กณฑ์อ้างอิง (Terms of Reference)
การจ้างเหมาบริหารจัดทำแผนความมั่นคงปลอดภัยสารสนเทศ (Cyber Security)
สำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)

1. หลักการและเหตุผล

สำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) (สนช.) มีศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) อยู่ภายในอุทยานนวัตกรรม ใช้สำหรับจัดเก็บอุปกรณ์ระบบเครื่องแม่ข่าย (Server) ระบบเครือข่าย (Network) และระบบอุปกรณ์ความมั่งคงปลอดภัยสารสนเทศของสำนักงาน ซึ่งศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ไม่ได้ถูกออกแบบตามมาตราฐาน จึงอาจส่งผลกระทบต่อระดับความพร้อมในการให้บริการ (Service Availability) ซึ่งถือเป็นหนึ่งในปัจจัยเสี่ยงต่อความต่อเนื่องทางธุรกิจ (Business Continuity) และความมั่นคงปลอดภัยสารสนเทศ (Cyber Security)

งานเทคโนโลยีสารสนเทศ ฝ่ายยุทธศาสตร์นวัตกรรม จึงเห็นควรให้มีการจัดทำแผนความมั่นคงปลอดภัยสารสนเทศ (Cyber Security) สำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) เพื่อกำหนดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และเป็นแผนกลยุทธ์การพัฒนาระบบสารสนเทศและเครือข่ายของสำนักงาน โดยอ้างอิงจากความเสี่ยงของสำนักงาน ให้สอดคล้องกับมาตรฐานและแนวปฏิบัติที่ดีที่เป็นสากลทั้งในด้านเทคโนโลยีสารสนเทศและด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

2. วัตถุประสงค์

2.1 เพื่อทำการระบุระดับสถานภาพในปัจจุบันของกระบวนการ ขั้นตอนปฏิบัติ แผนการดำเนินงาน ตัวชี้วัดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของสำนักงาน ตามมาตรฐานและแนวปฏิบัติที่ดีในการรักษาความมั่นคงปลอดภัยที่เหมาะสมกับสำนักงาน

2.2 เพื่อระบุความเสี่ยง วิเคราะห์ผลกระทบ และโอกาสการเกิดความเสี่ยงของศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) รวมถึงการกำหนดมาตรการลดความเสี่ยง

2.3 เพื่อกำหนดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)

2.4 เพื่อจัดทำแผนกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) พร้อมเสนอแผนที่นำทาง (Roadmap) ในการพัฒนาโครงสร้างสถาปัตยกรรมความมั่นคงปลอดภัยสารสนเทศและแผนปฏิบัติงาน (Action Plan/Implementation Plan) ในระยะสั้น (3 ปี) ระยะกลาง (5 ปี) และระยะยาว (10 ปี)

3. คุณสมบัติของผู้รับจ้าง

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นนิติบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นนิติบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอราคารายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

3.10ไม่เป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนด

3.11ผู้เสนอราคาต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e-GP) กรมบัญชีกลาง

3.12ผู้เสนอราคาต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่ายหรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญตามที่คณะกรรมการ ป.ป.ช. กำหนด

3.13ผู้เสนอราคาซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องรับและจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจจ่ายเป็นเงินสดก็ได้ตามที่คณะกรรมการ ป.ป.ช. กำหนด

3.14ผู้รับจ้างต้องมีประสบการณ์และมีผลงานที่สัมพันธ์กับหัวข้อที่กำหนด โดยมีมูลค่าของผลงานไม่น้อยกว่า 1,600,000.-บาท (หนึ่งล้านหกแสนบาทถ้วน) โดยเป็นผลงานที่เป็นคู่สัญญาเดียวและทำสัญญาโดยตรงกับส่วนราชการหรือเอกชนที่เชื่อถือได้ โดยผู้เสนอราคาจะต้องส่งเอกสารหนังสือรับรองผลงานหรือสำเนาสัญญาหรือสำเนาใบสั่งซื้อ/สั่งจ้าง มาประกอบการพิจารณา

4. ขอบเขตของโครงการ

ผู้รับจ้างต้องดำเนินการจัดทำแผนความมั่นคงปลอดภัยสารสนเทศ (Cyber Security) สำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ดังนี้

4.1 ผู้รับจ้างต้องกำหนดแผนการดำเนินงาน (Work Plan) แต่ละขั้นตอนตลอดทั้งโครงการ และวิธีการทำงาน (Methodology) รวมถึงมาตรฐาน/เกณฑ์วัดที่จะใช้ในการจัดทำแผนความมั่นคงปลอดภัยสารสนเทศ (Cyber Security) และกำหนดผู้รับผิดชอบในการดำเนินงานแต่ละขั้นตอน ผลการดำเนินงานและการนำเสนอผลการดำเนินงานในแต่ละขั้นตอน

4.2 ผู้รับจ้างต้องดำเนินการวิเคราะห์และระบุระดับสถานภาพในปัจจุบันของกระบวนการ ขั้นตอนปฏิบัติ แผนการดำเนินงาน/เกณฑ์วัดที่ผู้รับจ้างเสนอ เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของสำนักงานเทียบกับมาตรฐานและแนวปฏิบัติที่ดีในการรักษาความมั่นคงปลอดภัย (Gap Analysis) พร้อมทั้งระบุประเด็นหลักที่ควรปรับปรุงรวมถึงข้อเสนอแนะในการเพิ่มประสิทธิภาพความมั่นคงปลอดภัยสารสนเทศ สำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)

4.3 ผู้รับจ้างต้องดำเนินการประเมินความเสี่ยง (Risk Assessment) สำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) พร้อมทั้งกำหนดแนวทางในการวัดและประเมินผลการปฏิบัติงานด้านการบริหารความเสี่ยง

4.4 ผู้รับจ้างต้องดำเนินการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (ICT Security Policy) สำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)

4.5 ผู้รับจ้างต้องดำเนินการจัดทำแผนกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) พร้อมนำเสนอแผนที่นำทาง (Roadmap) ในการพัฒนาโครงสร้างสถาปัตยกรรมความมั่นคงปลอดภัยสารสนเทศและแผนปฏิบัติงาน (Action Plan/Implementation Plan) ในระยะสั้น (3 ปี) ระยะกลาง (5 ปี) และระยะยาว (10 ปี)

4.6 ผู้รับจ้างต้องเข้าร่วมชี้แจงแผนความมั่นคงปลอดภัยสารสนเทศ (Cyber Security) สำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ที่ส่งมอบต่อผู้บริหารระดับสูง และฝ่ายงานที่เกี่ยวข้อง รวมทั้งจะต้องนำเสนอสรุปผลการดำเนินงานของโครงการต่อคณะกรรมการ/คณะอนุกรรมการของสำนักงานในชุดต่างๆ ที่เกี่ยวข้องตามความเหมาะสม โดยจัดเตรียมผู้เชี่ยวชาญเพื่อสนับสนุนข้อมูลรายละเอียดในเชิงลึก ตอบข้อซักถาม (ถ้ามี) ทุกครั้งที่มีการนำเสนอ

4.7 ผู้รับจ้างต้องมีประสบการณ์ในการดำเนินการวิเคราะห์ Gap Analysis ตามมาตรฐาน ISO/IEC 27001:2013 ประเมินความเสี่ยง จัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศ และแผนกลยุทธ์การพัฒนาความมั่นคงปลอดภัยสารสนเทศสำหรับศูนย์คอมพิวเตอร์ (Data Center) ให้กับหน่วยงานภาครัฐหรือเอกชน พร้อมทั้งได้รับการรับรองมาตรฐาน ความรู้ความสามารถ และความปลอดภัยสารสนเทศโดยหน่วยงานในระดับสากล โดยมีบุคลากรไม่น้อยกว่าดังนี้ ผู้จัดการโครงการ จำนวน 1 คน ที่ปรึกษาทางเทคนิค จำนวน 1 คน ที่ปรึกษา จำนวน 2 คน โดยมีคุณสมบัติดังนี้

ตำแหน่ง	คุณสมบัติ	จำนวนอย่างน้อย (คน)
ผู้จัดการโครงการ	- มีประสบการณ์บริหารโครงการด้านการทดสอบหรือการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ไม่น้อยกว่า 10 ปี - ได้รับใบรับรอง (Certificate) ด้านความมั่นคงปลอดภัยอย่างน้อย 3 ฉบับในรายการต่อไปนี้ - Certified Ethical Hacker (C|EH) - Certified Information Security Audit (CISA) – ISACA - Certified Information Security Manager (CISM) – ISACA	1

ตำแหน่ง	คุณสมบัติ	จำนวนอย่างน้อย (คน)
	- Certified Information Systems Security Professional (CISSP) – ISC2 - PECB ISO/IEC 27001:2013 Senior Lead Implementer - Certified Ethical Hacker (C|EH)	
ที่ปรึกษาทางเทคนิค	- มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศระบบเครือข่ายสื่อสารและความมั่นคงปลอดภัยคอมพิวเตอร์อย่างน้อย 2 ปี - ได้รับใบรับรอง (Certificate) ด้านความมั่นคงปลอดภัย CompTIA Security+ เป็นอย่างน้อย	1
ที่ปรึกษา	- มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศระบบเครือข่ายสื่อสารและความมั่นคงปลอดภัยคอมพิวเตอร์ อย่างน้อย 2 ปี - ได้รับใบรับรอง (Certificate) ด้านความมั่นคงปลอดภัย อย่างน้อย 2 ฉบับในรายการต่อไปนี้ - CompTIA Security+ - EC-Council Certified Ethical Hacking (CEH) - PECB ISO/IEC 27001:2013 Lead Implementer - IRCA ISO/IEC 27001:2013 Lead Auditor	2
รวมทั้งสิ้นไม่น้อยกว่า		**4**

5. คุณลักษณะเฉพาะ

ผู้รับจ้างต้องดำเนินการวิเคราะห์ Gap Analysis ตามมาตรฐาน ISO/IEC 27001:2013 ประเมินความเสี่ยง นโยบายความมั่นคงปลอดภัยสารสนเทศและนโยบายอื่นๆ ที่เกี่ยวข้อง และจัดทำกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) พร้อมนำเสนอแผนที่นำทาง (Roadmap) ในการพัฒนาโครงสร้างสถาปัตยกรรมความมั่นคงปลอดภัยสารสนเทศ ในระยะสั้น (3 ปี) ระยะกลาง (5 ปี) และระยะยาว (10 ปี) สำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ดังนี้

5.1 ผู้รับจ้างต้องเสนอแผนการดำเนินงาน ซึ่งมีรายละเอียดอย่างน้อยดังต่อไปนี้

5.1.1 ขอบเขตของการดำเนินงาน

5.1.2 ระยะเวลาดำเนินงาน โดยจะต้องระบุ วัน เวลา สถานที่และบุคลากรที่ดำเนินการ

5.1.3 วิธีการและขั้นตอนในการดำเนินการวิเคราะห์ Gap Analysis ตามมาตรฐาน ISO/IEC 27001:2013 ประเมินความเสี่ยง นโยบายความมั่นคงปลอดภัยสารสนเทศ และแผนกล

ยุทธ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)

5.1.4 รายละเอียดหน้าที่และความรับผิดชอบของบุคลากรในโครงการ

5.1.5 แผนผังของบุคลากรและช่องทางการติดต่อสื่อสารของผู้รับจ้าง

5.2 ผู้รับจ้างต้องดำเนินการวิเคราะห์ Gap Analysis ตามมาตรฐาน ISO/IEC 27001:2013 ประกอบด้วยกิจกรรม ดังนี้

5.2.1 ผู้รับจ้างต้องดำเนินการทบทวน วิสัยทัศน์ พันธกิจ วัตถุประสงค์ นโยบาย มาตรฐาน รวมทั้งแผนกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ของสำนักงาน

5.2.2 ผู้รับจ้างต้องศึกษากฎหมาย ระเบียบ ข้อบังคับ ที่เกี่ยวข้องกับสำนักงาน

5.2.3 ผู้รับจ้างต้องศึกษา ตรวจสอบศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ระบบเครือข่ายและระบบเครื่องแม่ข่ายคอมพิวเตอร์ รวมถึงระบบสารสนเทศที่มีอยู่

5.2.4 ผู้รับจ้างต้องศึกษามาตรฐานและแนวปฏิบัติที่ดีศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ที่เหมาะสมกับสำนักงาน ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของระบบเครือข่าย (Network) ระบบเครื่องแม่ข่ายคอมพิวเตอร์ (Server) แอพพลิเคชั่น (Application) โดยอ้างอิงตามมาตรฐาน ISO/IEC 27001:2013

5.2.5 ผู้รับจ้างต้องดำเนินการจัดทำ Gap Analysis ตามมาตรฐาน ISO/IEC 27001:2013 ทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงาน

5.2.6 ผู้รับจ้างต้องจัดทำรายงานสรุปผลการวิเคราะห์ Gap Analysis ตามมาตรฐาน ISO/IEC 27001:2013

5.3 ผู้รับจ้างต้องดำเนินการประเมินความเสี่ยง ประกอบด้วยกิจกรรม ดังนี้

5.3.1 ผู้รับจ้างต้องทบทวนหรือปรับปรุงหลักวิธีการประเมินความเสี่ยง (Risk Assessment Methodology) ตามแนวปฏิบัติ ISO/IEC 27005 หรือ ISO/IEC 31000

5.3.2 ผู้รับจ้างต้องให้คำปรึกษาและทำงานร่วมกับสำนักงาน จัดทำบัญชีรายการทรัพย์สิน (Asset Inventory) พร้อมระบุผู้เป็นเจ้าของความเสี่ยงของทรัพย์สินภายในสำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)

5.3.3 ผู้รับจ้างต้องให้คำปรึกษาและทำงานร่วมกับสำนักงาน ดำเนินการระบุปัจจัยเสี่ยงและผลกระทบต่อการสูญเสียด้านการรักษาความมั่นคงปลอดภัย (C-I-A) ตามหลักวิธีการประเมินความเสี่ยง

5.3.4 ผู้รับจ้างต้องให้คำปรึกษาและทำงานร่วมกับสำนักงานในการประเมิน (Risk Assessment) พร้อมทั้งจัดเตรียมเอกสารรายงานการประเมินความเสี่ยง (Risk Assessment Report)

5.3.5 ผู้รับจ้างต้องให้คำปรึกษาและทำงานร่วมกับสำนักงาน กำหนดทางเลือกที่เหมาะสมในการจัดการความเสี่ยงและกำหนดมาตรการควบคุมความเสี่ยงทั้งหมดที่จำเป็นเพื่อดำเนินการตามทางเลือกที่กำหนดไว้ (Risk Treatment Options)

5.3.6 ผู้รับจ้างต้องให้คำปรึกษาและทำงานร่วมกับสำนักงาน ดำเนินการในการวางแผนควบคุมความเสี่ยง (Risk Treatment Plan)

5.4 ผู้รับจ้างต้องดำเนินการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)

5.5 ผู้รับจ้างต้องนำเสนอผลการศึกษาของโครงการฯ ต่อผู้บริหารของสำนักงาน ในรูปแบบของเอกสารรายงานการศึกษาพร้อมทั้งเสนอแผนกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) พร้อมนำเสนอแผนที่นำทาง (Roadmap) ในการพัฒนาโครงสร้างสถาปัตยกรรมความมั่นคงปลอดภัยสารสนเทศ และแผนปฏิบัติงาน (Action Plan/Implementation Plan) ในระยะสั้น (3 ปี) ระยะกลาง (5 ปี) และระยะยาว (10 ปี)

6. ระยะเวลาดำเนินงาน

6.1. ต้องดำเนินการตามขอบเขตของงานแล้วเสร็จภายใน 6 เดือน นับถัดจากวันที่ลงนามในสัญญา

ลำดับที่	กิจกรรม	จำนวนเดือน		
		1	3	6
1	แผนการดำเนินงานจัดทำแผนความมั่นคงปลอดภัยสารสนเทศ	X		
2	- ศึกษา วิเคราะห์ Gap Analysis ตามมาตรฐาน ISO/IEC 27001:2013 - ทบทวนหรือปรับปรุงหลักวิธีการประเมินความเสี่ยงตามแนวปฏิบัติ ISO/IEC 27005 หรือ ISO/IEC 31000 - ตรวจสอบบัญชีรายการทรัพย์สิน (Asset Inventory) - จัดประเมินความเสี่ยงและจัดทำแผนควบคุมความเสี่ยง		X	
3	- กำหนดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) - จัดทำแผนกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) - จัดทำแผนที่นำทาง (Roadmap) ในการพัฒนาโครงสร้างสถาปัตยกรรมความมั่นคงปลอดภัยสารสนเทศและแผนปฏิบัติงาน (Action Plan/Implementation Plan) ในระยะสั้น (3 ปี) ระยะกลาง (5 ปี) และระยะยาว (10 ปี)			X

7. งบประมาณ

งบประมาณในการดำเนินการ 1,600,000.- บาท (หนึ่งล้านหกแสนบาทถ้วน) ซึ่งรวมภาษีมูลค่าเพิ่ม และภาษีเงินได้หัก ณ ที่จ่าย

8. ราคากลางและแหล่งที่มา

8.1 ราคากลาง 1,505,180.-บาท (หนึ่งล้านห้าแสนห้าพันหนึ่งร้อยแปดสิบบาทถ้วน)

8.2 แหล่งที่มาของราคากลาง

- บริษัท โกไฟว์ จำกัด
- บริษัท ไอเอสอีที (ประเทศไทย) จำกัด
- บริษัท อาร์ วี คอนเน็กซ์ จำกัด

9. ผลงานที่ต้องส่งมอบ

9.1 เอกสารแผนการดำเนินงาน รายละเอียดแผนประกอบด้วย กิจกรรม ช่วงเวลาดำเนินการ ผลลัพธ์ และผู้รับผิดชอบ

9.2 แผนความมั่นคงปลอดภัยสารสนเทศ (Cyber Security) สำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ที่ประกอบด้วยรายงานสรุปผลการวิเคราะห์ Gap Analysis

9.2.1 รายงานการทบทวนหรือปรับปรุงหลักวิธีการประเมินความเสี่ยง (Risk Assessment Methodology) ตามแนวปฏิบัติ ISO/IEC 27005 หรือ ISO/IEC 31000

9.2.2 บัญชีรายการทรัพย์สิน (Asset Inventory) พร้อมระบุผู้เป็นเจ้าของความเสี่ยงของทรัพย์สินภายในศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)

9.2.3 รายงานการประเมินความเสี่ยง (Risk Assessment Report) และแผนควบคุมความเสี่ยง (Risk Treatment Plan)

9.2.4 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ สำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)

9.2.5 แผนกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) พร้อม แผนที่นำทาง (Roadmap) ในการพัฒนาโครงสร้างสถาปัตยกรรมความมั่นคงปลอดภัยสารสนเทศและแผนปฏิบัติงาน (Action Plan/Implementation Plan) ในระยะสั้น (3 ปี) ระยะกลาง (5 ปี) และระยะยาว (10 ปี)

10 ค่าจ้างและวิธีการจ่ายค่าจ้าง

ผู้ว่าจ้างจะจ่ายเงินซึ่งเป็นเงินบาทโดยตรงให้แก่ผู้รับจ้าง โดยจะจ่ายค่าจ้างให้ภายหลังจากผู้รับจ้างได้ส่งมอบผลงานให้แก่คณะกรรมการตรวจรับพัสดุของผู้ว่าจ้าง และคณะกรรมการตรวจรับพัสดุได้ตรวจรับผลงานดังกล่าวเป็นที่เรียบร้อยแล้ว

โดยกำหนดการจ่ายค่าจ้าง จำนวน 3 (สาม) งวด ดังนี้

งวดที่ 1 กำหนดจ่ายเงินค่าจ้างร้อยละ 30 ของวงเงินจัดจ้าง เมื่อผู้รับจ้างส่งมอบงานการดำเนินการตามข้อ 9.1 ภายใน 1 เดือน นับถัดจากวันที่ลงนามในสัญญา และคณะกรรมการตรวจรับพัสดุได้ตรวจรับผลงานดังกล่าวเป็นที่เรียบร้อยแล้ว

งวดที่ 2 กำหนดจ่ายเงินค่าจ้างร้อยละ 40 ของวงเงินจัดจ้าง เมื่อผู้รับจ้างส่งมอบงานการดำเนินการตามข้อ 9.2.1 – 9.2.4 ภายใน 3 เดือน นับจากวันที่ลงนามในสัญญาและคณะกรรมการตรวจรับพสดุได้ตรวจรับผลงานดังกล่าวเป็นที่เรียบร้อยแล้ว

งวดที่ 3 (สุดท้าย) กำหนดจ่ายเงินค่าจ้างร้อยละ 30 ของวงเงินจัดจ้าง เมื่อผู้รับจ้างส่งมอบงานการดำเนินการ ตามข้อ 9.2.5 – 9.2.6 ภายใน 6 เดือน นับถัดจากวันที่ลงนามในสัญญาและคณะกรรมการตรวจรับพัสดุได้ตรวจรับผลงานดังกล่าวเป็นที่เรียบร้อยแล้ว

11. หลักเกณฑ์และสิทธิในการพิจารณา

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิคส์ครั้งนี้ สำนักงานพิจารณาตัดสินโดยใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance) และจะพิจารณาจากราคารวม

โดยพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนด ดังนี้

1) ราคาที่ยื่นเสนอ (Price) กำหนดน้ำหนักเท่ากับร้อยละ 20
2) ข้อเสนอทางด้านเทคนิคหรือข้อเสนออื่นๆ กำหนดน้ำหนักเท่ากับร้อยละ 80

12. หน่วยงานที่รับผิดชอบ

ฝ่ายยุทธศาสตร์นวัตกรรม
สำนักงานนวัตกรรมห่งชาติ (องค์การมหาชน)
โทร. 02 017 5555 ต่อ 627
โทรสาร 02 017 5566