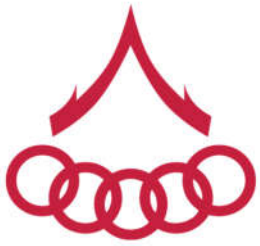

บริษัท สยามราชธานี จำกัด (มหาชน)

นโยบายด้านความมั่นคงปลอดภัย
ระบบเทคโนโลยีสารสนเทศ

สารบัญ

วัตถุประสงค์

การจัดให้มีนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ มีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้าน ต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย

บริษัทฯ ได้ตระหนักดีถึงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จึงได้มีการวางแผนจัดทำนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศฉบับนี้ขึ้น เพื่อเป็นกรอบแนวทางปฏิบัติของพนักงานในองค์กร เพื่อให้พนักงานมีความตระหนักถึงความปลอดภัยของเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยของระบบข้อมูลสารสนเทศของบริษัท และเป็นมาตรการป้องกันความเสี่ยงต่อการเกิดปัญหา รวมทั้งเพื่อให้สอดคล้องกับนโยบายความปลอดภัยของบริษัท ด้านอื่น ๆ ที่มุ่งเน้นการปฏิบัติงานภายในบริษัทให้มีความมั่นคงปลอดภัยในการดำเนินกิจการของบริษัท

ความมั่นคงปลอดภัยสำหรับสารสนเทศ และแนวทางในการรักษาความปลอดภัย

ความมั่นคงปลอดภัยสำหรับสารสนเทศ หมายถึง การสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศ เพื่อป้องกันความเสียหายที่มีต่อองค์ประกอบทางด้านความมั่นคงปลอดภัย 3 ส่วน ดังนี้

1. Confidentialityทรัพย์สินสารสนเทศจะต้องสามารถเข้าถึงได้โดยบุคคลที่ได้รับอนุญาตแล้วเท่านั้น
2. Integrity ทรัพย์สินสารสนเทศจะต้องมีความถูกต้องและสมบูรณ์
3. Availability ทรัพย์สินสารสนเทศจะต้องสามารถเข้าถึงได้เมื่อมีความจำเป็นที่ต้องใช้งาน

บริษัทจะต้องกำหนดมาตรการเพื่อรักษาความมั่นคงปลอดภัยสำหรับทรัพย์สินสารสนเทศโดยบริษัทจะใช้แนวทางดังนี้ ในการรักษาความมั่นคงปลอดภัย

• นโยบายความมั่นคงปลอดภัย (Security Policy) ซึ่งจะประกอบด้วยระเบียบปฏิบัติต่างๆ ที่พนักงานต้องปฏิบัติตามโดยเคร่งครัด

• ขั้นตอนปฏิบัติ (Procedure) ระเบียบปฏิบัติบางข้ออาจจะมีการอ้างอิงถึงการปฏิบัติงานที่เกี่ยวข้อง เช่น ระเบียบปฏิบัติของการใช้ข้อมูลอ้างอิงถึง ขั้นตอนปฏิบัติสำหรับความมั่นคงปลอดภัยของข้อมูลข่าวสาร

ขอบเขตของการสร้างความมั่นคงปลอดภัย

เอกสารฉบับนี้มีขอบเขตคลอบคลุมถึงการสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศต่างๆ ของบริษัท ดังนี้

• พนักงานและลูกจ้างของบริษัททั้งหมด
• ข้อมูล/สารสนเทศของบริษัท
• เครื่องคอมพิวเตอร์แม่ข่าย (Server) ต่างๆ ขององค์กร
• เครื่องคอมพิวเตอร์ส่วนบุคคล
• เครื่องคอมพิวเตอร์แบบพกพา
• อุปกรณ์เครือข่าย
• ระบบไฟฟ้าสำรอง
• สายสัญญาณเครือข่าย
• ซอฟท์แวร์ระบบ ซอฟท์แวร์จ้างพัฒนา ซอฟท์แวร์พัฒนาเอง ซอฟท์แวร์สำเร็จรูป

• สื่อบันทึกข้อมูล
• เอกสารของบริษัท

นโยบายความมั่นคงปลอดภัย

นโยบายด้านความมั่นคงปลอดภัยครอบคลุมนโยบาย 12 ด้าน ดังนี้

1. นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
2. โครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัย และการแบ่งแยกอำนาจหน้าที่
3. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)
4. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)
5. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)
6. การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)
7. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)
8. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)
9. การปฏิบัติงานการจัดการข้อมูลสารสนเทศ
10. การปฏิบัติงานการจัดการบัญชีผู้ใช้งานและการเปลี่ยน Password
11. การบริหารจัดการความเสี่ยงด้านคอมพิวเตอร์
12. การปฏิบัติการจัดการเหตุการณ์และปัญหา

สาระสำคัญของนโยบายมีดังต่อไปนี้

1. นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งมีสาระสำคัญดังนี้

บริษัทต้องจัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยประเมินถึงความเสี่ยงของข้อมูลและระบบคอมพิวเตอร์ เพื่อจัดทำนโยบายให้สามารถรองรับความเสี่ยงที่เกิดขึ้นได้ รวมทั้งการประกาศใช้นโยบายให้แก่บุคลากรที่เกี่ยวข้องได้ตระหนักและปฏิบัติตามนโยบายความปลอดภัยของด้านเทคโนโลยีสารสนเทศที่กำหนดไว้

2. โครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัย และการแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) ซึ่งมีสาระสำคัญดังนี้

บริษัทต้องจัดให้มีโครงสร้างการกำกับดูแลและบทบาทหน้าที่ของหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศในบริษัท และมีการแบ่งแยกหน้าที่การปฏิบัติงานระหว่างบุคลากรภายในฝ่ายคอมพิวเตอร์อย่างเพียงพอ เพื่อช่วยให้มีการสอบยันการปฏิบัติงานและมีการอนุมัติการปฏิบัติงานอย่างเพียงพอและเหมาะสม รวมทั้งการมีขอบเขตการปฏิบัติงานของพนักงานที่ชัดเจนและมีบุคลากรที่เพียงพอต่อการปฏิบัติงานของฝ่ายเทคโนโลยีสารสนเทศ

3. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security) ซึ่งมีสาระสำคัญดังนี้

การควบคุมการเข้าออกศูนย์คอมพิวเตอร์อย่างเพียงพอจะเป็นการป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าสู่ศูนย์คอมพิวเตอร์ และความเสียหายอันจะเกิดจากอุปกรณ์หรือหรือระบบต่างๆ เช่น ระบบไฟฟ้า ระบบอุณหภูมิและความชื้น ซึ่งย่อมมีความเสี่ยงต้องอุปกรณ์และข้อมูลของบริษัท ดังนั้นบริษัทต้องมีการควบคุมเพื่อให้สามารถระบุตัวตนของผู้เข้าถึงศูนย์

คอมพิวเตอร์ได้ และการเข้าถึงดังกล่าวต้องมีการอนุมัติอย่างเพียงพอ ซึ่งจำกัดไว้เฉพาะบุคคลที่จำเป็นเท่านั้น รวมทั้งการควบคุมให้มีระบบป้องกันความเสียหายที่อาจจะเกิดขึ้น เช่นการป้องกันไฟไหม้ หรือไฟฟ้าขัดข้อง

4. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security) ซึ่งมีสาระสำคัญดังนี้

บริษัทต้องควบคุมความปลอดภัยของข้อมูลเพื่อป้องกันความเสี่ยงจากการเข้าถึงระบบคอมพิวเตอร์และการเข้าถึงข้อมูลของบริษัท ตั้งแต่ระดับข้อมูลข่าวสารทั่วไป จนถึงระดับข้อมูลข่าวสารที่ลับที่สุด และควรจะมีหน่วยงานที่มีหน้าที่ควบคุมหรืออนุมัติการที่จะเผยแพร่ข้อมูลข่าวสารให้กับหน่วยงานอื่นๆ หรือนำข้อมูลออกไปเผยแพร่ภายนอกองค์การ ซึ่งอาจส่งผลให้เกิดข้อมูลถูกทำลายหรือนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต ดังนั้นการกำหนดนโยบายการรักษาความปลอดภัยของข้อมูลระบบคอมพิวเตอร์ และระบบเครือข่ายรวมทั้งวิธีการปฏิบัติงานอย่างเพียงพอจะช่วยป้องกันความเสี่ยงที่จะเกิดขึ้นได้

5. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management) ซึ่งมีสาระสำคัญดังนี้

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ เพื่อสร้างความมั่นใจว่าการซื้อหรือการพัฒนามีความสอดคล้องกับแผนงานของบริษัท มีหลักเกณฑ์ในการคัดเลือก พัฒนา มีการจัดลำดับความสำคัญของงาน รวมทั้งกระบวนการพัฒนาได้มีการทดสอบอย่างเพียงพอว่าระบบงานที่แก้ไขเปลี่ยนแปลงมีความถูกต้องและให้ผลลัพธ์ตามที่ได้กำหนดไว้

6. การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan) ซึ่งมีสาระสำคัญดังนี้

บริษัท ต้องกำหนดวิธีการปฏิบัติในกรณีที่เกิดเหตุการณ์ฉุกเฉินในกรณีต่างๆ และกำหนดหน้าที่รับผิดชอบของตัวบุคคล พร้อมทั้งมีการซักซ้อมเป็นระยะ เพื่อให้เกิดผลกระทบต่อการบริการของบริษัทแก่ลูกค้าให้น้อยที่สุด และเพื่อให้การดำเนินการของบริษัท ยังสามารถดำเนินต่อได้โดยไม่ติดขัด

7. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation) ซึ่งมีสาระสำคัญดังนี้

บริษัทต้องกำหนดวิธีการปฏิบัติงานประจำด้านคอมพิวเตอร์ไว้เป็นลายลักษณ์อักษร เพื่อเป็นแนวทางในการปฏิบัติงานของเจ้าหน้าที่ และควรมีการจัดทำบันทึกผลการปฏิบัติงานไว้เพื่อให้สามารถตรวจสอบได้ว่ามีการจัดทำอย่างครบถ้วนและเป็นไปตามวิธีการปฏิบัติงานที่กำหนดไว้

8. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) ซึ่งมีสาระสำคัญดังนี้

การกำหนดนโยบาย ระเบียบปฏิบัติ มาตรฐานและแนวทางในการคัดเลือกผู้ให้บริการภายนอกจะช่วยให้การตัดสินใจที่จะได้รับประสิทธิผลที่ดีขึ้น ซึ่งจะส่งผลต่อค่าใช้จ่ายที่เหมาะสมในการเลือกใช้บริการ และผลของการให้บริการเป็นไปตามที่คาดหวังไว้

9. การปฏิบัติงานการจัดการข้อมูลสารสนเทศ ซึ่งมีสาระสำคัญดังนี้

เพื่อให้บุคลากรของบริษัทที่เกี่ยวข้องกับการใช้ระบบงานคอมพิวเตอร์รวมทั้งเทคโนโลยีสารสนเทศที่เกี่ยวข้องนำไปใช้เป็นมาตรฐานและมีแนวทางแบบเดียวกัน รับรู้สิทธิ์ในการเข้าถึงข้อมูลสารสนเทศและระบบต่างๆสำหรับพนักงานสำหรับบุคคลอื่นที่ไม่ใช่พนักงาน และสำหรับผู้ดูแลระบบ

10. การปฏิบัติงานการจัดการบัญชีผู้ใช้งานและการเปลี่ยน Password ซึ่งมีสาระสำคัญดังนี้

เพื่อให้บุคลากรของบริษัทได้รับสิทธิ์เข้าถึงระบบงานอย่างเหมาะสม และป้องกันไม่ให้ผู้ไม่มีสิทธิ์ใช้งานสามารถเข้าถึงระบบได้ เพื่อสร้างความมั่นใจในการรักษาความลับ และการรักษาความสมบูรณ์ของข้อมูลสารสนเทศ และให้บุคคลากรรับทราบขั้นตอนการเปลี่ยน Password ในการ Login เข้าใช้งานระบบภายในองค์กร

11. การบริหารจัดการความเสี่ยงด้านคอมพิวเตอร์ ซึ่งมีสาระสำคัญดังนี้

เพื่อกำหนดความเสี่ยงที่อาจกระทบต่อการให้บริการของแผนกเทคโนโลยีสารสนเทศ ซึ่งผลจากการประเมินความเสี่ยงจะถูกนำมากำหนดมาตรการควบคุมด้านความมั่นคงปลอดภัย

12. การปฏิบัติการจัดการเหตุการณ์และปัญหา ซึ่งมีสาระสำคัญดังนี้

เพื่อพิจารณาระดับความรุนแรงของผลกระทบ ความเร่งด่วนในการแก้ปัญหา และการพิจารณาระดับความวิกฤติจากเหตุการณ์ละเมิดด้านความมั่นคงปลอดภัย รวมถึงการแจ้งเตือนเหตุการณ์กรณีความวิกฤติในระดับต่างๆ

ระเบียบปฏิบัติ

นโยบายแต่ละด้านจะประกอบไปด้วยระเบียบปฏิบัติที่พนักงานหรือผู้ที่เกี่ยวข้องต้องปฏิบัติตามโดยเคร่งครัดดังต่อไปนี้

นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

การจัดให้มีนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ มีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ความสำคัญ

บริษัทต้องจัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยประเมินถึงความเสี่ยงของข้อมูลและระบบคอมพิวเตอร์ เพื่อจัดทำนโยบายให้สามารถรองรับความเสี่ยงที่เกิดขึ้นได้ รวมทั้งการประกาศใช้นโยบายให้แก่บุคลากรที่เกี่ยวข้องได้ตระหนักและปฏิบัติตามนโยบายความปลอดภัยของด้านเทคโนโลยีสารสนเทศที่กำหนดไว้

ผู้รับผิดชอบหลัก

- ผู้บริหารระดับสูง
- ผู้บริหารระดับผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติ

1. จัดให้มีการทำนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศและมีการปรับปรุงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือตามความจำเป็นต่อการใช้งาน และนโยบายดังกล่าวได้รับการอนุมัติจากคณะกรรมการบริษัทหรือผู้มีอำนาจที่ได้รับมอบหมายไว้

2. จัดทำนโยบายที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้องสามารถเข้าถึงได้ง่าย

3. จัดให้มีการสร้างความตระหนักที่เกี่ยวข้องกับภัยคุกคามทางอินเทอร์เน็ตใหม่ๆ เพื่อให้พนักงานขององค์กร มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้ในระดับหนึ่งอย่างน้อยปีละ 1 ครั้ง

4. จัดให้มีการทำรายงานสรุปปัญหาและแนวทางแก้ไขที่มีระดับความสำคัญสูง เช่น ปัญหาการใช้เครือข่าย การติดไวรัส โครงการพัฒนาระบบงาน ปัญหาจากผู้ใช้งานและเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ และปัญหาอื่นๆ ที่เกี่ยวข้องโดยประมาณเดือนละ 1 ครั้งหรือตามความเหมาะสม

5. จัดให้มีการประเมินความเสี่ยงสำหรับเทคโนโลยีสารสนเทศขององค์กรปีละ 1 ครั้ง และจัดให้มีการทำแผนเพื่อปรับปรุงความเสี่ยงหรือปัญหาที่พบ

6. จัดให้มีการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยปีละ 1 ครั้งและจัดให้มีการทำแผนเพื่อปรับปรุงหรือแก้ไขปัญหาที่พบ

7. จัดให้มีการวางแผนกลยุทธ์ด้านสารสนเทศเพื่อให้สอดคล้องกับกลยุทธ์ทางธุรกิจของบริษัท ทั้งแผนระยะสั้นและแผนระยะยาว

โครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัย

วัตถุประสงค์

เพื่อแสดงโครงสร้างการกำกับดูแลและบทบาทหน้าที่ของหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศในบริษัท สยามราชธานี จำกัด (มหาชน) โดยคำนึงถึงความสำคัญของการปกป้องข้อมูลและระบบเทคโนโลยีอย่างมีประสิทธิภาพและครอบคลุม และเป็นแนวทางในการกำกับดูแลและบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้เกิดความเข้มแข็งและยั่งยืนในบริษัท สยามราชธานี จำกัด (มหาชน)

1. โครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัย

1.1 คณะกรรมการบริหารความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

กรรมการผู้จัดการเทคโนโลยีสารสนเทศ, ผู้อำนวยการฝ่าย IT

หน้าที่: กำหนดนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย, ตรวจสอบและรับรองผลการดำเนินงาน, ส่งเสริมการประสานงานระหว่างแผนกต่างๆ ในเรื่องความมั่นคงปลอดภัย.

1.2 ฝ่าย IT

กรรมการผู้จัดการเทคโนโลยีสารสนเทศ, ผู้อำนวยการฝ่าย IT

หน้าที่: นำทีมฝ่าย IT ในการพัฒนาและบำรุงรักษาเทคโนโลยีที่ปลอดภัยและเสถียร

หัวหน้าแผนกโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ

หน้าที่: จัดการและรักษาพื้นฐานของเทคโนโลยีสารสนเทศ ให้แน่ใจว่าทุกระบบปฏิบัติการสามารถทำงานได้อย่างปลอดภัยและมีประสิทธิภาพ

เจ้าหน้าที่ Network และดำเนินการด้านความปลอดภัยสารสนเทศ

หน้าที่: ติดตั้ง จัดการ และรักษาเครือข่ายภายในองค์กรให้มีความปลอดภัย

เจ้าหน้าที่ควบคุมมาตรฐานด้านสารสนเทศ

หน้าที่: กำหนดและบำรุงรักษามาตรฐานด้านความปลอดภัยข้อมูล

เจ้าหน้าที่ปฏิบัติการด้านสารสนเทศ

หน้าที่: ดำเนินการตามแผนการจัดการเหตุการณ์ความมั่นคงปลอดภัยและรายงานเหตุการณ์ที่เกิดขึ้นให้แก่ผู้บริหาร.

2. บทบาทและหน้าที่ของหน่วยงาน

2.1 จัดทำและปรับปรุงนโยบายความมั่นคงปลอดภัยอย่างสม่ำเสมอ.

2.2 จัดการฝึกอบรมและสร้างความตระหนักเกี่ยวกับความมั่นคงปลอดภัยให้แก่พนักงาน.

2.3 พัฒนาและตรวจสอบระบบเทคโนโลยีสารสนเทศเพื่อรักษาความปลอดภัยข้อมูล.

2.4 ตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัย

ระดับโครงสร้าง	**บทบาทหน้าที่**	**คณะกรรมการ/หน่วยงาน**
ระดับกำกับดูแล	กำหนดนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย, ตรวจสอบและรับรองผลการดำเนินงาน, ส่งเสริมการประสานงานระหว่างแผนกต่างๆ ในเรื่องความมั่นคงปลอดภัย.	คณะกรรมการบริหารความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กรรมการผู้จัดการเทคโนโลยีสารสนเทศ ผู้อำนวยการฝ่าย IT
ระดับบริหารจัดการ	นำทีมฝ่าย IT ในการพัฒนาและบำรุงรักษาเทคโนโลยีที่ปลอดภัยและเสถียร	กรรมการผู้จัดการเทคโนโลยีสารสนเทศ ผู้อำนวยการฝ่าย IT
ระดับปฏิบัติการ	1. จัดการและรักษาพื้นฐานของเทคโนโลยีสารสนเทศ ให้แน่ใจว่าทุกระบบปฏิบัติการสามารถทำงานได้อย่างปลอดภัยและมีประสิทธิภาพ 2. จัดการ และรักษาเครือข่ายภายในองค์กรให้มีความปลอดภัย 3. กำหนดและบำรุงรักษามาตรฐานด้านความปลอดภัยข้อมูล 4. ดำเนินการตามแผนการจัดการเหตุการณ์ความมั่นคงปลอดภัยและรายงานเหตุการณ์ที่เกิดขึ้นให้แก่ผู้บริหาร.	หัวหน้าแผนกโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เจ้าหน้าที่ Network และดำเนินการด้านความปลอดภัยสารสนเทศ เจ้าหน้าที่ควบคุมมาตรฐานด้านสารสนเทศ เจ้าหน้าที่ปฏิบัติการด้านสารสนเทศ

ตารางที่ 1 ตารางโครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและบทบาทหน้าที่ของหน่วยงาน

ประกาศ ณ วันที่ 17 ธันวาคม 2566

บริษัท สยามราชธานี จำกัด (มหาชน)

ลงชื่อ.....

(นายณัฐพล วิมลเฉลา)

ประธานเจ้าหน้าที่บริหาร