ขอบเขตของงาน (Terms of Reference : TOR)
โครงการจ้างที่ปรึกษาพัฒนาแนวการกำกับดูแลผู้ให้บริการขนส่งทางรางและจัดทำมาตรการความมั่นคงปลอดภัยไซเบอร์ของกรมการขนส่งทางราง ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๑. ความเป็นมา

ด้วยนโยบายด้านการบริหารจัดการภาครัฐ และการผลักดันให้ประเทศไทยไปสู่ยุคดิจิทัลโดยการนำเทคโนโลยีเข้ามาช่วยในการบริหารจัดการ การสนับสนุนการทำงานรวมไปถึงการให้บริการกับประชาชน เพื่อความสะดวก รวดเร็ว และทันต่อเหตุการณ์ต่าง ๆ ทำให้มีการใช้งานอินเทอร์เน็ต ระบบงานต่าง ๆ อย่างแพร่หลาย ทั้งนี้ข้อมูลต่าง ๆ ของทางภาครัฐได้ถูกเข้าสู่ระบบโลกออนไลน์เป็นจำนวนมาก มีการแลกเปลี่ยน หมุนเวียน และส่งต่อข้อมูลดังกล่าวทุกเวลา อีกทั้งเทคโนโลยียังถูกนำมาใช้เป็นเครื่องมือในการก่อให้เกิดภัยคุกคามไซเบอร์ การก่อให้เกิดอาชญากรรมในรูปแบบที่หลากหลาย การบริหารจัดการข้อมูล การป้องกันเพื่อไม่ให้ข้อมูลที่เป็นความลับและข้อมูลที่สำคัญเพื่อไม่ให้ข้อมูลรั่วไหล กระทำการเพื่อให้เกิดความเสียหายที่ไม่สามารถประเมินค่าได้ หน่วยงานภาครัฐซึ่งเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศเมื่อนำเทคโนโลยีมาใช้ในการขับเคลื่อนองค์กร จึงไม่อาจละเลยกับภัยคุกคามด้านไซเบอร์ รวมถึงการปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

กรมการขนส่งทางราง (ขร.) ในฐานะหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศด้านการให้บริการขนส่งทางราง ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๕ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ดังนี้

มาตรา ๔๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง อย่างน้อยต้องประกอบด้วยเรื่อง ดังต่อไปนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมินผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์

เพื่อประโยชน์ในการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง ให้สำนักงานโดยความเห็นชอบของคณะกรรมการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานดังกล่าวยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ

กรมการขนส่งทางราง

มาตรา ๔๕ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) ด้วย

ในกรณีที่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่อาจดำเนินการหรือปฏิบัติตามวรรคหนึ่งได้ สำนักงานอาจให้ความช่วยเหลือด้านบุคลากรหรือเทคโนโลยีแก่หน่วยงานนั้นตามที่ร้องขอได้

มาตรา ๕๓ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตนหากพบว่าหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่ได้มาตรฐาน ให้หน่วยงานควบคุมหรือกำกับดูแลนั้นรีบแจ้งให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ต่ำกว่ามาตรฐานแก้ไขให้ได้มาตรฐานโดยเร็วหากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นยังคงเพิกเฉยไม่ดำเนินการหรือไม่ดำเนินการให้แล้วเสร็จภายในระยะเวลาที่หน่วยงานควบคุมหรือกากับดูแลกำหนด ให้หน่วยงานควบคุมหรือกำกับดูแลส่งเรื่องให้ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) พิจารณาโดยไม่ชักช้า

เมื่อได้รับคำร้องเรียนตามวรรคหนึ่ง หาก กกม. พิจารณาแล้วเห็นว่า มีเหตุดังกล่าวและอาจทำให้เกิดภัยคุกคามทางไซเบอร์ ให้ กกม. ดำเนินการ ดังต่อไปนี้

(๑) กรณีเป็นหน่วยงานของรัฐ ให้แจ้งต่อผู้บริหารระดับสูงสุดของหน่วยงานเพื่อใช้อำนาจในทางบริหารสั่งการไปยังหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น เพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว

(๒) กรณีเป็นหน่วยงานเอกชน ให้แจ้งไปยังผู้บริหารระดับสูงสุดของหน่วยงาน ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นเพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว ให้เลขาธิการดำเนินการติดตามเพื่อให้เป็นไปตามความในวรรคสองด้วย

มาตรา ๕๔ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง

ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ

มาตรา ๕๖ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องกำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแลและตามประมวลแนวทางปฏิบัติ รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการหรือ กกม. กำหนด และต้องเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

มาตรา ๕๗ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ ๔ ทั้งนี้ กกม. อาจกำหนดหลักเกณฑ์และวิธีการการรายงานด้วยก็ได้

ดังนั้น ขร. จึงจำเป็นต้องจ้างที่ปรึกษาเพื่อวิเคราะห์ จัดทำมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สอดรับกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยที่ปรึกษาจะทำการวิเคราะห์บริบทขององค์กรตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อนำไปจัดทำ หรือปรับปรุงนโยบายความมั่นคงปลอดภัยไซเบอร์ของ ขร. พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงแนวทางในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ ขร. มีนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ และโครงสร้างการดำเนินงาน เพื่อป้องกัน และพร้อมรับมือกับภัยความมั่นคงปลอดภัยไซเบอร์ และจำเป็นต้องดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในมาตรา ๕๓ ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อขับเคลื่อนการดำเนินงานให้บรรลุผลสำเร็จตามพันธกิจขององค์กร ในการนี้ เพื่อยกระดับการกำกับดูแลการขนส่งทางรางให้เป็นไปตามกฎหมาย กฎระเบียบ มีคุณภาพ การให้บริการที่ดี และปฏิบัติงานตามหลักธรรมาภิบาล จัดทำ หรือปรับปรุงแนวทางการกำหนดมาตรฐานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้สอดคล้องกับบริบทของอุสาหกรรมการขนส่งทางราง พร้อมทั้งพัฒนาแบบตรวจประเมินแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงสำรวจความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางรางภายใต้การกำกับดูแลของ ขร. และจัดทำรายงานสรุปความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. วิเคราะห์ ปรับปรุงมาตรการด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้สอดรับกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยวิเคราะห์บริบทขององค์กรตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อนำไปจัดทำ หรือปรับปรุงนโยบายความมั่นคงปลอดภัยไซเบอร์ของ ขร. พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงแนวทางในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ ขร. มีนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ และโครงสร้างการดำเนินงาน เพื่อป้องกัน และพร้อมรับมือกับภัยความมั่นคงปลอดภัยไซเบอร์

๒. วัตถุประสงค์

๒.๑ ศึกษาและวิเคราะห์บริบทขององค์กร ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และที่เกี่ยวข้อง

๒.๒ ศึกษาและวิเคราะห์ข้อกำหนดตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และข้อกำหนดอื่น ๆ เพื่อจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ทางราง ให้สอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

๒.๓ จัดทำประมวลแนวทางปฏิบัติ (แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์) และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

๒.๔ จัดทำมาตรฐานขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๕ ดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ตามมาตรฐานขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กรมการขนส่งทางราง

๓. คุณสมบัติของที่ปรึกษา

๓.๑ ที่ปรึกษาต้องมีคุณสมบัติอย่างน้อยดังนี้

๓.๑.๑ มีความสามารถตามกฎหมาย

๓.๑.๒ ไม่เป็นบุคคลล้มละลาย

๓.๑.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๑.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๑.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๑.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๑.๗ เป็นบุคคลธรรมดาหรือนิติบุคคลที่มีอาชีพรับจ้างงานดังกล่าว

๓.๑.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับที่ปรึกษารายอื่นที่เข้ายื่นข้อเสนอให้แก่ ขร. ณ วันที่ได้รับประกาศเชิญชวนหรือหนังสือเชิญชวนให้เข้ามายื่นข้อเสนอจากหน่วยงานของรัฐหรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการยื่นข้อเสนอในครั้งนี้

๓.๑.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

๓.๑.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติ ดังนี้

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

๓.๑.๑๑ ที่ปรึกษาที่จะเข้าร่วมการเสนองานกับหน่วยงานของรัฐ ต้องเป็นที่ปรึกษาที่ได้ขึ้นทะเบียนไว้กับศูนย์ข้อมูลที่ปรึกษา กระทรวงการคลัง

๓.๑.๑๒ คุณสมบัติอื่น ๆ เช่น ไม่เป็นผู้ถูกพิทักษ์ทรัพย์เด็ดขาดหรือฟื้นฟูกิจการ

๓.๒ ต้องมีผู้จัดการโครงการเป็นคนไทยและ/หรือรองผู้จัดการโครงการ ปฏิบัติงานรับผิดชอบบริหารจัดการตลอดระยะเวลาการดำเนินโครงการ ส่วนบุคลากรหลักตำแหน่งอื่นสามารถจัดหามาเพื่อปฏิบัติงานตามแผนปฏิบัติงานที่ ขร. ให้ความเห็นชอบ

๓.๓ บุคลากรหลักในแต่ละตำแหน่งที่ได้เสนอชื่อในโครงการแต่ละรายจะต้องลงนามรับรองความถูกต้องในเอกสารประวัติการทำงานของตนเอง โดยให้ถือว่าที่ปรึกษาได้รับรองว่าบุคลากรหลักทุกรายได้ลงนามด้วยตนเอง เพื่อยืนยันการร่วมงานในโครงการนี้ หากบุคลากรหลักรายใดมิได้ลงนามด้วยตนเอง ขร. จะไม่พิจารณาบุคลากรหลักในรายที่เสนอนั้น

๓.๔ ที่ปรึกษาต้องแสดงแผนการทำงานของบุคลากรหลัก กรณีบุคลากรหลักของที่ปรึกษาเป็นคนต่างด้าว เมื่อจะปฏิบัติงานจะต้องได้รับอนุญาตให้ทำงานได้ในราชอาณาจักรไทยตามนัยกฎหมายว่าด้วยการทำงานของคนต่างด้าว

๓.๕ บุคลากรหลักของที่ปรึกษาต้องมีระยะเวลาปฏิบัติงานไม่ซ้ำซ้อนกับงานในโครงการอื่น ๆ ของที่ปรึกษาที่ดำเนินการในช่วงเวลาเดียวกัน หาก ขร. พบว่าบุคลากรหลักไม่ว่าคนใดคนหนึ่งหรือหลายคนปฏิบัติงานซ้ำซ้อนกับงานในโครงการอื่น ๆ ไม่ว่าจะพบในระหว่างปฏิบัติงานตามสัญญาหรือในภายหลัง ขร. มีสิทธิ์บอกเลิกสัญญาและ/หรือเรียกค่าเสียหายจากที่ปรึกษาหรือปรับลดค่าจ้างได้

๔. ขอบเขตของงานจ้างที่ปรึกษา

ขอบเขตของงานประกอบด้วย ๔ ส่วน โดยมีรายละเอียดของงาน ดังนี้

๔.๑ งานส่วนที่ ๑ ศึกษา รวบรวม วิเคราะห์หลักเกณฑ์ มาตรฐาน และข้อมูลการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

ศึกษา รวบรวม วิเคราะห์หลักเกณฑ์ มาตรฐาน และข้อมูลการดำเนินงานด้าน Cybersecurity ตามมาตรฐานสากลของระบบการขนส่งทางราง ที่มีข้อมูลหรืองานวิจัยในปัจจุบันทั้งในประเทศและต่างประเทศอย่างน้อย ๗ ประเทศ เช่น ประเทศไทย ประเทศญี่ปุ่น ประเทศอินเดีย สาธารณรัฐประชาชนจีน สหรัฐอเมริกา สหพันธรัฐรัสเซีย และประเทศในกลุ่มสหภาพยุโรป หรือตามที่ ขร. กำหนด ตามกรอบมาตรฐานยกตัวอย่าง ดังนี้

๑) มาตรฐานสากล ISO/IEC ๒๗๐๐๑ : ๒๐๒๒ มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ Information Security Management System (ISMS)

๒) มาตรฐาน National Institute of Standards and Technology (NIST) Cybersecurity Framework (กรอบการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ)

๓) มาตรฐาน IEC ๖๒๔๔๓ มาตรฐานเกี่ยวข้องกับการวิเคราะห์ ประเมิน และทดสอบ เพื่อควบคุม ด้านเทคโนโลยีสารสนเทศที่เหมาะสม

๔) มาตรฐาน Control Objectives for information and Related Technology (COBIT) กรอบมาตราฐานด้านการกำกับดูแลและการบริหารจัดการระบบสารสนเทศระดับองค์กร

๕) มาตรฐาน Information Technology Infrastructure Library (ITIL) กรอบการบริหารจัดการ IT service Management (ITSM)

๖) มาตรฐานที่เกี่ยวข้องกับ (Cybersecurity in Railway) หรือมาตรฐานอื่น ๆ ที่เกี่ยวข้อง

๔.๒ งานส่วนที่ ๒ จัดทำมาตรการความมั่นคงปลอดภัยไซเบอร์ของ ขร.

จัดทำมาตรการความมั่นคงปลอดภัยไซเบอร์ของ ขร. โดยมีรายละเอียดอย่างน้อย ดังนี้

๔.๒.๑ ศึกษาและวิเคราะห์บริบทขององค์กรด้านความมั่นคงปลอดภัยไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงกฎหมายด้านไซเบอร์ และกฎกระทรวงที่เกี่ยวข้องกับ ขร. รวบรวมพร้อมจัดทำเล่มรายงานสรุปผลการศึกษาและวิเคราะห์ด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร

๔.๒.๒ ศึกษาและวิเคราะห์สถานะปัจจุบันของการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ของ ขร. ประเมินความพร้อมด้านไซเบอร์ (GAP Analysis) ของ ขร. ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และบริบทขององค์กรด้านความมั่นคงปลอดภัยไซเบอร์

๔.๒.๓ จัดทำรายงานผลประเมินความพร้อมด้านไซเบอร์ของ ขร. รวมถึงให้ข้อเสนอแนะที่เป็นประโยชน์ ในการปรับปรุงกระบวนการภายในและเตรียมความพร้อมให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และบริบทขององค์กรด้านความมั่นคงปลอดภัยไซเบอร์

๔.๒.๔ จัดทำนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร. (พ.ศ. ๒๕๖๙-๒๕๗๓) โดยทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ขร. (Information Security Policy) ที่มีอยู่ในปัจจุบัน หรือจัดทำนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร. (พ.ศ. ๒๕๖๙-๒๕๗๓) ขึ้นใหม่ โดยเนื้อหาให้เกิดการบูรณาการระหว่างกันอย่างน้อยประกอบด้วย แผนงานโครงการ และรายละเอียดโครงการ เช่น วัตถุประสงค์ ประโยชน์ที่คาดว่าจะได้รับ ระยะเวลา ตัวชี้วัด ผลลัพธ์ และจัดลำดับความสำคัญของโครงการ

๔.๒.๕ จัดทำโครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับ ขร. ครอบคลุมถึงการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ภายใน ขร. และการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง เพื่อสนับสนุนศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๔.๒.๖ จัดทำรายงานการกำหนดผู้รับผิดชอบและบทบาทหน้าที่ในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นแนวทางให้กับ ขร. ครอบคลุมถึงการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ภายใน ขร. และการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ประกอบด้วยหัวข้ออย่างน้อย ดังนี้

๔.๒.๖.๑ ผู้รับผิดชอบและบทบาทหน้าที่

๔.๒.๖.๒ คุณสมบัติที่เหมาะสม

๔.๒.๖.๓ อำนาจในการดำเนินการ สั่งการ และอนุมัติ

๔.๒.๗ จัดทำแนวปฏิบัติในการบริหารความเสี่ยง (Risk Management) ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นแนวทางในการบริหารจัดการความเสี่ยงด้านไซเบอร์ ประกอบด้วยหัวข้ออย่างน้อย ดังนี้

๔.๒.๗.๑ การรวบรวมและประเมินความสำคัญทรัพย์สิน

๔.๒.๗.๒ การระบุภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ

๔.๒.๗.๓ การระบุช่องโหว่ความมั่นคงปลอดภัยสารสนเทศ

๔.๒.๗.๔ การระบุมาตรการควบคุมปัจจุบัน

๔.๒.๗.๕ ประเมินโอกาสเกิดเหตุการณ์

๔.๒.๗.๖ การวิเคราะห์ผลกระทบความมั่นคงปลอดภัยสารสนเทศ

๔.๒.๗.๗ การคำนวนระดับความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ

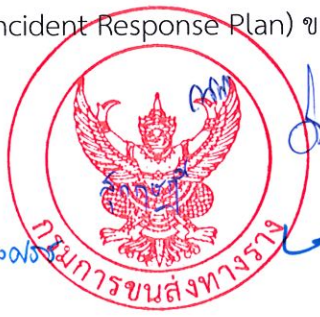
๔.๒.๗.๘ หลักเกณฑ์การเลือกตอบสนองต่อความเสี่ยงที่ครอบคลุม

๔.๒.๗.๙ แบบฟอร์มการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สามารถคำนวนผลระดับความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์

๔.๒.๘ จัดทำแนวปฏิบัติสำหรับการจัดทำสรุปรายงานการบริหารความเสี่ยง (Risk Management) ด้านความมั่นคงปลอดภัยไซเบอร์ และสรุปรายงานผลการตรวจสอบ (Audit) ด้านความมั่นคงปลอดภัยไซเบอร์ของ ขร. ตามมาตรา ๕๔ ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๔.๒.๙ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร. ให้สอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ที่จัดทำขึ้น ตามมาตรา ๔๔ ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๔.๒.๑๐ จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) ของ ขร. เพื่อกำหนดกระบวนการปฏิบัติงานหากเกิดภัยคุกคามทางไซเบอร์



๔.๓ งานส่วนที่ ๓ จัดทำแนวการกำกับดูแลผู้ให้บริการขนส่งทางราง

จัดทำมาตรฐานสำหรับบริการซึ่งเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศการขนส่งทางราง และสำรวจความพร้อมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. และจัดทำแนวปฏิบัติ เครื่องมือ และจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ให้บริการขนส่งทางราง ภายใต้กำกับของ ขร. โดยมีรายละเอียดอย่างน้อย ดังนี้

๔.๓.๑ พัฒนาแบบตรวจประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. (Audit Form) ที่ครอบคลุมถึงหัวข้อ อย่างน้อยประกอบด้วย

๔.๓.๑.๑ แนวทางการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔.๓.๑.๒ แนวทางการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

๔.๓.๑.๓ แผนการรับมือภัยคุกคามทางไซเบอร์

๔.๓.๑.๔ มาตรการหรือแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๔.๓.๒ ดำเนินการสำรวจความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. พร้อมทั้งจัดทำรายงานสรุปความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. ไม่น้อยกว่า ๑ ครั้ง อย่างน้อย ๔ ราย

๔.๓.๓ ดำเนินการเข้าตรวจประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. พร้อมทั้งจัดทำสรุปรายงานผลการตรวจสอบ (Audit) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. ไม่น้อยกว่า ๑ ครั้ง อย่างน้อย ๔ ราย

๔.๓.๔ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. ให้สอดคล้องกับมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ โดยมีการกำหนดคุณลักษณะให้แก่ข้อมูลหรือระบบสารสนเทศ และการจำแนกหมวดหมู่ภัยคุกคาม

๔.๓.๕ จัดทำแผนปฏิบัติการและกำกับดูแลผู้ให้บริการขนส่งทางราง (พ.ศ. ๒๕๖๙-๒๕๗๓) ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พร้อมทั้งให้ข้อเสนอแนะที่เป็นประโยชน์ในการดำเนินการตามแผนปฏิบัติการและกำกับดูแลผู้ให้บริการขนส่งทางราง (พ.ศ. ๒๕๖๙-๒๕๗๓) ให้ได้ประสิทธิผลตามที่กำหนด

๔.๓.๖ จัดทำมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของระบบการขนส่งทางราง (Cybersecurity in Railway) โดยทบทวนร่าง มขร. มาตรฐานความมั่นคงปลอดภัยไซเบอร์ของระบบการขนส่งทางราง (Cybersecurity in Railway) ที่มีอยู่ในปัจจุบัน หรือจัดทำมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของระบบการขนส่งทางราง (Cybersecurity in Railway) ขึ้นใหม่ เพื่อกำหนดมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ให้บริการขนส่งทางรางภายใต้การกำกับดูแลของ ขร. โดยเนื้อหาให้เกิดการบูรณาการระหว่างกัน

๔.๓.๗ จัดหาเครื่องแม่ข่ายแบบที่ ๑ และระบบจัดเก็บฐานข้อมูลพร้อมติดตั้งระบบบนเครื่องแม่ข่ายและจัดให้มีการทดสอบระบบ พร้อมทั้งนำเข้าข้อมูล เพื่อจัดเก็บข้อมูลการติดตามการปฏิบัติของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. ตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของระบบการขนส่งทางราง (Cybersecurity in Railway) ในรูปแบบ Web Application ระยะเวลาอย่างน้อย ๑ ปี นับถัดจากวันที่ผ่านการตรวจรับงานงวดสุดท้ายเรียบร้อยแล้ว โดยมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๔.๓.๗.๑ ระบบประมวลข้อมูลแนวทางปฏิบัติและกรอบมาตรฐาน (Guidelines and framework)

(๑) สามารถ Upload ไฟล์เอกสารเข้าระบบ

(๒) สามารถจัดเก็บเวอร์ชันเอกสาร

(๓) สามารถระบุรายละเอียดของเอกสาร เช่น ผู้จัดทำ ผู้อนุมัติ วันประกาศใช้

(๔) สามารถจัดเก็บข้อมูลการรับฟังความคิดเห็น

(๕) สามารถสร้างเอกสารเผยแพร่ทางอิเล็กทรอนิกส์โดยแบ่งหมวดหมู่หัวข้อให้ผู้อ่านสามารถเข้าใจได้โดยง่าย

๔.๓.๗.๒ ระบบประเมินผลความสอดคล้อง (Conformance Audit and Assessment)

(๑) สามารถสร้างรายการประเมินความสอดคล้องจากเอกสารเผยแพร่ทางอิเล็กทรอนิกส์

(๒) สามารถอนุมัติรายการประเมินความสอดคล้องที่สร้างขึ้น

(๓) สามารถกำหนดวันเวลาที่อนุญาติให้นำข้อมูลเข้ารายการประเมินความสอดคล้อง

(๔) สามารถแบ่งแยกผู้ใช้งานระบบได้ เช่น ผู้ใช้จากบุคลากรของ ขร. ผู้ใช้จากผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร.

(๕) สามารถนำเสนอข้อมูลสรุปออกมาในรูปแบบ Dashboard

๔.๔ งานส่วนที่ ๔ การจัดประชุม ฝึกอบรม สัมมนา และประชาสัมพันธ์

๔.๔.๑ จัดฝึกอบรมให้บุคลากรของ ขร. ตามหลักสูตรอย่างน้อย ดังนี้

ลำดับ	หลักสูตร	จำนวนวัน (อย่างน้อย)	จำนวนคน (อย่างน้อย)
๔.๔.๑.๑	ข้อกำหนดตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒	๑ วัน	๑๐ คน
๔.๔.๑.๒	แนวปฏิบัติและกรอบมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์	๑ วัน	๑๐ คน
๔.๔.๑.๓	มาตรฐานสากลด้านความมั่นคงปลอดภัยไซเบอร์	๑ วัน	๑๐ คน
๔.๔.๑.๔	สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์	๓ ชั่วโมง	๖๐ คน
๔.๔.๑.๕	จัดหาหลักสูตรอบรม วุฒิบัตรผู้ตรวจสอบระบบสารสนเทศ ๒๗๐๐๑ ISO/IEC ๒๗๐๐๑:๒๐๒๒ Lead Auditor*	๕ วัน	๕ คน

หมายเหตุ: * หลักสูตรลำดับที่ ๔.๔.๑.๕ หรือหลักสูตรอื่นตามที่ ขร. กำหนด

ที่ปรึกษาต้องจัดทำแผนการฝึกอบรมหลักสูตร โดยมีรายละเอียดอย่างน้อย ได้แก่ วัตถุประสงค์ หัวข้อการฝึกอบรม วิธีการฝึกอบรม ระยะเวลาการฝึกอบรม สถานที่ฝึกอบรม และรายละเอียดอื่น ๆ (ถ้ามี)

๔.๔.๒ จัดประชุมสรุปผลการดำเนินโครงการ และความเชื่อมโยงกับรายงานผลการประเมินความมั่นคงปลอดภัยไซเบอร์ (NCSA SPA – Full Report) ให้กับบุคลากรของ ขร. จำนวน ๑ ครั้ง มีผู้เข้าร่วมไม่น้อยกว่า ๓๐ คน

๔.๔.๓ จัดอบรมการใช้งานระบบฐานข้อมูลสำหรับจัดเก็บข้อมูลการติดตามการปฏิบัติตามมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ดูแลระบบ จำนวนไม่น้อยกว่า ๑ ครั้ง มีผู้เข้าร่วมไม่น้อยกว่า ๑๐ คน

กรมการขนส่งทางราง

๔.๔.๔ จัดประชุมกลุ่มย่อย (Focus Group) สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. ตามหัวข้อ ดังนี้

ลำดับ	หลักสูตร	จำนวนวัน (อย่างน้อย)	จำนวนคน (อย่างน้อย)
๔.๔.๔.๑	แบบตรวจประเมินแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๑ วัน	๒๐ คน
๔.๔.๔.๒	ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์	๑ วัน	๒๐ คน
๔.๔.๔.๓	มาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร.	๑ วัน	๒๐ คน

๔.๔.๕ จัดประชุมเผยแพร่แนวทางการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และอบรมการใช้งานระบบฐานข้อมูลสำหรับจัดเก็บข้อมูลการติดตามการปฏิบัติตามมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีผู้เข้าร่วมไม่น้อยกว่า ๕๐ คน พร้อมทั้งจัดทำสื่อประชาสัมพันธ์อย่างน้อย ดังนี้

๑) บอร์ดนิทรรศการขนาด ๐.๘๐ x ๒.๐๐ เมตร ชนิดไวนิลทึบแสง จำนวน ๒ ชุด

๒) บอร์ดประชาสัมพันธ์ขนาด ๔.๐๐ x ๒.๐๐ เมตร ชนิดไวนิลทึบแสง จำนวน ๑ ชุด

๔.๔.๖ จัดทำสื่อประชาสัมพันธ์ ในรูปแบบ Infographic เกี่ยวกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. จำนวนไม่น้อยกว่า ๔ ชิ้นงาน

๔.๔.๗ จัดทำสื่อประชาสัมพันธ์ ในรูปแบบ วีดีทัศน์ หรือ Vlog เกี่ยวกับประมวลแนวทางปฏิบัติกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ และมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. จำนวนไม่น้อยกว่า ๒ ชิ้นงาน ความยาวชิ้นงานละไม่น้อยกว่า ๓ นาที พากย์ภาษาไทย และคำบรรยาย (Subtitle) ภาษาไทยและภาษาอังกฤษ

๕. กำหนดเวลาแล้วเสร็จของงานจ้างที่ปรึกษา

ระยะเวลาดำเนินการ ๖๖๐ วัน นับถัดจากวันลงนามในสัญญา

๖. ผลงานที่จะต้องส่งมอบ

ผลงานที่จะต้องส่งมอบและงวดงานที่ส่งมอบมีรายละเอียด ดังนี้

งวดงาน	งานที่จะส่งมอบ	กำหนดส่งมอบ
งวดงานที่ ๑	๑. รายงานเบื้องต้น (Inception Report) จำนวน ๑๐ ชุด โดยแสดงรายละเอียดการเนินงานโครงการ ระยะเวลาดำเนินงาน วิธีการเก็บรวบรวมข้อมูล อย่างน้อยประกอบด้วย ๑.๑ แผนการดำเนินงานโครงการ (Project Plan) ๑.๒ สรุปผลการจัดฝึกอบรมหลักสูตร สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (ตามข้อ ๔.๔.๑.๔) ๑.๓ สรุปผลการจัดฝึกอบรมหลักสูตร วุฒิบัตรผู้ตรวจสอบระบบสารสนเทศ ๒๗๐๐๑ ISO/IEC ๒๗๐๐๑:๒๐๒๒ Lead Auditor (ตามข้อ ๔.๔.๑.๕) (ถ้ามี) ๒. รายงานและเอกสาร ในลักษณะ Digital Report อยู่ใน USB Flash drive ขนาดความจุไม่น้อยกว่า ๑๒๘ GB จำนวน ๑ ชุด	ภายใน ๓๐ วันนับถัดจากวันลงนามในสัญญา

งวดงาน	งานที่จะส่งมอบ	กำหนดส่งมอบ
งวดงานที่ ๒	๑. รายงานความก้าวหน้า (Progress Report) ฉบับที่ ๑ จำนวน ๑๐ ชุด อย่างน้อยประกอบด้วย ๑.๑ ผลการศึกษา รวบรวม วิเคราะห์หลักเกณฑ์ มาตรฐาน และข้อมูลการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) (ตามข้อ ๔.๑) ๑.๒ ผลการศึกษาและวิเคราะห์บริบทขององค์กรด้านความมั่นคงปลอดภัยไซเบอร์ (ตามข้อ ๔.๒.๑) ๑.๓ ผลประเมินความพร้อมด้านไซเบอร์ของ ขร. (ตามข้อ ๔.๒.๓) ๑.๔ นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร. (พ.ศ. ๒๕๖๙-๒๕๗๓) (ตามข้อ ๔.๒.๔) ๒. รายงานและเอกสาร ในลักษณะ Digital Report อยู่ใน USB Flash drive ขนาดความจุไม่น้อยกว่า ๑๒๘ GB จำนวน ๑ ชุด	ภายใน ๑๒๐ วันนับถัดจากวันลงนามในสัญญา
งวดงานที่ ๓	๑. รายงานความก้าวหน้า (Progress Report) ฉบับที่ ๒ จำนวน ๑๐ ชุด อย่างน้อยประกอบด้วย ๑.๑ ผลการประเมินความพร้อมด้านไซเบอร์ (GAP Analysis) ของ ขร. (ตามข้อ ๔.๒.๒) ๑.๒ โครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (ตามข้อ ๔.๒.๕) ๑.๓ รายงานการกำหนดผู้รับผิดชอบและบทบาทหน้าที่ (ตามข้อ ๔.๒.๖) ๑.๔ แนวปฏิบัติในการบริหารความเสี่ยง (Risk Management) ด้านความมั่นคงปลอดภัยไซเบอร์ (ตามข้อ ๔.๒.๗) ๑.๕ แนวปฏิบัติสำหรับการจัดทำสรุปรายงานการบริหารความเสี่ยง (Risk Management) ด้านความมั่นคงปลอดภัยไซเบอร์ (ตามข้อ ๔.๒.๘) ๒. รายงานและเอกสาร ในลักษณะ Digital Report อยู่ใน USB Flash drive ขนาดความจุไม่น้อยกว่า ๑๒๘ GB จำนวน ๑ ชุด	ภายใน ๒๕๐ วันนับถัดจากวันลงนามในสัญญา
งวดงานที่ ๔	๑. รายงานฉบับกลาง (Interim Report) จำนวน ๑๐ ชุด อย่างน้อยประกอบด้วย ๑.๑ สรุปรายงานผลการตรวจสอบ (Audit) ด้านความมั่นคงปลอดภัยไซเบอร์ของ ขร. (ตามข้อ ๔.๒.๘) ๑.๒ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร. (ตามข้อ ๔.๒.๙) ๑.๓ แผนรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) ของ ขร. (ตามข้อ ๔.๒.๑๐) ๑.๔ ผลการฝึกอบรม ให้แก่บุคลากรของ ขร. (ตามข้อ ๔.๔.๑) จำนวน ๕ หลักสูตร ๑.๕ สรุปผลการจัดประชุมกลุ่มย่อย (Focus Group) (ตามข้อ ๔.๔.๔) โดยประกอบด้วยหัวข้อ ดังนี้ - แบบตรวจประเมินแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ - มาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. ๒. รายงานและเอกสาร ในลักษณะ Digital Report อยู่ใน USB Flash drive ขนาดความจุไม่น้อยกว่า ๑๒๘ GB จำนวน ๑ ชุด	ภายใน ๓๓๐ วันนับถัดจากวันลงนามในสัญญา
งวดงานที่ ๕	๑. รายงานความก้าวหน้า (Progress Report) ฉบับที่ ๓ จำนวน ๑๐ ชุด อย่างน้อยประกอบด้วย ๑.๑ แบบตรวจประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ตามข้อ ๔.๓.๑) ๑.๒ สรุปความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. (ตามข้อ ๔.๓.๒) ๑.๓ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. (ตามข้อ ๔.๓.๔) ๑.๔ แผนปฏิบัติการและกำกับดูแลผู้ให้บริการขนส่งทางราง (พ.ศ. ๒๕๖๙-๒๕๗๓) (ตามข้อ ๔.๓.๕)	ภายใน ๔๕๐ วันนับถัดจากวันลงนามในสัญญา

งวดงาน	งานที่จะส่งมอบ	กำหนดส่งมอบ
	๒. รายงานและเอกสาร ในลักษณะ Digital Report อยู่ใน USB Flash drive ขนาดความจุไม่น้อยกว่า ๑๒๘ GB จำนวน ๑ ชุด	
งวดงานที่ ๖	๑. รายงานความก้าวหน้า (Progress Report) ฉบับที่ ๔ จำนวน ๑๐ ชุด อย่างน้อยประกอบด้วย ๑.๑ สรุปรายงานผลการตรวจสอบ (Audit) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ตามข้อ ๔.๓.๓) ๑.๒ มาตรฐานความมั่นคงปลอดภัยไซเบอร์ของระบบการขนส่งทางราง (Cybersecurity in Railway) (ตามข้อ ๔.๓.๖) ๑.๓ สรุปผลการติดตั้งเครื่องแม่ข่ายและการใช้งานระบบจัดเก็บฐานข้อมูลการติดตามการปฏิบัติของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. (ตามข้อ ๔.๓.๗) ๑.๔ สื่อประชาสัมพันธ์ ในรูปแบบ Infographic (ตามข้อ ๔.๔.๖) ๑.๕ สื่อประชาสัมพันธ์ ในรูปแบบ วีดีทัศน์ หรือ Vlog (ตามข้อ ๔.๔.๗) ๒. รายงานและเอกสาร ในลักษณะ Digital Report อยู่ใน USB Flash drive ขนาดความจุไม่น้อยกว่า ๑๒๘ GB จำนวน ๑ ชุด	ภายใน ๕๗๐ วันนับถัดจากวันลงนามในสัญญา
งวดงานที่ ๗	๑. ร่างรายงานฉบับสมบูรณ์ (Draft Final Report) จำนวน ๑๐ ชุด ๒. ร่างรายงานสรุปสำหรับผู้บริหาร (Draft Executive Summary Report) จำนวน ๑๐ ชุด ๓. รายงานและเอกสาร ในลักษณะ Digital Report อยู่ใน USB Flash drive ขนาดความจุไม่น้อยกว่า ๑๒๘ GB จำนวน ๑ ชุด	ภายใน ๖๓๐ วันนับถัดจากวันลงนามในสัญญา
งวดงานที่ ๘	๑. รายงานฉบับสมบูรณ์ (Final Report) จำนวน ๑๐ ชุด ๒. รายงานสรุปสำหรับผู้บริหาร (Executive Summary Report) จำนวน ๑๐ ชุด ๓. คู่มือปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ให้บริการขนส่งทางราง จำนวน ๑๐ ชุด อย่างน้อยประกอบด้วย - ประมวลแนวทางปฏิบัติ - กรอบมาตรฐาน - มาตรฐานขั้นต่ำ - แบบฟอร์มการตรวจประเมิน - คู่มือการใช้งานระบบฐานข้อมูลสำหรับจัดเก็บข้อมูลการติดตามการปฏิบัติตามมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ให้บริการขนส่งทางรางภายใต้การกำกับดูแลของ ขร. ๔. คู่มือปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับ ขร. จำนวน ๑๐ ชุด อย่างน้อยประกอบด้วย - ประมวลแนวทางปฏิบัติ - กรอบมาตรฐาน - คู่มือการใช้งานระบบฐานข้อมูลสำหรับจัดเก็บข้อมูลการติดตามการปฏิบัติตามมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับ ขร. ในฐานะหน่วยงานควบคุมกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศการขนส่งทางราง ๕. มาตรฐานความมั่นคงปลอดภัยไซเบอร์ของระบบการขนส่งทางราง (Cybersecurity in Railway) จำนวน ๑๐ ชุด ๖. รายงานและเอกสาร ในลักษณะ Digital Report อยู่ใน USB Flash drive ขนาดความจุไม่น้อยกว่า ๑๒๘ GB จำนวน ๑๐ ชุด ๗. รายงานตามงวดงานทั้งหมดและไฟล์ข้อมูลของโครงการทั้งหมดที่สามารถแก้ไขได้ รวมทั้ง Presentation ของโครงการทั้งหมด รวมทั้งไฟล์ วีดีทัศน์ หรือ Vlog และสื่อประชาสัมพันธ์ในรูปแบบ Infographic บันทึกใน External Hard disk ขนาดความจุไม่น้อยกว่า ๒ TB จำนวน ๒ ชุด	ภายใน ๖๖๐ วันนับถัดจากวันลงนามในสัญญา

กรมการขนส่งทางราง

๗. เงื่อนไขการชำระเงิน

๗.๑ จะแบ่งงวดการชำระเงินออกเป็น ๘ งวด ตามเงื่อนไขดังนี้

๗.๑.๑ งวดที่ ๑ ชำระเงินจำนวนร้อยละ ๕ ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและผ่านการตรวจรับตามงวดงานที่ ๑ ของสัญญาเสร็จสมบูรณ์

๗.๑.๒ งวดที่ ๒ ชำระเงินจำนวนร้อยละ ๕ ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและผ่านการตรวจรับตามงวดงานที่ ๒ ของสัญญาเสร็จสมบูรณ์

๗.๑.๓ งวดที่ ๓ ชำระเงินจำนวนร้อยละ ๕ ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและผ่านการตรวจรับตามงวดงานที่ ๓ ของสัญญาเสร็จสมบูรณ์

๗.๑.๔ งวดที่ ๔ ชำระเงินจำนวนร้อยละ ๕ ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและผ่านการตรวจรับตามงวดงานที่ ๔ ของสัญญาเสร็จสมบูรณ์

๗.๑.๕ งวดที่ ๕ ชำระเงินจำนวนร้อยละ ๒๐ ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและผ่านการตรวจรับตามงวดงานที่ ๕ ของสัญญาเสร็จสมบูรณ์

๗.๑.๖ งวดที่ ๖ ชำระเงินจำนวนร้อยละ ๒๐ ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและผ่านการตรวจรับตามงวดงานที่ ๖ ของสัญญาเสร็จสมบูรณ์

๗.๑.๗ งวดที่ ๗ ชำระเงินจำนวนร้อยละ ๒๐ ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและผ่านการตรวจรับตามงวดงานที่ ๗ ของสัญญาเสร็จสมบูรณ์

๗.๑.๘ งวดที่ ๘ ชำระเงินจำนวนร้อยละ ๒๐ ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและผ่านการตรวจรับตามงวดงานที่ ๘ ของสัญญาเสร็จสมบูรณ์

๗.๒ ขร. จะดำเนินการจ่ายค่าจ้างล่วงหน้าให้แก่ที่ปรึกษาเมื่อมีการร้องขอจากที่ปรึกษาไม่เกินร้อยละสิบห้าของค่าจ้างตามสัญญา และที่ปรึกษาที่เป็นคู่สัญญาจะต้องนำหนังสือค้ำประกันหรือหนังสือค้ำประกันอิเล็กทรอนิกส์ของธนาคารภายในประเทศมาค้ำประกันเงินที่ได้รับล่วงหน้าไปนั้น และ ขร. จะคืนหนังสือค้ำประกันดังกล่าวให้แก่คู่สัญญาเมื่อ ขร. ได้หักเงินที่จ่ายล่วงหน้าจากเงินค่าจ้างที่จ่ายตามผลงานแต่ละงวดครบถ้วนแล้ว

สำหรับการจ้างหน่วยงานของรัฐ ให้จ่ายเงินค่าจ้างล่วงหน้าได้ไม่เกินร้อยละห้าสิบของค่าจ้างตามสัญญา และไม่ต้องมีหลักประกันเงินล่วงหน้าที่รับไปก็ได้

๘. วงเงินในการจัดหา

วงเงินงบประมาณทั้งสิ้น ๒๕,๖๙๘,๒๐๐ บาท (ยี่สิบห้าล้านหกแสนเก้าหมื่นแปดพันสองร้อยบาทถ้วน) รวมภาษีมูลค่าเพิ่ม แบ่งเป็น

๘.๑ ปี ๒๕๖๘ งบประมาณ ๕,๑๓๙,๖๔๐ บาท (ห้าล้านหนึ่งแสนสามหมื่นเก้าพันหกร้อยสี่สิบบาทถ้วน)

๘.๒ ปี ๒๕๖๙ ผูกพันงบประมาณ ๒๐,๕๕๘,๕๖๐ บาท (ยี่สิบล้านห้าแสนห้าหมื่นแปดพันห้าร้อยหกสิบบาทถ้วน)

๙. เกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ขร. จะพิจารณาเลือกเกณฑ์ด้านคุณภาพตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ มาตรา ๗๕ โดยในการพิจารณาผู้ชนะการยื่นข้อเสนอจะพิจารณาให้คะแนนและน้ำหนัก เพื่อใช้ในการประเมินการคัดเลือกข้อเสนอร้อยละ ๑๐๐ โดยต้องผ่านเกณฑ์คะแนนด้านคุณภาพไม่น้อยกว่าร้อยละ ๗๐ โดยมีรายละเอียด ดังนี้

กรมการขนส่งทางราง

เกณฑ์ด้านคุณภาพ	ร้อยละ	คะแนนเต็ม
๙.๑ ผลงานและประสบการณ์ของที่ปรึกษา	**๒๐**	**๒๐**
๙.๑.๑ ผลงานของที่ปรึกษา	๑๐	๑๐
๙.๑.๒ ประสบการณ์เฉพาะ	๑๐	๑๐
๙.๒ วิธีการบริหารและวิธีการปฏิบัติงาน	**๔๕**	**๔๕**
๙.๒.๑ วิธีการบริหารงาน	๑๐	๑๐
๙.๒.๒ วิธีการปฏิบัติงานตามขอบเขตงาน	๓๕	๓๕
๙.๓ จำนวนบุคลากรที่ร่วมงาน	**๓๕**	**๓๕**
รวมทั้งสิ้น	**๑๐๐**	**๑๐๐**

ซึ่งมีรายละเอียดหลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ ดังนี้

๙.๑ ผลงานและประสบการณ์ของที่ปรึกษา (ร้อยละ ๒๐)

ที่ปรึกษาจะต้องแสดงรายละเอียดผลงานและประสบการณ์ที่ดำเนินการในช่วง ๕ ปีที่ผ่านมา (ตั้งแต่ ๑ มกราคม ๒๕๖๒ ถึงวันปิดรับการยื่นข้อเสนอ) พร้อมเอกสารหลักฐานอ้างอิง เช่น หนังสือรับรอง หรือสำเนาสัญญาโครงการที่ได้ดำเนินการแล้วเสร็จตามสัญญา

๙.๑.๑ <u>ผลงานของที่ปรึกษา</u> : ที่ปรึกษามีผลงานการจ้างที่ปรึกษาในโครงการที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งจะต้องเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ หรือหน่วยงานเอกชนที่ ขร. เชื่อถือ ทั้งนี้ กรณีผลงานของแต่ละที่ปรึกษาที่รวมอยู่ในแต่ละกลุ่ม (ในกรณีที่ผู้ยื่นข้อเสนอเป็นกลุ่มที่ปรึกษา จะพิจารณาประสบการณ์และผลงานของผู้ร่วมยื่นข้อเสนอทุกรายในกลุ่มรวมกันในกลุ่มเดียวกัน โดยโครงการเดียวกันให้นับเป็น ๑ โครงการเท่านั้น) (ร้อยละ ๑๐)

เกณฑ์การพิจารณาที่ให้คะแนน	คะแนนเต็ม
(๑) ผลงานของที่ปรึกษา ในวงเงินตั้งแต่ ๘,๐๐๐,๐๐๐ บาทขึ้นไป	๑๐
(๒) ผลงานของที่ปรึกษา วงเงินตั้งแต่ ๕,๐๐๐,๐๐๐ บาท ถึง ๗,๙๙๙,๙๙๙ บาท	๘
(๓) ผลงานของที่ปรึกษา วงเงินตั้งแต่ ๑,๐๐๐,๐๐๐ บาท ถึง ๔,๙๙๙,๙๙๙ บาท	๖

หมายเหตุ : ๑) พิจารณาให้คะแนนผลงานของที่ปรึกษา ที่มีวงเงินตั้งแต่ ๑,๐๐๐,๐๐๐ บาทขึ้นไป

๒) ให้พิจารณาจำนวน ๑ โครงการ เท่ากับ ๑ คะแนน โดยพิจารณาข้อ (๑) ก่อน เมื่อครบ ๑๐ คะแนนแล้วไม่ต้องพิจารณาข้อ (๒) หากคะแนนรวมไม่ถึง ๑๐ คะแนน ให้พิจารณาข้อ (๒) เพิ่มเติม ทั้งนี้ ข้อ (๒) ต้องไม่เกิน ๘ คะแนน และหากคะแนนรวมไม่ถึง ๑๐ คะแนน ให้พิจารณาข้อ (๓) เพิ่มเติม ทั้งนี้ข้อ (๓) ต้องไม่เกิน ๖ คะแนน และเมื่อรวมคะแนน ข้อ (๑) (๒) และ (๓) แล้ว ต้องไม่เกิน ๑๐ คะแนน

๙.๑.๒ <u>ประสบการณ์เฉพาะ</u> : จำนวนผลงานประสบการณ์ที่ดำเนินการในช่วง ๕ ปีที่ผ่านมา ซึ่งเป็นผลงานประเภทที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ หรือเป็นผลงานประเภทเดียวกันกับขอบเขตของงานจ้างที่ปรึกษา (ร้อยละ ๑๐)

เกณฑ์การพิจารณาที่ให้คะแนน	คะแนน
(๑) ผลงานของที่ปรึกษา จำนวนตั้งแต่ ๕ งาน ขึ้นไป	๑๐
(๒) ผลงานของที่ปรึกษา จำนวน ๓ – ๔ งาน	๘
(๓) ผลงานของที่ปรึกษา จำนวน ๑ – ๒ งาน	๖

กรมการขนส่งทางราง

๙.๒ วิธีการบริหารและวิธีการปฏิบัติงาน (ร้อยละ ๔๕)

๙.๒.๑ <u>วิธีการบริหารงาน</u> นำเสนอแนวทางในการบริหารงานของที่ปรึกษา โดยให้ผู้ยื่นข้อเสนอนำเสนอรายการ (ร้อยละ ๑๐) ดังนี้

เกณฑ์การพิจารณาที่ให้คะแนน	คะแนนเต็ม	วิธีการประเมิน
(๑) ความเข้าใจในวัตถุประสงค์ของการศึกษา	๕	ผู้ประเมินจะพิจารณาจากเอกสารที่ผู้ยื่นข้อเสนอยื่นมา โดยจัดทำเป็นรูปแบบเอกสารขนาด A๔ และผู้ประเมินจะให้คะแนนตามรายการที่ผู้ยื่นข้อเสนอนำเอกสารมายื่น
(๒) แผนการดำเนินงานและการจัดสรรบุคลากรที่เหมาะสมกับขอบเขตการศึกษา	๕	
รวม	๑๐	

โดยมีรายละเอียด ดังนี้

(๑) ความเข้าใจวัตถุประสงค์ของการศึกษา (คะแนนเต็ม ๕ คะแนน) จะพิจารณาตามวัตถุประสงค์ของโครงการทั้ง ๕ ข้อ ของการศึกษา ดังนี้

ลำดับ	หัวข้อการพิจารณา	คะแนนเต็ม
๑	ศึกษาและวิเคราะห์บริบทขององค์กร ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และที่เกี่ยวข้อง	๑
๒	ศึกษาและวิเคราะห์ข้อกำหนดตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และข้อกำหนดอื่น ๆ เพื่อจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ทางรางให้สอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)	๑
๓	จัดทำประมวลแนวทางปฏิบัติ (แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์) และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)	๑
๔	จัดทำมาตรฐานขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๑
๕	ดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางรางตามมาตรฐานขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๑
รวม		**๕**

(๒) แผนการดำเนินงานและการจัดสรรบุคลากรที่เหมาะสมกับขอบเขตการศึกษา (คะแนนเต็ม ๕ คะแนน) จะพิจารณา ๕ ข้อดังนี้

ลำดับ	หัวข้อการพิจารณา	คะแนนเต็ม
๑	โครงสร้างองค์กรของบุคลากรของที่ปรึกษา	๑
๒	หน้าที่รับผิดชอบของบุคลากรหลัก	๑
๓	รายละเอียดการทำงานของบุคลากรหลัก	๑
๔	การแบ่งการดำเนินงานเป็นกลุ่มงานอย่างมีประสิทธิภาพ	๑
๕	แผนการดำเนินงานให้สอดคล้องกับระยะเวลาดำเนินงานโครงการ	๑
รวม		**๕**

กรมการขนส่งทางราง

๙.๒.๒ <u>วิธีปฏิบัติงานตามขอบเขตของงาน</u> โดยนำเสนอแนวคิด แผนงาน และวิธีการปฏิบัติที่สอดคล้องและครอบคลุมครบถ้วนตามขอบเขตของงานจ้างที่ปรึกษา พร้อมกำหนดระยะเวลาที่เหมาะสม (ร้อยละ ๓๕) ดังนี้

ลำดับ	หัวข้อการพิจารณา	คะแนนเต็ม
(๑)	**งานส่วนที่ ๑ ศึกษา รวบรวม วิเคราะห์หลักเกณฑ์ มาตรฐาน และข้อมูลการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)**	
	ศึกษา รวบรวม วิเคราะห์หลักเกณฑ์ มาตรฐาน และข้อมูลการดำเนินงานด้าน Cybersecurity ตามมาตรฐานสากลของระบบการขนส่งทางราง ที่มีข้อมูลหรืองานวิจัยในปัจจุบันทั้งในประเทศและต่างประเทศ อย่างน้อย ๗ ประเทศ เช่น ประเทศไทย ประเทศญี่ปุ่น ประเทศอินเดีย สาธารณรัฐประชาชนจีน สหรัฐอเมริกา สหพันธรัฐรัสเซีย และประเทศในกลุ่มสหภาพยุโรป หรือตามที่ ขร. กำหนด ตามกรอบมาตรฐาน ดังนี้ ๑) มาตรฐานสากล ISO/IEC ๒๗๐๐๑ : ๒๐๒๒ มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ Information Security Management System (ISMS) ๒) มาตรฐาน National Institute of Standards and Technology (NIST) Cybersecurity Framework (กรอบการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ) ๓) มาตรฐาน IEC ๖๒๔๔๓ มาตรฐานเกี่ยวข้องกับการวิเคราะห์ ประเมิน และทดสอบ เพื่อควบคุมด้านเทคโนโลยีสารสนเทศที่เหมาะสม ๔) มาตรฐาน Control Objectives for information and Related Technology (COBIT) กรอบมาตราฐานด้านการกำกับดูแลและการบริหารจัดการระบบสารสนเทศระดับองค์กร ๕) มาตรฐาน Information Technology Infrastructure Library (ITIL) กรอบการบริหารจัดการ IT service Management (ITSM) ๖) มาตรฐานที่เกี่ยวข้องกับ (Cybersecurity in Railway) หรือมาตรฐานอื่น ๆ ที่เกี่ยวข้อง	๑
(๒)	**งานส่วนที่ ๒ จัดทำมาตรการความมั่นคงปลอดภัยไซเบอร์ของ ขร.**	
(๒.๑)	ศึกษาและวิเคราะห์บริบทขององค์กรด้านความมั่นคงปลอดภัยไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงกฎหมายด้านไซเบอร์ และกฎกระทรวงที่เกี่ยวข้องกับ ขร. รวบรวมพร้อมจัดทำรายงานสรุปผลการศึกษาและวิเคราะห์ด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร	๑
(๒.๒)	ศึกษาและวิเคราะห์สถานะปัจจุบันของการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ของ ขร. ประเมินความพร้อมด้านไซเบอร์ (GAP Analysis) ของ ขร. ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และบริบทขององค์กรด้านความมั่นคงปลอดภัยไซเบอร์	๑
(๒.๓)	จัดทำรายงานผลประเมินความพร้อมด้านไซเบอร์ของ ขร. รวมถึงให้ข้อเสนอแนะที่เป็นประโยชน์ ในการปรับปรุงกระบวนการภายในและเตรียมความพร้อมให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และบริบทขององค์กรด้านความมั่นคงปลอดภัยไซเบอร์	๑
(๒.๔)	จัดทำนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร. (พ.ศ. ๒๕๖๙-๒๕๗๓) โดยทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ขร. (Information Security Policy) ที่มีอยู่ในปัจจุบัน หรือจัดทำนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร. (พ.ศ. ๒๕๖๙-๒๕๗๓) ขึ้นใหม่ โดยเนื้อหาให้เกิดการบูรณาการระหว่างกัน อย่างน้อยประกอบด้วย แผนงานโครงการ และรายละเอียดโครงการ เช่น วัตถุประสงค์ ประโยชน์ที่คาดว่าจะได้รับ ระยะเวลา ตัวชี้วัด ผลลัพธ์ และจัดลำดับความสำคัญของโครงการ	๒

ลำดับ	หัวข้อการพิจารณา	คะแนนเต็ม
(๒.๕)	จัดทำโครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับ ขร. ครอบคลุมถึงการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ภายใน ขร. และการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง เพื่อสนับสนุนศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	๑
(๒.๖)	จัดทำรายงานการกำหนดผู้รับผิดชอบและบทบาทหน้าที่ในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นแนวทางให้กับ ขร. ครอบคลุมถึงการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ภายใน ขร. และการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ประกอบด้วยหัวข้ออย่างน้อย ดังนี้ ๑. ผู้รับผิดชอบและบทบาทหน้าที่ ๒. คุณสมบัติที่เหมาะสม ๓. อำนาจในการดำเนินการ สั่งการ และอนุมัติ	๑
(๒.๗)	จัดทำแนวปฏิบัติในการบริหารความเสี่ยง (Risk Management) ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นแนวทางในการบริหารจัดการความเสี่ยงด้านไซเบอร์ ประกอบด้วยหัวข้ออย่างน้อย ดังนี้ ๑. การรวบรวมและประเมินความสำคัญทรัพย์สิน ๒. การระบุภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ๓. การระบุช่องโหว่ความมั่นคงปลอดภัยสารสนเทศ ๔. การระบุมาตรการควบคุมปัจจุบัน ๕. ประเมินโอกาสเกิดเหตุการณ์ ๖. การวิเคราะห์ผลกระทบความมั่นคงปลอดภัยสารสนเทศ ๗. การคำนวนระดับความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ ๘. หลักเกณฑ์การเลือกตอบสนองต่อความเสี่ยงที่ครอบคลุม ๙. แบบฟอร์มการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่สามารถคำนวนผลระดับความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์	๒
(๒.๘)	จัดทำแนวปฏิบัติสำหรับการจัดทำสรุปรายงานการบริหารความเสี่ยง (Risk Management) ด้านความมั่นคงปลอดภัยไซเบอร์ และสรุปรายงานผลการตรวจสอบ (Audit) ด้านความมั่นคงปลอดภัยไซเบอร์ ของ ขร. ตามมาตรา ๕๔ ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒	๑
(๒.๙)	จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร. ให้สอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ที่จัดทำขึ้น ตามมาตรา ๔๔ ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒	๒
(๒.๑๐)	จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) ของ ขร. เพื่อกำหนดกระบวนการปฏิบัติงานหากเกิดภัยคุกคามทางไซเบอร์	๑
(๓)	**งานส่วนที่ ๓ จัดทำแนวการกำกับดูแลผู้ให้บริการขนส่งทางราง**	
(๓.๑)	พัฒนาแบบตรวจประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. (Audit Form) ที่ครอบคลุมถึงหัวข้อ อย่างน้อยประกอบด้วย ๑. แนวทางการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๒. แนวทางการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ๓. แผนการรับมือภัยคุกคามทางไซเบอร์ ๔. มาตรการหรือแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	๒

ลำดับ	หัวข้อการพิจารณา	คะแนนเต็ม
(๓.๒)	ดำเนินการสำรวจความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. พร้อมทั้งจัดทำรายงานสรุปความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. ไม่น้อยกว่า ๑ ครั้ง อย่างน้อย ๔ ราย	๒
(๓.๓)	ดำเนินการเข้าตรวจประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. พร้อมทั้งจัดทำรายงานการตรวจสอบ (Audit) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. ไม่น้อยกว่า ๑ ครั้ง อย่างน้อย ๔ ราย	๒
(๓.๔)	จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. ให้สอดคล้องกับมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ โดยมีการกำหนดคุณลักษณะให้แก่ข้อมูลหรือระบบสารสนเทศ และการจำแนกหมวดหมู่ภัยคุกคาม	๒
(๓.๕)	จัดทำแผนปฏิบัติการและกำกับดูแลผู้ให้บริการขนส่งทางราง (พ.ศ. ๒๕๖๙-๒๕๗๓) ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พร้อมทั้งให้ข้อเสนอแนะที่เป็นประโยชน์ในการดำเนินการตามแผนปฏิบัติการและกำกับดูแลผู้ให้บริการขนส่งทางราง (พ.ศ. ๒๕๖๙-๒๕๗๓) ให้ได้ประสิทธิผลตามที่กำหนด	๒
(๓.๖)	จัดทำมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของระบบการขนส่งทางราง (Cybersecurity in Railway) โดยทบทวนร่าง มขร. มาตรฐานความมั่นคงปลอดภัยไซเบอร์ของระบบการขนส่งทางราง (Cybersecurity in Railway) ที่มีอยู่ในปัจจุบัน หรือจัดทำมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของระบบการขนส่งทางราง (Cybersecurity in Railway) ขึ้นใหม่ เพื่อกำหนดมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ให้บริการขนส่งทางรางภายใต้การกำกับดูแลของ ขร. โดยเนื้อหาให้เกิดการบูรณาการระหว่างกัน	๒
(๓.๗)	จัดหาเครื่องแม่ข่ายแบบที่ ๑ และระบบจัดเก็บฐานข้อมูลพร้อมติดตั้งระบบบนเครื่องแม่ข่าย และจัดให้มีการทดสอบระบบ พร้อมทั้งนำเข้าข้อมูล เพื่อจัดเก็บข้อมูลการติดตามการปฏิบัติของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. ตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของระบบการขนส่งทางราง (Cybersecurity in Railway) ในรูปแบบ Web Application ระยะเวลาอย่างน้อย ๑ ปี นับถัดจากวันที่ผ่านการตรวจรับงานงวดสุดท้ายเรียบร้อยแล้ว	๒
(๔)	**งานส่วนที่ ๔ การจัดประชุม ฝึกอบรม สัมมนา และประชาสัมพันธ์**	
(๔.๑)	จัดฝึกอบรมให้บุคลากรของ ขร. ตามหลักสูตรอย่างน้อย ดังนี้ ๑. ข้อกำหนดตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ๒. แนวปฏิบัติและกรอบมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ ๓. มาตรฐานสากลด้านความมั่นคงปลอดภัยไซเบอร์ ๔. สร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ ๕. จัดหาหลักสูตรอบรม วุฒิบัตรผู้ตรวจสอบระบบสารสนเทศ ๒๗๐๐๑ ISO/IEC ๒๗๐๐๑:๒๐๒๒ Lead Auditor	๑
(๔.๒)	จัดประชุมสรุปผลการดำเนินโครงการ และความเชื่อมโยงกับรายงานผลการประเมินความมั่นคงปลอดภัยไซเบอร์ (NCSA SPA – Full Report) ให้กับบุคลากรของ ขร. จำนวน ๑ ครั้ง มีผู้เข้าร่วมไม่น้อยกว่า ๓๐ คน	๑

กรมการขนส่งทางราง

ลำดับ	หัวข้อการพิจารณา	คะแนนเต็ม
(๔.๓)	จัดอบรมการใช้งานระบบฐานข้อมูลสำหรับจัดเก็บข้อมูลการติดตามการปฏิบัติตามมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ดูแลระบบ จำนวนไม่น้อ ยกว่า ๑ ครั้ง มีผู้เข้าร่วมไม่น้อยกว่า ๑๐ คน	๑
(๔.๔)	จัดประชุมกลุ่มย่อย (Focus Group) สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. ตามหัวข้อ ดังนี้ ๑. แบบตรวจประเมินแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๒. ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ ๓. มาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร.	๑
(๔.๕)	จัดประชุมเผยแพร่แนวทางการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และอบรมการใช้งานระบบฐานข้อมูลสำหรับจัดเก็บข้อมูลการติดตามการปฏิบัติตามมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีผู้เข้าร่วมไม่น้อยกว่า ๕๐ คน พร้อมทั้งจัดทำสื่อประชาสัมพันธ์อย่างน้อย ดังนี้ ๑. บอร์ดนิทรรศการขนาด ๐.๘๐ x ๒.๐๐ เมตร ชนิดไวนิลทึบแสง จำนวน ๒ ชุด ๒. บอร์ดประชาสัมพันธ์ขนาด ๔.๐๐ x ๒.๐๐ เมตร ชนิดไวนิลทึบแสง จำนวน ๑ ชุด	๑
(๔.๖)	จัดทำสื่อประชาสัมพันธ์ ในรูปแบบ Infographic เกี่ยวกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. จำนวนไม่น้อยกว่า ๔ ชิ้นงาน	๑
(๔.๗)	จัดทำสื่อประชาสัมพันธ์ ในรูปแบบ วีดีทัศน์ หรือ Vlog เกี่ยวกับประมวลแนวทางปฏิบัติ กรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ และมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. จำนวนไม่น้อยกว่า ๒ ชิ้นงาน ความยาวชิ้นงานละไม่น้อยกว่า ๓ นาที พากย์ภาษาไทย และคำบรรยาย (Subtitle) ภาษาไทยและภาษาอังกฤษ	๑
รวม		๓๕

โดยกำหนดหลักเกณฑ์พิจารณาแต่ละส่วนตามข้อ ๙.๒.๑ – ๙.๒.๒ จากระดับความครบถ้วนสมบูรณ์ของข้อเสนอ ดังนี้

เกณฑ์การพิจารณา	คะแนน (ร้อยละ)	ระดับคะแนน	วิธีการประเมิน
มีเนื้อหาสาระครบถ้วนสมบูรณ์ถูกต้องตามขอบเขตของงาน รวมทั้งมีข้อเสนอแนะเพิ่มเติมจากขอบเขตของงานที่ทำให้การดำเนินงานมีความสมบูรณ์และมีประสิทธิภาพมากยิ่งขึ้น	๑๐๐	ดีมาก	ผู้ประเมินจะพิจารณาจากเอกสารที่ผู้ยื่นข้อเสนอยื่นมาโดยจัดทำเป็นรูปแบบเอกสารขนาด A๔ และผู้ประเมินจะให้คะแนนตามรายการตามข้อ ๙.๒.๑ – ๙.๒.๒ ที่ผู้ยื่นข้อเสนอนำเอกสารมายื่น
มีเนื้อหาสาระครบถ้วนสมบูรณ์ถูกต้องตามขอบเขตของงาน รวมทั้งมีข้อเสนอแนะเพิ่มเติมจากขอบเขตของงาน	๘๕	ดี	
มีเนื้อหาสาระครบถ้วนสมบูรณ์ถูกต้องตามขอบเขตของงานและเพียงพอในการปฏิบัติงานได้	๗๐	พอใช้	
มีเนื้อหาสาระไม่ครบถ้วนสมบูรณ์ถูกต้องตามขอบเขตของงานเพียงเล็กน้อย และเพียงพอในการปฏิบัติงานได้	๕๐	ต่ำกว่าเกณฑ์	
มีเนื้อหาสาระไม่ครบถ้วนสมบูรณ์ถูกต้องตามขอบเขตของงาน (ไม่เขียน หรือ เขียนไม่ตรงประเด็น)	๐	ปรับปรุง	

กรมการขนส่งทางราง

๙.๓ จำนวนบุคลากรที่ร่วมงาน

โดยที่ปรึกษาจะต้องแสดงรายละเอียดคุณวุฒิการศึกษา ความเชี่ยวชาญหรือประสบการณ์ของบุคลากรหลัก แต่ละคนที่รับผิดชอบโครงการ พร้อมเอกสารหลักฐานอ้างอิง โดยมีคะแนนในส่วนบุคลากรที่ร่วมงานร้อยละ ๓๕ ซึ่งผู้ประเมินจะให้คะแนนแก่ผู้ยื่นข้อเสนอ โดยแบ่งสัดส่วนการให้คะแนนของบุคลากรแต่ละตำแหน่งเป็น ๓ ส่วน (ร้อยละ ๑๐๐) ดังนี้

๙.๓.๑ ด้านระยะเวลาทำงาน (สัดส่วนร้อยละ ๔๐ ของคะแนนเต็มแต่ละตำแหน่ง) ระยะเวลาทำงานพิจารณาจากจำนวนปีประสบการณ์ คิดจากระยะเวลาการปฏิบัติงานตั้งแต่ปีที่จบปริญญาตรี

๙.๓.๒ ด้านประสบการณ์เฉพาะตำแหน่ง (สัดส่วนร้อยละ ๔๐ ของคะแนนเต็มแต่ละตำแหน่ง) พิจารณาจากจำนวนผลงานโครงการที่เกี่ยวข้องโดยตรงกับการศึกษาและตำแหน่งที่รับผิดชอบ

๙.๓.๓ ด้านวุฒิการศึกษา (สัดส่วนร้อยละ ๒๐ ของคะแนนเต็มแต่ละตำแหน่ง)

โดยพิจารณาให้คะแนนกับที่ปรึกษา จำนวน ๑๑ รายการ ดังนี้

ลำดับ	ตำแหน่ง	สัดส่วนคะแนน
(๑)	ผู้จัดการโครงการ	๕
(๒)	รองผู้จัดการโครงการ	๓
(๓)	ผู้เชี่ยวชาญด้านแผนงานเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัย	๓
(๔)	ผู้เชี่ยวชาญด้านวิศวกรรมระบบราง	๓
(๕)	ผู้เชี่ยวชาญด้านการจัดการนโยบายและบริหารความเสี่ยง	๓
(๖)	ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ	๓
(๗)	ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์	๓
(๘)	ผู้เชี่ยวชาญด้านการประเมินความมั่นคงปลอดภัยไซเบอร์ทางเทคโนโลยีสารสนเทศ (IT Assessment)	๓
(๙)	ผู้เชี่ยวชาญด้านการตรวจสอบความมั่นคงปลอดภัยสารสนเทศ	๓
(๑๐)	ผู้เชี่ยวชาญด้านการพัฒนาระบบ	๓
(๑๑)	ผู้เชี่ยวชาญด้านระบบคอมพิวเตอร์	๓
รวม		**๓๕**

(๑) **ผู้จัดการโครงการ** : จะต้องมีประสบการณ์ทำงานไม่น้อยกว่า ๑๕ ปี และวุฒิการศึกษาไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ/สาขาคอมพิวเตอร์/สาขาวิศวกรรม/สาขาวิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง

รายการ	ประสบการณ์ (ปี)	วุฒิการศึกษา	สาขาวิชา
ผู้จัดการโครงการ	๑๕	ไม่ต่ำกว่าปริญญาโท	เทคโนโลยีสารสนเทศ/คอมพิวเตอร์/วิศวกรรม/วิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง

คะแนนเต็ม ๕ คะแนน (ร้อยละ ๑๐๐)							
ระยะเวลาทำงาน (๒ คะแนน/ ร้อยละ ๔๐)			ด้านประสบการณ์เฉพาะตำแหน่ง (๒ คะแนน/ ร้อยละ ๔๐)			วุฒิการศึกษา (๑ คะแนน/ ร้อยละ ๒๐)	
ตั้งแต่ ๒๕ ปีขึ้นไป	๒๐ - ๒๔ ปี	๑๕ - ๑๙ ปี	๕ โครงการขึ้นไป	๓ - ๔ โครงการ	๑ - ๒ โครงการ	ปริญญาเอก	ปริญญาโท
๑๐๐ (๒ คะแนน)	๘๕ (๑.๗ คะแนน)	๗๐ (๑.๔ คะแนน)	๑๐๐ (๒ คะแนน)	๘๕ (๑.๗ คะแนน)	๗๐ (๑.๔ คะแนน)	๑๐๐ (๑ คะแนน)	๗๐ (๐.๗ คะแนน)

หมายเหตุ: ด้านประสบการณ์เฉพาะตำแหน่ง ให้พิจารณาในตำแหน่งผู้จัดการโครงการหรือหัวหน้าโครงการหรือหัวหน้าโครงการวิจัย

(๒) รองผู้จัดการโครงการ : จะต้องมีประสบการณ์ทำงานไม่น้อยกว่า ๑๐ ปี และวุฒิการศึกษาไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ/สาขาคอมพิวเตอร์/สาขาวิศวกรรม/สาขาวิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง

รายการ	ประสบการณ์ (ปี)	วุฒิการศึกษา	สาขาวิชา
รองผู้จัดการโครงการ	๑๐	ไม่ต่ำกว่าปริญญาโท	เทคโนโลยีสารสนเทศ/คอมพิวเตอร์/วิศวกรรม/วิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง

คะแนนเต็ม ๓ คะแนน (ร้อยละ ๑๐๐)							
ระยะเวลาทำงาน (๑.๒ คะแนน/ ร้อยละ ๔๐)			ด้านประสบการณ์เฉพาะตำแหน่ง (๑.๒ คะแนน/ ร้อยละ ๔๐)			วุฒิการศึกษา (๐.๖ คะแนน/ ร้อยละ ๒๐)	
ตั้งแต่ ๒๐ ปีขึ้นไป	๑๖ - ๑๙ ปี	๑๐ – ๑๕ ปี	๕ โครงการขึ้นไป	๓ - ๔ โครงการ	๑ - ๒ โครงการ	ปริญญาเอก	ปริญญาโท
๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๐.๖ คะแนน)	๗๐ (๐.๔๒ คะแนน)

หมายเหตุ: ด้านประสบการณ์เฉพาะตำแหน่ง ให้พิจารณาในตำแหน่งผู้จัดการโครงการหรือหัวหน้าโครงการหรือหัวหน้าโครงการวิจัย หรือรองผู้จัดการโครงการหรือรองหัวหน้าโครงการหรือรองหัวหน้าโครงการวิจัย

(๓) **ผู้เชี่ยวชาญด้านแผนงานเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัย** : จะต้องมีประสบการณ์ทำงานไม่น้อยกว่า ๑๕ ปี และวุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี สาขาเทคโนโลยีสารสนเทศ/สาขาคอมพิวเตอร์/สาขาวิศวกรรม/สาขาวิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านความมั่นคงปลอดภัยสารสนเทศ CompTIA Security+ หรือ ISO/IEC ๒๗๐๐๑

รายการ	ประสบการณ์ (ปี)	วุฒิการศึกษา	สาขาวิชา
ผู้เชี่ยวชาญด้านแผนงานเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัย	๑๕	ไม่ต่ำกว่าปริญญาตรี	เทคโนโลยีสารสนเทศ/คอมพิวเตอร์/วิศวกรรม/วิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านความมั่นคงปลอดภัยสารสนเทศ CompTIA Security+ หรือ ISO/IEC ๒๗๐๐๑

	คะแนนเต็ม ๓ คะแนน (ร้อยละ ๑๐๐)								
	ระยะเวลาทำงาน (๑.๒ คะแนน/ ร้อยละ ๔๐)			ด้านประสบการณ์เฉพาะตำแหน่ง (๑.๒ คะแนน/ ร้อยละ ๔๐)			วุฒิการศึกษา* (๐.๖ คะแนน/ ร้อยละ ๒๐)		
	ตั้งแต่ ๒๕ ปีขึ้นไป	๒๐ - ๒๔ ปี	๑๕ – ๑๙ ปี	๕ โครงการขึ้นไป	๓ - ๔ โครงการ	๑ - ๒ โครงการ	ปริญญาเอก	ปริญญาโท	ปริญญาตรี
	๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๐.๖ คะแนน)	๘๕ (๐.๕๑ คะแนน)	๗๐ (๐.๔๒ คะแนน)

หมายเหตุ: * กรณีไม่มีใบประกาศนียบัตรตามที่ระบุ จะคิดคะแนนร้อยละ ๕๐ ของคะแนนวุฒิการศึกษาที่ได้

(๔) ผู้เชี่ยวชาญด้านวิศวกรรมระบบราง : จะต้องมีประสบการณ์ทำงานไม่น้อยกว่า ๑๐ ปี และวุฒิการศึกษาไม่ต่ำกว่าปริญญาโท สาขาวิศวกรรมระบบราง/สาขาวิศวกรรมขนส่งทางราง/สาขาวิศวกรรมโยธา/สาขาวิศวกรรมโลจิสติกส์/สาขาโลจิสติกส์/สาขาที่เกี่ยวข้อง

รายการ	ประสบการณ์ (ปี)	วุฒิการศึกษา	สาขาวิชา
ผู้เชี่ยวชาญด้านวิศวกรรมระบบราง	๑๐	ไม่ต่ำกว่าปริญญาโท	วิศวกรรมระบบราง/วิศวกรรมขนส่งทางราง/วิศวกรรมโยธา/วิศวกรรมโลจิสติกส์/โลจิสติกส์/สาขาที่เกี่ยวข้อง

คะแนนเต็ม ๓ คะแนน (ร้อยละ ๑๐๐)							
ระยะเวลาทำงาน (๑.๒ คะแนน/ ร้อยละ ๔๐)			ด้านประสบการณ์เฉพาะตำแหน่ง (๑.๒ คะแนน/ ร้อยละ ๔๐)			วุฒิการศึกษา (๐.๖ คะแนน/ ร้อยละ ๒๐)	
ตั้งแต่ ๒๐ ปีขึ้นไป	๑๖ - ๑๙ ปี	๑๐ – ๑๕ ปี	๕ โครงการขึ้นไป	๓ - ๔ โครงการ	๑ - ๒ โครงการ	ปริญญาเอก	ปริญญาโท
๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๐.๖ คะแนน)	๗๐ (๐.๔๒ คะแนน)

(๕) **ผู้เชี่ยวชาญด้านการจัดการนโยบายและบริหารความเสี่ยง :** จะต้องมีประสบการณ์ทำงานไม่น้อยกว่า ๑๐ ปี และวุฒิการศึกษาไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ/สาขาคอมพิวเตอร์/สาขาวิศวกรรม/สาขาวิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑

รายการ	ประสบการณ์ (ปี)	วุฒิการศึกษา	สาขาวิชา
ผู้เชี่ยวชาญด้านการจัดการนโยบายและบริหารความเสี่ยง	๑๐	ไม่ต่ำกว่าปริญญาโท	เทคโนโลยีสารสนเทศ/คอมพิวเตอร์/วิศวกรรม/วิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑

คะแนนเต็ม ๓ คะแนน (ร้อยละ ๑๐๐)							
ระยะเวลาทำงาน (๑.๒ คะแนน/ ร้อยละ ๔๐)			ด้านประสบการณ์เฉพาะตำแหน่ง (๑.๒ คะแนน/ ร้อยละ ๔๐)			วุฒิการศึกษา* (๐.๖ คะแนน/ ร้อยละ ๒๐)	
ตั้งแต่ ๒๐ ปีขึ้นไป	๑๖ - ๑๙ ปี	๑๐ – ๑๕ ปี	๕ โครงการขึ้นไป	๓ - ๔ โครงการ	๑ - ๒ โครงการ	ปริญญาเอก	ปริญญาโท
๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๐.๖ คะแนน)	๗๐ (๐.๔๒ คะแนน)

หมายเหตุ: * กรณีไม่มีใบประกาศนียบัตรตามที่ระบุ จะคิดคะแนนร้อยละ ๕๐ ของคะแนนวุฒิการศึกษาที่ได้

(๖) **ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ** : จะต้องมีประสบการณ์ทำงานไม่น้อยกว่า ๑๕ ปี และวุฒิการศึกษาไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ/สาขาคอมพิวเตอร์/สาขาวิศวกรรม/สาขาวิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง

รายการ	ประสบการณ์ (ปี)	วุฒิการศึกษา	สาขาวิชา
ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ	๑๕	ไม่ต่ำกว่าปริญญาโท	เทคโนโลยีสารสนเทศ/คอมพิวเตอร์/วิศวกรรม/วิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง

คะแนนเต็ม ๓ คะแนน (ร้อยละ ๑๐๐)							
ระยะเวลาทำงาน (๑.๒ คะแนน/ ร้อยละ ๔๐)			ด้านประสบการณ์เฉพาะตำแหน่ง (๑.๒ คะแนน/ ร้อยละ ๔๐)			วุฒิการศึกษา* (๐.๖ คะแนน/ ร้อยละ ๒๐)	
ตั้งแต่ ๒๕ ปีขึ้นไป	๒๐ - ๒๔ ปี	๑๕ - ๑๙ ปี	๕ โครงการขึ้นไป	๓ - ๔ โครงการ	๑ - ๒ โครงการ	ปริญญาเอก	ปริญญาโท
๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๐.๖ คะแนน)	๗๐ (๐.๔๒ คะแนน)

(๗) **ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ :** จะต้องมีประสบการณ์ทำงานไม่น้อยกว่า ๑๕ ปี และวุฒิการศึกษาไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ/สาขาคอมพิวเตอร์/สาขาวิศวกรรม/สาขาวิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านความมั่นคงปลอดภัยไซเบอร์ CCE (Certified Cybersecurity Expert)

รายการ	ประสบการณ์ (ปี)	วุฒิการศึกษา	สาขาวิชา
ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์	๑๕	ไม่ต่ำกว่าปริญญาโท	เทคโนโลยีสารสนเทศ/คอมพิวเตอร์/วิศวกรรม/วิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านความมั่นคงปลอดภัยไซเบอร์ CCE (Certified Cybersecurity Expert)

คะแนนเต็ม ๓ คะแนน (ร้อยละ ๑๐๐)							
ระยะเวลาทำงาน (๑.๒ คะแนน/ ร้อยละ ๔๐)			ด้านประสบการณ์เฉพาะตำแหน่ง (๑.๒ คะแนน/ ร้อยละ ๔๐)			วุฒิการศึกษา* (๐.๖ คะแนน/ ร้อยละ ๒๐)	
ตั้งแต่ ๒๕ ปีขึ้นไป	๒๐ - ๒๔ ปี	๑๕ - ๑๙ ปี	๕ โครงการขึ้นไป	๓ - ๔ โครงการ	๑ - ๒ โครงการ	ปริญญาเอก	ปริญญาโท
๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๐.๖ คะแนน)	๗๐ (๐.๔๒ คะแนน)

หมายเหตุ: * กรณีไม่มีใบประกาศนียบัตรตามที่ระบุ จะคิดคะแนนร้อยละ ๕๐ ของคะแนนวุฒิการศึกษาที่ได้

(๘) **ผู้เชี่ยวชาญด้านการประเมินความมั่นคงปลอดภัยไซเบอร์ทางเทคโนโลยีสารสนเทศ (IT Assessment)** : จะต้องมีประสบการณ์ทำงานไม่น้อยกว่า ๑๐ ปี และวุฒิการศึกษาไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ/สาขาคอมพิวเตอร์/สาขาวิศวกรรม/สาขาวิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านความมั่นคงปลอดภัยไซเบอร์ CCE (Certified Cybersecurity Expert)

รายการ	ประสบการณ์ (ปี)	วุฒิการศึกษา	สาขาวิชา
ผู้เชี่ยวชาญด้านการประเมินความมั่นคงปลอดภัยไซเบอร์ทางเทคโนโลยีสารสนเทศ (IT Assessment)	๑๐	ไม่ต่ำกว่าปริญญาโท	เทคโนโลยีสารสนเทศ/คอมพิวเตอร์/วิศวกรรม/วิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านความมั่นคงปลอดภัยไซเบอร์ CCE (Certified Cybersecurity Expert)

คะแนนเต็ม ๓ คะแนน (ร้อยละ ๑๐๐)							
ระยะเวลาทำงาน (๑.๒ คะแนน/ ร้อยละ ๔๐)			ด้านประสบการณ์เฉพาะตำแหน่ง (๑.๒ คะแนน/ ร้อยละ ๔๐)			วุฒิการศึกษา* (๐.๖ คะแนน/ ร้อยละ ๒๐)	
ตั้งแต่ ๒๐ ปีขึ้นไป	๑๖ - ๑๙ ปี	๑๐ – ๑๕ ปี	๕ โครงการขึ้นไป	๓ - ๔ โครงการ	๑ - ๒ โครงการ	ปริญญาเอก	ปริญญาโท
๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๐.๖ คะแนน)	๗๐ (๐.๔๒ คะแนน)

หมายเหตุ: * กรณีไม่มีใบประกาศนียบัตรตามที่ระบุจะคิดคะแนนร้อยละ ๕๐ ของคะแนนวุฒิการศึกษาที่ได้

(๙) **ผู้เชี่ยวชาญด้านการตรวจสอบความมั่นคงปลอดภัยสารสนเทศ:** จะต้องมีประสบการณ์ทำงานไม่น้อยกว่า ๑๐ ปี และวุฒิการศึกษาไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ/สาขาคอมพิวเตอร์/สาขาวิศวกรรม/สาขาวิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านการตรวจสอบ (audit) เทคโนโลยีสารสนเทศ Certified Information Systems Auditor (CISA) และด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ Lead Auditor

รายการ	ประสบการณ์ (ปี)	วุฒิการศึกษา	สาขาวิชา
ผู้เชี่ยวชาญด้านการตรวจสอบความมั่นคงปลอดภัยสารสนเทศ	๑๐	ไม่ต่ำกว่าปริญญาโท	เทคโนโลยีสารสนเทศ/คอมพิวเตอร์/วิศวกรรม/วิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านการตรวจสอบ (audit) เทคโนโลยีสารสนเทศ Certified Information Systems Auditor (CISA) และด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ Lead Auditor

คะแนนเต็ม ๓ คะแนน (ร้อยละ ๑๐๐)							
ระยะเวลาทำงาน (๑.๒ คะแนน/ ร้อยละ ๔๐)			ด้านประสบการณ์เฉพาะตำแหน่ง (๑.๒ คะแนน/ ร้อยละ ๔๐)			วุฒิการศึกษา* (๐.๖ คะแนน/ ร้อยละ ๒๐)	
ตั้งแต่ ๒๐ ปีขึ้นไป	๑๖ - ๑๙ ปี	๑๐ – ๑๕ ปี	๕ โครงการขึ้นไป	๓ - ๔ โครงการ	๑ - ๒ โครงการ	ปริญญาเอก	ปริญญาโท
๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๐.๖ คะแนน)	๗๐ (๐.๔๒ คะแนน)

หมายเหตุ: * กรณีไม่มีใบประกาศนียบัตรตามที่ระบุ จะคิดคะแนนร้อยละ ๕๐ ของคะแนนวุฒิการศึกษาที่ได้

(๑๐) ผู้เชี่ยวชาญด้านการพัฒนาระบบ : จะต้องมีประสบการณ์ทำงานไม่น้อยกว่า ๑๐ ปี และวุฒิการศึกษาไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ/สาขาคอมพิวเตอร์/สาขาวิศวกรรม/สาขาวิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง

รายการ	ประสบการณ์ (ปี)	วุฒิการศึกษา	สาขาวิชา
ผู้เชี่ยวชาญด้านการพัฒนาระบบ	๑๐	ไม่ต่ำกว่าปริญญาโท	เทคโนโลยีสารสนเทศ/คอมพิวเตอร์/วิศวกรรม/วิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง

คะแนนเต็ม ๓ คะแนน (ร้อยละ ๑๐๐)							
ระยะเวลาทำงาน (๑.๒ คะแนน/ ร้อยละ ๔๐)			ด้านประสบการณ์เฉพาะตำแหน่ง (๑.๒ คะแนน/ ร้อยละ ๔๐)			วุฒิการศึกษา* (๐.๖ คะแนน/ ร้อยละ ๒๐)	
ตั้งแต่ ๒๐ ปีขึ้นไป	๑๖ - ๑๙ ปี	๑๐ – ๑๕ ปี	๕ โครงการขึ้นไป	๓ - ๔ โครงการ	๑ - ๒ โครงการ	ปริญญาเอก	ปริญญาโท
๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๐.๖ คะแนน)	๗๐ (๐.๔๒ คะแนน)

(๑๑) ผู้เชี่ยวชาญด้านระบบคอมพิวเตอร์ จะต้องมีประสบการณ์ทำงานไม่น้อยกว่า ๑๐ ปี และวุฒิการศึกษาไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ/สาขาคอมพิวเตอร์/สาขาวิศวกรรม/สาขาวิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง

รายการ	ประสบการณ์ (ปี)	วุฒิการศึกษา	สาขาวิชา
ผู้เชี่ยวชาญด้านระบบคอมพิวเตอร์	๑๐	ไม่ต่ำกว่าปริญญาโท	เทคโนโลยีสารสนเทศ/คอมพิวเตอร์/วิศวกรรม/วิทยาการคอมพิวเตอร์/สาขาที่เกี่ยวข้อง

คะแนนเต็ม ๓ คะแนน (ร้อยละ ๑๐๐)							
ระยะเวลาทำงาน (๑.๒ คะแนน/ ร้อยละ ๔๐)			ด้านประสบการณ์เฉพาะตำแหน่ง (๑.๒ คะแนน/ ร้อยละ ๔๐)			วุฒิการศึกษา* (๐.๖ คะแนน/ ร้อยละ ๒๐)	
ตั้งแต่ ๒๐ ปีขึ้นไป	๑๖ - ๑๙ ปี	๑๐ – ๑๕ ปี	๕ โครงการขึ้นไป	๓ - ๔ โครงการ	๑ - ๒ โครงการ	ปริญญาเอก	ปริญญาโท
๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๑.๒ คะแนน)	๘๕ (๑.๐๒ คะแนน)	๗๐ (๐.๘๔ คะแนน)	๑๐๐ (๐.๖ คะแนน)	๗๐ (๐.๔๒ คะแนน)

๑๐. บุคลากรที่ต้องการ

บุคลากรของทีมงานที่ปรึกษา จะต้องมีความรู้ ความเชี่ยวชาญ และประสบการณ์ ในด้านต่าง ๆ ดังนี้

ลำดับ	รายการ	จำนวน (คน)	ประสบการณ์ในด้านที่เกี่ยวข้องไม่น้อยกว่า (ปี)	วุฒิการศึกษา
(๑) บุคลากรหลัก				
(๑.๑)	ผู้จัดการโครงการ	๑	๑๕	ไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ สาขาคอมพิวเตอร์ สาขาวิศวกรรม สาขาวิทยาการคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้อง
(๑.๒)	รองผู้จัดการโครงการ	๑	๑๐	ไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ สาขาคอมพิวเตอร์ สาขาวิศวกรรม สาขาวิทยาการคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้อง
(๑.๓)	ผู้เชี่ยวชาญด้านแผนงานเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัย	๑	๑๕	ไม่ต่ำกว่าปริญญาตรี สาขาเทคโนโลยีสารสนเทศ สาขาคอมพิวเตอร์ สาขาวิศวกรรม สาขาวิทยาการคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านความมั่นคงปลอดภัยสารสนเทศ CompTIA Security+ หรือ ISO/IEC ๒๗๐๐๑
(๑.๔)	ผู้เชี่ยวชาญด้านวิศวกรรมระบบราง	๑	๑๐	ไม่ต่ำกว่าปริญญาโท สาขาวิศวกรรมระบบราง สาขาวิศวกรรมขนส่งทางราง สาขาวิศวกรรมโยธา สาขาวิศวกรรมโลจิสติกส์ สาขาโลจิสติกส์ หรือสาขาที่เกี่ยวข้อง
(๑.๕)	ผู้เชี่ยวชาญด้านการจัดการนโยบายและบริหารความเสี่ยง	๑	๑๐	ไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ สาขาคอมพิวเตอร์ สาขาวิศวกรรม สาขาวิทยาการคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑

ลำดับ	รายการ	จำนวน (คน)	ประสบการณ์ในด้านที่เกี่ยวข้องไม่น้อยกว่า (ปี)	วุฒิการศึกษา
(๑.๖)	ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ	๑	๑๕	ไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ สาขาคอมพิวเตอร์ สาขาวิศวกรรม สาขาวิทยาการคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้อง
(๑.๗)	ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์	๑	๑๕	ไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ สาขาคอมพิวเตอร์ สาขาวิศวกรรม สาขาวิทยาการคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านความมั่นคงปลอดภัยไซเบอร์ CCE (Certified Cybersecurity Expert)
(๑.๘)	ผู้เชี่ยวชาญด้านการประเมินความมั่นคงปลอดภัยไซเบอร์ทางเทคโนโลยีสารสนเทศ (IT Assessment)	๑	๑๐	ไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ สาขาคอมพิวเตอร์ สาขาวิศวกรรม สาขาวิทยาการคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านความมั่นคงปลอดภัยไซเบอร์ CCE (Certified Cybersecurity Expert)
(๑.๙)	ผู้เชี่ยวชาญด้านการตรวจสอบความมั่นคงปลอดภัยสารสนเทศ	๑	๑๐	ไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ สาขาคอมพิวเตอร์ สาขาวิศวกรรม สาขาวิทยาการคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้อง และมีประกาศนียบัตรด้านการตรวจสอบ (audit) เทคโนโลยีสารสนเทศ Certified Information Systems Auditor (CISA) และด้านความมั่นคงปลอดภัยสารสนเทศISO/IEC ๒๗๐๐๑ Lead Auditor

ลำดับ	รายการ	จำนวน (คน)	ประสบการณ์ในด้านที่เกี่ยวข้องไม่น้อยกว่า (ปี)	วุฒิการศึกษา
(๑.๑๐)	ผู้เชี่ยวชาญด้านการพัฒนาระบบ	๑	๑๐	ไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ สาขาคอมพิวเตอร์ สาขาวิศวกรรม สาขาวิทยาการคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้อง
(๑.๑๑)	ผู้เชี่ยวชาญด้านระบบคอมพิวเตอร์	๑	๑๐	ไม่ต่ำกว่าปริญญาโท สาขาเทคโนโลยีสารสนเทศ สาขาคอมพิวเตอร์ สาขาวิศวกรรม สาขาวิทยาการคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้อง
(๒) บุคลากรสนับสนุน				
(๒.๑)	ผู้ช่วยผู้เชี่ยวชาญ	๔	๕	ไม่ต่ำกว่าปริญญาตรี
(๒.๒)	เลขานุการ	๑	๕	ไม่ต่ำกว่าปริญญาตรี
(๒.๓)	เจ้าหน้าที่บันทึกข้อมูล	๓	๕	ไม่ต่ำกว่า ปวส.
(๒.๔)	พนักงานรับ-ส่งเอกสาร	๑	-	-

๑๑. อัตราค่าปรับ

กรณีที่ที่ปรึกษาไม่ทำงานแล้วเสร็จตามเวลาที่กำหนด ที่ปรึกษาจะต้องเสียค่าปรับให้แก่ผู้ว่าจ้างเป็นรายวันในอัตราร้อยละ ๐.๐๒ ของวงเงินค่าจ้าง นับถัดจากวันครบกำหนด จนถึงวันที่ที่ปรึกษาปฏิบัติตามสัญญาถูกต้องครบถ้วน และได้ตรวจรับงานแล้ว

๑๒. เงินประกันผลงาน

ในการจ่ายเงินให้แก่ที่ปรึกษาแต่ละงวด ผู้ว่าจ้างจะหักเงินจำนวนร้อยละ ๕ (ห้า) ของเงินที่ต้องจ่ายในงวดนั้นเพื่อเป็นประกันผลงาน หรือที่ปรึกษาอาจนำหนังสือค้ำประกันของธนาคารหรือหนังสือค้ำประกันอิเล็กทรอนิกส์ของธนาคารภายในประเทศซึ่งมีอายุการค้ำประกันตลอดอายุสัญญามามอบให้ผู้ว่าจ้าง ทั้งนี้ เพื่อเป็นหลักประกันแทนก็ได้

ผู้ว่าจ้างจะคืนเงินประกันผลงาน และ/หรือหนังสือค้ำประกันของธนาคารดังกล่าวตามวรรคหนึ่ง โดยไม่มีดอกเบี้ยให้แก่ที่ปรึกษาพร้อมกับการจ่ายเงินค่าจ้างงวดสุดท้าย

๑๓. หลักประกันสัญญา

ที่ปรึกษาซึ่งมิใช่หน่วยงานของรัฐที่ได้รับคัดเลือกให้ทำสัญญาจ้างที่ปรึกษากับ ขร. ต้องวางหลักประกันสัญญาจ้างที่ปรึกษาเป็นจำนวนเงินเท่ากับร้อยละ ๕ ของราคาจ้างที่ปรึกษาให้ ขร. ยึดถือไว้ในขณะทำสัญญาโดยใช้หลักประกันอย่างหนึ่งอย่างใด ดังต่อไปนี้

๑๓.๑ เงินสด

๑๓.๒ เช็คหรือดราฟท์ ที่ธนาคารเซ็นสั่งจ่าย โดยเป็นเช็คหรือดราฟท์ลงวันที่ที่ใช้เช็คหรือดราฟท์นั้นชำระต่อเจ้าหน้าที่ในวันทำสัญญา หรือก่อนวันนั้นไม่เกิน ๓ วันทำการ

๑๓.๓ หนังสือค้ำประกันของธนาคารภายในประเทศ ตามแบบที่คณะกรรมการนโยบายกำหนด โดยอาจเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนดก็ได้

๑๓.๔ หนังสือค้ำประกันของบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด

๑๓.๕ พันธบัตรรัฐบาลไทย

หลักประกันนี้จะคืนให้ โดยไม่มีดอกเบี้ยภายใน ๑๕ วันนับถัดจากวันที่ที่ปรึกษาพ้นจากข้อผูกพันตามสัญญาจ้างที่ปรึกษาแล้ว

๑๔. เอกสารการยื่นข้อเสนอ

ที่ปรึกษาจะต้องยื่นซองข้อเสนอซึ่งประกอบด้วย ซองใบเสนอราคา และเอกสารตามข้อ ๑๔.๑ และข้อ ๑๔.๒ ซึ่งแยกไว้นอกซองใบเสนอราคา โดยแยกเป็น ๒ ส่วน ดังต่อไปนี้

๑๔.๑ ส่วนที่ ๑ อย่างน้อยต้องมีเอกสารดังต่อไปนี้

๑๔.๑.๑ ในกรณีที่ปรึกษาเป็นนิติบุคคล

๑) ห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล บัญชีรายชื่อหุ้นส่วนผู้จัดการ ผู้มีอำนาจควบคุม (ถ้ามี) พร้อมรับรองสำเนาถูกต้อง

๒) บริษัทจำกัดหรือบริษัทมหาชนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล หนังสือบริคณห์สนธิ บัญชีรายชื่อกรรมการผู้จัดการ ผู้มีอำนาจควบคุม (ถ้ามี) และบัญชีผู้ถือหุ้นรายใหญ่ (ถ้ามี) พร้อมรับรองสำเนาถูกต้อง

๑๔.๑.๒ ในกรณีที่ปรึกษาเป็นบุคคลธรรมดาหรือคณะบุคคลที่มิใช่นิติบุคคล ให้ยื่นสำเนาบัตรประจำตัวประชาชนของผู้นั้น สำเนาข้อตกลงที่แสดงถึงการเข้าเป็นหุ้นส่วน (ถ้ามี) สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วน พร้อมทั้งรับรองสำเนาถูกต้อง

๑๔.๑.๓ ในกรณีที่ปรึกษาเป็นที่ปรึกษาร่วมกันในฐานะเป็นผู้ร่วมค้า ให้ยื่นสำเนาสัญญาของการเข้าร่วมค้าและเอกสารตามที่ระบุไว้ใน ๑๔.๑.๑ หรือ ๑๔.๑.๒ ของผู้ร่วมค้า แล้วแต่กรณี

๑๔.๑.๔ เอกสารเพิ่มเติมอื่น ๆ

(๑) สำเนาใบทะเบียนภาษีมูลค่าเพิ่ม (ถ้ามี) พร้อมรับรองสำเนาถูกต้อง

(๒) สำเนาทะเบียนพาณิชย์ พร้อมรับรองสำเนาถูกต้อง

(๓) เอกสารแสดงฐานะทางการเงิน

๑๔.๑.๕ บัญชีเอกสารส่วนที่ ๑ ทั้งหมดที่ได้ยื่นพร้อมกับซองใบเสนอราคา

๑๔.๒ ส่วนที่ ๒ อย่างน้อยต้องมีเอกสารดังต่อไปนี้

๑๔.๒.๑ หนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมายในกรณีที่ที่ปรึกษามอบอำนาจให้บุคคลอื่นลงลายมือชื่อให้ชัดเจน หรือหลักฐานแสดงตัวตนของที่ปรึกษาในการเสนอราคาแทน

๑๔.๒.๒ สำเนาหนังสือรับรองการขึ้นทะเบียนเป็นที่ปรึกษาของศูนย์ข้อมูลที่ปรึกษากระทรวงการคลัง พร้อมรับรองสำเนาถูกต้อง

๑๔.๒.๓ การเสนอที่ปรึกษาหลักจะต้องแสดงหลักฐานเพื่อการตรวจสอบ ดังนี้

(๑) หากเป็นที่ปรึกษาประจำทำงานเต็มเวลาในบริษัทที่ปรึกษา หมายถึง ที่ปรึกษาที่เป็นพนักงานประจำเต็มเวลา (Full Time) และมีระยะเวลาปฏิบัติงานกับบริษัทไม่น้อยกว่า ๖ เดือน การเสนอที่ปรึกษาหลักจะต้องแสดงหลักฐานเพื่อการตรวจสอบ ๒ ประเภท ได้แก่

ประเภทที่ ๑ หลักฐานบุคคล ประกอบด้วย

๑) หลักฐานแสดงการเป็นพนักงานประจำเต็มเวลากับบริษัทที่ปรึกษา โดยมีระยะเวลาไม่น้อยกว่า ๖ เดือน

๒) หนังสือแสดงอัตราเงินเดือนที่นำไปใช้เป็นเงินเดือนพื้นฐาน (Basic Salary) ในการคิดค่าตอบแทน ซึ่งจะต้องเป็นหลักฐานแสดงการยื่นชำระภาษีเงินได้ต่อกรมสรรพากรที่สามารถแสดงความเป็นพนักงานประจำของบริษัท เช่น แบบ ภง.ด. ๑ , ภง.ด. ๑ก , ภง.ด. ๙๐ หรือ ภง.ด. ๙๑ เฉพาะบุคคลที่เสนอเท่านั้น พร้อมใบปะหน้าและใบเสร็จรับเงินจากกรมสรรพากร

ประเภทที่ ๒ หลักฐานแสดงการพัฒนาของบริษัทตามวัตถุประสงค์ ประกอบด้วย

๑) ใบรับรองระบบคุณภาพที่เป็นที่ยอมรับตามมาตรฐานสากล เพื่อเป็นการแสดงว่าบริษัทมีการพัฒนาระบบคุณภาพอย่างต่อเนื่อง เช่น ระบบ ISO

๒) มีหลักฐานการมีซอฟแวร์ที่ถูกกฎหมายสำหรับพนักงานไว้ใช้งานอย่างน้อยร้อยละ ๓๐ ของพนักงานบริษัท

๓) มีใบรับรองการประกันวิชาชีพ (Professional Indemnity Insurance) ของบริษัทในมูลค่าไม่ต่ำกว่า ๓๐ ล้านบาท ในปีที่ยื่นข้อเสนอ

ทั้งนี้ หากบริษัทที่ปรึกษาไม่สามารถแสดงหลักฐานตามประเภทที่ ๒ ได้ครบทั้งหมดได้ ตัวคูณอัตราค่าตอบแทนจะปรับลดตามกรณีต่าง ๆ ดังนี้

หลักฐานบริษัท	ตัวคูณอัตราค่าตอบแทน
กรณีที่ ๑ มีหลักฐานครบทั้ง ๓ ข้อ	๒.๖๔๐
กรณีที่ ๒ มีหลักฐานเพียง ๒ ข้อ	๒.๕๘๕
กรณีที่ ๓ มีหลักฐานเพียง ๑ ข้อ	๒.๕๓๐
กรณีที่ ๔ ไม่มีหลักฐาน	๒.๔๗๕

(๒) หากเป็นที่ปรึกษาที่ไม่ได้ทำงานประจำในบริษัทที่ปรึกษา เช่น ที่ปรึกษาอิสระและที่ปรึกษาจากสถาบันของรัฐ โดยค่าตัวคูณสำหรับที่ปรึกษาที่ไม่ได้ทำงานประจำเต็มเวลาตัวคูณอัตราค่าตอบแทนเท่ากับ ๑.๔๓ เท่าของเงินเดือนพื้นฐาน ทั้งนี้ ที่ปรึกษาดังกล่าวจะต้องแสดงหลักฐานอัตราค่าตอบแทนที่เคยได้รับและสามารถอ้างอิงได้มาแสดง

สำหรับกรณีสถาบันของรัฐที่ให้บริการงานที่ปรึกษา อัตราค่าตอบแทนเท่ากับ ๑.๗๖ ซึ่งในการเสนองานจะต้องแสดงหลักฐาน ดังนี้

(๒.๑) หลักฐานการจ้างที่สามารถนำมาคำนวณเป็นอัตราเงินเดือนพื้นฐานได้ เช่น ที่ปรึกษาในโครงการในอดีต (ถ้าหากไม่สามารถนำหลักฐานมาแสดง ให้ใช้อัตราเงินเดือนของบุคลากรที่มีคุณสมบัติเท่าเทียมกันภายในบริษัทมาแสดง)

(๒.๒) หนังสือรับรองการชำระภาษีเงินได้บุคคลธรรมดาของที่ปรึกษาแต่ละคน

- ในกรณีบริษัทที่ปรึกษาเสนองานและได้รับการคัดเลือกมีการยืมตัวที่ปรึกษาที่มีคุณสมบัติเหมาะสมกับตำแหน่งจากบริษัทอื่น ให้ใช้หลักฐานอัตราเงินเดือนจากบริษัทที่สังกัดมาแสดง

- ในกรณีที่ปรึกษาอิสระสามารถอ้างอิงอัตราเงินเดือนจากงานในลักษณะเดียวกันที่เคยได้รับ

๑๔.๒.๔ รายละเอียดและขอบเขตงานจ้าง เช่น

(๑) หนังสือรับรองผลงานการจ้างที่ปรึกษาประเภทเดียวกันและเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ หรือหน่วยงานเอกชนที่ ขร. เชื่อถือ

(๒) รายละเอียดคุณวุฒิการศึกษา ความเชี่ยวชาญหรือประสบการณ์ของบุคลากรหลัก พร้อมเอกสารหลักฐานอ้างอิง

(๓) งบแสดงฐานะทางการเงินที่มีการตรวจรับรองแล้ว

(๔) วิธีการบริหารและวิธีการปฏิบัติงาน ประกอบด้วย ความเข้าใจวัตถุประสงค์ของการศึกษา แนวทางการศึกษา วิธีการทำงาน และความครอบคลุมครบถ้วนตาม TOR แผนการดำเนินงานและการจัดสรรบุคลากรที่เหมาะสมกับขอบเขตการศึกษา และข้อเสนออื่น ๆ ตามขอบเขตของงาน

๑๔.๒.๕ บัญชีเอกสารส่วนที่ ๒ ทั้งหมดที่ได้ยื่นพร้อมกับซองข้อเสนอ

๑๕. ความรับผิดชอบของที่ปรึกษา

๑๕.๑ ที่ปรึกษาต้องจัดหาอุปกรณ์สำนักงานทั้งหมดที่จำเป็นเพื่อให้การทำงานตามขอบเขตของงานจ้างที่ปรึกษาบรรลุตามวัตถุประสงค์ และเมื่อการศึกษาเสร็จสิ้นต้องส่งมอบอุปกรณ์สำนักงานที่จัดหาโดยงบประมาณของโครงการนี้ทั้งหมดให้แก่ ขร.

๑๕.๒ ที่ปรึกษาต้องดำเนินการโดยจะต้องใช้ความรู้ความชำนาญทางเทคนิคและวิทยาการอย่างดีที่สุดให้สอดคล้องเหมาะสมตามมาตรฐานสากลและจะต้องเข้าร่วมประชุมชี้แจงและจัดเตรียมเอกสารข้อมูลสนับสนุนเมื่อได้รับแจ้งจาก ขร. อย่างไรก็ตาม การใช้มาตรฐานดังกล่าวอาจจำเป็นต้องปรับแก้เป็นอย่างอื่น หากพิจารณาแล้วเห็นว่าเหมาะสมกับประเทศไทย

๑๕.๓ ในระหว่างการศึกษาที่ปรึกษาต้องจัดเตรียมข้อมูลทั้งหมดที่เกี่ยวข้องกับการศึกษานี้และพร้อมให้ ขร. ตรวจสอบได้ตลอดเวลา รวมทั้งจะต้องดำเนินการปรับปรุงแก้ไขข้อมูลตามที่ ขร. แจ้ง โดยที่ปรึกษาต้องรับผิดชอบค่าใช้จ่ายทั้งสิ้น

๑๕.๔ ในระหว่างการศึกษา ที่ปรึกษาต้องเก็บรักษาข้อมูล เอกสารต้นฉบับ สำเนา หรือรูปภาพที่เกี่ยวข้องกับการศึกษานี้ทั้งหมดไว้เป็นความลับ และห้ามนำมาเปิดเผยหรือเผยแพร่หากไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจาก ขร. และจะต้องส่งมอบให้ ขร. เมื่อการศึกษาเสร็จสิ้น

๑๕.๕ เมื่อมีความจำเป็นเกิดขึ้นระหว่าง และ/หรือหลังสิ้นสุดสัญญาจ้างแล้ว ที่ปรึกษาต้องพร้อมที่จะช่วยเหลือ สนับสนุนการดำเนินงาน และให้บริการคำปรึกษาเป็นอย่างดีโดยไม่ชักช้าแก่ ขร. และหน่วยงานที่เกี่ยวข้อง โดยไม่คิดค่าใช้จ่ายใด ๆ เพิ่มเติม

๑๕.๖ ที่ปรึกษาจะต้องเป็นผู้ดำเนินการและรับผิดชอบค่าใช้จ่ายของงานทั้งหมดในการดำเนินงานและวิธีการได้มาซึ่งข้อมูลและวัสดุทั้งหลายตามสัญญาจ้างตาม TOR ประกอบสัญญาจ้างและข้อเสนอต่าง ๆ ของที่ปรึกษา

๑๕.๗ ในระหว่างการศึกษา หากมีความจำเป็นต้องเชิญผู้แทนอื่นหรือผู้ทรงคุณวุฒิเข้าร่วมประชุม เพื่อให้ข้อมูล ข้อคิดเห็น หรือข้อเสนอแนะ ที่ปรึกษาจะต้องรับผิดชอบค่าใช้จ่ายยานพาหนะหรือสิ่งอำนวยความสะดวกต่าง ๆ ที่จำเป็นของผู้แทนหรือผู้ทรงคุณวุฒิดังกล่าว

๑๕.๘ ข้อมูล เอกสารต้นฉบับ สำเนา แบบแปลน หรือรูปภาพที่เกี่ยวข้องกับการศึกษานี้ ถือเป็นสมบัติของ ขร. โดยระหว่างการศึกษา ที่ปรึกษาต้องเก็บรักษาไว้เป็นความลับ และห้ามนำมาเปิดเผยหรือเผยแพร่หากไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจาก ขร. ทั้งนี้ ต้องส่งมอบให้ ขร. เมื่อการศึกษาเสร็จสิ้น

๑๖. การบริหารโครงการ

เพื่อให้การดำเนินงานสำเร็จลุล่วงตามวัตถุประสงค์ของโครงการ ขร. จะสนับสนุนการดำเนินงานของที่ปรึกษาตามความจำเป็น โดยจะแต่งตั้งคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เพื่อกำกับและติดตามงานจ้างที่ปรึกษาให้เป็นไปตามเงื่อนไขที่กำหนดไว้ในสัญญา

๑๗. เงื่อนไขและคุณสมบัติของที่ปรึกษาที่จะเข้าเป็นคู่สัญญา

๑๗.๑ ที่ปรึกษาที่จะเข้าเป็นคู่สัญญากับ ขร. ซึ่งได้ดำเนินการจัดซื้อจัดจ้างด้วยระบบอิเล็กทรอนิกส์ (e-Government Procurement : e-GP) ต้องลงทะเบียนในระบบอิเล็กทรอนิกส์ของกรมบัญชีกลางที่เว็บไซต์ระบบการจัดซื้อจัดจ้างภาครัฐ (www.gprocurement.go.th)

๑๗.๒ ที่ปรึกษาที่จะเข้าเป็นคู่สัญญาต้องดาวน์โหลดไฟล์ Excel Loader ทางอินเทอร์เน็ตได้ที่เว็บไซต์ https://consult.mot.go.th/PreProject/ExportExcelForm/๑๘๖๒๒ และกรอกข้อมูลในไฟล์ Excel Loader ให้ถูกต้องและครบถ้วนบรรจุลงในสื่อบันทึกข้อมูลชนิด USB Flash Drive ส่งมาพร้อมข้อเสนอในวันยื่นข้อเสนอ

๑๗.๓ ข้อมูลบุคลากรที่ที่ปรึกษาที่จะเข้าเป็นคู่สัญญายื่นต่อ ขร. นั้น ที่ปรึกษายินยอมให้จัดเก็บไว้ในระบบศูนย์ข้อมูลบุคลากรที่ปรึกษากลางของกระทรวงคมนาคม และยินยอมให้ดำเนินการตามแนวปฏิบัติการใช้งานของศูนย์ข้อมูลบุคลากรที่ปรึกษากลางของกระทรวงคมนาคม

๑๘. ข้อสงวนสิทธิ์

๑๘.๑ ที่ปรึกษาที่ได้รับคัดเลือกให้ดำเนินการตามโครงการนี้จะต้องลงนามในสัญญากับ ขร. ภายในระยะเวลาที่ ขร. แจ้งให้ทราบ หากพ้นระยะเวลาดังกล่าวแล้วยังไม่ลงนามในสัญญา ขร. จะถือว่าที่ปรึกษาสละสิทธิ์ในการทำสัญญาและอาจพิจารณาเรียกร้องให้ชดใช้ความเสียหาย (ถ้ามี) รวมทั้งพิจารณาให้เป็นผู้ทิ้งงานตามระเบียบของทางราชการ

๑๘.๒ การจัดซื้อจัดจ้างครั้งนี้จะมีการลงนามในสัญญาหรือข้อตกลงเป็นหนังสือได้ต่อเมื่อพระราชบัญญัติงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๘ มีผลใช้บังคับ และได้รับจัดสรรงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๘ จากสำนักงบประมาณแล้ว และกรณีที่หน่วยงานของรัฐไม่ได้รับจัดสรรงบประมาณเพื่อการจัดซื้อจัดจ้างในครั้งดังกล่าว หน่วยงานของรัฐสามารถยกเลิกการจัดซื้อจัดจ้างได้

๑๘.๓ ขร. ขอสงวนสิทธิ์ที่จะยกเลิกการดำเนินการจ้างครั้งนี้ได้ทุกขั้นตอนโดยไม่จำเป็นต้องแจ้งเหตุผลใด ๆ ให้ผู้ยื่นข้อเสนอทราบ และผู้ยื่นข้อเสนอไม่มีสิทธิ์โต้แย้งและเรียกร้องค่าใช้จ่ายหรือค่าเสียหายใด ๆ ทั้งสิ้น ทั้งนี้ จะก่อหนี้ผูกพันได้ก็ต่อเมื่อได้รับอนุมัติเงินประจำงวดจากสำนักงบประมาณแล้ว

๑๙. ผลที่คาดว่าจะได้รับจากการศึกษา

๑๙.๑ ผลการศึกษาและวิเคราะห์บริบทขององค์กรตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และที่เกี่ยวข้อง

๑๙.๒ นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ทางราง ที่สอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ – ๒๕๗๐)

๑๙.๓ ประมวลแนวทางปฏิบัติ (แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และแผนการรับมือภัยคุกคามทางไซเบอร์) และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑๙.๔ มาตรฐานขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑๙.๕ ผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางรางตามมาตรฐานขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒๐. กรรมสิทธิ์ในข้อมูล เอกสารและผลการดำเนินงาน

ข้อมูลและเอกสารที่เกิดขึ้นจากการดำเนินงานของผู้รับจ้างภายใต้โครงการนี้ ถือเป็นกรรมสิทธิ์ของผู้ว่าจ้าง ผู้รับจ้างจะนำไปเผยแพร่หรือใช้เพื่อวัตถุประสงค์ใด ๆ มิได้ เว้นแต่จะได้รับการยินยอมเป็นลายลักษณ์อักษรจากผู้ว่าจ้างเท่านั้น

๒๑. หน่วยงานผู้รับผิดชอบดำเนินการ

หน่วยงานที่รับผิดชอบ : กลุ่มเทคโนโลยีและสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมการขนส่งทางราง

สถานที่ติดต่อ : อาคาร ณ ถลาง ชั้น ๔ เลขที่ ๕๑๔/๑ อาคาร ณ ถลาง แขวงสี่แยกมหานาค เขตดุสิต กรุงเทพมหานคร ๑๐๓๐๐

หมายเลขโทรศัพท์ : ๐ ๒๑๖๔ ๒๖๒๖ ต่อ ๕๗๐๑ Email : it@drt.go.th

๒๒. สถานที่ติดต่อเพื่อขอรับข้อมูลเพิ่มเติมหรือเสนอแนะวิจารณ์ หรือแสดงความคิดเห็นโดยเปิดเผยตัว

ผู้สนใจสามารถดูรายละเอียดได้ที่ www.drt.go.th หรือสอบถามมายังหมายเลขโทรศัพท์ ๐ ๒๑๖๔ ๒๖๒๖ ต่อ ๕๗๐๑ ในวัน เวลาราชการ

กรมการขนส่งทางราง