

	การจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)	รหัสเอกสาร	NKH MOPH Protect -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	23 มีนาคม 2569 ใช้ภายในเท่านั้น


การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็น			
ชื่อ-สกุล	นายอิสรภาพ เบ้าน้อย	นางพรณี วรรณธรรม	นายชนสันตชัย พรหมบุตร
ตำแหน่ง	นักวิชาการคอมพิวเตอร์	พยาบาลวิชาชีพชำนาญการพิเศษ (Lead Implementer)	นายแพทย์ชำนาญการพิเศษ รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลโนนคูณ (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 โรงพยาบาลโนนคูณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคูณ เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ครอบครองจะถูกระงับในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	การจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)	รหัสเอกสาร	NKH MOPH Protect -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มีนาคม 2569 ใช้ภายในเท่านั้น

สารบัญ

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

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของ โรงพยาบาลโนนคูณ ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากโรงพยาบาลโนนคูณ เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระงับในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	การจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)	รหัสเอกสาร	NKH MOPH Protect -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	23 มีนาคม 2569 ใช้ภายในเท่านั้น

การจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม.43), ประมวลและกรอบ [ข้อ 22.1.1, ข้อ 22.1.2, ข้อ 22.1.3, ข้อ 22.1.4]

1. วัตถุประสงค์

กระบวนการนี้จัดทำขึ้นเพื่อควบคุมและกำกับดูแลการเข้าถึงบริการที่สำคัญของหน่วยงาน สำหรับป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและเป็นการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

2. ขอบเขต

กระบวนการนี้ครอบคลุมถึงการควบคุมการเข้าถึงสำหรับบุคลากร อุปกรณ์ และอินเทอร์เน็ตเฟส รวมถึงการตรวจสอบและจัดเก็บบันทึกการเข้าถึงบริการที่สำคัญของหน่วยงาน เพื่อให้แน่ใจว่าการเข้าถึงเหล่านี้เป็นไปตามข้อกำหนดที่กำหนดไว้

3. คำจำกัดความ/นิยามศัพท์เฉพาะ

ลำดับ	คำศัพท์	คำจำกัดความ
1	เจ้าหน้าที่ของหน่วยงาน	เจ้าหน้าที่ของหน่วยงานต่าง ๆ ของ โรงพยาบาลโนนคุณ
2	ผู้ดูแลระบบ	เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลระบบสารสนเทศ หรือ ระบบคอมพิวเตอร์และเครือข่าย
3	ISM	หัวหน้าคณะทำงานระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

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

	การจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)	รหัสเอกสาร	NKH MOPH Protect -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มีนาคม 2569 ใช้ภายในเท่านั้น

4. หน้าที่และความรับผิดชอบ

ลำดับ	ผู้รับผิดชอบ	ความรับผิดชอบ
1	Top Management / ISM	รับผิดชอบในการกำกับดูแลการดำเนินการตามกระบวนการควบคุมการเข้าถึง และตรวจสอบให้แน่ใจว่ามีการปฏิบัติตามข้อกำหนดอย่างครบถ้วน
2	ผู้ดูแลระบบ	รับผิดชอบในการกำหนดและจัดการสิทธิ์การเข้าถึง รวมถึงการตรวจสอบบันทึกการเข้าถึงอย่างสม่ำเสมอ
3	เจ้าหน้าที่ของหน่วยงาน	มีหน้าที่ปฏิบัติตามนโยบายและข้อกำหนดที่เกี่ยวข้องกับการเข้าถึงบริการที่สำคัญของหน่วยงาน

5. ขั้นตอนปฏิบัติ

5.1 การจำกัดการเข้าถึง (Access Restrictions)


1) การจำกัดการเข้าถึงบริการที่สำคัญ

ขั้นตอน: ตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญถูกจำกัดเฉพาะบุคลากรที่ได้รับอนุญาต (กิจกรรมที่ได้รับอนุญาต อุปกรณ์ และอินเทอร์เน็ตที่ได้รับอนุญาตเท่านั้น) โดยการกำหนดสิทธิ์การเข้าถึงระบบให้กับผู้ดูแลระบบและบุคลากรที่มีหน้าที่เกี่ยวข้องโดยตรงเท่านั้น

2) การใช้เทคนิคการตรวจสอบสิทธิ์

ขั้นตอน: กำหนดให้บุคลากรและกิจกรรมที่ได้รับอนุญาตใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สำหรับแต่ละโหมดการเข้าถึง โดยการใช้การยืนยันตัวตนสองปัจจัย (Two-Factor Authentication) สำหรับการเข้าถึงระบบที่มีข้อมูลสำคัญ

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

	การจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)	รหัสเอกสาร	NKH MOPH Protect -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	23 มีนาคม 2569 ใช้ภายในเท่านั้น

5.2 การบันทึกและตรวจสอบการเข้าถึง (Access Logging and Monitoring)

1) การเก็บรักษาบันทึกการเข้าถึง

ขั้นตอน: เก็บรักษาบันทึกของการเข้าถึงทั้งหมดและความพยายามในการเข้าถึงบริการที่สำคัญ รวมถึงตรวจสอบบันทึกเหล่านี้เป็นประจำเพื่อหากิจกรรมที่ผิดปกติ โดยการจัดทำระบบบันทึกการเข้าถึง เซิร์ฟเวอร์และตรวจสอบบันทึกเหล่านี้รายสัปดาห์เพื่อหากิจกรรมที่น่าสงสัย

2) ความสม่ำเสมอในการตรวจสอบบันทึก

ขั้นตอน: กำหนดความสม่ำเสมอในการตรวจสอบบันทึกการเข้าถึงตามความถี่ของกิจกรรมการเข้าถึงและระดับความเสี่ยงที่เกี่ยวข้อง โดยการตรวจสอบบันทึกการเข้าถึงของระบบเครือข่าย ภายในทุกวัน และการตรวจสอบบันทึกการเข้าถึงข้อมูลสำคัญอย่างน้อยรายสัปดาห์

5.3 การควบคุมการเข้าถึงอินเทอร์เน็ตเฟสและการเข้าถึงทางลอจิกคอล (Interface and Logical Access Control)

1) การควบคุมการเข้าถึงอินเทอร์เน็ตเฟส

ขั้นตอน: ตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เน็ตเฟส เช่น USB และพอร์ตอนุกรม ต้องถูกควบคุมและดำเนินการภายใต้การดูแลของหน่วยงานที่เกี่ยวข้องเท่านั้น โดยได้รับการตั้งค่าข้อจำกัดในการใช้งานพอร์ต USB บนอุปกรณ์คอมพิวเตอร์ที่ใช้ในหน่วยงาน

2) การเข้าถึงทางลอจิกคอล

ขั้นตอน: กำกับดูแลการเข้าถึงทางลอจิกคอลของบริการที่สำคัญ โดยให้ดำเนินการในสถานที่ที่ได้รับอนุญาตและอยู่ภายใต้การควบคุมของหน่วยงาน โดยการกำหนดให้การเข้าถึงระบบจัดการ ข้อมูลต้องทำจากภายในหน่วยงานเท่านั้น และห้ามเข้าถึงจากภายนอกหน่วยงาน

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

	การจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)	รหัสเอกสาร	NKH MOPH Protect -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	23 มีนาคม 2569 ใช้ภายในเท่านั้น

5.4 การควบคุมกำกับดูแลให้มีการลงนามในเอกสารข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

ขั้นตอน: ในกรณีที่ผู้ให้บริการภายนอกมีการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของหน่วยงาน หน่วยงานจะต้องดำเนินการให้ผู้ให้บริการภายนอกลงนามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) และต้องปฏิบัติตามนโยบายกฎระเบียบ ขั้นตอนการปฏิบัติงาน และวิธีปฏิบัติงานของหน่วยงานอย่างเคร่งครัด

5.5 การควบคุมกำกับดูแลผู้ให้บริการภายนอกที่ต้องการใช้ระบบเทคโนโลยีสารสนเทศของหน่วยงาน

ขั้นตอน: 1. ในกรณีที่ผู้ให้บริการภายนอกต้องการใช้ระบบเทคโนโลยีสารสนเทศของหน่วยงานผู้ให้บริการภายนอกต้องดำเนินการขออนุมัติจาก Top Management / ISM

2. ผู้ดูแลระบบ ดำเนินการกำหนดระยะเวลาของสิทธิ์ในการใช้งาน/เข้าใช้งาน ทำการบันทึกสิทธิ์ในการเข้าถึงระบบต่าง ๆ และตรวจสอบการใช้งานของผู้ให้บริการภายนอก

3. ผู้ดูแลระบบ ดำเนินการเพิกถอนสิทธิ์ในการใช้ระบบต่าง ๆ ของผู้ให้บริการภายนอก เมื่อหมดความจำเป็นตามวัตถุประสงค์ที่ได้ขออนุมัติไว้

6. การทบทวนกระบวนการดำเนินการ

กระบวนการดำเนินการนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

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

	การจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)	รหัสเอกสาร	NKH MOPH
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	23 มีนาคม 2569 ใช้ภายในเท่านั้น

7. เอกสารที่เกี่ยวข้อง

ลำดับ	หมายเลขเอกสาร	ชื่อเอกสาร
1		

8. เอกสารอ้างอิง

ลำดับ	ชื่อเอกสาร
1	ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวล แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 - กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect) - การควบคุมการเข้าถึง (Access Control)
2	หลักฐาน Logs of Access
3	หลักฐานสิทธิ์การเข้าถึงระบบ (User Permission Matrix)
4	หลักฐานการจัดการตัวตน (Identity Users)

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

หลักฐานจริง

9. Log Management

ปัจจุบันโรงพยาบาลน้ำโนนคุณมีระบบจัดเก็บ Log อินเทอร์เน็ต และคอมพิวเตอร์ ตาม พ.ร.บ. คอมฯ อย่างน้อย 90 วัน จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ดำเนินการด้วย Log Setting from Fortigate firewall และส่งข้อมูลไปจัดเก็บแบ่งเป็นประเภทได้ดังนี้

1. Traffic Log คือ การบันทึกข้อมูลจราจร จากพฤติกรรมการใช้งาน

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
Minute ago	192.168.1.100	DESKTOP-VKAOFGO	52.230.59.222 (licensing.mp.microsoft.com)	Microsoft Portal	✓ 3.59 KB / 13.03 KB	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	NKHOS-AR02	15.206.217.8 (aruba.brightcloud.com)	SSL	Deny: policy violation	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	NKHOS-AR02	13.234.171.199 (aruba.brightcloud.com)	SSL	Deny: policy violation	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	DESKTOP-H9F2UBP	142.250.204.163 (bmscons.gpx.v2.com)	QUIC	✓ 6.65 KB / 8.38 KB	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	ITSAND	8.8.8.8 (dns.google)	DNS	✓ 128 B / 213 B	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	ROXOPD	15.235.230.206	AnyDesk	✓ 52.97 KB / 65.45 KB	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	OPPO-A15	142.250.4.94 (www.gstatic.com)	Google.Services	Deny: policy violation	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	realme-C35	142.250.4.95	Google.Services	Deny: policy violation	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	OPPO-A15	203.113.111.98 (whoami.akamai.net)	DNS	✓ 60 B / 156 B	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	NKHOS-AR02	203.113.111.98 (whoami.akamai.net)	DNS	✓ 67 B / 136 B	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	Samsung	203.113.111.98 (whoami.akamai.net)	DNS	✓ 74 B / 194 B	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	Aruba207-2	13.234.171.199 (aruba.brightcloud.com)	SSL	Deny: policy violation	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	9a4c3bf9-28.05	203.113.111.11	DNS	✓ 152 B / 0 B	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	9a4c3bf9-28.05	203.113.111.11	DNS	✓ 136 B / 0 B	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	NKHOS-AR02	35.154.21.213 (aruba.brightcloud.com)	SSL	Deny: policy violation	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	Driver	149.154.175.4	Telegram	Deny: policy violation	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	NKHOS-AR02	15.206.217.8 (aruba.brightcloud.com)	SSL	Deny: policy violation	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	realme-C35	74.125.130.95	Google.Services	Deny: policy violation	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	LR	147.92.249.105 (legy-jp-line-apps.com)	SSL_TLSv1.3	Deny: policy violation	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	Driver	172.217.194.139 (docs.google.com)	HTTPS BROWSER	Deny: policy violation	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	DESKTOP-VKAOFGO	52.230.59.222 (licensing.mp.microsoft.com)	Microsoft Portal	✓ 3.55 KB / 13.09 KB	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	Aruba207-2	15.206.217.8 (aruba.brightcloud.com)	SSL	Deny: policy violation	BlockBittorrent_Intf_x1_Int_Ext (10)
Minute ago	192.168.1.100	LR	192.168.112.5	MySQL	✓ 43.55 KB / 40.58 KB	Internal to Internal (11)
Minute ago	192.168.1.100	OPPO-A15	142.251.12.104 (www.google.com)	SSL_TLSv1.3	Deny: policy violation	BlockBittorrent_Intf_x1_Int_Ext (10)

2.Event Log คือ ล็อกไฟล์สำหรับการตั้งค่าเกี่ยวกับความปลอดภัย และการตั้งค่าบัญชีผู้ใช้

The screenshot shows a network device's Event Log interface. The left sidebar contains a navigation menu with categories like 'Dashboard', 'Network', 'Security Profiles', 'VPN', 'User & Authentication', 'WiFi Switch Controller', 'System', 'Security Fabric', and 'Log & Report'. The 'Log & Report' section is expanded, showing various log types such as 'Forward Traffic', 'Local Traffic', 'Sniffer Traffic', 'ZTNA Traffic', 'Events', 'AntiVirus', 'Web Filter', 'SSL', 'DNS Query', 'File Filter', 'Web Application Firewall', 'Application Control', 'Intrusion Prevention', 'Anomaly', and 'FortiGate Cloud'. The main area displays a table of system events.

Date/Time	Level	User	Message	Log Description
34 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
35 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
35 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
36 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
37 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
37 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
37 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
38 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
39 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
39 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
40 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
41 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
41 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
41 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
42 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
43 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
51 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
52 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
53 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
53 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
54 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
54 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
55 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log
55 seconds ago	Info		DHCP server sends a DHCPACK	DHCP Ack log

3. LogAntiVirus Log คือ ผลประวัติ รายงาน การป้องกัน การตรวจจับ

The screenshot shows a network device's LogAntiVirus Log interface. The top bar indicates the date range from 2026/01/07 08:40:21 to 2026/02/01 08:40:21. The table lists various blocked items with their details and actions.

Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action
2026/02/01 00:53:40	HTTP	185.34.144.177	upload.exe	EICAR_TEST_FILE		URL: http://www.baidu.com/upload.exe	blocked
2026/01/28 17:06:01	HTTP	192.168.9.18	datalogger2.php	JS/Redirect.AQR!tr		URL: http://159.192.104.60/lot/datalogger2.php	blocked
2026/01/28 17:05:25	HTTP	192.168.9.14	datalogger2.php	JS/Redirect.AQR!tr		URL: http://159.192.104.60/lot/datalogger2.php	blocked
2026/01/28 17:05:05	HTTP	192.168.9.13	datalogger2.php	JS/Redirect.AQR!tr		URL: http://159.192.104.60/lot/datalogger2.php	blocked
2026/01/28 02:22:40	HTTP	185.34.144.177	upload.exe	EICAR_TEST_FILE		URL: http://www.google.com/upload.exe	blocked
2026/01/28 02:22:40	HTTP	185.34.144.177	upload.exe	EICAR_TEST_FILE		URL: http://www.google.com/upload.exe	blocked
2026/01/27 15:16:48	HTTP	192.168.14.2	1653359	JS/Redirector.PIY!tr		URL: http://ww38.tamping.net/go/1653359	blocked
2026/01/27 15:16:45	HTTP	192.168.14.2	1653359	JS/Redirector.PIY!tr		URL: http://ww38.tamping.net/go/1653359	blocked
2026/01/27 15:15:24	HTTP	192.168.14.2	1653359	JS/Redirector.PIY!tr		URL: http://ww38.tamping.net/go/1653359	blocked
2026/01/19 04:06:06	HTTP	206.168.191.185	upload.php	EICAR_TEST_FILE		URL: http://www.microsoft.com/upload.php	blocked
2026/01/19 01:18:34	HTTP	206.168.191.185	upload.php	EICAR_TEST_FILE		URL: http://www.microsoft.com/upload.php	blocked
2026/01/19 01:13:49	HTTP	206.168.191.185	upload.php	EICAR_TEST_FILE		URL: http://www.microsoft.com/upload.php	blocked
2026/01/18 02:19:34	HTTP	206.168.191.185	upload.php	EICAR_TEST_FILE		URL: http://www.microsoft.com/upload.php	blocked
2026/01/17 20:20:10	HTTP	206.168.191.185	upload.php	EICAR_TEST_FILE		URL: http://www.microsoft.com/upload.php	blocked

4. Web Filter Log คือ ข้อมูลการบล็อก และจำกัดสิทธิการเข้าถึงเว็บไซต์ที่ไม่ปลอดภัย

Date/Time	User	Source	Action	URL	Category Description	Initiator	Sent / Received
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	http://ocps.comedoca.com/MFAwTjBMMEowSDAHBglrDgMCgqQUfyX...			371 B / 0 B
18 minutes ago	h10938	h10938 (192.168.6.72)	passthrough	https://mask-app.icloud.com/	Proxy Avoidance		517 B / 0 B
18 minutes ago	h10938	h10938 (192.168.6.72)	passthrough	https://mask-app.icloud.com/	Proxy Avoidance		517 B / 0 B
18 minutes ago	h10938	h10938 (192.168.6.72)	passthrough	https://mask-app.icloud.com/	Proxy Avoidance		517 B / 0 B
18 minutes ago	h10938	h10938 (192.168.6.72)	passthrough	https://mask-app.icloud.com/	Proxy Avoidance		517 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://ontolog.health.apple.com/			518 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://acsegateway.icloud.com/			518 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://i4.apple.com/			518 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://acsegateway.icloud.com/			518 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://updates.cdn-apple.com/			517 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://api-gb-aapoc1.csmoot.apple.com/			517 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://ocsegateway.icloud.com/			518 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://api-gb-aapoc1.csmoot.apple.com/			517 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://ontolog.health.apple.com/			518 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://updates.cdn-apple.com/			517 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://acsegateway.icloud.com/			518 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://api-gb-aapoc1.csmoot.apple.com/			517 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://ontolog.health.apple.com/			518 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://updates.cdn-apple.com/			517 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://acsegateway.icloud.com/			518 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://api-gb-aapoc1.csmoot.apple.com/			517 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://ontolog.health.apple.com/			518 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://updates.cdn-apple.com/			517 B / 0 B
19 minutes ago	h10938	h10938 (192.168.6.72)	blocked	https://acsegateway.icloud.com/			518 B / 0 B

5. IPS Log คือ ข้อมูลตรวจสอบการบุกรุก การโจมตีกลับหรือหยุดยั้งผู้บุกรุก

Date/Time	Severity	Source	User	Action	Count	Attack Name
31 seconds ago	High	204.76.203.219		detected		Mirai.Botnet
32 seconds ago	High	204.76.203.211		detected		Mirai.Botnet
Minute ago	High	204.76.203.211		detected		Mirai.Botnet
Minute ago	High	204.76.203.219		detected		Mirai.Botnet
Minute ago	High	204.76.203.211		detected		Mirai.Botnet
2 minutes ago	High	204.76.203.219		detected		Mirai.Botnet
2 minutes ago	High	204.76.203.211		detected		Mirai.Botnet
2 minutes ago	High	204.76.203.219		detected		Mirai.Botnet
3 minutes ago	High	204.76.203.211		detected		Mirai.Botnet
3 minutes ago	High	204.76.203.219		detected		Mirai.Botnet
3 minutes ago	High	204.76.203.211		detected		Mirai.Botnet
4 minutes ago	High	204.76.203.219		detected		Mirai.Botnet
4 minutes ago	High	204.76.203.211		detected		Mirai.Botnet
5 minutes ago	High	204.76.203.219		detected		Mirai.Botnet
5 minutes ago	High	204.76.203.211		detected		Mirai.Botnet
5 minutes ago	High	204.76.203.211		detected		Mirai.Botnet
5 minutes ago	High	204.76.203.219		detected		Mirai.Botnet
6 minutes ago	High	204.76.203.211		detected	6	Mirai.Botnet
6 minutes ago	High	204.76.203.219		detected	6	Mirai.Botnet
6 minutes ago	High	204.76.203.211		detected	6	Mirai.Botnet
6 minutes ago	High	95.214.52.169		detected	6	Yifan.VF325.https.debug.credentials.Authentication.Bypass
6 minutes ago	High	204.76.203.211		detected	6	Mirai.Botnet
7 minutes ago	High	204.76.203.219		detected	6	Mirai.Botnet
7 minutes ago	High	204.76.203.211		detected	6	Mirai.Botnet
7 minutes ago	High	204.76.203.211		detected	6	Mirai.Botnet

6. Application Control Log คือ ข้อมูลการใช้งาน Application

Date/Time	Source	Destination	Application Name	Action	Application User	Application Details
13 seconds ago	192.168.9.113	104.21.96.1 (cittanatra.com)	HTTPS.BROWSER	pass		
13 seconds ago	192.168.9.113	104.21.96.1 (cittanatra.com)	SSL	pass		
13 seconds ago	h10938 (192.168.7.12)	163.70.148.35 (star-mini.c10r.facebook.com)	Facebook	pass		
13 seconds ago	h10938 (192.168.7.12)	163.70.148.35 (star-mini.c10r.facebook.com)	SSL	pass		
13 seconds ago	192.168.200.22	103.21.25.187 (prod-streaming-video-msn-com.akamaized.net)	HTTP.BROWSER	pass		
14 seconds ago	h10938 (192.168.7.12)	23.11.200.17 (acrobot.adobe.com)	Microsoft.Portals	pass		
14 seconds ago	h10938 (192.168.7.12)	23.11.200.17 (acrobot.adobe.com)	SSL	pass		
15 seconds ago	192.168.7.64	142.251.10.94 (clientservices.googleapis.com)	Google.Services	pass		
15 seconds ago	192.168.6.232	147.92.165.194 (cxl.line-apps.com)	SSL_TLSv1.3	pass		TLSv1.3
15 seconds ago	192.168.6.232	147.92.165.194 (cxl.line-apps.com)	SSL	pass		
13 seconds ago	192.168.200.243	23.11.200.147 (mon-boot.tiktokv.com)	Microsoft.Portals	pass		
13 seconds ago	192.168.200.243	23.11.200.147 (mon-boot.tiktokv.com)	SSL	pass		
14 seconds ago	192.168.200.243	13.69.239.74 (v10.events.data.microsoft.com)	SSL_TLSv1.3	pass		TLSv1.3
14 seconds ago	192.168.200.243	13.69.239.74 (v10.events.data.microsoft.com)	SSL	pass		
15 seconds ago	192.168.9.135	203.147.59.16 (time.navy.mi.th)	NTP	pass		
15 seconds ago	192.168.7.46	35.154.21.213 (aruba.brightcloud.com)	SSL	pass		
15 seconds ago	192.168.7.46	13.234.171.199 (aruba.brightcloud.com)	SSL	pass		
13 seconds ago	192.168.7.64	172.217.194.101 (suggestqueries-clients.youtube.com)	HTTPS.BROWSER	pass		
13 seconds ago	192.168.7.64	172.217.194.101 (suggestqueries-clients.youtube.com)	SSL	pass		
14 seconds ago	192.168.7.46	13.234.171.199 (aruba.brightcloud.com)	SSL	pass		
14 seconds ago	192.168.7.46	74.125.68.94 (ssl.gstatic.com)	SSL_TLSv1.3	pass		TLSv1.3

7. WAF Log คือ ข้อมูลการใช้งานการป้องกัน Web application

Date/Time	Source	Destination	Application Name	Action	Application User	Application Details
14 seconds ago	192.168.200.137	172.217.194.95	Services	pass		
14 seconds ago	192.168.4.111	147.92.165.67 (legyline-apps.com)	Line	pass		
14 seconds ago	h10938 (192.168.200.41)	17.253.61.204	Services	pass		
14 seconds ago	192.168.201.151	203.153.50.58 (conn-service-us-04.allavmos.cc)	BROWSER	pass		
15 seconds ago	192.168.7.46	13.234.171.199 (aruba.brightcloud.com)		pass		
15 seconds ago	h10938 (192.168.6.182)	163.70.148.13 (api.facebook.com)	ok	pass		
15 seconds ago	192.168.7.46	35.154.21.213 (aruba.brightcloud.com)		pass		
15 seconds ago	192.168.200.151	35.154.21.213 (aruba.brightcloud.com)	SSL	pass		
15 seconds ago	192.168.7.46	13.234.171.199 (aruba.brightcloud.com)	SSL	pass		
15 seconds ago	192.168.200.243	23.11.200.17 (acrobot.adobe.com)	Microsoft.Portals	pass		
15 seconds ago	192.168.200.243	23.11.200.17 (acrobot.adobe.com)	SSL	pass		
15 seconds ago	h10938 (192.168.200.41)	17.253.60.253 (time.gaplimg.com)	NTP	pass		
15 seconds ago	192.168.7.46	15.206.217.8 (aruba.brightcloud.com)	SSL	pass		
15 seconds ago	192.168.7.46	162.159.61.4 (mozilla.cloudflare-dns.com)	DNS.OverHTTPS	pass		
15 seconds ago	192.168.7.46	35.154.21.213 (aruba.brightcloud.com)	SSL	pass		
15 seconds ago	192.168.7.46	13.234.171.199 (aruba.brightcloud.com)	SSL	pass		
15 seconds ago	192.168.7.46	142.251.10.95	Google.Services	pass		
15 seconds ago	h10938 (192.168.200.41)	17.253.64.251 (time.apple.com)	NTP	pass		
15 seconds ago	192.168.7.46	91.108.56.129	Telegram	pass		
15 seconds ago	192.168.7.46	91.108.56.129	Telegram	pass		
15 seconds ago	192.168.9.135	203.147.59.16 (time.navy.mi.th)	NTP	pass		
15 seconds ago	192.168.200.151	13.234.171.199 (aruba.brightcloud.com)	SSL	pass		
15 seconds ago	192.168.7.46	15.206.217.8 (aruba.brightcloud.com)	SSL	pass		

8. DNS Query Log คือ ข้อมูลการค้นหาโดเมน

9. SSL Log คือ ข้อมูลใบรับรองดิจิทัลที่รับรองความถูกต้องของข้อมูลเว็บไซต์ และเปิดใช้งานการเชื่อมต่อที่เข้ารหัส SSL