รายละเอียดประกอบการจ้างเหมาบำรุงรักษาและตรวจประเมินการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC27001 : 2022 สำหรับศูนย์คอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

1. วัตถุประสงค์ของโครงการ

เพื่อเตรียมความพร้อมในการตรวจประเมินติดตามครั้งที่ 2 (2nd Surveillance Audit) ของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 สำหรับศูนย์คอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

2. ขอบเขตการดำเนินงาน

2.1 ขั้นตอนการวางแผนดำเนินงาน (Plan)

2.1.1 บริษัทจะดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของศูนย์คอมพิวเตอร์ (Risk Assessment)

- บริษัทจะประชุมเชิงปฏิบัติการ (Workshop) ร่วมกับคณะทำงานในการประเมินความเสี่ยง
- บริษัทจะประชุมร่วมกับคณะทำงานในการสรุปผลการประเมินความเสี่ยง

2.1.2 บริษัทจะจัดทำเอกสารสรุปมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ (Statement of Applicability)

- บริษัทจะปรับปรุงเอกสารสรุปมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ (Statement of Applicability)
- บริษัทจะนำเสนอเอกสารสรุปมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ (Statement of Applicability) ให้กับคณะทำงานพิจารณา

2.2 ขั้นตอนการดำเนินการ (Operation)

2.2.1 บริษัทจะดำเนินการติดตามการดำเนินการตามแผนการควบคุมความเสี่ยงจากการประเมินความเสี่ยง

- บริษัทจะจัดตรียมเอกสารแผนจัดการความเสี่ยง (Risk Treatment Plan)
- บริษัทจะดำเนินการประชุมร่วมกับคณะทำงานในการดำเนินการตามแผนจัดการความเสี่ยง (Risk Treatment Plan)
- บริษัทจะดำเนินการติดตามผลการดำเนินการตามแผนการควบคุมความเสี่ยง (Risk Treatment Plan)

2.2.2 บริษัทจะดำเนินการตรวจสอบช่องโหว่ทางเทคนิค (Vulnerability Assessment (VA)

- บริษัทจะดำเนินการตรวจสอบช่องโหว่ทางเทคนิค (Vulnerability Assessment (VA)
- บริษัทจะจัดทำรายงานผลการตรวจสอบช่องโหว่ทางเทคนิค (Vulnerability Assessment (VA)

2.2.3 บริษัทจะดำเนินการทดสอบเจาะระบบ (Penetration Testing)

- บริษัทจะดำเนินการทดสอบเจาะระบบ (Penetration Testing)
- บริษัทจะจัดทำรายงานผลการทดสอบเจาะระบบ (Penetration Testing)

2.2.4 บริษัทจะดำเนินการติดตามจัดเก็บหลักฐานการดำเนินงานของศูนย์คอมพิวเตอร์

- ตรวจสอบ/ติดตาม การจัดเก็บหลักฐานการดำเนินงาน

2.3 ขั้นตอนตรวจสอบการดำเนินงาน (Performance Evaluation)

2.3.1 บริษัทจะติดตามการดำเนินการตามเกณฑ์วัดผลประสิทธิผลลัพธ์จากการปฏิบัติตามเกณฑ์ของมาตรฐาน ISO/IEC 27001:2022

- บริษัทจะตรวจสอบ/ติดตาม การดำเนินการตามเกณฑ์วัดผลประสิทธิผลลัพธ์จากการปฏิบัติตามเกณฑ์ของมาตรฐาน ISO/IEC 27001:2022

2.3.2 บริษัทจะดำเนินการเตรียมความพร้อมก่อนการตรวจสอบภายในของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ สำหรับศูนย์คอมพิวเตอร์

- บริษัทจะดำเนินการจัดประชุมเพื่อเตรียมความพร้อมก่อนการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ

2.3.3 บริษัทจะดำเนินการสนับสนุนการตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Internal audit and Internal auditor supporting)

- บริษัทจะดำเนินการสนับสนุนการตรวจสอบภายในด้านความมั่นคงปลอดภัยสารสนเทศ (Internal audit and Internal auditor supporting) ทั้งทีมผู้ตรวจสอบ และทีมผู้รับตรวจ
- บริษัทจะดำเนินการสรุปผลการตรวจสอบภายในด้านความมั่นคงปลอดภัยสารสนเทศ

2.4 ขั้นตอนปรับปรุงการดำเนินงาน (Improvement)

2.4.1 บริษัทจะติดตามการดำเนินการปรับปรุงแก้ไขความไม่สอดคล้อง (Non-Conformity) ที่พบจากการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ

- บริษัทจะจัดประชุมร่วมกับคณะทำงานเพื่อติดตามการดำเนินการปรับปรุงแก้ไขความไม่สอดคล้อง (Non-Conformity) ที่พบจากการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ

2.4.2 บริษัทจะดำเนินการสนับสนุนการเตรียมความพร้อมสำหรับการตรวจสอบ เพื่อขอใบรับรองในรอบการตรวจประเมินติดตามครั้งที่ 2 (2^{nd} Surveillance Audit)

- บริษัทจะดำเนินการสนับสนุนการตรียมความพร้อมสำหรับการตรวจสอบเพื่อขอใบรับรองในรอบการตรวจประเมินติดตามครั้งที่ 2 (2nd Surveillance Audit) ทั้งทีมผู้ตรวจสอบ และทีมผู้รับตรวจ

2.4.3 บริษัทจะดำเนินการสนับสนุนการตรวจรับรองระบบบริหารความมั่นคงปลอดภัยสารสนเทศจาก Certification Body เพื่อขอใบรับรองในรอบการตรวจประเมินติดตามครั้งที่ 2 (2nd Surveillance Audit)

3. ระยะเวลาการส่งมอบ

ระยะเวลา 210 วัน โดยแบ่งชำระเงินเป็น 2 งวดดังนี้

3.1 งวดที่ 1 ชำระ 40% หลังจัดทำรายงานผลการตรวจสอบช่องโหว่ทางเทคนิค Vulnerability Assessment (VA)

- บริษัทจัดทำเอกสารสรุปมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ (Statement of Applicability)
- บริษัทปรับปรุงเอกสารสรุปมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ (Statement of Applicability)
- บริษัทนำเสนอเอกสารสรุปมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ (Statement of Applicability) ให้กับคณะทำงานพิจารณา
- บริษัทส่งเอกสารแผนจัดการความเสี่ยง (Risk Treatment Plan)
- บริษัทจัดทำรายงานผลการตรวจสอบช่องโหว่ทางเทคนิค (Vulnerability Assessment (VA)

3.2 งวดที่ 2 ชำระ 60% หลังสนับสนุนการตรวจรับรองระบบบริหารความมั่นคงปลอดภัยสารสนเทศจาก Certification Body (Surveillance Audit)

- บริษัทตรวจสอบ/ติดตาม การดำเนินการตามเกณฑ์วัดผลประสิทธิผลลัพธ์จากการปฏิบัติตามเกณฑ์ของมาตรฐาน ISO/IEC 27001:2022
- บริษัทดำเนินการเตรียมความพร้อมก่อนการตรวจสอบภายในของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ สำหรับศูนย์คอมพิวเตอร์
- บริษัทดำเนินการจัดประชุมเพื่อเตรียมความพร้อมก่อนการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ
- บริษัทดำเนินการสนับสนุนการตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Internal audit and Internal auditor supporting)
- บริษัทติดตามการดำเนินการปรับปรุงแก้ไขความไม่สอดคล้อง (Non-Conformity) ที่พบจากการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ

- บริษัทจัดประชุมร่วมกับคณะทำงานเพื่อติดตามการดำเนินการปรับปรุงแก้ไขความไม่สอดคล้อง (Non-Conformity) ที่พบจากการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ
- บริษัทดำเนินการสนับสนุนการเตรียมความพร้อมสำหรับการตรวจสอบ เพื่อขอใบรับรองในรอบการตรวจประเมินติดตามครั้งที่ 2 (2nd Surveillance Audit)
- บริษัทดำเนินการสนับสนุนการตรียมความพร้อมสำหรับการตรวจสอบเพื่อขอใบรับรองในรอบการตรวจประเมินติดตามครั้งที่ 2 (2nd Surveillance Audit) ทั้งทีมผู้ตรวจสอบ และทีมผู้รับตรวจ
- บริษัทดำเนินการสนับสนุนการตรวจรับรองระบบบริหารความมั่นคงปลอดภัยสารสนเทศจาก Certification Body เพื่อขอใบรับรองในรอบการตรวจประเมินติดตามครั้งที่ 2 (2nd Surveillance Audit)

4. การส่งมอบ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ต.คลองหก อ.ธัญบุรี จ.ปทุมธานี

ลงชื่อ..... ผู้กำหนดรายละเอียด
ผู้ช่วยศาสตราจารย์นิสิต ภูครองตา

ลงชื่อ .....
(รองศาสตราจารย์ ดร.อำนวย เรืองวารี)
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ