ที่ เอ็นที บภน.3.1(บร.)/553

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
ส่วนขายและบริการลูกค้าบุรีรัมย์
เลขที่ 55 ถนนรมย์บุรี ตำบลในเมือง
อำเภอเมือง จังหวัดบุรีรัมย์ 31000

18 ตุลาคม 2567

เรื่อง รับรองการสำรวจระบบสารสนเทศโรงพยาบาลบ้านด่าน

เรียน ผู้อำนวยการโรงพยาบาลบ้านด่าน

อ้างถึง แบบฟอร์มการสำรวจระบบสารสนเทศ Check List

สิ่งที่ส่งมาด้วย 1. เอกสารรางวัล/ใบประกาศ จำนวน 2 แผ่น

บริษัท โทรคมนาคมแห่งชาติ จำกัด) มหาชน (หรือ บมจ .โทรคมนาคมแห่งชาติ เป็นรัฐวิสาหกิจภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) โดยมีกระทรวงการคลังถือหุ้น 100 เปอร์เซ็นต์ บมจ . โทรคมนาคมแห่งชาติ เป็นผู้นำด้านการให้บริการสื่อสารและโทรคมนาคม ซึ่งให้บริการสื่อสารทุกประเภทรวมทั้งบริการเสริมอื่นๆ ทั้งในประเทศและทั่วโลก บมจ .โทรคมนาคมแห่งชาติ เป็นผู้ให้บริการหลักทางด้านโทรศัพท์ระหว่างประเทศรายใหญ่ที่สุดในประเทศไทย และมีเครือข่ายสื่อสารข้อมูลที่เชื่อมโยงไปทั่วโลก ปัจจุบัน บมจ . โทรคมนาคมแห่งชาติ ให้บริการสื่อสารข้อมูล อินเทอร์เน็ต ดาวเทียม โทรศัพท์เคลื่อนที่ และบริการด้าน Cybersecurity

บมจ.โทรคมนาคมแห่งชาติ ได้รับรางวัล “ **2016 และ 2017 Thailand Managed Security Service Provider of the Year** ”จากงาน Frost & Sullivan Thailand Excellence Awards โดย ฟรอสต์ แอนด์ ซัลลิเวน องค์กรให้คำปรึกษาและวิจัยระดับโลก ของผู้ให้บริการ Managed Security Service Provider (MSSP) ผ่านศูนย์ Security Operation Center (SOC) ที่ได้รับมาตรฐาน **ISO 27001** แห่งแรก ในประเทศไทย ที่การันตีการเป็นผู้ให้บริการ MSSP ในเวทีระดับโลกด้านการให้บริการบริหารจัดการและเฝ้าระวังภัยคุกคามระบบสารสนเทศตลอด 24 x 7

ทั้งนี้ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) โดย ส่วนขายและบริการลูกค้าบุรีรัมย์ ได้ดำเนินการจัดทำแบบสำรวจระบบสารสนเทศ เพื่อยกระดับและประเมินความมั่นคงปลอดภัยในการถูกภัยคุกคามตามนโยบายของกระทรวงฯ มีวัตถุประสงค์ เพื่อสำรวจระบบสารสนเทศภายในหน่วยงานของท่าน มีระบบการป้องกันดูแลรักษาข้อมูล และแผนงานป้องกันความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์หรือไม่

จึงขอรายงานผลการสำรวจระบบสารสนเทศ ซึ่งดำเนินการสำรวจร่วมกับเจ้าหน้าที่ของ **โรงพยาบาลบ้านด่าน** รายละเอียด ดังนี้

เกณฑ์การประเมินความมั่นคงปลอดภัย	ดำเนินการแล้ว	ยังไม่ได้ดำเนินการ	หมายเหตุ
1. หัวข้อความมั่นคงปลอดภัยสูง			
1.1 Backup การสำรองข้อมูลเก็บไว้ที่อื่น	✓		-
1.2 Antivirus Softwareโปรแกรมป้องกันไวรัส	✓		-
1.3 Access Control (Public และ Private) การควบคุมอุปกรณ์หรือการเข้าถึงระบบผ่านทางช่องทาง Public/Private	✓		-
1.4 Privileged Access Management (PAM) โซลูชันการรักษาความปลอดภัยของข้อมูล	✓		-
2. หัวข้อความมั่นคงปลอดภัยปานกลาง			
2.1 Business Continuity Plan (BCP) แผนที่กำหนดแนวทางการดำเนินการของหน่วยงาน	✓		-
2.2 Disaster Recovery site (DR) ศูนย์สำรองข้อมูล			
2.3 OS Patching การซ่อมแซมจุดบกพร่องของระบบปฏิบัติการ	✓		-
2.4 Multi-Factor Authentication (2FA)การยืนยันตัวตน 2 ชั้น	✓		-
2.5 Web Application Firewall (WAF) ระบบป้องกันการโจมตีทางไซเบอร์สำหรับเว็บแอพพลิเคชั่น	✓		-
2.6 Log Management การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์	✓		-
2.7 Security Information & Event Management (SIEM) ระบบที่ใช้ในการจัดการกับ Log และ Event ต่างๆ	✓		-
2.8 Vulnerability Assessment (VA Scan) การตรวจสอบช่องโหว่ของระบบ	✓		-
3. หัวข้อประเมินความมั่นคงปลอดภัยต่ำ			
3.1 Software Update	✓		-
3.2 Penetration Testing การทดสอบการเจาะระบบ	✓		-

ทั้งนี้ **การประเมินตามเกณฑ์ความมั่นคงปลอดภัย** CYBER SECURITY ของระบบสารสนเทศสำหรับ โรงพยาบาลบ้านด่าน ได้มีระบบการป้องกันตามเกณฑ์คุณลักษณะระบบสารสนเทศ ทั้ง 3 ระดับ คือ

1. เกณฑ์ความมั่นคงปลอดภัยสูง
2. เกณฑ์ความมั่นคงปลอดภัยปานกลาง
3. เกณฑ์ความมั่นคงปลอดภัยต่ำ

โดย ผลการประเมิน ได้ดำเนินการร่วมกับเจ้าหน้าที่ **โรงพยาบาลบ้านด่าน** เรียบร้อยแล้ว จากรายละเอียดแบบสำรวจและการประเมินตามเกณฑ์ความมั่นคงปลอดภัย CYBER SECURITY ของระบบสารสนเทศข้างต้น **ผลการประเมิน เป็น เกณฑ์ความมั่นคงปลอดภัยสูง**

จึงเรียนมาเพื่อโปรดทราบ และพิจารณาในส่วนที่เกี่ยวข้อง

ขอแสดงความนับถือ

(นายพูนโชค วิชชุเวทิน)
ผู้ช่วยโทรคมนาคมจังหวัดบุรีรัมย์
รักษาการแทน โทรคมนาคมจังหวัดบุรีรัมย์

ส่วนขายและบริการลูกค้าบุรีรัมย์ (สุภาวดีฯ)
โทรศัพท์ 08 1238 0131

ผลการประเมินตามเกณฑ์ CO-CERT ของโรงพยาบาล/หน่วยงาน

รพ.บ้านด่าน เขตสุขภาพที่ 9 จังหวัด บุรีรัมย์

ผู้ให้ข้อมูล : น.ส.ดวงจันทร์ ชะงักรัมย์ ตำแหน่ง : นักวิชาการคอมพิวเตอร์ปฏิบัติการ

ลำดับ	เกณฑ์การประเมินความมั่นคงปลอดภัย	มีการใช้งาน	ไม่มีการใช้งาน	หมายเหตุ
1	**หัวข้อความมั่นคงปลอดภัยสูง**			
1.1	Backup การสำรองข้อมูลเก็บไว้ที่อื่น	✓		มีการสำรองข้อมูล เป็นไปตามเกณฑ์การประเมิน
1.2	Antivirus Softwareโปรแกรมป้องกันไวรัส	✓		ใช้งาน EDR เป็นไปตามเกณฑ์การประเมิน
1.3	Access Control (Public และ Private) การควบคุมอุปกรณ์หรือการเข้าถึงระบบ ผ่านทางช่องทาง Public/Private	✓		มีการทำ Access Control (Public และ Private) เป็นไปตามเกณฑ์การประเมิน
1.4	Privileged Access Management (PAM) โซลูชันการรักษาความปลอดภัยของข้อมูล	✓		มีการ จัดการสิทธิ เป็นไปตามเกณฑ์การประเมิน
2	**หัวข้อความมั่นคงปลอดภัยปานกลาง**			
2.1	Business Continuity Plan (BCP) แผนที่กำหนดแนวทางการดำเนินการของหน่วยงาน	✓		มีแผนหรือแนวทางการดำเนินการของหน่วยงานเมื่อเกิดสภาวะวิกฤตหรือภัยต่าง ๆ เป็นไปตามเกณฑ์การประเมิน
2.2	Disaster Recovery site (DR) ศูนย์สำรองข้อมูล			
2.3	OS Patching การซ่อมแซมจุดบกพร่องของระบบปฏิบัติการ	✓		OS Linux ALma update patch เป็นไปตามเกณฑ์การประเมิน
2.4	Multi-Factor Authentication (2FA)การยืนยันตัวตน 2 ชั้น	✓		มีการยืนยันตัวตน 2 ชั้น เป็นไปตามเกณฑ์การประเมิน
2.5	Web Application Firewall (WAF) ระบบป้องกันการโจมตีทางไซเบอร์สำหรับเว็บแอพพลิเคชั่น	✓		มีการใช้บริการ WAF ของ NT ป้องกันการโจมตีทางไซเบอร์สำหรับเว็บแอพพลิเคชั่น เป็นไปตามเกณฑ์การประเมิน
2.6	Log Management การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์	✓		ใช้บริการ CSM ของ NT มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ เป็นไปตามเกณฑ์การ
2.7	Security Information & Event Management (SIEM) ระบบที่ใช้ในการจัดการกับ Log และ Event ต่างๆ	✓		ใช้บริการ CSM ของ NT ในการจัดการกับ Log และ Event เป็นไปตามเกณฑ์การประเมิน
2.8	Vulnerability Assessment (VA Scan) การตรวจสอบช่องโหว่ของระบบ	✓		ใช้บริการ VA Scan ของ NT มีรายงานเพื่อปิดช่องโหว่
3	**หัวข้อความมั่นคงปลอดภัยต่ำ**			
3.1	Software Update	✓		HOSxp 3.67.8.28 Software Update เป็นไปเกณฑ์การประเมิน
3.2	Penetration Testing การทดสอบการเจาะระบบ	✓		ใช้บริการ Pentest ของ NT มีสรุปผลการทดสอบ

ผู้ให้ข้อมูล
น.ส.ดวงจันทร์ ชะงักรัมย์ ตำแหน่ง : นักวิชาการคอมพิวเตอร์ปฏิบัติการ

TÜV NORD

CERTIFICATE

Management system as per

ISO/IEC 27001 : 2013

(Including Cor 1:2014 and Cor 2:2015)

The Certification Body TÜV NORD CERT GmbH hereby confirms as a result of the audit, assessment and certification decision according to ISO/IEC 17021-1:2015, that the organization

National Telecom Public Company Limited
Security Operation Center (SOC)
53/58 Moo 8, Tiwanon Rd., Bang Krasor, Mueang,
Nonthaburi 11000,
Thailand

nt National Telecom

with the locations according to the annex

operates a management system in accordance with the requirements of ISO/IEC 27001 : 2013 and will be assessed for conformity within the 3 year term of validity of the certificate.

Scope

Provision for the management, operation and maintenance of Security Operation Center providing Cyber Security Monitoring and Secure Log Management including the infrastructure required to supporting the provision of stated services

As per the Statement of Applicability, V.7.5, Date 17.05.2021

Certificate Registration No. 44 121 091547
Audit Report No. 3530 1891

Valid from 2021-11-04
Valid until 2024-11-03
Initial certification 2009

Certification Body
at TÜV NORD CERT GmbH

Essen, 2021-12-08

Validity can be verified at https://www.tuev-nord.de/de/unternehmen/zertifizierung/zertifikatsdatenbank.

TÜV NORD CERT GmbH Am TÜV 1 45307 Essen www.tuev-nord-cert.com

IAF

DAkkS Deutsche Akkreditierungsstelle D-ZM-12007-01-00

FROST & SULLIVAN
2017
BEST
PRACTICES
AWARD
THAILAND
MANAGED SECURITY
SERVICE PROVIDER OF THE YEAR

FROST & SULLIVAN
2016
BEST
PRACTICES
AWARD
THAILAND
MANAGED SECURITY SERVICE
PROVIDER OF THE YEAR