opportunity for Improvement)</li><li>o สรุปจำนวนข้อบกพร่อง ข้อสังเกต และข้อเสนอแนะ</li></ul></li><li>• หัวหน้าผู้ตรวจสอบภายใน (Lead Auditor) ต้องเป็นผู้นำเสนอรายงานการตรวจสอบแก่คณะกรรมการหรือผู้บริหารที่เกี่ยวข้อง</li></ul>		

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลโนนคูณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคูณ เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	<b>แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</b>  <b>(Cybersecurity Audit Plan Procedure)</b>	รหัสเอกสาร	NKH 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"> <li>o ไม่ปฏิบัติตาม หรือปฏิบัติตามแต่ไม่มีประสิทธิภาพตามผู้บริหารหรือคณะกรรมการที่มีอำนาจหน้าที่</li> <li>o ไม่ปฏิบัติตาม หรือปฏิบัติตามแต่ไม่มีประสิทธิภาพตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน</li> <li>o ไม่ปฏิบัติตาม หรือปฏิบัติตามแต่ไม่มีประสิทธิภาพตามนโยบายความมั่นคงปลอดภัยสารสนเทศ (Policy)</li> <li>o ไม่ปฏิบัติตาม หรือปฏิบัติตามแต่ไม่มีประสิทธิภาพตามเอกสารประกอบการปฏิบัติงานที่เกี่ยวข้อง (Process, Procedure, Work Instructions etc.)</li> <li>o ไม่ปฏิบัติตาม หรือปฏิบัติตามแต่ไม่มีประสิทธิภาพตามกฎหมายที่เกี่ยวข้อง (Law and relevant legislation)</li> <li>o ไม่ปฏิบัติตาม หรือปฏิบัติตามแต่ไม่มีประสิทธิภาพตามระเบียบข้อบังคับที่เกี่ยวข้องกับอุตสาหกรรม ระเบียบข้อบังคับกระทรวงสาธารณสุข</li> <li>o ไม่ปฏิบัติตาม หรือปฏิบัติตามแต่ไม่มีประสิทธิภาพตามสัญญาการให้บริการ (Contract)</li> </ul>
2.	การปฏิบัติงานที่ไม่เป็นไปตามข้อกำหนด (Non-Conformance) จำแนกออกเป็น 2 ประเภท ได้แก่ 'Minor' หรือ 'Major' โดยเหตุการณ์ที่จะเป็น 'Major'	<ul style="list-style-type: none"> <li>o เป็นเหตุการณ์ที่ส่งผลกระทบต่อทั้งระบบ ข้อบังคับ กระบวนการหรือขั้นตอนการทำงาน</li> <li>o ขาดเอกสารการดำเนินงานหลักตามที่กำหนดไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน</li> </ul>

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลโนนคุณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคุณ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ครอบครองจะถูกระงับในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



**แผนการตรวจสอบด้านการรักษาความ  
มั่นคงปลอดภัยไซเบอร์  
(Cybersecurity Audit Plan  
Procedure)**

รหัสเอกสาร	NKH MOPH Audit Plan -01
แก้ไขครั้งที่	00
วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

ลำดับ	คำศัพท์	ความหมาย
		○ มีเหตุการณ์ระดับ Minor ตั้งแต่ 5 เหตุการณ์ที่เกี่ยวข้องกับข้อกำหนดเดียวกัน ตามที่กำหนดไว้ในมาตรฐานและเอกสารกระบวนการหรือเอกสารขั้นตอนการทำงาน
3.	ข้อสังเกต (Observation)	○ ข้อมูลที่ได้จากการตรวจสอบไม่เพียงพอที่จะสามารถสรุปผลได้ในเวลาที่ดำเนินการตรวจสอบว่าเป็น Non-conformance หรือไม่ ○ ข้อสังเกตทุกประเด็น จะต้องถูกนำไปใส่ไว้ใน รายการตรวจสอบ (Audit Checklist) สำหรับการตรวจสอบครั้งต่อไป
4.	ข้อเสนอแนะ (Opportunity for Improvement)	○ 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	-	-	✓

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ในส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลโนนคูณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคูณ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ครอบครองจะถูกระงับในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	<b>แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</b>  <b>(Cybersecurity Audit Plan Procedure)</b>	รหัสเอกสาร	NKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

ประเภทความไม่สอดคล้อง	ระยะเวลาแก้ไข	การแก้ไข ปัญหาแบบ ชั่วคราว	วิเคราะห์ สาเหตุ	แนวทางการ แก้ไข
โอกาสในการปรับปรุง (Opportunity for Improvement: OFI)	ภายใน 365 วัน	-	-	✓

#### 7. สรุปผลการตรวจสอบ (Audit Closing)


- เมื่อสิ้นสุดการตรวจสอบ ให้ทีมผู้ตรวจสอบภายในประชุมร่วมกับผู้รับการตรวจสอบ เพื่อสรุปผลการตรวจสอบทุกครั้ง
- หัวหน้าผู้ตรวจสอบควรทำการประชุมปิดการตรวจสอบโดยกล่าวสรุปถึงผลการตรวจสอบที่ได้ดำเนินการไป สิ่งที่ตรวจพบทั้งหมด โดยแยกตามประเด็นที่ตรวจพบตามที่ได้กำหนดไว้ และควรกล่าวถึงส่วนที่ดีที่สุดที่ได้ตรวจพบก่อน 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)

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของ โรงพยาบาลโนนคุณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคุณ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	<b>แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</b>  <b>(Cybersecurity Audit Plan Procedure)</b>	รหัสเอกสาร	NKH MOPH Audit Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

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

## 8.2 External Audit Finding

- กลุ่มงานหรือเจ้าหน้าที่ที่ได้รับมอบหมายเป็นผู้รายงานการดำเนินการแก้ไขและป้องกัน (Corrective and Preventive Action Report : CAR)

## 9. การตอบรับการแก้ไขและป้องกัน

### 9.1 Internal Audit Finding

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

### 9.2 External Audit Finding

- ให้ปฏิบัติตามมาตรา 54 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยดำเนินการตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ดังนี้
  - กรณี เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อ สกมช. ภายในกำหนด 30 วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา 54 พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย ทั้งนี้ รูปแบบและรายละเอียดผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปตามที่ สกมช. กำหนด

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของ โรงพยาบาลโนนคูณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคูณ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



แผนการตรวจสอบด้านการรักษาความ  
มั่นคงปลอดภัยไซเบอร์  
(Cybersecurity Audit Plan  
Procedure)

รหัสเอกสาร	NKH MOPH Audit Plan -01
แก้ไขครั้งที่	00
วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มี.ค. 2569 ใช้ภายในเท่านั้น

- ในกรณีที่ การตรวจสอบดำเนินการภายใต้มาตรา 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 ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสกมช. ภายในระยะเวลาที่ กกม. กำหนด พร้อมส่งทั้งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย
- เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การพิจารณาของ กกม.

10. การแก้ไขและการป้องกัน (Corrective and Preventive Action)

- ผู้ที่ได้รับมอบหมายให้ตรวจสอบผลการแก้ไขและป้องกัน ต้องดำเนินการตรวจสอบตามระเบียบการปฏิบัติงาน เรื่อง การแก้ไขและป้องกัน (Corrective and Preventive action Procedure)

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลโนนคูณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคูณ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

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

- ผู้ที่ได้รับมอบหมายให้ตรวจสอบฯ ต้องตรวจสอบจากข้อเท็จจริง หรือหลักฐานที่ปรากฏให้เชื่อถือได้ว่า ผู้ที่ได้รับมอบหมาย ได้ดำเนินการแล้วเสร็จอย่างมีประสิทธิภาพ

## 11. การติดตามผลการแก้ไขและป้องกัน (Corrective and Preventive Action Follow up)

### 11.1 Internal Audit Finding

- กลุ่มงานหรือเจ้าหน้าที่ที่ได้รับมอบหมายมีหน้าที่ในการติดตามสถานะการดำเนินงานการแก้ไขและป้องกัน

### 11.2 External Audit Finding 1

- กลุ่มงานหรือเจ้าหน้าที่ที่ได้รับมอบหมายมีหน้าที่ในการติดตามสถานะการดำเนินงานการแก้ไขและป้องกัน

## 12. การตรวจสอบผลการแก้ไขและป้องกัน (Verification of Corrective and Preventive Action)

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

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของ โรงพยาบาลโนนคูณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคูณ เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	<p style="text-align: center;"><b>แผนการตรวจสอบด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์</b></p> <p style="text-align: center;"><b>(Cybersecurity Audit Plan Procedure)</b></p>	รหัสเอกสาร	NKH 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 โรงพยาบาลโนนคุณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคุณ เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกประเมินโทษแจกจ่ายเอกสารที่เป็นสื่อกระดาษ