มหาวิทยาลัยเกริก

บันทึกข้อความ

หน่วยงาน ศูนย์เทคโนโลยีสารสนเทศ

ที่ 720000/ 55 วันที่ 1 สิงหาคม 2568

เรื่อง ขออนุมัติว่าจ้างที่ปรึกษาด้านระบบความปลอดภัยและเครือข่ายคอมพิวเตอร์

เรียน อธิการบดี ผ่านรองอธิการบดีฝ่ายบริหาร ผ่านผู้ช่วยรองอธิการบดีฝ่ายบริหาร(ฝ่ายเทคโนโลยีสารสนเทศ)

สิ่งที่ส่งมาด้วย 1. ข้อเสนอขอบเขตงาน (Terms of Reference - TOR) สำหรับการว่าจ้างที่ปรึกษา

2. ประวัติและประสบการณ์ของที่ปรึกษา

ตามที่ศูนย์เทคโนโลยีสารสนเทศ มีภารกิจหลักในการดูแลและพัฒนาระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของหน่วยงานให้มีประสิทธิภาพและมีความมั่นคงปลอดภัยนั้น ปัจจุบันระบบและเครือข่ายของหน่วยงานมีความซับซ้อนเพิ่มขึ้นอย่างต่อเนื่อง รวมถึงภัยคุกคามทางไซเบอร์ที่มีความหลากหลายและรุนแรงขึ้น

เพื่อให้มั่นใจว่าระบบและเครือข่ายของหน่วยงานมีความปลอดภัยในระดับสูงสุด สามารถป้องกันการโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพ และเป็นไปตามมาตรฐานด้านความปลอดภัยสารสนเทศที่เกี่ยวข้อง ศูนย์พิจารณาแล้วเห็นว่ามีความจำเป็นต้องว่าจ้างที่ปรึกษาผู้เชี่ยวชาญภายนอกด้านระบบความปลอดภัยและเครือข่ายคอมพิวเตอร์ เพื่อให้คำแนะนำประเมินสถานะปัจจุบันของระบบและเครือข่าย ตรวจสอบช่องโหว่ รวมถึงจัดทำแผนด้านความปลอดภัยและข้อเสนอแนะในการปรับปรุงแก้ไขให้มีความรัดกุมยิ่งขึ้น ซึ่งจะช่วยยกระดับความสามารถในการป้องกันและรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพ

การว่าจ้างที่ปรึกษาในครั้งนี้ จะครอบคลุมขอบเขตงานหลักดังนี้ (รายละเอียดเพิ่มเติมตามสิ่งที่ส่งมาด้วย 1)

- การให้ปรึกษาแนะนำและถ่ายทอดความรู้: แนะนำแนวปฏิบัติที่ดีที่สุด (Best Practice) และถ่ายทอดองค์ความรู้ให้แก่บุคลากรของศูนย์
- การประเมินและวิเคราะห์ความเสี่ยงด้านความปลอดภัย: ตรวจสอบและประเมินช่องโหว่ของระบบและเครือข่ายทั้งหมด
- การให้คำปรึกษาจัดทำแผนด้านความปลอดภัย: วางแผนและออกแบบมาตรการป้องกันและแก้ไขในระยะสั้นและระยะยาว

ดังนั้นจึงขออนุมัติให้ศูนย์เทคโนโลยีสารสนเทศดำเนินการว่าจ้างที่ปรึกษาด้านระบบความปลอดภัยและเครือข่ายคอมพิวเตอร์ ทั้งนี้ศูนย์จะดำเนินการประสานงานส่วนงานที่เกี่ยวข้องต่อไป

จึงเรียนมาเพื่อโปรดพิจารณา

(อาจารย์ชัยมาศ คะมา)
หัวหน้าศูนย์เทคโนโลยีสารสนเทศ

เรียนท่านอธิการบดี
ด้วยศูนย์ฯ มีความประสงค์ว่าจ้างบุคลากร
ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันระบบสารสนเทศ
ของมหาวิทยาลัยฯ
จึงเรียนมาเพื่อโปรดทราบ

ดร.ชุตพงศ์ ไทยอุปถัมภ์

ข้อเสนอขอบเขตงาน (Terms of Reference - TOR)

สำหรับการว่าจ้างที่ปรึกษาด้านระบบความปลอดภัยและเครือข่ายคอมพิวเตอร์

1. ความเป็นมา

ปัจจุบันระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย มีความสำคัญอย่างยิ่งต่อการดำเนินงานและให้บริการแก่นักศึกษา/บุคลากร โดยมีการประยุกต์ใช้เทคโนโลยีที่ทันสมัยและมีการเชื่อมโยงกับระบบภายนอกเพิ่มมากขึ้นอย่างต่อเนื่อง ในขณะเดียวกัน ภัยคุกคามทางไซเบอร์ก็ทวีความรุนแรงและหลากหลายรูปแบบมากขึ้น ไม่ว่าจะเป็นการโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware), การโจมตีแบบปฏิเสธการให้บริการ (DDoS Attack), หรือการเจาะระบบเพื่อขโมยข้อมูล ทำให้หน่วยงานมีความเสี่ยงต่อการถูกโจมตีและอาจส่งผลกระทบต่อความต่อเนื่องในการดำเนินงานและภาพลักษณ์ขององค์กร

เพื่อให้มั่นใจว่าระบบและเครือข่ายของของมหาวิทยาลัย มีความมั่นคงปลอดภัยตามมาตรฐานสากล สามารถรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพ และเป็นไปตามกฎหมายหรือข้อบังคับที่เกี่ยวข้อง (เช่น พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์) จึงมีความจำเป็นต้องว่าจ้างที่ปรึกษาผู้เชี่ยวชาญภายนอก เพื่อเข้ามาให้คำปรึกษาแนะนำและช่วยประเมินสถานะปัจจุบัน ให้คำแนะนำ และถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยสารสนเทศและเครือข่ายให้กับบุคลากรของหน่วยงานศูนย์เทคโนโลยีสารสนเทศของมหาวิทยาลัย

2. วัตถุประสงค์

การว่าจ้างที่ปรึกษาครั้งนี้มีวัตถุประสงค์หลักดังนี้:

2.1 เพื่อถ่ายทอดองค์ความรู้และเทคนิคที่สำคัญด้านความมั่นคงปลอดภัยให้กับบุคลากรของศูนย์เทคโนโลยีสารสนเทศ/ผู้ที่เกี่ยวข้อง

2.2 เพื่อประเมินสถานะปัจจุบันของระบบความปลอดภัยและเครือข่ายคอมพิวเตอร์ของหน่วยงาน โดยครอบคลุมทั้งด้านนโยบาย บุคลากร เทคโนโลยี และกระบวนการ

2.3 เพื่อระบุและวิเคราะห์ช่องโหว่ (Vulnerability) และความเสี่ยง (Risk) ด้านความมั่นคงปลอดภัยของระบบและเครือข่ายทั้งหมด

2.4 เพื่อให้คำแนะนำและจัดทำข้อเสนอแนะเชิงเทคนิคในการปรับปรุง เสริมสร้าง และพัฒนาระบบความปลอดภัยและเครือข่ายให้มีประสิทธิภาพและได้มาตรฐาน

3. ขอบเขตของงาน (Scope of Work)

ที่ปรึกษาจะต้องดำเนินการตามขอบเขตงานดังต่อไปนี้:

3.1 ถ่ายทอดองค์ความรู้เกี่ยวกับการรวบรวมข้อมูลและประเมินสถานะปัจจุบัน (As-Is Assessment): โดยช่วยการปฏิบัติงานบุคลากรของมหาวิทยาลัยในด้าน

- ศึกษาและทำความเข้าใจโครงสร้างพื้นฐานระบบเครือข่าย, Server, Database, Application และอุปกรณ์ความปลอดภัยที่มีอยู่
- ทบทวนนโยบาย, มาตรฐาน, และกระบวนการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน
- ตรวจสอบระบบควบคุมการเข้าถึง, ระบบสำรองข้อมูล, ระบบป้องกันมัลแวร์ เป็นต้น

3.2 ถ่ายทอดองค์ความรู้เกี่ยวกับการวิเคราะห์ช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment & Penetration Testing - VAPT): โดยช่วยฝึกปฏิบัติบุคลากรของมหาวิทยาลัยในด้าน

- การทดสอบหาช่องโหว่ของระบบและเครือข่าย ทั้งจากภายนอก (External) และภายใน (Internal)
- การทดสอบเจาะระบบ (Penetration Testing) ในส่วนที่สำคัญและมีความเสี่ยงสูง (เช่น Web Application, Database Server, Mail Server)
- การจัดทำรายงานผลการวิเคราะห์ช่องโหว่และข้อเสนอแนะในการแก้ไข

3.3 ให้คำปรึกษาในการวิเคราะห์ความเสี่ยงและการจัดทำแผนบริหารจัดการความเสี่ยง (Risk Assessment & Management):

- ระบุสินทรัพย์สารสนเทศที่สำคัญ (Critical Assets)
- ประเมินระดับความเสี่ยงที่อาจเกิดขึ้นกับสินทรัพย์เหล่านั้น และผลกระทบต่อการดำเนินงานของหน่วยงาน
- จัดทำแผนบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัย

3.4 ให้คำปรึกษาในการจัดทำแผนด้านความปลอดภัยและข้อเสนอแนะในประเด็น:

- การจัดทำสถาปัตยกรรมด้านความมั่นคงปลอดภัย (Security Architecture) ที่เหมาะสมกับหน่วยงาน
- เสนอแนะมาตรการทางเทคนิค (Technical Controls) และมาตรการทางด้านบริหารจัดการ (Administrative Controls) เพื่อยกระดับความปลอดภัย
- ให้ความแนะนำในด้าการจัดทำแผนด้านความมั่นคงปลอดภัยสารสนเทศและเครือข่าย โดยระบุโครงการ/กิจกรรมที่ต้องดำเนินการในแต่ละช่วงเวลา (ระยะสั้นและระยะยาว)
- ประมาณการงบประมาณโดยคร่าวสำหรับแต่ละโครงการ/กิจกรรมในแผนแม่บท
- แนะนำเทคโนโลยีใหม่ๆ ที่จำเป็น

4. คุณสมบัติของที่ปรึกษา

ที่ปรึกษาจะต้องมีคุณสมบัติและประสบการณ์ดังต่อไปนี้:

4.1 เป็นผู้ประสบการณ์ในการทำงานด้านความมั่นคงปลอดภัยสารสนเทศและเครือข่ายคอมพิวเตอร์

4.2 มีวุฒิการศึกษาและประกาศนียบัตรรับรองด้านความมั่นคงปลอดภัยสารสนเทศที่เป็นที่ยอมรับในระดับสากล เช่น CISSP, CISM, CEH, OSCP, CompTIA Security+ หรือเทียบเท่า

4.3 มีความเข้าใจในกฎหมายและข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย (เช่น พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์, พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล)

5. ระยะเวลาดำเนินการ

ทำสัญญาปีต่อปี

6. ผลผลิตที่คาดว่าจะได้รับ (Deliverables)

บุคลากรศูนย์เทคโนโลยีสารสนเทศสามารถเรียนรู้และจัดทำรายงานที่เกี่ยวข้องได้ ดังต่อไปนี้:

6.1 รายงานผลการประเมินสถานะปัจจุบันของระบบความปลอดภัยและเครือข่าย (As-Is Assessment Report)

6.2 รายงานผลการวิเคราะห์ช่องโหว่และการทดสอบเจาะระบบ (VAPT Report) พร้อมแนวทางในการแก้ไข

6.3 รายงานผลการวิเคราะห์ความเสี่ยงและแผนบริหารจัดการความเสี่ยง (Risk Assessment & Management Report)

6.4 สามารถวางแผนแม่บทด้านความมั่นคงปลอดภัยสารสนเทศและเครือข่าย (Security Master Plan)

7. งบประมาณ

งบกลาง

8. เงื่อนไขและข้อกำหนดอื่นๆ

8.1 ที่ปรึกษาจะต้องรักษาความลับของข้อมูลที่ได้รับจากหน่วยงานอย่างเคร่งครัด

8.2 ในกรณีที่มีข้อมูลส่วนบุคคลเกี่ยวข้อง ที่ปรึกษาจะต้องปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างเคร่งครัด

8.3 ที่ปรึกษาต้องสามารถให้คำปรึกษาแนะนำทั้งในแบบ Online และ Onsite

8.4 ที่ปรึกษาต้องเข้ามาปฏิบัติงานที่มหาวิทยาลัยอย่างน้อย 12 วัน ในรอบสัญญา

Thitipong Maneewan

Bangkok, Thailand

E-mail: thitipong_manee@rtaf.mi.th

Objective

I am a motivated security specialist. I am a team leader and a fast learner. I have provided internal training for the juniors and worked with other military units globally regarding cybersecurity in practice.

EDUCATION

BSc in Computer Science, Royal Thai Air Force Academy. (GPA 2.98) **2009 – 2013**

- Network Specialized track

MSc Information Security, Royal Holloway, University of London. (GPA 60.8%) **2015 – 2017**

Modules include:

- Cryptography
- Security management
- Network security
- Computer security (Operating Systems)
- Security testing - Theory and Practice
- Software security

EMPLOYMENT AND EXPERIENCE

Network Specialist, Directorate of Communication and Electronic **Apr 2013 – Present**

Responsible for the network system at Royal Thai Air Force.

Duties involved:

- Led the design, configuration, and maintenance of network infrastructure supporting 12 branches and 30k users across the Royal Thai Air Force, ensuring 99% network uptime for critical operations.
- Design, Configure and Maintain Network Security devices, such as Palo Alto (NGFW), Arbor (DDoS protection), SangFor IAG and Cisco Firepower
- Perform Network Operations in NOC
- Provided strategic advisory to senior leadership on critical network and information security initiatives, influencing decisions that led to improvement in security posture.
- Mentored and developed a team of 10 junior network specialists, improving team efficiency and contributing to projects succession.
- Involve in an investigation on cyber incidents