1. **บทนำ**

บริษัท ที-เน็ต จำกัด ก่อตั้งขึ้นเมื่อ วันที่ 2 กันยายน 2551 โดยสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ภายใต้กระทรวงวิทยาศาสตร์และเทคโนโลยี ตามนโยบายการแปรรูปหน่วยงานวิจัยเป็นบริษัท เพื่อเป็นกลไกสำหรับการถ่ายทอดเทคโนโลยีสู่ภาคธุรกิจ รวมทั้งเป็นการส่งเสริมให้เกิดผู้ประกอบการเทคโนโลยีรายใหม่ที่มีความสามารถ ทั้งในด้านการพัฒนาเทคโนโลยี และด้านธุรกิจ ซึ่งสามารถสร้างคุณค่าต่อการพัฒนาวิทยาศาสตร์และเทคโนโลยี ต่อระบบเศรษฐกิจของประเทศ โดยมีวัตถุประสงค์ทางธุรกิจหลักคือ การให้บริการรักษาความปลอดภัยระบบเครือข่ายสารสนเทศขององค์กรที่ครบวงจร เน้นการให้บริการที่หลากหลาย ปัจจุบันบริษัทฯ ดำเนินงานมาแล้วเป็นระยะเวลา 15 ปี ได้รับความไว้วางใจจากลูกค้าทั้งภาครัฐ และเอกชนให้ที่ปรึกษามาตรฐานสากล และกฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ อีกทั้งยังมีความร่วมมือกับหน่วยงานภาครัฐในการดำเนินงานร่วมกัน เช่น สถาบันพัฒนาบุคลากรแห่งอนาคต ของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (Career for the Future Academy : CFA) เป็นต้น บริษัทฯ มีพนักงานที่มีพื้นฐานการเป็นนักวิจัย นักวิชาการ และได้ถ่ายทอดแนวคิดการดำเนินงานเชิงวิชาการแก่พนักงานรุ่นใหม่ เพื่อพัฒนาและส่งเสริมบุคลากรทางด้านInformation & Cyber Security ให้เพิ่มมากยิ่งขึ้นอันเป็นที่ต้องการของประเทศ

ตามที่สำหรับกองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล มีความประสงค์ จัดทำกิจกรรมโครงการจ้างดำเนินงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2022 ได้มีการศึกษาและจัดทำแบบประเมิน ระดับความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมคู่มือ จะเป็นการนำแบบประเมินดังกล่าวไปใช้ในการประเมินหน่วยงานเป้าหมาย ประกอบด้วย หน่วยงานของรัฐหน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ในการนี้ บริษัท ที-เน็ต จำกัด จึงได้จัดทำข้อเสนอโครงการจ้างดำเนินงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2022 สำหรับกองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล โดยมีรายละเอียดตามเอกสารฉบับนี้

1. **วัตถุประสงค์**
   1. เพื่อปรับปรุงระบบบริหารความมั่นคงปลอดภัยสารสนเทศของศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ให้มีความมั่นคงปลอดภัย
   2. เพื่อให้การบริการโครงสร้างพื้นฐานสารสนเทศของศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล มีความมั่นคงปลอดภัยสอดคล้องกับมาตรฐานสากล ISO/IEC 27001:2022
   3. เพื่อขอการรับรองมาตรฐานสากล ISO/IEC 27001:2022 สำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล
2. **ความสอดคล้องคุณสมบัติของที่ปรึกษา**

|  |  |  |  |
| --- | --- | --- | --- |
| **คุณสมบัติตามที่กำหนดใน TOR** | **คุณสมบัติของบริษัทฯ** | **ความสอดคล้อง** | **เอกสารอ้างอิง** |
| * 1. มีความสามารถตามกฎหมาย | 1. มีความสามารถตามกฎหมาย | สอดคล้อง | ภาคผนวก ก. เอกสารบริษัทฯ  ปปปป |
| * 1. ไม่เป็นบุคคลลมละลาย | 1. ไม่เป็นบุคคลลมละลาย | สอดคล้อง | ภาคผนวก ก. เอกสารบริษัทฯ  ปปปป |
| * 1. ไม่อยูระหวางเลิกกิจการ | 1. ไม่อยูระหวางเลิกกิจการ | สอดคล้อง | ภาคผนวก ก. เอกสารบริษัทฯ  ปปปป |
| * 1. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไวชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผานเกณฑการประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพรในระบบเครือข่ายสารสนเทศของ กรมบัญชีกลาง | 1. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไวชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผานเกณฑการประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพรในระบบเครือข่ายสารสนเทศของ กรมบัญชีกลาง | สอดคล้อง | ภาคผนวก ก. เอกสารบริษัทฯ  ปปปป |
| * 1. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไวในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อใหเป็นผู้ทิ้งงานของหนวยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดําเนินงานในกิจการของนิติบุคคลนั้นดวย | 1. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไวในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อใหเป็นผู้ทิ้งงานของหนวยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดําเนินงานในกิจการของนิติบุคคลนั้นดวย | สอดคล้อง | ภาคผนวก ก. เอกสารบริษัทฯ  ปปปป |
| * 1. มีคุณสมบัติและไม่มีลักษณะ ตองหามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหาร พัสดุภาครัฐกำหนดในราชกิจจานุเบกษา | 1. มีคุณสมบัติและไม่มีลักษณะตอง หามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหาร พัสดุภาครัฐกำหนดในราชกิจจานุเบกษา | สอดคล้อง | ภาคผนวก ก. เอกสารบริษัทฯ  ปปปป |
| * 1. เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกสหรือที่จะดําเนินการ | 1. เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกสหรือที่จะดําเนินการ | สอดคล้อง | ภาคผนวก ก. เอกสารบริษัทฯ  ปปปป |
| * 1. ไม่เป็นผู้มีผลประโยชนรวมกันกับผู้ยื่นข้อเสนอรายอื่นที่เขายื่นข้อเสนอใหแกมหาวิทยาลัยมหิดล ณ วันประกาศประกวดราคาอิเล็กทรอนิกส/วันยื่นข้อเสนอ หรือไม่เป็นผู้กระทําการอันเป็นการขัดขวางการแขงขันอยางเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส/ในการยื่นข้อเสนอครั้งนี้ | 1. ไม่เป็นผู้มีผลประโยชนรวมกันกับผู้ยื่นข้อเสนอรายอื่นที่เขายื่นข้อเสนอใหแกมหาวิทยาลัยมหิดล ณ วันประกาศประกวดราคาอิเล็กทรอนิกส/วันยื่นข้อเสนอ หรือไม่เป็นผู้กระทําการอันเป็นการขัดขวางการแขงขันอยางเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส/ในการยื่นข้อเสนอครั้งนี้ | สอดคล้อง | ภาคผนวก ก. เอกสารบริษัทฯ  ปปปป |
| * 1. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุมกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเวนแตรัฐบาลของผู้ยื่นข้อเสนอได้มีคําสั่งใหสละเอกสิทธิ์และความคุมกันเชนวานั้น | 1. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุมกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเวนแตรัฐบาลของผู้ยื่นข้อเสนอได้มีคําสั่งใหสละเอกสิทธิ์และความคุมกันเชนวานั้น | สอดคล้อง | ภาคผนวก ก. เอกสารบริษัทฯ  ปปปป |
| * 1. ผู้ยื่นข้อเสนอตองลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐดวยอิเล็กทรอนิกส (Electronic Government Procurement: e-GP) ของกรมบัญชีกลาง | 1. ผู้ยื่นข้อเสนอตองลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐดวยอิเล็กทรอนิกส (Electronic Government Procurement: e-GP) ของกรมบัญชีกลาง | สอดคล้อง | ภาคผนวก ก. เอกสารบริษัทฯ  ปปปป |
| * 1. ผู้ยื่นข้อเสนอตองมีมูลค่าสุทธิของกิจการ ดังนี้  1. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกวา 1 ป ตองมีมูลค่าสุทธิของกิจการ จากผลตางระหวางสินทรัพยสุทธิหักดวยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแลว ซึ่งจะตองแสดงคาเป็นบวก 1 ปสุดทายกอนวันยื่นข้อเสนอ 2. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการคา ใหพิจารณาการกำหนดมูลค่าของทุนจดทะเบียนโดยผู้ยื่นข้อเสนอจะตองมีทุนจดทะเบียนที่เรียกชําระมูลค่าหุนแลว ณ วันที่ยื่นข้อเสนอ ดังนี้ 3. มูลค่าการจัดชื้อจัดจ้างเกิน 1 ล้านบาท แต่ไม่เกิน5 ล้านบาท ตองมีทุนจดทะเบียนไม่ตํ่ากวา 1 ล้านบาท | 1. ผู้ยื่นข้อเสนอตองมีมูลค่าสุทธิของกิจการ ดังนี้    1. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกวา 1 ป ตองมีมูลค่าสุทธิของกิจการ จากผลตางระหวางสินทรัพยสุทธิหักดวยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแลว ซึ่งจะตองแสดงคาเป็นบวก 1 ปสุดทายกอนวันยื่นข้อเสนอ    2. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการคา ใหพิจารณาการกำหนดมูลค่าของทุนจดทะเบียนโดยผู้ยื่นข้อเสนอจะตองมีทุนจดทะเบียนที่เรียกชําระมูลค่าหุนแลว ณ วันที่ยื่นข้อเสนอ ดังนี้       1. มูลค่าการจัดชื้อจัดจ้างเกิน 1 ล้านบาท แต่ไม่เกิน5 ล้านบาท ตองมีทุนจดทะเบียนไม่ตํ่ากวา 1 ล้านบาท | สอดคล้อง | ภาคผนวก ก. เอกสารบริษัทฯ  ปปปป |
| * 1. ผู้เสนอราคาตองเป็นบุคคลธรรมดา หรือนิติบุคคล และมีผลงานประเภทเดียวกัน กับงานที่จางในวงเงินไม่นอยกวา 1,000,000.- บาท (หนึ่งล้านบาทถวน) ตองเป็นผลงานสัญญาเดียวยอนหลังไม่เกิน 3 ป นับจากวันที่งานแลวเสร็จจนถึงวันที่ยื่นเอกสาร และ ผลงานที่เป็นคูสัญญาโดยตรงกับหนวยงานภาครัฐโดยจะต้องแนบสำเนาหนังสือรับรองผลงาน และ สำเนาสัญญาพรอมรับรองสำเนาถูกตองมาพรอมกันในวันยื่นข้อเสนอโครงการ | 1. ผู้เสนอราคาตองเป็นบุคคลธรรมดา หรือนิติบุคคล และมีผลงานประเภทเดียวกัน กับงานที่จางในวงเงินไม่นอยกวา 1,000,000.- บาท (หนึ่งล้านบาทถวน) ตองเป็นผลงานสัญญาเดียวยอนหลังไม่เกิน 3 ป นับจากวันที่งานแลวเสร็จจนถึงวันที่ยื่นเอกสาร และ ผลงานที่เป็นคูสัญญาโดยตรงกับหนวยงานภาครัฐโดยจะต้องแนบสำเนาหนังสือรับรองผลงาน และ สำเนาสัญญาพรอมรับรองสำเนาถูกตองมาพรอมกันในวันยื่นข้อเสนอโครงการ | สอดคล้อง | ภาคผนวก ก. เอกสารบริษัทฯ  ปปปป |
| * 1. เป็นนิติบุคคลที่ประกอบอาชีพเป็นที่ปรึกษาสาขาเทคโนโลยีสารสนเทศและการสื่อสาร (ICT : Information and Communication Technology Sector) และได้ขึ้นทะเบียนไวกับศูนยข้อมูลที่ปรึกษา สํานักงานบริหารหนี้สาธารณะ กระทรวงการคลัง | 1. เป็นนิติบุคคลที่ประกอบอาชีพเป็นที่ปรึกษาสาขาเทคโนโลยีสารสนเทศและการสื่อสาร (ICT : Information and Communication Technology Sector) และได้ขึ้นทะเบียนไวกับศูนยข้อมูลที่ปรึกษา สํานักงานบริหารหนี้สาธารณะ กระทรวงการคลัง | สอดคล้อง | ภาคผนวก ก. เอกสารบริษัทฯ  ปปปป |
| * 1. ผู้ประสงคจะเสนอราคาตองเสนอบุคลากรหลักที่มีความรู และมีประสบการณในการใหคําปรึกษา และสนับสนุนข้อมูลดานความมั่นคงปลอดภัยสารสนเทศ และได้รับได้รับประกาศนียบัตร (Certification) ดานความมั่นคงปลอดภัยข้อมูลสารสนเทศ ISO/IEC 27001 Lead Auditor ในระดับสากล และบุคลากรหลักตองเป็นบุคลสัญชาติไทย หรือสามารถสื่อสารภาษาไทยได้เป็นอยางดี โดยจะจัดหาบุคลากรใหมีจํานวนเหมาะสมกับขอบเขตของงานที่จะดําเนินการตามจํานวน และละเอียดอยางนอย ดังนี้  1. ที่ปรึกษาโครงการ จำนวนไม่น้อยกว่า 1 คน  * คุณวุฒิไม่ต่ำกว่าปริญญาโท * มีประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 10 ป  1. ผู้จัดการโครงการ จำนวนไม่น้อยกว่า 1 คน  * คุณวุฒิไม่ต่ำกว่าปริญญาโท * มีประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 5 ป  1. ผู้เชี่ยวชาญดานความมั่นคงปลอดภัยของข้อมูลจำนวนไม่น้อยกว่า 1 คน  * คุณวุฒิไม่ต่ำกว่าปริญญาตรี * มีประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 3 ป  1. ผู้เชี่ยวชาญดานความมั่นคงปลอดภัยทางเทคนิค จำนวนไม่น้อยกว่า 2 คน  * คุณวุฒิไม่ต่ำกว่าปริญญาตรี * มีประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 5 ป  1. ผู้ประสานงานโครงการ จำนวนไม่น้อยกว่า 2 คน มีคุณสมบัติ ดังนี้  * คุณวุฒิไม่ต่ำกว่าปริญญาตรี * มีประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 2 ป | 1. ผู้ประสงคจะเสนอราคาตองเสนอบุคลากรหลักที่มีความรู และมีประสบการณในการใหคําปรึกษา และสนับสนุนข้อมูลดานความมั่นคงปลอดภัยสารสนเทศ และได้รับได้รับประกาศนียบัตร (Certification) ดานความมั่นคงปลอดภัยข้อมูลสารสนเทศ ISO/IEC 27001 Lead Auditor ในระดับสากล และบุคลากรหลักตองเป็นบุคลสัญชาติไทย หรือสามารถสื่อสารภาษาไทยได้เป็นอยางดี โดยจะจัดหาบุคลากรใหมีจํานวนเหมาะสมกับขอบเขตของงานที่จะดําเนินการตามจํานวน และละเอียดอยางนอย ดังนี้    * 1. ที่ปรึกษาโครงการ จำนวนไม่น้อยกว่า 1 คน  * คุณวุฒิไม่ต่ำกว่าปริญญาโท * มีประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 10 ป   + 1. ผู้จัดการโครงการ จำนวนไม่น้อยกว่า 1 คน * คุณวุฒิไม่ต่ำกว่าปริญญาโท * มีประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 5 ป   + 1. ผู้เชี่ยวชาญดานความมั่นคงปลอดภัยของข้อมูลจำนวนไม่น้อยกว่า 1 คน   - คุณวุฒิไม่ต่ำกว่าปริญญาตรี  - มีประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 3 ป   * + 1. ผู้เชี่ยวชาญดานความมั่นคงปลอดภัยทางเทคนิค จำนวนไม่น้อยกว่า 2 คน * คุณวุฒิไม่ต่ำกว่าปริญญาตรี * มีประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 5 ป   + 1. ผู้ประสานงานโครงการ จำนวนไม่น้อยกว่า 2 คน มีคุณสมบัติ ดังนี้ * คุณวุฒิไม่ต่ำกว่าปริญญาตรี * มีประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 2 ป | สอดคล้อง | ภาคผนวก ก. เอกสารบริษัทฯ  ปปปป |

1. **ความสอดคล้องของข้อเสนอกับขอบเขตการดำเนินงาน**

|  |  |  |
| --- | --- | --- |
| **ขอบเขตงานตาม TOR** | **ขอบเขตงานตามข้อเสนอ** | **ความสอดคล้อง** |
| * 1. ศึกษา วิเคราะห์ จัดทำแผนการดำเนินงานโครงการ พร้อมจัดทำเป็นเอกสารแผนการดำเนินงานโครงการ (Project Plan) | 1. ศึกษา วิเคราะห์ จัดทำแผนการดำเนินงานโครงการ พร้อมจัดทำเป็นเอกสารแผนการดำเนินงานโครงการ (Project Plan) | สอดคล้อง |
| * 1. ศึกษา วิเคราะห์ กำหนดขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารแสดงขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Scope : ISMS Scope) | 1. ศึกษา วิเคราะห์ กำหนดขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารแสดงขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Scope : ISMS Scope) | สอดคล้อง |
| * 1. ศึกษา วิเคราะห์ จัดทำนโยบายความมั่นคงปลอดภัยข้อมูลสารสนเทศ ที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง พร้อมจัดทำเป็นเอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy : IS Policy) | 1. ศึกษา วิเคราะห์ จัดทำนโยบายความมั่นคงปลอดภัยข้อมูลสารสนเทศ ที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง พร้อมจัดทำเป็นเอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy : IS Policy) | สอดคล้อง |
| * 1. ศึกษา วิเคราะห์ กำหนดโครงสร้างคณะทำงานในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารแสดงบทบาทหน้าที่ความรับผิดชอบของคณะทำงานในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Roles & Responsibilities) | 1. ศึกษา วิเคราะห์ กำหนดโครงสร้างคณะทำงานในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารแสดงบทบาทหน้าที่ความรับผิดชอบของคณะทำงานในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Roles & Responsibilities) | สอดคล้อง |
| * 1. ดำเนินการจัดอบรมหลักสูตรข้อกำหนดมาตรฐานสากล ISO/IEC27001:2022 โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 20 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบรมหลักสูตรข้อกำหนดมาตรฐานสากล ISO/IEC27001:2022 โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | 1. ดำเนินการจัดอบรมหลักสูตรข้อกำหนดมาตรฐานสากล ISO/IEC27001:2022 โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 20 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบรมหลักสูตรข้อกำหนดมาตรฐานสากล ISO/IEC27001:2022 โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | สอดคล้อง |
| * 1. ศึกษา วิเคราะห์ กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ และแผนการดำเนินงานเพื่อให้บรรลุตามวัตถุประสงค์ที่กำหนดไว้ พร้อมจัดทำเป็นเอกสารแสดงวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ และแผนบรรลุวัตถุประสงค์ (Information Security Objectives and Plan to achieve them) | 1. ศึกษา วิเคราะห์ กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ และแผนการดำเนินงานเพื่อให้บรรลุตามวัตถุประสงค์ที่กำหนดไว้ พร้อมจัดทำเป็นเอกสารแสดงวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ และแผนบรรลุวัตถุประสงค์ (Information Security Objectives and Plan to achieve them) | สอดคล้อง |
| * 1. ศึกษา วิเคราะห์ กำหนดกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารขั้นตอนปฏิบัติสำหรับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Procedure for Information Security Risk Management) | 1. ศึกษา วิเคราะห์ กำหนดกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารขั้นตอนปฏิบัติสำหรับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Procedure for Information Security Risk Management) | สอดคล้อง |
| * 1. ทบทวนผลการประเมินความเสี่ยง (Risk Assessment Result) และแผนการบรรเทาความเสี่ยง (Risk Treatment Plan) ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นรายงานผลการประเมินความเสี่ยง และแผนการบรรเทาความเสี่ยง (Risk Assessment and Risk Treatment Plan Report) | 1. ทบทวนผลการประเมินความเสี่ยง (Risk Assessment Result) และแผนการบรรเทาความเสี่ยง (Risk Treatment Plan) ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นรายงานผลการประเมินความเสี่ยง และแผนการบรรเทาความเสี่ยง (Risk Assessment and Risk Treatment Plan Report) | สอดคล้อง |
| * 1. ศึกษา วิเคราะห์ มาตรการที่นำมาใช้ในการบรรเทาความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารแสดงการประยุกต์ใช้มาตรการควบคุม (Statement of Applicability : SOA) | 1. ศึกษา วิเคราะห์ มาตรการที่นำมาใช้ในการบรรเทาความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารแสดงการประยุกต์ใช้มาตรการควบคุม (Statement of Applicability : SOA) | สอดคล้อง |
| * 1. ดำเนินการจัดฝึกอบรมหลักสูตรสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 30 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบหลักสูตรการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารเทศ (Information Security Awareness) โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | 1. ดำเนินการจัดฝึกอบรมหลักสูตรสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 30 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบหลักสูตรการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารเทศ (Information Security Awareness) โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | สอดคล้อง |
| * 1. ศึกษา วิเคราะห์ จัดทำแผนการสื่อสาร สำหรับใช้ในการสื่อสารในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเอกสารแผนการสื่อสารสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Communication Plan) | 1. ศึกษา วิเคราะห์ จัดทำแผนการสื่อสาร สำหรับใช้ในการสื่อสารในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเอกสารแผนการสื่อสารสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Communication Plan) | สอดคล้อง |
| * 1. รวบรวม ศึกษา วิเคราะห์ข้อมูล จัดทำชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Topic Specific Policies & Procedures for Information Security Management System) ที่สอดคล้องกับการประยุกต์ใช้มาตรการควบคุม (Statement of Applicability : SOA) ตามที่กำหนดไว้ | 1. รวบรวม ศึกษา วิเคราะห์ข้อมูล จัดทำชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Topic Specific Policies & Procedures for Information Security Management System) ที่สอดคล้องกับการประยุกต์ใช้มาตรการควบคุม (Statement of Applicability : SOA) ตามที่กำหนดไว้ | สอดคล้อง |
| * 1. ศึกษา วิเคราะห์ การบริหารจัดการเอกสารสารสนเทศ ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารขั้นตอนปฏิบัติสำหรับบริหารจัดการเอกสารสารสนเทศ (Procedure for Documented Information management) | 1. ศึกษา วิเคราะห์ การบริหารจัดการเอกสารสารสนเทศ ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารขั้นตอนปฏิบัติสำหรับบริหารจัดการเอกสารสารสนเทศ (Procedure for Documented Information management) | สอดคล้อง |
| * 1. ดำเนินการจัดฝึกอบรมหลักสูตรการสร้างความเข้าใจในชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 20 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบหลักสูตรการสร้างความเข้าใจในชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | 1. ดำเนินการจัดฝึกอบรมหลักสูตรการสร้างความเข้าใจในชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 20 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบหลักสูตรการสร้างความเข้าใจในชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | สอดคล้อง |
| * 1. ดำเนินการจัดฝึกอบรมหลักสูตรการเป็นผู้ตรวจประเมินภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 5 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบรมหลักสูตรการเป็นผู้ตรวจประเมินภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Internal Auditor) โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | 1. ดำเนินการจัดฝึกอบรมหลักสูตรการเป็นผู้ตรวจประเมินภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 5 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบรมหลักสูตรการเป็นผู้ตรวจประเมินภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Internal Auditor) โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | สอดคล้อง |
| * 1. ดำเนินการตรวจประเมินภายใน (Internal Audit) ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำรายงานผลการตรวจประเมินภายใน (Internal Audit Report) | 1. ดำเนินการตรวจประเมินภายใน (Internal Audit) ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำรายงานผลการตรวจประเมินภายใน (Internal Audit Report) | สอดคล้อง |
| * 1. ศึกษา วิเคราะห์ และร่วมดำเนินการตรวจประเมินหาจุดอ่อนในระบบเทคโนโลยีสารสนเทศ (Vulnerability Assessment) ไม่น้อยกว่า 100 IP Address ที่อยู่ในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยจัดทำเป็นแผนการตรวจประเมินหาจุดอ่อนในระบบเทคโนโลยีสารสนเทศ (Vulnerability Assessment Plan) พร้อมรายงานผลการตรวจประเมิน (Vulnerability Assessment Result) อย่างน้อย 2 ครั้ง | 1. ศึกษา วิเคราะห์ และร่วมดำเนินการตรวจประเมินหาจุดอ่อนในระบบเทคโนโลยีสารสนเทศ (Vulnerability Assessment) ไม่น้อยกว่า 100 IP Address ที่อยู่ในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยจัดทำเป็นแผนการตรวจประเมินหาจุดอ่อนในระบบเทคโนโลยีสารสนเทศ (Vulnerability Assessment Plan) พร้อมรายงานผลการตรวจประเมิน (Vulnerability Assessment Result) อย่างน้อย 2 ครั้ง | สอดคล้อง |
| * 1. ร่วมประชุม และสนับสนุนการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศโดยฝ่ายบริหาร (ISMS Management Review) พร้อมจัดทำสรุปผลการประชุมทบทวนโดยฝ่ายบริหาร (ISMS Management Review Report) | 1. ร่วมประชุม และสนับสนุนการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศโดยฝ่ายบริหาร (ISMS Management Review) พร้อมจัดทำสรุปผลการประชุมทบทวนโดยฝ่ายบริหาร (ISMS Management Review Report) | สอดคล้อง |
| * 1. จัดหาหน่วยงานสำหรับการตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Certification Body) โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | 1. จัดหาหน่วยงานสำหรับการตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Certification Body) โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | สอดคล้อง |
| * 1. สนับสนุนการตรวจประเมินเพื่อรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ทั้งระหว่าง และหลังการตรวจประเมินจนได้รับมอบใบรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Certificate for Information Security Management System) | 1. สนับสนุนการตรวจประเมินเพื่อรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ทั้งระหว่าง และหลังการตรวจประเมินจนได้รับมอบใบรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Certificate for Information Security Management System) | สอดคล้อง |

1. **ระยะเวลาดำเนินการ**

ระยะเวลา 180 วัน นับจากวันที่ลงนามในสัญญา

1. **การส่งมอบงาน**

ผู้ชนะการเสนอราคาต้องส่งมอบงานโดยแบ่งเป็น 2 งวด โดยส่งมอบงานในแต่ละงวดเป็นรูปเล่มจำนวน 3 ชุด และในรูปแบบ Flash Drive จำนวน 2 ชุด โดยมีรายละเอียดดังนี้

* 1. งวดที่ 1 ภายใน 120 วัน นับถัดจากวันที่ลงนามสัญญา โดย ผู้ชนะการเสนอราคาต้องดำเนินการส่งมอบงานโดยมีรายละเอียดดังนี้

1. เอกสารแผนการดำเนินงานโครงการ (Project Plan)
2. เอกสารแสดงขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Scope : ISMS Scope)
3. เอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy : IS Policy)
4. เอกสารแสดงบทบาทหน้าที่ความรับผิดชอบของคณะทำงานในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Roles & Responsibilities)
5. เอกสารแสดงวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ และแผนบรรลุวัตถุประสงค์ (Information Security Objectives and Plan to achieve them)
6. รายงานผลการประเมินความเสี่ยง และแผนการบรรเทาความเสี่ยง (Risk Assessment and Risk Treatment Plan Report)
7. เอกสารแสดงการประยุกต์ใช้มาตรการควบคุม (Statement of Applicability : SOA)
   1. งวดที่ 2 ภายใน 180 วัน นับถัดจากวันที่ลงนามสัญญา โดย ผู้ชนะการเสนอราคาต้องดำเนินการส่งมอบงานโดยมีรายละเอียดดังนี้
8. รายงานผลการฝึกอบรม
9. รายงานผลการตรวจประเมินภายใน (Internal Audit Report)
10. รายงานผลการตรวจประเมิน (Vulnerability Assessment Result)
11. รายงานผลการตรวจประเมินโดยผู้ตรวจประเมินภายนอก (CB Audit Report)
12. ใบประกาศ หรือหนังสือรับรองการผ่านการรับรองมาตรฐานสากล โดยบริษัทผู้ตรวจประเมินภายนอก
13. **ผลงานและประสบการณ์ของที่ปรึกษา**
    1. ผลงานและประสบการณ์ของที่ปรึกษา

ที่มีมูลค่ามากกว่า 1,000,000 บาทและย้อนหลังไม่เกิน 3 ปี

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ลำดับ** | **ชื่อหน่วยงาน** | **โครงการ** | **มูลค่า** | **เอกสารอ้างอิง** |
| 1 | องค์การส่งเสริมกิจการโคนมแห่งประเทศไทย | ที่ปรึกษาด้านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC27001:2013 | 1,681,933.00 | ภาคผนวก ค. หนังสือรับรองผลงาน |
| 2 | สํานักงานเทคโนโลยีสารสนเทศและดิจิทัล  สภากาชาดไทย | ที่ปรึกษาในโครงการพัฒนาการบริหารจัดการความมั่นคงปลอดภัยของศูนย์ข้อมูลคอมพิวเตอร์ เพื่อผ่านการรับรองมาตรฐาน ISO/IEC 27001 | 1,498,000.00 | ภาคผนวก ค. หนังสือรับรองผลงาน |
| 3 | สถาบันเทคโนโลยีป้องกันประเทศ | โครงการพัฒนาการบริหารจัดการความมั่นคงปลอดภัยของศูนย์ข้อมูลคอมพิวเตอร์ เพื่อผ่านการรับรองมาตรฐาน ISO/IEC 2700 | 1,028,270.00 | ภาคผนวก ค. หนังสือรับรองผลงาน |
| 4 | สํานักงาน กสทช. | ที่ปรึกษาเพื่อตรวจสอบและติดตามการดำเนินงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC ๒๗๐๐๑ Surveillance Audit) | 2,151,288.75 | ภาคผนวก ค. หนังสือรับรองผลงาน |

1. **วิธีการบริหารและวิธีการปฏิบัติงาน** 
   1. วิธีการบริหารงาน
      1. โครงสร้างองค์กรของบุคลากรของที่ปรึกษา



* + 1. หน้าที่รับผิดชอบของบุคลกรหลัก

|  |  |  |  |
| --- | --- | --- | --- |
| **ลำดับ** | **ชื่อ** | **ตำแหน่ง** | **หน้าที่** |
| 1 | ดร. โกเมน พิบูลย์โรจน์ | ผู้จัดการโครงการ |  |
| 2 | ดร. บรรจง หะรังสี | ที่ปรึกษาโครงการ |  |
| 3 | นาย จิรพงศ์ วงษ์เกตุ | ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย |  |
| 4 | นาย พงศกร โสธนนท์ | ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย |  |
| 5 | น.ส. รุ้งตะวัน หวังศิริ | ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย |  |
| 6 | นายรมย์รวินท์ ศรีรัตน์ | เชี่ยวชาญด้านความมั่นคงปลอดภัยทางเทคนิค |  |
| 7 | นายชเล ชะเอม | เชี่ยวชาญด้านความมั่นคงปลอดภัยทางเทคนิค |  |
| 8 | น.ส. กรรณิกา ศรีแก้ว | ผู้ประสานงานโครงการ |  |
| 9 | น.ส. จิตติมา กงแก้ว | ผู้ประสานงานโครงการ |  |

**T-NET**

* 1. แผนการดำเนินงานและวิธีปฏิบัติงานตามขอบเขตงาน
     1. แผนการดำเนินงานโครงการ
     2. วิธีการปฏิบัติงานตามขอบเขตงาน

|  |  |
| --- | --- |
| **ขอบเขตงานตาม TOR** | **วิธีการปฏิบัติงาน** |
| 1. ศึกษา วิเคราะห์ จัดทำแผนการดำเนินงานโครงการ พร้อมจัดทำเป็นเอกสารแผนการดำเนินงานโครงการ (Project Plan) | 1. ศึกษา วิเคราะห์ขอบเขตการดำเนินงาน 2. ศึกษา วิเคราะห์กำหนดการส่งงวดงานในแต่ละงวด 3. ศึกษา วิเคราะห์ความต้องการ ความคาดหวังของผู้ที่เกี่ยวข้อง 4. นำผลการวิเคราะห์ และดำเนินการไปจัดทำแผนการดำเนินงานโครงการ (Project Plan) 5. นำเสนอแผนการดำเนินงานกับคณะทำงาน และผู้ที่เกี่ยวข้องเพื่อทำความเข้าใจร่วมกัน |
| 1. ศึกษา วิเคราะห์ กำหนดขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารแสดงขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Scope : ISMS Scope) | 1. ศึกษา วิเคราะห์บริทบองค์กร วิสัยทัศน์ พันธะกิจ 2. ศึกษา วิเคราะห์ความต้องการ และความคาดหวังของผู้ที่เกี่ยวข้อง 3. นำผลการวิเคราะห์ไปกำหนดขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Scope) โดยแสดงข้อมูลของขอบเขตให้สอดคล้องตามข้อกำหนดของมาตรฐาน 4. จัดทำเป็นเอกสารแสดงถึงขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Scope : ISMS Scope) |
| 1. ศึกษา วิเคราะห์ จัดทำนโยบายความมั่นคงปลอดภัยข้อมูลสารสนเทศ ที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง พร้อมจัดทำเป็นเอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy : IS Policy) | 1. ศึกษาเป้าหมาย เจตนาของการจัดทำนโยบายความมั่นคงปลอดภัยข้อมูลสารสนเทศ 2. ศึกษากฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง 3. นำผลการศึกษามากำหนดเนื้อหาของนโยบายความมั่นคงปลอดภัยข้อมูลสารสนเทศ 4. จัดทำนโยบายความมั่นคงปลอดภัยข้อมูลสารสนเทศ (Information Security Policy : IS Policy) |
| 1. ศึกษา วิเคราะห์ กำหนดโครงสร้างคณะทำงานในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารแสดงบทบาทหน้าที่ความรับผิดชอบของคณะทำงานในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Roles & Responsibilities) | 1. ศึกษาโครงสร้างการบริหารจัดการของหน่วยงานภายใต้ขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ 2. ศึกษา วิเคราะห์บทบาทหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้อง 3. นำผลการศึกษา วิเคราะห์ ไปกำหนด ปรับปรุง บทบาทหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS Roles & Responsibilities) |
| 1. ดำเนินการจัดอบรมหลักสูตรข้อกำหนดมาตรฐานสากล ISO/IEC27001:2022 โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 20 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบรมหลักสูตรข้อกำหนดมาตรฐานสากล ISO/IEC27001:2022 โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | 1. ประสานงานนัดหมายกำหนดการในการอบรมหลักสูตรมาตรฐานสากล ISO/IEC 27001:2022 2. จัดทำสื่อการอบรม แบบทดสอบก่อนเรียนหลังเรียน (Pre-Test, Post-Test) สำหรับนำไปใช้ในการอบรม 3. ดำเนินการฝึกอบรม และวัดผลการอบรม 4. จัดทำรายงานผลการฝึกอบรมหลักสูตรข้อกำหนดมาตรฐานสากล ISO/IEC27001:2022 |
| 1. ศึกษา วิเคราะห์ กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ และแผนการดำเนินงานเพื่อให้บรรลุตามวัตถุประสงค์ที่กำหนดไว้ พร้อมจัดทำเป็นเอกสารแสดงวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ และแผนบรรลุวัตถุประสงค์ (Information Security Objectives and Plan to achieve them) | 1. ศึกษา วิเคราะห์ เป้าหมาย เจตนาของการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัย 2. นำผลการศึกษา วิเคราะห์ ไปกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัย (Information Security Objectives) พร้อมกำหนดตัวชี้วัด วิธีการ ความถี่ และผู้รับผิดชอบในการวัดผล ร่วมกับคณะทำงาน 3. จัดทำแผนบรรลุวัตถุประสงค์ดังกล่าวข้างต้น ร่วมกับคณะทำงาน และผู้ที่เกี่ยวข้อง |
| 1. ศึกษา วิเคราะห์ กำหนดกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารขั้นตอนปฏิบัติสำหรับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Procedure for Information Security Risk Management) | 1. ศึกษา วิเคราะห์ การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานในปัจจุบัน 2. นำผลการศึกษา วิเคราะห์ มาจัดทำขั้นตอนปฏิบัติสำหรับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Procedure for Information Security Risk Management) โดยมีองค์ประกอบอย่างน้อยดังนี้    * การวิเคราะห์ความเสี่ยง (Risk Assessment)    * การประเมินความเสี่ยง (Risk Evaluation) และ    * การบรรเทาความเสี่ยง (Risk Treatment) เป็นต้น |
| 1. ทบทวนผลการประเมินความเสี่ยง (Risk Assessment Result) และแผนการบรรเทาความเสี่ยง (Risk Treatment Plan) ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นรายงานผลการประเมินความเสี่ยง และแผนการบรรเทาความเสี่ยง (Risk Assessment and Risk Treatment Plan Report) | 1. ศึกษา ทบทวน จัดทำผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ร่วมกับคณะทำงานที่เกี่ยวข้อง (Risk Assessment Result) 2. นำผลการประเมินความเสี่ยงที่ได้ ไปกำหนดลำดับ (Priorities) และแนวทางในการบรรเทาความเสี่ยง (Options) ร่วมกับคณะทำงานที่เกี่ยวข้องเพื่อจัดทำแผนบรรเทาความเสี่ยงร่วมกัน (Risk Treatment Plan) 3. ทำการสรุปผล และจัดทำรายงานผลการประเมินความเสี่ยง และแผนการบรรเทาความเสี่ยง (Risk Assessment and Risk Treatment Plan Report) |
| 1. ศึกษา วิเคราะห์ มาตรการที่นำมาใช้ในการบรรเทาความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารแสดงการประยุกต์ใช้มาตรการควบคุม (Statement of Applicability : SOA) | 1. ศึกษา วิเคราะห์ แผนการบรรเทาความเสี่ยง เพื่อสรุปมาตรการบรรเทาความเสี่ยงต่างๆ ที่นำมาใช้งาน 2. นำมาตรความเสี่ยงที่ได้ข้างต้นไปเปรียบเทียบกับมาตรการควบคุมที่ปรากฏใน Annex A ของมาตรฐานสากล ISO/IEC 27001:2022 3. นำผลการเปรียบเทียบไปจัดทำเป็นเอกสารแสดงการประยุกต์ใช้มาตรการควบคุม (Statement of Applicability : SOA) |
| 1. ดำเนินการจัดฝึกอบรมหลักสูตรสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 30 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบหลักสูตรการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารเทศ (Information Security Awareness) โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | 1. ประสานงานนัดหมายกำหนดการในการฝึกอบรมหลักสูตรสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ 2. จัดทำสื่อการอบรม สำหรับนำไปใช้ในการอบรม 3. ดำเนินการฝึกอบรม 4. จัดทำรายงานผลการฝึกอบหลักสูตรการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารเทศ (Information Security Awareness) |
| 1. ศึกษา วิเคราะห์ จัดทำแผนการสื่อสาร สำหรับใช้ในการสื่อสารในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเอกสารแผนการสื่อสารสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Communication Plan) | 1. ศึกษา วิเคราะห์ เจตนาของมาตรฐานสากลที่ต้องการให้สื่อสารประเด็นต่างๆ ที่สำคัญ 2. ศึกษา วิเคราะห์ แนวทางการสื่อสารประเด็นต่างๆ ในปัจจุบันตามขอบเขต (Scope) 3. นำผลการศึกษา วิเคราะห์ ไปจัดทำแผนการสื่อสารสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ร่วมกับคณะทำงาน 4. จัดทำเอกสารแผนการสื่อสารสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Communication Plan) |
| 1. รวบรวม ศึกษา วิเคราะห์ข้อมูล จัดทำชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Topic Specific Policies & Procedures for Information Security Management System) ที่สอดคล้องกับการประยุกต์ใช้มาตรการควบคุม (Statement of Applicability : SOA) ตามที่กำหนดไว้ | 1. รวบรวม ศึกษา วิเคราะห์ นโยบาย ขั้นตอนปฏิบัติงานต่างๆ ด้านความมั่นคงปลอดภัยสารสนเทศที่องค์กรประกาศใช้งานในปัจจุบัน 2. ศึกษา วิเคราะห์ นโยบาย ขั้นตอนปฏิบัติงานต่างๆ ที่มาตรฐานแนะนำให้จัดทำในระบบบริหารความมั่นคงปลอดภัยสารสนเทศ และมาตรการควบคุมที่นำมาประยุกต์ใช้ (SOA) 3. จัดทำเป็นสรุปรายการเอกสารนโยบาย และขั้นตอนปฏิบัติงานต่างๆ (Document Master List) ที่จะนำไปใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารเทศ 4. ดำเนินการจัดทำเอกสารนโยบาย และขั้นตอนปฏิบัติต่างๆ ร่วมกับคณะทำงานตามสรุปรายการเอกสาร |
| 1. ศึกษา วิเคราะห์ การบริหารจัดการเอกสารสารสนเทศ ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารขั้นตอนปฏิบัติสำหรับบริหารจัดการเอกสารสารสนเทศ (Procedure for Documented Information management) | 1. ศึกษา วิเคราะห์ แนวทางการบริหารจัดการเอกสารต่างๆ ด้านความั่นคงปลอดภัยสารสนเทศขององค์กรที่ดำเนินการในปัจจุบัน 2. ศึกษา วิเคราะห์ แนวทางการบริหารจัดการเอกสาสารสนเทศตามข้อกำหนดของมาตรฐาน (Standard Requirements) 3. นำผลการศึกษา วิเคราะห์ จัดทำขั้นตอนปฏิบัติสำหรับบริหารจัดการเอกสารสารสนเทศ (Procedure for Documented Information management) ร่วมกับคณะทำงาน |
| 1. ดำเนินการจัดฝึกอบรมหลักสูตรการสร้างความเข้าใจในชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 20 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบหลักสูตรการสร้างความเข้าใจในชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | 1. ประสานงานนัดหมายกำหนดการในฝึกอบรมหลักสูตรการสร้างความเข้าใจในชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ 2. จัดทำสื่อการอบรม แบบทดสอบก่อนเรียนหลังเรียน (Pre-Test, Post-Test) สำหรับนำไปใช้ในการอบรม 3. ดำเนินการฝึกอบรม และวัดผลการอบรม 4. จัดทำรายงานผลการฝึกอบรมหลักสูตรการสร้างความเข้าใจในชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ |
| 1. ดำเนินการจัดฝึกอบรมหลักสูตรการเป็นผู้ตรวจประเมินภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 5 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบรมหลักสูตรการเป็นผู้ตรวจประเมินภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Internal Auditor) โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | 1. ประสานงานนัดหมายกำหนดการในฝึกอบรมหลักสูตรการเป็นผู้ตรวจประเมินภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ 2. จัดทำสื่อการอบรม แบบทดสอบก่อนเรียนหลังเรียน (Pre-Test, Post-Test) สำหรับนำไปใช้ในการอบรม 3. ดำเนินการฝึกอบรม และวัดผลการอบรม 4. จัดทำรายงานผลการฝึกอบรมหลักสูตรการเป็นผู้ตรวจประเมินภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Internal Auditor) |
| 1. ดำเนินการตรวจประเมินภายใน (Internal Audit) ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำรายงานผลการตรวจประเมินภายใน (Internal Audit Report) | 1. จัดทำโปรแกรม และแผนการตรวจประเมินภายใน (Internal Audit Program & Plan) ร่วมกับคณะทำงาน 2. แจ้งโปรแกรม และแผนการตรวจประเมินภายใน ให้ผู้ที่เกี่ยวข้องรับทราบ 3. ดำเนินการตรวจประเมินภายใน (Internal Audit) ตามแผน (Audit Plan) ที่กำหนดร่วมกับคณะทำงาน 4. จัดทำรายงานผลการตรวจประเมินภายใน (Internal Audit Report) |
| 1. ศึกษา วิเคราะห์ และร่วมดำเนินการตรวจประเมินหาจุดอ่อนในระบบเทคโนโลยีสารสนเทศ (Vulnerability Assessment) ไม่น้อยกว่า 100 IP Address ที่อยู่ในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยจัดทำเป็นแผนการตรวจประเมินหาจุดอ่อนในระบบเทคโนโลยีสารสนเทศ (Vulnerability Assessment Plan) พร้อมรายงานผลการตรวจประเมิน (Vulnerability Assessment Result) อย่างน้อย 2 ครั้ง | 1. ศึกษา วิเคราะห์ ระบบเทคโนโลยีสารสนเทศตามขอบเขต (IT System) ของการจัดทำระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Scope) 2. ระบุรายการอุปกรณ์ หรือระบบที่ควรดำเนินการตรวจสอบหาจุดอ่อนช่องโหว่ในระบบเทคโนโลยีสารสนเทศ ไม่น้อยกว่า 100 IP Address 3. วางแผนการตรวจประเมินหาจุดอ่อนในระบบเทคโนโลยีสารสนเทศ (Vulnerability Assessment Plan) ร่วมกับคณะทำงาน 4. ดำเนินการตรวจประเมินหาจุดอ่อนในระบบฯ ครั้งที่ 1 ตามแผนการดำเนินงาน ร่วมกับคณะทำงาน 5. รายงานผลการตรวจประเมิน (Vulnerability Assessment Result) ครั้งที่ 1 ให้ผู้ที่เกี่ยวข้องรับทราบ 6. ดำเนินการตรวจประเมินหาจุดอ่อนในระบบฯ ครั้งที่ 2 ตามแผนการดำเนินงาน ร่วมกับคณะทำงาน 7. รายงานผลการตรวจประเมิน (Vulnerability Assessment Result) ครั้งที่ 2 ให้ผู้ที่เกี่ยวข้องรับทราบ |
| 1. ร่วมประชุม และสนับสนุนการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศโดยฝ่ายบริหาร (ISMS Management Review) พร้อมจัดทำสรุปผลการประชุมทบทวนโดยฝ่ายบริหาร (ISMS Management Review Report) | 1. กำหนดวาระการประชุมทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศร่วมกับคณะทำงาน 2. กำหนดวันประชุม และวาระ ที่จะประชุมในแต่ละครั้งร่วมกับคณะทำงาน 3. ร่วมประชุม และสนับสนุนการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ให้กับคณะทำงานในแต่ละครั้ง 4. จัดทำสรุปผลการประชุมทบทวนโดยฝ่ายบริหาร (ISMS Management Review Report) ในแต่ละครั้ง |
| 1. จัดหาหน่วยงานสำหรับการตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Certification Body) โดยรับผิดชอบค่าใช้จ่ายในการดำเนินงานทั้งหมด | 1. ดำเนินการจัดหาหน่วยงาน (Certify Body) ที่สามารถให้บริการได้ตามแผนการดำเนินงานโครงการ (Project Plan) 2. ประสานงานในการเตรียมการตรวจรับรอง (Certification) ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ 3. แจ้งแผนการตรวจประเมิน (Audit Plan) กับคณะทำงานให้รับทราบโดยทั่วกัน |
| 1. สนับสนุนการตรวจประเมินเพื่อรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ทั้งระหว่าง และหลังการตรวจประเมินจนได้รับมอบใบรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Certificate for Information Security Management System) | 1. เตรียมความพร้อมรับการตรวจประเมินร่วมกับคณะทำงาน 2. สนับสนุนการตรวจประเมินให้กับคณะทำงาน 3. สนับสนุน ตอบประเด็นความไม่สอดคล้องที่พบระหว่างการตรวจประเมินร่วมกับคณะทำงาน 4. ประสานงานอื่นๆ เพื่อการรับมอบใบรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Certificate for Information Security Management System) |

**-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------**

**AIIT**

วิธีการปฏิบัติงานตามขอบเขตงาน

|  |  |
| --- | --- |
| **ขอบเขตงานตาม TOR** | **วิธีการปฏิบัติงาน** |
| 1. ศึกษา วิเคราะห์ จัดทำแผนการดำเนินงานโครงการ พร้อมจัดทำเป็นเอกสารแผนการดำเนินงานโครงการ (Project Plan) | ดำเนินการไปจัดทำแผนการดำเนินงานโครงการ (Project Plan) ตามข้อเสนอโครงการ (Proposal) |
| 1. ศึกษา วิเคราะห์ กำหนดขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารแสดงขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Scope : ISMS Scope) | จัดทำขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Scope) ตามข้อเสนอโครงการ และนำไปอธิบายให้ผู้ที่เกี่ยวข้องรับทราบ |
| 1. ศึกษา วิเคราะห์ จัดทำนโยบายความมั่นคงปลอดภัยข้อมูลสารสนเทศ ที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง พร้อมจัดทำเป็นเอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy : IS Policy) | จัดทำนโยบายความมั่นคงปลอดภัยข้อมูลสารสนเทศ (IS Policy) และนำไปอธิบายให้ผู้ที่เกี่ยวข้องรับทราบ |
| 1. ศึกษา วิเคราะห์ กำหนดโครงสร้างคณะทำงานในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารแสดงบทบาทหน้าที่ความรับผิดชอบของคณะทำงานในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Roles & Responsibilities) | จัดทำบทบาทหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS Roles & Responsibilities) และนำไปอธิบายให้ผู้ที่เกี่ยวข้องรับทราบ |
| 1. ดำเนินการจัดอบรมหลักสูตรข้อกำหนดมาตรฐานสากล ISO/IEC27001:2022 โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 20 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบรมหลักสูตรข้อกำหนดมาตรฐานสากล ISO/IEC27001:2022 โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | กำหนดวันอบรมหลักสูตรมาตรฐานสากล ISO/IEC 27001:2022 กับผู้ประสานงาน และดำเนินการฝึกอบรม พร้อมจัดทำเป็นรายงานผลการฝึกอบรม |
| 1. ศึกษา วิเคราะห์ กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ และแผนการดำเนินงานเพื่อให้บรรลุตามวัตถุประสงค์ที่กำหนดไว้ พร้อมจัดทำเป็นเอกสารแสดงวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ และแผนบรรลุวัตถุประสงค์ (Information Security Objectives and Plan to achieve them) | กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัย (Information Security Objectives) และนำไปอธิบายให้ผู้ที่เกี่ยวข้องรับทราบ |
| 1. ศึกษา วิเคราะห์ กำหนดกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารขั้นตอนปฏิบัติสำหรับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Procedure for Information Security Risk Management) | จัดทำขั้นตอนปฏิบัติสำหรับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และนำไปอธิบายให้ผู้ที่เกี่ยวข้องรับทราบ |
| 1. ทบทวนผลการประเมินความเสี่ยง (Risk Assessment Result) และแผนการบรรเทาความเสี่ยง (Risk Treatment Plan) ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นรายงานผลการประเมินความเสี่ยง และแผนการบรรเทาความเสี่ยง (Risk Assessment and Risk Treatment Plan Report) | ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และนำไปอธิบายให้ผู้ที่เกี่ยวข้องรับทราบ |
| 1. ศึกษา วิเคราะห์ มาตรการที่นำมาใช้ในการบรรเทาความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารแสดงการประยุกต์ใช้มาตรการควบคุม (Statement of Applicability : SOA) | จัดทำเอกสารแสดงการประยุกต์ใช้มาตรการควบคุม (Statement of Applicability : SOA) และนำไปอธิบายให้ผู้ที่เกี่ยวข้องรับทราบ |
| 1. ดำเนินการจัดฝึกอบรมหลักสูตรสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 30 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบหลักสูตรการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารเทศ (Information Security Awareness) โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | กำหนดวันอบรมหลักสูตรสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ กับผู้ประสานงาน และดำเนินการฝึกอบรม พร้อมจัดทำเป็นรายงานผลการฝึกอบรม |
| 1. ศึกษา วิเคราะห์ จัดทำแผนการสื่อสาร สำหรับใช้ในการสื่อสารในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเอกสารแผนการสื่อสารสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Communication Plan) | จัดทำแผนการสื่อสารสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และนำไปอธิบายให้ผู้ที่เกี่ยวข้องรับทราบ |
| 1. รวบรวม ศึกษา วิเคราะห์ข้อมูล จัดทำชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Topic Specific Policies & Procedures for Information Security Management System) ที่สอดคล้องกับการประยุกต์ใช้มาตรการควบคุม (Statement of Applicability : SOA) ตามที่กำหนดไว้ | จัดทำเอกสารนโยบาย และขั้นตอนปฏิบัติต่างๆ และนำไปอธิบายให้ผู้ที่เกี่ยวข้องรับทราบ |
| 1. ศึกษา วิเคราะห์ การบริหารจัดการเอกสารสารสนเทศ ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำเป็นเอกสารขั้นตอนปฏิบัติสำหรับบริหารจัดการเอกสารสารสนเทศ (Procedure for Documented Information management) | จัดทำขั้นตอนปฏิบัติสำหรับบริหารจัดการเอกสารสารสนเทศ และนำไปอธิบายให้ผู้ที่เกี่ยวข้องรับทราบ |
| 1. ดำเนินการจัดฝึกอบรมหลักสูตรการสร้างความเข้าใจในชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 20 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบหลักสูตรการสร้างความเข้าใจในชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | กำหนดวันอบรมหลักสูตรการสร้างความเข้าใจในชุดเอกสารนโยบายและขั้นตอนปฏิบัติสำหรับใช้ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ กับผู้ประสานงาน และดำเนินการฝึกอบรม พร้อมจัดทำเป็นรายงานผลการฝึกอบรม |
| 1. ดำเนินการจัดฝึกอบรมหลักสูตรการเป็นผู้ตรวจประเมินภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยมีผู้เข้ารับการอบรมไม่น้อยกว่า 5 ท่าน อย่างน้อย 1 ครั้ง สถานที่อบรมตามผู้ว่าจ้างจัดหาให้ พร้อมจัดทำรายงานผลการฝึกอบรมหลักสูตรการเป็นผู้ตรวจประเมินภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Internal Auditor) โดยรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด | กำหนดวันอบรมหลักสูตรการเป็นผู้ตรวจประเมินภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ กับผู้ประสานงาน และดำเนินการฝึกอบรม พร้อมจัดทำเป็นรายงานผลการฝึกอบรม |
| 1. ดำเนินการตรวจประเมินภายใน (Internal Audit) ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดทำรายงานผลการตรวจประเมินภายใน (Internal Audit Report) | กำหนดวัน และดำเนินการตรวจประเมินภายใน (Internal Audit) พร้อมจัดทำรายงานผลการตรวจประเมินภายใน (Internal Audit Report) |
| 1. ศึกษา วิเคราะห์ และร่วมดำเนินการตรวจประเมินหาจุดอ่อนในระบบเทคโนโลยีสารสนเทศ (Vulnerability Assessment) ไม่น้อยกว่า 100 IP Address ที่อยู่ในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยจัดทำเป็นแผนการตรวจประเมินหาจุดอ่อนในระบบเทคโนโลยีสารสนเทศ (Vulnerability Assessment Plan) พร้อมรายงานผลการตรวจประเมิน (Vulnerability Assessment Result) อย่างน้อย 2 ครั้ง | ประสานงานนัดหมาย และดำเนินการตรวจประเมินหาจุดอ่อนในระบบฯ พร้อมจัดทำรายงานผลการตรวจประเมิน (Vulnerability Assessment Result) อย่างน้อย 2 ครั้ง |
| 1. ร่วมประชุม และสนับสนุนการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศโดยฝ่ายบริหาร (ISMS Management Review) พร้อมจัดทำสรุปผลการประชุมทบทวนโดยฝ่ายบริหาร (ISMS Management Review Report) | นัดหมาย กำหนดวันประชุมการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และจัดทำสรุปผลการประชุมในแต่ละครั้ง |
| 1. จัดหาหน่วยงานสำหรับการตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Certification Body) โดยรับผิดชอบค่าใช้จ่ายในการดำเนินงานทั้งหมด | ประสานงานในการเตรียมการตรวจรับรอง (Certification) ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศกับหน่วยงานรับรอง และแจ้งให้คณะทำงานรับทราบ |
| 1. สนับสนุนการตรวจประเมินเพื่อรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ทั้งระหว่าง และหลังการตรวจประเมินจนได้รับมอบใบรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Certificate for Information Security Management System) | สนับสนุนการตรวจประเมินให้กับคณะทำงาน จนได้รับการรับรอง |

1. **ความสอดคล้องของบุคลากรโครงการ**
   1. ดร. บรรจง หะรังษี (ที่ปรึกษาโครงการ)

|  |  |  |  |
| --- | --- | --- | --- |
| **คุณสมบัติที่กำหนด** | **คุณสมบัติบุคลากร** | **ความสอดคล้อง** | **เอกสารอ้างอิง** |
| * คุณวุฒิไม่ต่ำกว่าปริญญาโท * ประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 10 ป | * วุฒิการศึกษาปริญญาเอก * สาขา Computer Science and Engineering * ประสบการณ์ 25 ปี |  | ภาคผนวก ข ประวัติบุคลากร |

* 1. ดร. โกเมน พิบูลย์โรจน์ (ผู้จัดการโครงการ)

|  |  |  |  |
| --- | --- | --- | --- |
| **คุณสมบัติที่กำหนด** | **คุณสมบัติบุคลากร** | **ความสอดคล้อง** | **เอกสารอ้างอิง** |
| * คุณวุฒิไม่ต่ำกว่าปริญญาโท * ประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 10 ป | * วุฒิการศึกษาปริญญาเอก * สาขา Computer Engineering * ประสบการณ์ 23 ปี |  | ภาคผนวก ข ประวัติบุคลากร |

* 1. นาย จิรพงศ์ วงษ์เกตุ (ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย)

|  |  |  |  |
| --- | --- | --- | --- |
| **คุณสมบัติที่กำหนด** | **คุณสมบัติบุคลากร** | **ความสอดคล้อง** | **เอกสารอ้างอิง** |
| * คุณวุฒิไม่ต่ำกว่าปริญญาตรี * ประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 10 ป | * วุฒิการศึกษาปริญาตรี * สาขาวิศวกรรมคอมพิวเตอร์ * ประสบการณ 20 ปี |  | ภาคผนวก ข ประวัติบุคลากร |

* 1. นาย พงศกร โสธนนท์ (ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย)

|  |  |  |  |
| --- | --- | --- | --- |
| **คุณสมบัติที่กำหนด** | **คุณสมบัติบุคลากร** | **ความสอดคล้อง** | **เอกสารอ้างอิง** |
| * คุณวุฒิไม่ต่ำกว่าปริญญาตรี * ประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 10 ป | * วุฒิการศึกษาปริญาโท * สาขาการจัดการในเศรษฐกิจดิจิทัล * ประสบการณ์ 9 ปี |  | ภาคผนวก ข ประวัติบุคลากร |

* 1. น.ส. รุ้งตะวัน หวังศิริ (ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย)

|  |  |  |  |
| --- | --- | --- | --- |
| **คุณสมบัติที่กำหนด** | **คุณสมบัติบุคลากร** | **ความสอดคล้อง** | **เอกสารอ้างอิง** |
| * คุณวุฒิไม่ต่ำกว่าปริญญาตรี * ประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 10 ป | * วุฒิการศึกษาปริญาโท * สาขาการจัดการเศรษฐกิจดิจิทัล * ประสบการณ์ 7 ปี |  | ภาคผนวก ข ประวัติบุคลากร |

* 1. นายรมย์รวินท์ ศรีรัตน์ (เชี่ยวชาญด้านความมั่นคงปลอดภัยทางเทคนิค)

|  |  |  |  |
| --- | --- | --- | --- |
| **คุณสมบัติที่กำหนด** | **คุณสมบัติบุคลากร** | **ความสอดคล้อง** | **เอกสารอ้างอิง** |
| * คุณวุฒิไม่ต่ำกว่าปริญญาตรี * ประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 5 ป | * วุฒิการศึกษาปริญาโท * สาขาความมั่นคงทางระบบสารสนเทศ * ประสบการณ์ 9 ปี |  | ภาคผนวก ข ประวัติบุคลากร |

* 1. นายชเล ชะเอม (เชี่ยวชาญด้านความมั่นคงปลอดภัยทางเทคนิค)

|  |  |  |  |
| --- | --- | --- | --- |
| **คุณสมบัติที่กำหนด** | **คุณสมบัติบุคลากร** | **ความสอดคล้อง** | **เอกสารอ้างอิง** |
| * คุณวุฒิไม่ต่ำกว่าปริญญาตรี * ประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 5 ป | * วุฒิการศึกษาปริญญาโท * สาขาความมั่นคงทางระบบสารสนเทศ * ประสบการณ์ 10 ปี |  | ภาคผนวก ข ประวัติบุคลากร |

* 1. น.ส. กรรณิกา ศรีแก้ว (ผู้ประสานงานโครงการ)

|  |  |  |  |
| --- | --- | --- | --- |
| **คุณสมบัติที่กำหนด** | **คุณสมบัติบุคลากร** | **ความสอดคล้อง** | **เอกสารอ้างอิง** |
| * คุณวุฒิไม่ต่ำกว่าปริญญาตรี * ประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 2 ป | * วุฒิการศึกษาปริญาตรี * สาขาวิศวกรรมโทรคมนาคม-สื่อสารโครงข่าย * ประสบการณ์ 3 ปี |  | ภาคผนวก ข ประวัติบุคลากร |

* 1. น.ส. จิตติมา กงแก้ว(ผู้ประสานงานโครงการ)

|  |  |  |  |
| --- | --- | --- | --- |
| **คุณสมบัติที่กำหนด** | **คุณสมบัติบุคลากร** | **ความสอดคล้อง** | **เอกสารอ้างอิง** |
| * คุณวุฒิไม่ต่ำกว่าปริญญาตรี * ประสบการณดานความมั่นคงปลอดภัยของข้อมูลสารสนเทศไม่นอยกวา 2 ป | * วุฒิการศึกษาปริญญาตรี * สาขาวิศวกรรมโทรคมนาคม * ประสบการณ์ 3 ปี |  | ภาคผนวก ข ประวัติบุคลากร |