แบบ บก.๐๖

# ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

๑. ชื่อโครงการ จ้างบำรุงรักษาระบบ Cyber Security จำนวน ๑ ระบบ

๒. (หน่วยงานเจ้าของโครงการ) โรงพยาบาลมหาราชนครศรีธรรมราช

๓. วงเงินงบประมาณที่ได้รับจัดสรร ๑,๐๐๐,๐๐๐.๐๐ บาท (หนึ่งล้านบาทถ้วน)

๔. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ ๒๔ เมษายน ๒๕๖๘
เป็นเงิน ๙๙๙,๕๙๔.๐๐ บาท (เก้าแสนเก้าหมื่นเก้าพันห้าร้อยเก้าสิบสี่บาทถ้วน)

๕. แหล่งที่มาของราคากลาง (ราคาอ้างอิง) สืบราคาจากท้องตลาด

๕.๑ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

๕.๒ บริษัท เน็ตสเปซ ไอที จำกัด

๕.๓ บริษัท รูธ วิคเตอร์ (ประเทศไทย) จำกัด

๖. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

๖.๑ นายอนุวัตร์ รินทร์วิฑูรย์ นายแพทย์ชำนาญการพิเศษ

๖.๒ นายสุริยา กองสุก นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๖.๓ นางสาวพลอยกนก จุลนวล นักวิชาการคอมพิวเตอร์ปฏิบัติการ

**ร่างขอบเขตของงาน (Terms of Reference : TOR )**
**จ้างบำรุงรักษาระบบ Cyber Security จำนวน ๑ ระบบ**
**โรงพยาบาลมหาราชนครศรีธรรมราช**

.....

**๑. ความเป็นมา**

แผนเงินนอกงบประมาณ ประจำปีงบประมาณ ๒๕๖๘ โรงพยาบาลมหาราชนครศรีธรรมราช แผนจ้างเหมาบริการอื่น (สนับสนุน) – ค่าบำรุงรักษาระบบคอมพิวเตอร์ ลำดับที่ ๙ รายการค่าบำรุงรักษาระบบ Cyber Security จำนวน ๑ ระบบ วงเงิน ๑,๐๐๐,๐๐๐.๐๐ บาท (หนึ่งล้านบาทถ้วน)

**๒. วัตถุประสงค์**

เพื่อปกป้องคอมพิวเตอร์ เครือข่าย ซอฟต์แวร์แอปพลิเคชัน ระบบที่สำคัญ และข้อมูล จากภัยคุกคามทางดิจิทัลที่อาจเกิดขึ้นได้

**๓. คุณสมบัติของผู้ยื่นข้อเสนอ**

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗ เป็นนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ จังหวัด ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ
(นายอนุวัตร์ รินทร์วิฑูรย์) (นายสุริยา กองสุก) (นางสาวพลอยกนก จุลนวล)

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

๓.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน หรือหนังสือเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

๓.๑๑ ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์(Electronic Government Procurement: e - GP) ของกรมบัญชีกลาง

๓.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ เป็นไปตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ด่วนที่สุด ที่ กค (กวจ) ๐๔๐๕.๒/ว๑๒๔ ลงวันที่ ๑ มีนาคม ๒๕๖๖ ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปีต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ มูลค่าการจัดซื้อจัดจ้างไม่เกิน ๑ ล้านบาท ไม่ต้องกำหนดทุนจดทะเบียน

(๓) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา โดยพิจารณาจากบัญชีเงินฝากธนาคาร ณ วันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะ การจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่ง ในวันลงนามในสัญญา

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ

(นายอนุวัตร์ รินทร์วิฑูรย์) (นายสุริยา กองสุก) (นางสาวพลอยกนก จุลนวล)

(๔) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในครั้งนั้น (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคาร

(๕) กรณีตาม (๑) - (๔) ยกเว้นสำหรับกรณีดังต่อไปนี้

(๕.๑) กรณีผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(๕.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการ ตามพระราชบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑

(๕.๓) งานก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงานก่อสร้างแล้ว และงานก่อสร้างที่หน่วยงานของรัฐได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้างที่มีคุณสมบัติเบื้องต้นไว้แล้วก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุมีผลใช้บังคับ

**๔. รายละเอียดคุณลักษณะเฉพาะหรือขอบเขตของงาน**

**๔.๑ คุณสมบัติทั่วไป**

๑.๑ ข้อกำหนดนี้เป็นรายละเอียดความต้องการ สำหรับงานบำรุงรักษาระบบ Cyber Security โรงพยาบาลมหาราช นครศรีธรรมราช ซึ่งประกอบด้วย บำรุงรักษาระบบ Cyber Security จำนวน ๔ งาน

๑.๒ ผู้เสนอราคาจะต้องศึกษาทำความเข้าใจกับข้อกำหนดฉบับนี้ และจะต้องเสนอราคาบริการ/ระบบที่สามารถทำงานได้ตรงตามความต้องการของ โรงพยาบาลมหาราช นครศรีธรรมราช ทั้งอุปกรณ์ Hardware, ระบบ Software ตามข้อกำหนด และอุปกรณ์ประกอบอื่น ๆ ที่จำเป็นในการจัดส่ง (ถ้ามี) การใช้งานและการบำรุงรักษาอุปกรณ์/ระบบ

๑.๓ ผู้เสนอราคาจะต้องรับผิดชอบการดำเนินงานต่างๆ ทั้งหมดให้ถูกต้องตามข้อกำหนด รวมทั้งปฏิบัติตามระเบียบ กฎ ข้อบังคับ ของ โรงพยาบาลมหาราช นครศรีธรรมราช หรือของหน่วยงานที่เกี่ยวข้องกับการดำเนินงานตามข้อกำหนดนี้ โดยผู้เสนอราคาจะอ้างเหตุไม่รับผิดชอบใด ๆ จากความเข้าใจผิด ความไม่ทราบความผิดพลาด หรือความไม่สมบูรณ์ ของข้อมูลที่มีในข้อกำหนดนี้ไม่ได้ การดำเนินการใดๆ ของผู้เสนอราคาที่ขัดกับระเบียบ กฎ ข้อบังคับที่เกี่ยวข้องกับการดำเนินงานตามข้อกำหนด และตามสัญญา ผู้เสนอราคาจะต้องรับผิดชอบต่อผลที่จะเกิดขึ้นและแก้ไขให้ถูกต้อง

**๔.๒ การดำเนินงาน**

๒.๑ ผู้ยื่นข้อเสนอต้องดำเนินการติดตั้งบริการที่ได้นำเสนอในโครงการนี้ ให้สามารถใช้งานได้กับระบบเครือข่ายอินเตอร์เน็ตของโรงพยาบาลมหาราชนครศรีธรรมราช และตรงตามคุณสมบัติที่ระบุไว้ข้างต้นให้เรียบร้อย และเป็นไปตามความต้องการของโรงพยาบาลมหาราชนครศรีธรรมราช

๒.๒ ในระหว่างการติดตั้งบริการที่นำเสนอมาไปโครงการนี้ จะต้องไม่มีผลกระทบต่อการทำงานของระบบงาน ต่าง ๆ หรือก่อให้เกิดความเสียหายแก่ โรงพยาบาลมหาราช นครศรีธรรมราช ทั้งนี้ หากเกิดผลกระทบหรือเกิดความ เสียหาย ทางผู้ยื่นข้อเสนอจะต้องเป็นผู้ดำเนินการแก้ไขให้สามารถใช้งานได้ตามปกติโดยทันที

๒.๓ กำหนดให้ผู้เสนอราคาต้องส่งมอบงาน ให้แล้วเสร็จภายใน ๙๐ วัน นับถัดจากวันลงนามในสัญญา

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ

(นายอนุวัตร์ รินทร์วิฑูรย์) (นายสุริยา กองสุก) (นางสาวพลอยกนก จุลนวล)

**๔.๓ ข้อกำหนดด้านเทคนิค ประกอบด้วยรายละเอียดดังนี้**

๔.๓.๑ <u>บริการระบบป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall : WAF) Bandwidth ๑๐ Mbps จำนวน ๑ IP เป็นเวลา ๑๒ เดือน</u>

๔.๓.๑.๑ เป็นบริการปกป้องเว็บแอปพลิเคชัน (Web Application Firewall) ในรูปแบบ Cloud Security

๔.๓.๑.๒ สามารถป้องกันการโจมตีตามรายการต่อไปนี้ได้เป็นอย่างน้อย

- OWASP TOP ๑๐ ปี ๒๐๑๗ หรือใหม่กว่า
- Brute Force
- Cross-site Script (XSS)
- Buffer Overflows
- Bot Detection/blocking
- Cookies encryption
- Geolocation Blocking

๔.๓.๑.๓ สามารถตั้งค่า format log ที่จะส่งไปยัง SIEM หรือ Syslog ภายนอกได้

๔.๓.๑.๔ ระบบสามารถจัดการ Blacklist/Whitelist IP Address ได้

๔.๓.๑.๕ มีศูนย์บริการรับแจ้งเหตุขัดข้องทุกวันตลอด ๒๔ ชั่วโมง (โทร.๑๘๘๘)

๔.๓.๑.๖ มีเจ้าหน้าที่เทคนิค Support ทุกวันทำการ ตลอด ๘ ชั่วโมง (๘x๕)

๔.๒.๒ <u>บริการดูแลและเฝ้าระวังความปลอดภัยระบบเครือข่ายและเทคโนโลยีสารสนเทศ (Cybersecurity Monitoring : CSM ) เป็นเวลา ๑๒ เดือน</u>

๔.๒.๒.๑ ผู้ให้บริการต้องมีศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามระบบเทคโนโลยีสารสนเทศ (Cybersecurity Operations Center: CSOC) ทั้งศูนย์หลัก และศูนย์สำรอง อยู่ในประเทศไทย โดยมีคุณสมบัติดังนี้

๔.๒.๒.๑.๑ ผู้ให้บริการต้องเก็บรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ของอุปกรณ์ความปลอดภัยทางด้านเครือข่าย แบบ Online บนระบบ SIEM เป็นระยะเวลา ๙๐ วัน และ แบบ Offline ที่ External Source เป็นระยะเวลา ไม่น้อยกว่า ๓๖๕ วัน ตามรายการระบบที่ใช้งานอยู่ในปัจจุบัน ได้แก่

๑) Internet firewall ๒ HA (xx Firewall)
๒) Datacenter firewall ๒ HA (xx Firewall)
๓) Antivirus/End-point protection for server ๑ centralize management (xx server)

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ

(นายอนุวัตร์ รินทร์วิฑูรย์) (นายสุริยา กองสุก) (นางสาวพลอยกนก จุลนวล)

๔) Antivirus/End-point protection for client ๑ centralize management (xx clients)

๕) E-mail Security Gateway (๑ gateway)

๖) Active directory (๒ server)

๗) Web Application Firewall

๘) Proxy Server (๑ server)

๙) Etc.

๔.๒.๒.๑.๒ ผู้ให้บริการต้องดำเนินการการตั้งค่า configuration ตามรายการระบบที่ใช้งานอยู่ในปัจจุบัน เพื่อให้มีการส่งข้อมูลจราจรทางคอมพิวเตอร์ (Log file) จากเครื่องและอุปกรณ์ดังกล่าวไปยังศูนย์ Cybersecurity Operations Center (CSOC) ของผู้ให้บริการ

๔.๒.๒.๑.๓ ผู้ให้บริการต้องสามารถวิเคราะห์เหตุการณผิดปกติทางด้านบริหารจัดการระบบคอมพิวเตอร์และ ระบบเครือข่ายสื่อสารและอินเทอร์เน็ต เพื่อวิเคราะห์ความเกี่ยวโยงของเหตุการณ์และภัยคุกคาม ด้านความปลอดภัยสารสนเทศ (IT Security Monitoring) แหล่งที่มาของภัยคุกคามนั้นๆ ตลอดเวลา ๒๔ ชั่วโมงต่อสัปดาห์ (๒๔x๗)

๔.๒.๒.๑.๔ ผู้ให้บริการต้องทำการเฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ ผ่านทาง E-mail, โทรศัพท์ และ ระบบ Ticket Management ตาม Service Level Agreement และระดับความรุนแรง

๔.๒.๒.๑.๕ การแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ต้องครอบคลุมเนื้อหาดังต่อไปนี้

- ระบุประเภทของภัยคุกคาม
- วัน-เวลา ที่พบภัยคุกคาม
- ระบุต้นทาง (Source) และปลายทาง (Target)
- ระบุระดับความรุนแรง (Severity)
- คำแนะนำและขั้นตอนการดำเนินการแก้ไขเชิงเทคนิค

๔.๒.๒.๑.๖ ผู้ให้บริการต้องมีระบบบริหารจัดการ ซึ่งแสดงสถานการตรวจสอบข้อมูลความปลอดภัยของระบบ เครือข่าย และข้อมูลการแจ้งเตือนและติดตามเหตุการณ์ (Ticket Management) เพื่อให้สามารถตรวจสอบข้อมูลได้ตลอดเวลา

๔.๒.๒.๑.๗ ผู้ให้บริการต้องสามารถกำหนดเงื่อนไขรูปแบบของการเฝ้าระวังและตรวจจับภัยคุกคาม (Use case) ตามที่ได้ทำการประเมินและตกลงร่วมกับทางผู้ใช้บริการ ได้ไม่น้อยกว่า ๘ use case ดังนี้

๑.Foot printing/Scanning/Reconnaissance/Probing

๒.Enumerating/System Hacking/Attempted Exploit

๓.SQL Injection/Cross site Scrip/Buffer Overflow

๔.Gaining Access

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ

(นายอนุวัตร์ รินทร์วิฑูรย์) (นายสุริยา กองสุก) (นางสาวพลอยกนก จุลนวล)

๕.Trojans/Backdoor/Malware

๖.Suspicious IP/Suspicious domain

๗.Denial of Service/Distribution Denial of Service

๘.Policy violation

๔.๒.๒.๑.๘ ระบบเฝ้าระวังและแจ้งเตือนภัยคุกคามของผู้ให้บริการต้องมีการ integrate ข้อมูล Threat intelligence จากภายนอก เพื่อประโยชน์ในการเฝ้าระวัง Threat ใหม่ๆ อย่างน้อย ๑๐ แหล่ง

๔.๒.๒.๑.๙ ระบบเฝ้าระวังและแจ้งเตือนภัยคุกคาม จะต้องติดตั้งภายในศูนย์ Data center ที่ได้รับการรับรอง ระบบบริหารจัดการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information security management system: ISO ๒๗๐๐๑)

๔.๒.๒.๑.๑๐ ผู้ให้บริการจะต้องมีเจ้าหน้าที่ผู้เชี่ยวชาญปฏิบัติงานเป็นพนักงานประจำของบริษัท ที่ได้รับการ รับรองมาตรฐานความรู้ ความสามารถทางด้านความมั่นคงปลอดภัยสารสนเทศจากหน่วยงานสากล CompTIA Security+ หรือ CompTIA CySA+ เป็นอย่างน้อย จำนวน ๒ ท่าน

๔.๒.๒.๑.๑๑ ผู้ให้บริการจะต้องมีเจ้าหน้าที่ผู้เชี่ยวชาญ ที่ให้บริการเฝ้าระวังแจ้งเตือนภัยคุกคาม พร้อมทั้งให้คำแนะนำแก่ลูกค้าแบบ ๒๔x๗ ชั่วโมง ผ่านศูนย์ปฏิบัติการ CSOC

๔.๒.๒.๑.๑๒ ผู้ให้บริการต้องจัดให้มีทีมงานผู้เชี่ยวชาญ เพื่อคอยสนับสนุนและติดตามข้อมูลข่าวสารเกี่ยวกับความ ปลอดภัยเทคโนโลยีสารสนเทศ (Security Expertise) เพื่ออัพเดทข้อมูลข่าวสารที่ทันสมัย หรือภัยคุกคามร้ายแรงด้านความปลอดภัยสารสนเทศอย่างสม่ำเสมอ รวมทั้งให้คำแนะนำด้านการเตรียมพร้อมและการป้องกันภัยคุกคาม ตลอดระยะเวลาสัญญา

๔.๒.๒.๑.๑๓ ผู้ให้บริการต้องรายงานผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจารจรทางคอมพิวเตอร์ และสรุปผลการดำเนินการเฝ้าระวังภัยคุกคามเหตุการณ์ผิดปกติที่เป็นภัยคุกคามเป็นรายเดือน (Monthly report) โดยมีรายละเอียดดังต่อไปนี้

- รายงานสรุปเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เกิดขึ้น โดยมี การวิเคราะห์ภัยคุกคามในเชิงลึก โดยมีเนื้อหาตามรายการดังต่อไปนี้ เป็นอย่างน้อย

๑. Top Attackers report

๒. Top Threat Report

๓. Top Successful and Failed Authentication Report

๔. Firewall action report

๕. รายงานสรุปการแจ้งเตือนเหตุการณ์ที่ตรวจพบ (Incident Report) ประจำเดือน

๖. รายงานสรุปปริมาณการใช้งานข้อมูลจราจรทางคอมพิวเตอร์ประจำเดือน พร้อมแจ้งเตือนในกรณีที่ใช้เกินตาม EPS ที่กำหนดไว้

๔.๒.๑.๑๔ มีผู้เชี่ยวชาญเข้าประชุมรายงานสรุปผลการดำเนินการประจำทุก ๓ เดือน เพื่อทำการอธิบายรายละเอียดและวิธีการแก้ไขของภัยคุกคามทางคอมพิวเตอร์ที่ตรวจพบในระบบ

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ

(นายอนุวัตร์ รินทร์วิฑูรย์) (นายสุริยา กองสุก) (นางสาวพลอยกนก จุลนวล)

๔.๓.๓ บริการตรวจสอบระบบเพื่อหาช่องโหว่ทางด้านความปลอดภัยไซเบอร์ ( Vulnerability Assessment : VA Scan ) ในเครื่องคอมพิวเตอร์แม่ข่าย จำนวน ๕ เครื่อง หรือ ๕ IP เครื่องละ ๑ ครั้ง

๔.๓.๓.๑ ดำเนินการตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศเครื่องแม่ข่าย ผ่านทางเครื่องคอมพิวเตอร์ โดยมีจำนวนเครื่องแม่ข่ายทั้งสิ้น ๕ IP

๔.๓.๓.๒ วิเคราะห์ และรายงานผลการทดสอบพร้อมคำแนะนำในการปรับปรุงระบบความปลอดภัย

๔.๓.๓.๓ ดำเนินการค้นหาช่องโหว่ทั้งแบบ Non-Credential Scan และ Credential Scan

๔.๓..๓.๔ ดำเนินการค้นหาช่องโหว่ ประเมินหาจุดอ่อน ประเมินความเสี่ยงและผลกระทบพร้อมข้อเสนอแนะแนวทางแก้ไขโดยอ้างอิงตามกรอบ ดังนี้เป็นอย่างน้อย

- NIST ๘๐๐-๔๒ Guideline on Network Security Testing
- Common Vulnerability Exposure, CVE
- Common Vulnerability Scoring System, CVSS-SIG
- OWASP Top ๑๐

๔.๓.๓.๕ ดำเนินการโดยใช้โปรแกรมหรือซอฟท์แวร์ที่มีความน่าเชื่อถือไม่น้อยกว่า ๒ โปรแกรม ยกตัวอย่างเช่น

- Commercial เช่น Nessus, Acunetix, Rapid๗ เป็นต้น
- Non-commercial เช่น Metasploit, Burp suit, NMAP, Havij, Firefox Add-on, Manual Script, Nexpose เป็นต้น

๔.๓.๓.๖ วิเคราะห์ จัดทำรายงานและให้คำแนะนำในการปรับปรุงระบบ ดังนี้

- วิเคราะห์และให้คำแนะนำในกรณีที่ระบบสารสนเทศมีความจำเป็นต้องได้รับการติดตั้งระบบหรือ อุปกรณ์เพิ่มเติมเพื่อเป็นการเพิ่มระดับการรักษาความปลอดภัยของระบบเครือข่าย และระบบความปลอดภัยคอมพิวเตอร์
- รายงานผลการตรวจสอบช่องโหว่ แนวทางแก้ไข (Hardening) และคำแนะนำเพิ่มเติม เป็นฉบับภาษาไทย

๔.๓.๓.๗ ดำเนินการอัพเดทฐานข้อมูลการตรวจสอบจากผู้ผลิต ให้เป็นปัจจุบันก่อนดำเนินการทุกครั้ง

๔.๓.๓.๘ การทดสอบตรวจสอบช่องโหว่ระบบจะใช้เวลาดำเนินการทั้งหมด ๑๖ วัน ต่อครั้ง นับจากวันลงนามในสัญญา

๔.๓.๓.๙ ดำเนินการส่งมอบรายงานผลการตรวจสอบช่องโหว่

๔.๓.๔ บริการทดสอบการบุกรุกระบบความปลอดภัยไซเบอร์ ( Penetration Test ) แบบ online จำนวน ๑ ระบบ ๑ ครั้ง

๔.๓.๔.๑ ดำเนินการทดสอบเจาะระบบเว็ปไซต์ หรือ แอปพลิเคชัน ของโรงพยาบาล

๔.๓.๔.๒ รูปแบบการทดสอบเจาะระบบที่ใช้คือ การทดสอบเจาะระบบแบบทราบข้อมูลบางส่วน (Grey-Box Penetration Testing)

๔.๓.๔.๓ การทดสอบเจาะระบบทีมงานได้ใช้หลักการ และวิธีการจากมาตรฐานการทดสอบพัฒนาขึ้นเอง โดยประยุกต์เพื่อให้เหมาะสมกับสภาพแวดล้อมของระบบโดยส่วนใหญ่ของประเทศไทย โดยมีการอ้างอิงจากมาตรฐานสากล ดังนี้

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ

(นายอนุวัตร์ รินทร์วิฑูรย์) (นายสุริยา กองสุก) (นางสาวพลอยกนก จุลนวล)

- NIST ๘๐๐-๔๒ Guideline on Network Security Testing
- CIEH (Certified Ethical Hacker) Methodology
- OWASP Testing Guide Version ๔
- OWASP Mobile Testing Guide
- ISSAF, Information Systems Security Assessment Framework

๔.๓.๔.๔ วิเคราะห์การทดสอบเจาะระบบ และรายงานผลการทดสอบพร้อมคำแนะนำในการปรับปรุงระบบความปลอดภัย

๔.๓.๔.๕ ดำเนินการส่งมอบรายงานผลการทดสอบเจาะระบบ

**๕. กำหนดเวลาส่งมอบพัสดุ**

ภายใน ๙๐ วัน นับถัดจากวันลงนามในสัญญา

**๖.หลักเกณฑ์ในการพิจารณาคัดเลือดข้อเสนอ**

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ จังหวัดจะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา โดยพิจารณาจากราคารวม

**๗. วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร**

เงินนอกงบประมาณ (เงินบำรุง) ประจำปีงบประมาณ ๒๕๖๘ โรงพยาบาลมหาราชนครศรีธรรมราช วงเงิน ๑,๐๐๐,๐๐๐ บาท (หนึ่งล้านบาทถ้วน)

**๘. งวดงานและการจ่ายเงิน**

โรงพยาบาลมหาราช นครศรีธรรมราช จะชำระเงินให้แก่ผู้เสนอราคาร้อยละ ๑๐๐ เมื่อผู้เสนอราคาดำเนินการติดตั้งอุปกรณ์ที่ได้ นำเสนอ ในโครงการนี้ทั้งหมดให้สามารถใช้งานได้กับระบบเครือข่ายคอมพิวเตอร์ของโรงพยาบาลมหาราชนครศรีธรรมราชตรงตามคุณสมบัติที่ระบุไว้ข้างต้น และทางคณะกรรมการตรวจรับ ได้รับมอบงานไว้เป็นที่เรียบร้อยแล้ว

**๙. อัตราค่าปรับ**

๙.๑ กรณีที่ผู้รับจ้างนำงานที่รับจ้างไปจ้างช่วงให้ผู้อื่นทำอีกทอดหนึ่งโดยไม่ได้รับอนุญาตจากจังหวัดจะกำหนดค่าปรับสำหรับการฝ่าฝืนดังกล่าวเป็นจำนวนร้อยละ ๑๐.๐๐ ของวงเงินของงานจ้างช่วงนั้น

๙.๒ กรณีที่ผู้รับจ้างปฏิบัติผิดสัญญาจ้างนอกเหนือจากข้อ ๙.๑ จะกำหนดค่าปรับเป็นรายวันในอัตราร้อยละ ๐.๑๐ ของราคาค่าจ้าง

| | | |
|---|---|---|
| ลงชื่อ.....ประธานกรรมการ | ลงชื่อ.....กรรมการ | ลงชื่อ.....กรรมการ |
| (นายอนุวัตร์ รินทร์วิฑูรย์) | (นายสุริยา กองสุก) | (นางสาวพลอยกนก จุลนวล) |

**๑๐. การกำหนดระยะเวลารับประกันความชำรุดบกพร่อง**

ผู้ยื่นข้อเสนอต้องรับประกันผลิตภัณฑ์ที่นำเสนอในโครงการนี้ทั้งหมด เป็นระยะเวลาทั้งสิ้น ๑๒ เดือน นับจากที่คณะกรรมการตรวจรับของโรงพยาบาลมหาราชนครศรีธรรมราช ลงนามในเอกสารรับมอบงานเป็นที่เรียบร้อยแล้ว ในกรณีที่เกิด ปัญหาเมื่อได้รับแจ้งปัญหา ทาง E-mail หรือทางโทรศัพท์ หรือโปรแกรม LINE หรือหนังสือราชการ ผู้ยื่นข้อเสนอจะต้อง ดำเนินการตรวจสอบลักษณะปัญหา และแก้ไขปัญหาเบื้องต้นผ่านทางโทรศัพท์ หรือผ่านช่องทางโปรแกรม LINE หรือ ด้วยวิธีการ Remote Desktop ผ่านช่องทาง VPN ของหน่วยงาน หากแก้ไขไม่เป็นผลสำเร็จ ผู้ยื่นข้อเสนอต้อง จัดส่ง เจ้าหน้าที่ที่มีความรู้ความชำนาญ เข้ามาดำเนินการแก้ไขปัญหา ณ โรงพยาบาลมหาราช นครศรีธรรมราช ด้วยวิธีการที่เหมาะสมกับลักษณะของปัญหาที่เกิดขึ้น ภายในระยะเวลาไม่เกิน ๔ ชั่วโมง ในเวลาทำการ ซึ่งต้องถือปฏิบัติใน ระยะเวลาประกัน ๑ ปี

ลงชื่อ.....ประธานกรรมการ
(นายอนุวัตร์ รินทร์วิฑูรย์)
นายแพทย์ชำนาญการพิเศษ

ลงชื่อ.....กรรมการ
(นายสุริยา กองสุก)
นักวิชาการคอมพิวเตอร์ปฏิบัติการ

ลงชื่อ.....กรรมการ
(นางสาวพลอยกนก จุลนวล)
นักวิชาการคอมพิวเตอร์ปฏิบัติการ