นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

(CAT IT Security Policy)

1. วัตถุประสงค์และขอบเขต

ด้วยบริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้นำระบบเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจ เพื่ออำนวยความสะดวกแก่พนักงานและลูกจ้างในการปฏิบัติงาน ดังนั้นเพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัย สามารถดำเนินธุรกิจได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ จำเห็นสมควรกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศที่ครอบคุลมถึงประเด็นสำคัญ

- **การรักษาความลับ (Confidentiality)** คือ การรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ ผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลได้ และไม่ถูกเปิดเผยสู่บุคคลหรือหน่วยงานอื่นที่ไม่มีสิทธิ
- **การรักษาความสมบูรณ์ (Integrity)** คือ การรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา ข้อมูลจะคงอยู่อย่างถูกต้องและสมบูรณ์ ตลอดขั้นตอนการประมวลผล และขั้นตอนการเก็บรักษา
- **ความพร้อมใช้ (Availability)** คือ การรับรองว่าข้อมูลและการบริการสื่อสารต่าง ๆ พร้อมที่จะใช้ได้ในเวลาที่ต้องการใช้งาน
- **การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation)** คือ วิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้อกับข้อมูลดังกล่าวในภายหลัง

2. องค์ประกอบของนโยบาย

นโยบายความมั่งคงปลอดภัยด้านสารสนเทศ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เป็นนโยบายที่ได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ตามข้อกำหนดของประกาศคณะกรรมการ

ธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ซึ่งประกอบด้วย 10 หมวด ตามเอกสารแนบท้ายคำสั่งนี้ ดังต่อไปนี้

หมวด 1 นโยบายความมั่นคงปลอดภัย

หมวด 2 การบริหารจัดการสินทรัพย์

หมวด 3 การบริหารข้อมูลบุคคล

หมวด 4 การควบคุมการเข้าถึง

หมวด 5 การเข้ารหัสข้อมูล

หมวด 6 ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

หมวด 7 การบริหารจัดการด้านการสื่อสารและการดำเนินงาน

หมวด 8 การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่ถึงประสงค์หรือไม่อาจคาดคิด

หมวด 9 การบริหารต่อเนื่องในการดำเนินงาน

หมวด 10 การปฏิบัติตามข้อกำหนด

นโยบายแต่ละหมวดที่กล่าวมาข้างต้นจะประกอบด้วย วัตถุประสงค์ในการดำเนินการที่เกี่ยวข้องกับหมวดนั้น ๆ และมีรายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนการปฏิบัติงาน (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เพื่อลดความเสียหายต่อการดำเนินธุรกิจ สินทรัพย์ ทรัพยากรบุคคล และรายได้ของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ทำให้ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เป็นหน่วยงานที่ได้รับการยอมรับจากองค์กรต่าง ๆ ในการดำเนินธุรกิจได้อย่างมั่นคงปลอดภัยตามมาตรฐานสากล

หมวด 1

นโยบายความมั่นคงปลอดภัย

(Security Policy)

1. คำแถลงนโยบาย

บริษัท กสท โทรคมนาคม จำกัด (มหาชน) จัดทำนโยบายนี้เพื่อเป็นส่วนหนึ่งของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ในการป้องกันภัยคุกคาม ลดความเสี่ยงจากช่องโหว่และผู้บุกรุก เพื่อให้สารสนเทศมีความปลอดภัย สามารถรักษาความลับและความถูกต้องของข้อมูล และมีความพร้อมในการให้บริการอยู่ในระดับที่ยอมรับได้ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) จึงได้กำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศเพื่อเป็นแนวทางเสริมสร้างความมั่นคงปลอดภัยด้านสารสนเทศให้กับ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) หรือหน่วยงานที่มีความเกี่ยวข้องในการทำธุรกิจกับ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) โดยนโยบายนี้มีจุดประสงค์เพื่อการสนับสนุนการดำเนินการเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ดังนี้

- เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ทำให้การดำเนินธุรกิจมีประสิทธิภาพและประสิทธิผล
- เพื่อเผยแพร่ให้พนักงานและลูกจ้างทุกระดับใน บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้รับทราบ แล้วต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
- เพื่อให้มีการดำเนินการที่เหมาะสมและสัมฤทธิ์ผล มีการตรวจสอบและประเมินนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง
- เพื่อสร้างความตื่นตัวให้ผู้บริหาร พนักงานและลูกจ้าง ผู้ดูแลระบบ และหน่วยงานภายนอกที่ปฏิบัติงานให้กับ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศ
- เพื่อดำเนินการหรือประสานงานกับหน่วยงานอื่น ๆ ทั้งภายในประเทศและต่างประเทศในการสนับสนุนความรู้หรือข้อมูลด้านความมั่นคงปลอดภัยที่เป็นประโยชน์ต้อการทำงานหรือการพัฒนาบุคลากรที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

2. องค์ประกอบของนโยบาย

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ใช้แนวทางและกระบวนการโดยอ้างอิงตามมาตรฐาน ISO/IEC 27001:2005 Annex A และศึกษารายละเอียดวิธีปฏิบัติทางเทคนิคจาก ISO/IEC 17799:2005

หมวด 2
การบริหารจัดการสินทรัพย์
(Asset Management)

1. วัตถุประสงค์

เพื่อเป็นการกำหนดมาตรฐานในการจัดหมวดหมู่และควบคุมสินทรัพย์ของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ป้องกันสินทรัพย์จากภัยคุกคาม ช่องโหว่ ผู้บุกรุก การถูกขโมย และสิ่งที่สร้างความเสียหายที่อาจเกิดขึ้นได้

2. การจัดหมวดหมู่และการควบคุมสินทรัพย์

2.1 การจัดทำบัญชีสินทรัพย์ (Inventory of Assets)

หัวหน้าหน่วยงานแต่ละหน่วยงาน ต้องทำบัญชีสินทรัพย์ของหน่วยงานและแบ่งประเภทให้ชัดเจน ซึ่งรวมถึงบัญชีครุภัณฑ์คอมพิวเตอร์และบัญชีข้อมูลที่เก็บไว้ในสื่อต่าง ๆ ทั้งหมด เพื่อใช้ในการกำหนดมูลค่าสินทรัพย์ระดับความสำคัญและวิธีการป้องกันที่เหมาะสม รวมทั้งต้องระบุผู้เป็นเจ้าของสารสนเทศ (แต่ละชนิด) ตามที่กำหนดไว้ในบัญชีสินทรัพย์

2.2 การตรวจสอบบัญชีสินทรัพย์ (Inventory Check)

หัวหน้าหน่วยงานแต่ละหน่วยงาน ต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ตามระยะเวลาที่กำหนดไว้ เช่น เดือนละครั้ง (สำหรับระบบสำคัญ) หรือปีละครั้ง(สำหรับระบบการใช้งานทั่วไป)

2.3 การจัดหมวดหมู่ข้อมูลและสารสนเทศ (Data and Information Classification)

2.3.1 หัวหน้าหน่วยงานแต่ละหน่วยงาน ต้องทำการจัดหมวดหมู่ กำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันสารสนเทศของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดย บริษัท กสท โทรคมนาคม จำกัด (มหาชน) จัดให้มีกระบวนการ

ในการจัดหมวดหมู่ของข้อมูลและสินทรัพย์ เช่น ชั้นลับที่สุด ชั้นลับมากและชั้นลับ การกำหนดแนวทางการแบ่งชั้นความลับของข้อมูล ต้องอยู่ในการควบคุมดูแลและรักษาความปลอดภัยที่เหมาะสมไม่ว่าจะอยู่ในรูปแบบใดก็ตาม

2.3.2 ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การเก็บรักษา จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้พนักงานและลูกจ้างของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย

2.4 จัดทำป้ายชื่อ ข้อมูล และสารสนเทศ (Data and Information Labeling and Handing)

หัวหน้าหน่วยงานแต่ละหน่วยงาน ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับข้อมูลและสารสนเทศ โดยแยกตามหมวดหมู่ที่กำหนดไว้ มีการส่งมอบและจัดเก็บ ตามขั้นตอนกระบวนการต่าง ๆ ซึ่งประกอบไปด้วย การถ่ายเอกสาร การจัดเก็บ การส่งต่อ การสื่อสารและการทำลาย จะต้องปฏิบัติตามแนวทางปฏิบัติงานที่ได้มีการกำหนดไว้

หมวด 3
การบริหารข้อมูลส่วนบุคคล
(Data Privacy)

1. วัตถุประสงค์

นโยบายนี้ระบุถึงข้อกำหนดเพื่อคุ้มครองข้อมูลส่วนบุคคลของพนักงาน ลูกจ้าง และลูกค้าเก็บรวบรวม การใช้งาน การเปิดเผย การเก็บรักษา การรักษาความปลอดภัย การเข้าถึง การโอนย้าย หรือการประมวลผลข้อมูลส่วนบุคคลในระดับสูง บริษัท กสท โทรคมนาคม จำกัด (มหาชน) อาจมีการดำเนินการปรับปรุงหรือแก้ไขนโยบายเพื่อให้สอดคล้องกับการดำเนินงานในอนาคต โดยนโยบายคุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้กับบริการต่าง ๆ ของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ที่ให้บริการกับพนักงาน ลูกจ้าง และลูกค้าของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

2. การเก็บรวบรวมข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลให้กระทำภายใต้กรอบวัตถุประสงค์และเพียงเท่าที่จำเป็นเพื่อประโยชน์ที่เกี่ยวข้องโดยตรงกับวัตถุประสงค์ โดยจะต้องแจ้งให้เจ้าของข้อมูลทราบก่อนหรือเก็บรวบรวมข้อมูลส่วนบุคคล ถึงรายละเอียดดังต่อไปนี้

2.1 วัตถุประสงค์ของการเก็บรวบรวม

2.2 ข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวม

2.3 กรณีที่เจ้าของข้อมูลต้องให้ข้อมูลส่วนบุคคล เพื่อปฏิบัติตามกฎหมายหรือสัญญา หรือเพื่อเข้าทำสัญญาโดยต้องแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบ

2.4 ประเภทของข้อมูลส่วนบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจถูกเปิดเผย

2.5 สิทธิของเจ้าของข้อมูล

3. การใช้หรือการเปิดเผยข้อมูลส่วนบุคคล

การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ให้เป็นไปตามวัตถุประสงค์หรือเป็นการจำเป็นเพื่อประโยชน์ที่มีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์การเก็บรวบรวม และต้องได้รับการยินยอมจากเจ้าของข้อมูลที่ให้ไว้ก่อนหรือในขณะนั้น เว้นแต่ในกรณีดังต่อไปนี้ไม่จำเป็นต้องขอความยินยอม

3.1 เพื่อประโยชน์ที่เกี่ยวกับการวางแผนหรือการสถิติหรือสำมะโนต่าง ๆ ของหน่วยงานของรัฐ

3.2 เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล

3.3 เป็นข้อมูลที่เปิดเผยต่อสาธารณะโดยชอบด้วยกฎหมาย

3.4 เพื่อประโยชน์แก่การสืบสวนของพนักงานเจ้าหน้าที่ตามกฎหมาย หรือในการพิพากษาคดีของศาล

3.5 เป็นการปฏิบัติตามที่กฎหมายกำหนด

4. คุณภาพของข้อมูลส่วนบุคคล

คุณภาพของข้อมูลส่วนบุคคลที่เก็บรวบรวมนั้นต้องถูกต้อง ทันสมัย สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด เว้นแต่จะมีกฎหมายกำหนดไว้เป็นอย่างอื่น

5. การรักษาความมั่นคงปลอดภัย

เพื่อประโยชน์ในการรักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคล บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้มีมาตรการดังนี้

5.1 กำหนดสิทธิในการเข้าถึง การใช้ การเปิดเผย การประเมินผลข้อมูลส่วนบุคคล รวมถึงการแสดงหรือยืนยันตัวบุคคล ผู้เข้าถึงหรือใช้ข้อมูลส่วนบุคคลตามนโยบายสารสนเทศของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) อย่างเคร่งครัด

5.2 ในการส่ง การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ รวมถึงการนำข้อมูลส่วนบุคคลไปเก็บบนฐานข้อมูลในระบบอื่น ซึ่งผู้ให้บริการรับโอนข้อมูลหรือบริการเก็บรักษาข้อมูลอยู่ต่างประเทศ ประเทศ

ปลายทางที่เก็บรักษาข้อมูลต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เทียบเท่าหรือดีกว่ามาตรการตามนโยบายนี้

5.3 ในกรณีที่มีการฝ่าฝืนมาตรการการรักษาความมั่นคงปลอดภัยของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) จนเป็นเหตุให้มีการละเมิดข้อมูลส่วนบุคคล หรือข้อมูลส่วนบุคคลรั่วไหลสู่สาธารณะ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) จะดำเนินการแจ้งเจ้าของข้อมูลให้ทราบโดยเร็วรวมทั้งแจ้งแผนการเยียวยาความเสียหายจากการละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคลสู่สาธารณะในกรณีที่เกิดจากความบกพร่องของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ทั้งนี้ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) จะไม่รับผิดชอบในกรณีความเสียหายใด ๆ อันเกิดจากการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลที่สาม รวมถึงการละเลย หรือเพิกเฉยการออกจากระบบฐานข้อมูล

5.4 บริษัท กสท โทรคมนาคม จำกัด (มหาชน) มีการดำเนินการสอบทานและประเมินประสิทธิภาพของระบบรักษาข้อมูลส่วนบุคคลโดยหน่วยงานตรวจสอบภายใน

6. สิทธิของเจ้าของข้อมูลส่วนบุคคล

6.1 สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตน หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลที่ตนไม่ได้ให้ความยินยอมโดย บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ต้องดำเนินการตามคำขอภายใน 30 วันนับแต่วันที่ได้รับคำขอ

6.2 สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลของตนตามที่กฎหมายกำหนด

6.3 สิทธิขอรับหรือขอให้ส่งหรือโอนย้ายข้อมูลส่วนบุคคลของตนไปยังบุคคลอื่นเพื่อวัตถุประสงค์ของตนเองเมื่อ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) สามารถทำได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ

6.4 สิทธิขอลบข้อมูลส่วนบุคคลของตนออกจากระบบ หรือขอให้ทำลาย หรือการระงับใช้ หรือการทำให้ข้อมูลส่วนบุคคลของตนเป็นข้อมูลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ เว้นแต่กรณีที่บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ต้องปฏิบัติตามกฎหมายที่เกี่ยวข้องในการเก็บรักษาข้อมูลดังกล่าว

6.5 สิทธิขอแก้ไขข้อมูลส่วนบุคคลของตนถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

โดยเจ้าของข้อมูลสามารถติดต่อ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้ที่
ที่อยู่ : 99 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210

เวลาทำการ : จันทร์-ศุกร์ 08.30-16.30 น.
โทรศัพท์ : 0-2104-3835
โทรสาร : 0-2104-3416

7. การบทบทวนนโยบาย

บริษัท กสท โทรคมนาคม จำกัด (มหาชน) จะมีทำการทบทวนนโยบายด้านการคุ้มครองข้อมูลส่วนบุคลเป็นประจำทุกปี อย่างน้อยปีละ 1 ครั้ง หรือกรณีที่กฎหมายมีการเปลี่ยนแปลงแก้ไขไปเป็นอย่างอื่น

หมวด 4
การควบคุมการเข้าถึง
(Access Control)

1. วัตถุประสงค์

นโยบายนี้ระบุถึงข้อกำหนดเพื่อควบคุมสำหรับการเข้าถึงระบบสารสนเทศของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เพื่อให้มีความมั่นคงปลอดภัย และป้องกันไม่ให้ผู้ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบได้

2. กระบวนการความมั่นคงปลอดภัยด้านสารสนเทศของการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

2.1 สถานที่ตั้งของระบบสารสนเทศที่สำคัญ ต้องมีการควบคุมการเข้าออกที่รัดกุมและให้เฉพาะบุคคลที่ได้รับอนุญาตและมีความจำเป็นเท่านั้นสามารถเข้าใช้งานได้ เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์บางอย่างของสำนักงานที่ไม่มีพนักงานและลูกจ้างดูแล

2.2 ผู้ดูแลระบบต้องกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบและข้อมูลให้เหมาะสมกับการใช้บริการและหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิอย่างสม่ำเสมอ

2.3 ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงบริการได้

2.4 ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลที่สำคัญ ทั้งนี้ ผู้ที่สามารถใช้ซอฟต์แวร์หรือฮาร์ดแวร์ในการตรวจตราและเฝ้าระวังในระบบเครือข่ายหรือระบบงานใด ๆ ต้องเป็นผู้ที่ได้รับอนุญาตจากหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ อย่างถูกต้องเท่านั้น

2.5 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบ หากมีปัญหาเกิดขึ้น

2.6 ในการขออนุญาตเข้าสู่ระบบงานต่าง ๆ จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบ กำหนดให้มีการลงนามอนุมัติและเก็บเอกสารดังกล่าวไว้เป็นหลักฐาน

2.7 เจ้าของข้อมูลและเจ้าของระบบงานนั้น ๆ จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

3. การบริหารจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management)

3.1 การลงทะเบียนผู้ใช้งาน (User Registration)

หัวหน้าหน่วยงานแต่ละหน่วยงาน และหัวหน้าหน่วยงานดูแลรับผิดชอบการบริหารงานบุคคลและสวัสดิการ ต้องร่วมกันจัดทำระเบียบปฏิบัติในการลงทะเบียนผู้ใช้งานใหม่ เพื่อให้สามารถใช้งานระบบสารสนเทศได้ นอกจากนี้ ต้องมีระเบียบปฏิบัติเพื่อยกเลิกการใช้งานของผู้ใช้งานทันที ในกรณีที่มีการลาออกหรือเปลี่ยนตำแหน่งงานภายใน บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

3.2 การบริหารจัดการสิทธิการใชงานระบบ (Privilege Management)

3.2.1 ผู้ดูแลระบบต้องกำหนดสิทธิของผู้ใช้งานตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน เช่น กำหนดสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศระบบงานตามความจำเป็นขั้นต่ำเท่านั้น

3.2.2 ผู้ใช้งานต้องได้รับการอนุมัติสิทธิให้เสร็จสมบูรณ์ก่อน จึงจะสามารถเข้าใช้งานระบบได้

3.3 การบริหารจัดการรหัสผ่านของผู้ใช้งาน (User Password Management)

เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลและสารสนเทศ ผู้ใช้งานควรปฏิบัติตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

3.4 การทบทวนสิทธิการเขาถึงของผู้ใช้งาน (Review of User Access Rights)

ผู้ดูแลระบบ เจ้าของข้อมูลและเจ้าของระบบงาน ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่เหมาะสม โดยต้องมีการสอบทานความเหมาะสมของสิทธิของผู้ใช้งานในการเข้าใช้ข้อมูลอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

4. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงหรือควบคุมการใช้งานสารสนเทศจากผู้ที่ไม่ได้รับอนุญาต ควรพิจารณาดังต่อไปนี้

4.1 ในกรณีที่อนุญาตให้ Protocol บางประเภทสามารถเข้าถึงระบบเครือข่ายของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) จะต้องมี มาตรการการป้องกันล่วงหน้าและขั้นตอนการปฏิบัติงานโดยเฉพาะ

4.2 แม้จะติดตั้ง Router และ Firewall อย่างปลอดภัยแล้วก็ตาม การแก้ไขในภายหลังอาจก่อให้เกิดความเสี่ยงต่อระบบงานได้ เพื่อลดความเสี่ยงต่าง ๆ ทุกครั้งที่มีการเปลี่ยนแปลง Router และ Firewall จะต้องปฏิบัติตามนโยบายการบริหารจัดการเปลี่ยนแปลงระบบสารสนเทศ

4.3 ห้ามทำ Packet Forwarding หรือ Re-routing สำหรับ Server ที่มีการติดตั้ง Protocol ที่สามารถทำได้ เช่น กำหนดให้ FTP ไม่สามารถทำ IP Forwarding หรือ Passive mode ได้

4.4 หมายเลขเครือข่ายภายใน (Internal Network Address) ของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) จำเป็นต้องมีการป้องกันมิให้ส่วนงานที่เชื่อมต่อจากภายนอกสามารถมองเห็นได้ เพื่อป้องกันไม่ให้ Hackers หรือหน่วยงานภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบงานเครือข่ายและส่วนประกอบของคอมพิวเตอร์ของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้โดยง่าย

4.5 เพื่อลดความเสี่ยงจากการใช้ TCP/IP ดังนั้น Router และ Firewall จะต้องปฏิเสธการเชื่อมต่อใด ๆ จากระบบภายนอก ซึ่งมี IP Address เหมือนกับ IP Address ที่ใช้ในเครือข่ายภายในของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

4.6 สำหรับข้อมูลที่ผ่านเข้าและส่งออกจากระบบเครือข่าย บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ต้องส่งข้อมูลผ่าน Firewall เพื่อป้องกันการเชื่อมต่อจากผู้ที่ไม่ได้รับอนุญาต โดยกำหนดให้ผู้ดูแลระบบเครือข่ายเป็นผู้อนุมัติการเชื่อมต่อระบบเครือข่ายจากภายนอกของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

4.7 การเข้าสู่ระบบเครือข่ายของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ผ่านอินเทอร์เน็ต จะต้องมีการ Log on เพื่อพิสูจน์ตัวตน และได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศก่อน

4.8 ระบบเครือข่ายทั้งหมดของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ต้องมีการใช้อุปกรณ์หรือซอฟต์แวร์ในการทำ Packet Filtering เช่น การใช้ Firewall หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

4.9 ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายัง บริษัท กสท โทรคมนาคม จำกัด (มหาชน) และการเชื่อมต่อนี้ต้องเข้ามายังเครื่องคอมพิวเตอร์หรือระบบงานที่กำหนดไว้เท่านั้น ควรกำหนดให้เครื่อง

คอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ทั้งด้าน Physical และ Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิเข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่าย บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้โดยอิสระ

4.10 ผู้ดูแลระบบต้องจัดแบ่งระหว่างเครือข่ายภายในและเครือข่ายภายนอก (Segregation in Networks) โดยพิจารณาจากบริการเครือข่ายของกลุ่มผู้ใช้งานทั้งสองฝ่าย

4.11 ผู้ดูแลระบบต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อบนเครือข่ายมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว เพื่อจำกัดสิทธิในการใช้งานระบบสารสนเทศของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

5. ความมั่นคงปลอดภัยสำหรับการให้บริการเครือข่าย (Security of Network Services)

หัวหน้าหน่วยงานแต่ละหน่วยงานและผู้ดูแลระบบ ต้องจัดทำข้อกำหนดหรือสัญญาดานความมั่นคงปลอดภัยของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกันระหว่าง บริษัท กสท โทรคมนาคม จำกัด (มหาชน) กับลูกค้า ซึ่งมีแนวทางปฏิบัติดังนี้

5.1 ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิของผู้ใช้งาน เพื่อควบคุมพนักงานและลูกจ้างให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

5.2 ผู้ดูแลระบบต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

5.3 ผู้ดูแลระบบต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้พนักงานและลูกจ้างสามารถใช้เส้นทางอื่นได้

5.4 ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายัง บริษัท กสท โทรคมนาคม จำกัด (มหาชน) และต้องกำหนดให้การเชื่อมต่อนี้เข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้เท่านั้น หากเป็นไปได้ ควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ทั้งทาง Physical และ Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิเข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่าย บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้โดยอิสระ

หมวด 5

การเข้ารหัสข้อมูล

(Cryptography)

1. วัตถุประสงค์

เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และป้องกันข้อมูลที่เป็นขั้นความลับ การปลอมแปลงหรือความถูกต้องของข้อมูลสารสนเทศ ไม่ให้มีการรั่วไหลออกไปสู่บุคคลภายนอกที่ไม่ได้เกี่ยวข้อหรือมีสิทธิในการเข้าถึงข้อมูล

2. มาตรการการเข้ารหัสข้อมูล

กำหนดนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูล และให้มีผลบังคับใช้ใน บริษัท กสท โทรคมนาคม จำกัด (มหาชน) และต้องกำหนดให้มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล โดยกุญแจเหล่านี้จะใช้งานร่วมกับเทคนิคการเข้ารหัสข้อมูลที่กำหนดเป็นมาตรฐานของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

2.1 นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)

ต้องมีนโยบายการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง ที่สอดคล้องกับนโยบายของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

2.2 การบริหารจัดการกุญแจในการเข้ารหัสข้อมูล (Key Management)

นโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจต้องมีการจัดทำและปฏิบัติตามตลอดวงจรชีวิตของกุญแจ โดยองค์กรควรมีการกำหนดมาตรการในการเก็บ Key ที่เป็นข้อมูลลับของแต่ละบุคคล

หมวด 6

ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

(Physical and Environmental Security)

1. วัตถุประสงค์

เพื่อเป็นมาตรฐานในความมั่นคงปลอดภัยด้านสารสนเทศทางกายภาพที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นสินทรัพย์ของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) โดยนโยบายนี้มีผลบังคับใช้กับผู้ใช้งานและหน่วยงาน บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ซึ่งมีส่วนเกี่ยวข้องกับการใช้ระบบสารสนเทศของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

2. มาตรฐานในการกำหนดบริเวณที่ต้องมีความมั่นคงปลอดภัยด้านสารสนเทศ (Secure Areas)

2.1 ทุกหน่วยงาน ตั้งแต่ระดับฝ่ายขึ้นไป จะต้องมีการจำแนกและกำหนดบริเวณพื้นที่ใช้งานระบบสารสนเทศตามที่ได้นิยามไว้ รวมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศ เพื่อการเฝ้าระวัง ควบคุมและรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ และประกาศให้รับทราบทั่วกัน (ควรระบุให้ชัดเจนว่ามีพื้นที่ใช้งานระบบสารสนเทศกี่ประเภทและประเภทใดบ้าง)

2.2 ทุกหน่วยงานต้องกำหนดการติดตั้งอุปกรณ์ในพื้นที่ใช้งานระบบสารสนเทศให้สอดคล้องกับหมวดหมู่และความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ

2.3 หน่วยงานที่รับผิดชอบอุปกรณ์ที่สำคัญของระบบสารสนเทศ ต้องดำเนินการติดตั้งอุปกรณ์ในการรักษาความปลอดภัย เช่น กล้องวงจรปิด ระบบ Access Control หรืออุปกรณ์ที่สามารถป้องกันภัยคุกคามจากผู้บุกรุก เป็นต้น ในพื้นที่ใช้งานระบบสารสนเทศของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้แก่ ห้อง Server/Data Center , ห้อง Network Control หรือห้อง Network Center ห้องเก็บข้อมูลสำรอง เพื่อให้เป็นไปตามมาตรฐานสากลที่กำหนดไว้

3. การควบคุมการเข้าออก (Physical Entry Controls)

3.1 ระบุตัวผู้ใช้งานและช่วงเวลาที่มีสิทธิผ่านเข้าออกในแต่ละพื้นที่อย่างชัดเจน

3.2 ผู้ใช้งานจะได้รับสิทธิให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณที่ถูกกำหนดเท่านั้น

3.3 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งาน ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาตหรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้จะต้องแสดงบัตรประจำตัวที่ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ออกให้ หรือ

บัตรประจำตัวประชาชน หรือบัตรประจำตัวอื่นที่ราชการออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการขอเข้าออกไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่)

4. ความมั่นคงปลอดภัยด้านสารสนเทศสำหรับสำนักงาน ห้องทำงาน และเครื่องมือต่างๆ (Securing Offices, Room and Facilities)

4.1 หัวหน้าหน่วยงานแต่ละหน่วยงาน ต้องจัดให้มีมาตรการความมั่นคงปลอดภัยด้านสารสนเทศให้กับสำนักงาน ห้องทำงานและเครื่องมือต่าง ๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก สำนักงานจะต้อง **ไม่มีป้าย** หรือ **สัญลักษณ์** ที่บ่งบอกถึงการมีระบบสำคัญในบริเวณดังกล่าว ประตูหน้าต่างของสำนักงานต้องใส่กุญแจเมื่อไม่มีคนอยู่ เครื่องโทรสารหรือเครื่องถ่ายเอกสารควรแยกออกมาจากบริเวณดังกล่าว เป็นต้น โดยมีแนวทางปฏิบัติ เช่น กั้นพื้นที่อย่างรอบด้าน (เช่น ติดตั้งผนัง ติดตั้งเหล็กดัด ล็อคประตูที่ใช้ดอกกุญแจหรือมีระบบ Access Control) และปรับปรุงให้มีความเหมาะสมทางสภาวะแวดล้อม (เช่น ติดตั้งระบบปรับอากาศ การควบคุมความชื้น เป็นต้น)

4.2 การปฏิบัติงานในพื้นที่ควบคุม (Working in Control Areas)

4.2.1 หัวหน้าหน่วยงานแต่ละหน่วยงาน ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวิดีโอในบริเวณนั้น เป็นต้น

4.2.2 ต้องมีป้ายประกาศข้อความ **“ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวิดีโอ”** และ “**ห้ามสูบบุหรี่**” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

4.3 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access, Delivery, and Loading Areas)หน่วยงานดูแลรับผิดชอบด้านอาคารและสถานที่ ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยหน่วยงานภายนอก เพื่อป้องกันการเข้าถึงสินทรัพย์ของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) โดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ ควรจัดเป็นบริเวณแยกออกมาต่างหาก

4.4 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

4.4.1 ผู้ใช้งานต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัยรวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

4.4.2 หัวหน้าหน่วยงานที่เป็นเจ้าของระบบงาน ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงปีละ 1 ครั้ง หรือระบบที่สำคัญมากอาจจะกำหนดให้มีการบำรุงรักษาทุกสิ้นเดือน เป็นต้น

4.4.3 หัวหน้าหน่วยงานแต่ละหน่วยงาน ต้องกำหนดให้มีการป้องกันสินทรัพย์และอุปกรณ์ของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เช่น Notebook, Mobile Phone เมื่อถูกนำไปใช้งานนอกสำนักงาน โดยต้องปฏิบัติตามระเบียบในการใช้งานการยืม-คืน

4.5 ระบบกระแสไฟฟ้าสำรอง (Power Supplies) และระบบป้องกันภัย

4.5.1 ต้องมีระบบไฟฟ้าสำรองอัตโนมัติ เพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง และต้องมีการตรวจสอบระบบไฟฟ้าสำรองและบำรุงรักษาอย่างน้อยปีละ 2 ครั้ง

4.5.2 ต้องจัดให้มีระบบเตือนภัย/ป้องกันภัย เช่น ระบบดับเพลิง ระบบเตือนอัคคีภัย

4.5.3 ต้องมีการวางแผน และซักซ้อมการปฏิบัติรับมือกับภัย เช่น อัคคีภัย อย่างน้อยปีละ 2 ครั้ง

4.5.4 ไม่ควรกระทำการใด ๆ ให้เกิดมีประกายไฟหรือเปลวไฟ

4.5.5 ระบบที่สำคัญของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) จะต้องมีการปฏิบัติตามนโยบายแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ เพื่อป้องกันผลกระทบที่จะเกิดขึ้นกับการดำเนินธุรกิจของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

4.6 การเดินสายไฟฟ้าหลัก (Main Power Cable) และสายเคเบิลหลัก (Backbone Cable)

หัวหน้าหน่วยงานแต่ละหน่วยงาน ต้องคำนึงถึงการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสำนักงาน เช่น ผ่านเข้ามาทางใต้ดิน ผ่านช่องพิเศษที่จัดไว้หรือเป็นบริเวณที่บุคคลทั่วไปไม่สามารถเข้าถึงได้ง่าย ซึ่งมีแนวทางปฏิบัติ เช่น บริเวณที่มีการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสำนักงาน และมีการติดตั้งตู้พักสาย ต้องล็อคไว้ตลอดเวลาและจำกัดการเข้าใช้งานได้เฉพาะเจ้าหน้าที่หรือบุคคลที่มีสิทธิเท่านั้น

หมวด 7
การบริหารจัดการด้านการสื่อสารและการดำเนินงาน
(Communication and Operations Management)

1. วัตถุประสงค์

นโยบายนี้กำหนดขึ้นเพื่อให้การใช้งานเครือข่ายคอมพิวเตอร์เป็นไปอย่างถูกต้องและปลอดภัย จึงจำเป็นต้องมีการบริหารจัดการเครือข่ายของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ให้มีความมั่นคงปลอดภัยด้านความถูกต้อง การเก็บรักษาเป็นความลับ และความพร้อมในการใช้งาน นโยบายดังกล่าวนี้มีผลบังคับใช้กับพนักงานและลูกจ้างของบริษัท กสท โทรคมนาคม จำกัด (มหาชน) และหน่วยงานภายนอกที่ขออนุญาตใช้งานระบบสารสนเทศของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

2. มาตรฐานทั่วไป

2.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational Procedures and Responsibilities)

2.1.1 หัวหน้าหน่วยงานที่เป็นเจ้าของระบบงาน ต้องจัดทำคู่มือและขั้นตอนการปฏิบัติงานของระบบงานนั้น ๆ โดยมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่าย

2.1.2 ในกรณีที่มีการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ หน่วยงานที่ดูแลระบบสารสนเทศนั้นต้องทำการบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่น ๆ ที่เกี่ยวข้องทราบ

2.1.3 หัวหน้าหน่วยงานที่เป็นเจ้าของระบบงาน ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวกับระบบสารสนเทศและเครือข่ายที่หน่วยงานนั้น ๆ รับผิดชอบ

2.1.4 หัวหน้าหน่วยงานที่เป็นเจ้าของระบบงาน ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัย และดำเนินการตรวจสอบผู้ละเมิด

2.1.5 หัวหน้าหน่วยงานที่เป็นเจ้าของระบบงาน ต้องแยกเครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบสารสนเทศออกจากเครื่องที่ทำงานจริงหรือเครื่องให้บริการ

2.1.6 ในกรณีที่มีการบริหารจัดการระบบสารสนเทศจากภายนอก บริษัท กสท โทรคมนาคม จำกัด (มหาชน) หน่วยงานที่รับผิดชอบต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศสำหรับหน่วยงานภายนอก โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิของผู้ใช้งานที่ได้รับและตรวจสอบการใช้งานอย่างสม่ำเสมอ

2.2 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการต่อหน่วยงานภายนอก (Managing Changes to Third Party Services)

ต้องปรับปรุงเงื่อนไขการให้บริการต้อหน่วยงานภายนอก เมื่อมีการเปลี่ยนแปลงที่สำคัญต้อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงหรือพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบายและขั้นตอนปฏิบัติสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ การใช้ผลิตภัณฑ์ใหม่ เป็นต้น ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอกโดยต้องได้รับการอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ก่อนจึงจะสามารถดำเนินการได้ รวมทั้งปรับปรุงเอกสารที่เกี่ยวข้องให้ทันสมัย เมื่อมีการเปลี่ยนแปลงสารสนเทศ

2.3 การวางแผนและตรวจรับทรัพยากรสารสนเทศ (System Planning and Acceptance)

2.3.1 หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ต้องมีการวางแผนกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคต โดยสำรวจความต้องการทรัพยากรสารสนเทศให้ครบถ้วน เพื่อไม่ให้โครงการเกิดความล้าช้าในการจัดซื้อจัดหา และควรคำนึงถึงความมั่นคงปลอดภัยของสารสนเทศด้วย ซึ่งจะทำให้ระบบมีความมั่นคงปลอดภัยและไม่เกิดค่าใช้จ่ายในภายหลัง

2.3.2 หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน เช่น การตรวจรับระบบตาม TOR ที่ได้กำหนดไว้ เป็นต้น

2.4 การสำรองข้อมูล

2.4.1 ผู้ดูแลระบบสารสนเทศที่สำคัญนั้น ๆ ต้องสำรองข้อมูลที่สำคัญเก็บไว้ตามระยะเวลาที่เหมาะสม

2.4.2 ผู้ดูแลระบบต้องบันทึกรายละเอียดการสำรองข้อมูลโดยมีรายละเอียด เวลาเริ่มต้นและสิ้นสุด ชื่อผู้ทำการสำรองข้อมูล และชนิดของข้อมูลที่บันทึก

2.4.3 กรณีที่เกิดการผิดพลาดในการสำรองข้อมูล ผู้สำรองข้อมูลต้องบันทึกรายละเอียดของข้อผิดพลาดที่เกิดขึ้นพร้อมแนวทางแก้ไข

2.44 ผู้ดูแลระบบต้องมีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสมเพื่อให้สามารถกู้ข้อมูลกลับคืนได้ ป้องกันระบบจากการถูกโจมตี หรือความเสียหายที่อาจเกิดขึ้น

2.4.5 ผู้ดูแลระบบต้องเข้ารหัสข้อมูลที่สำรองตามชั้นความลับ โดยใช้เทคโนโลยีที่เหมาะสม เพื่อป้องกันข้อมูลสำรองถูกเปิดเผย

2.5 การบริหารจัดการเครือข่าย (Network Management)

2.5.1 ผู้ดูแลระบบ ต้องบริหารจัดการความมั่นคงปลอดภัยในเครือข่าย ซึ่งมีแนวทางปฏิบัติดังนี้

2.5.1.1 ระบบเครือข่ายภายใน อุปกรณ์ที่ทำหน้าที่เชื่อมโยงกับระบบเครือข่าย เพื่อการทำงาน ภายใน กสท ได้แก่ Router, Switch และ HUB มีข้อปฏิบัติดังนี้

- อุปกรณ์ที่ทำหน้าที่ขยายการเชื่อมโยงเครือข่าย ต้องปิด Service Port ที่ไม่จำเป็น และในการส่งข้อมูลการทำงานของอุปกรณ์เครือข่ายจะต้องไม่ใช้ค่า Default Community, Default Username และ Default Password
- การเชื่อมโยงเครือข่ายเพื่อใช้งานระบบต่าง ๆ จะสามารถกระทำได้ก็ต่อเมื่อได้รับอนุญาตจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ การเชื่อมโยงเครือข่ายเองโดยพลการ หากทำให้เกิดความเสียหายกับระบบเครือข่ายจะต้องถูกลงโทษตามที่กำหนดไว้
- ผู้ดูแลระบบต้องมีแผนดำ เนินการบำรุงรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์ เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ
- ผู้ดูแลระบบต้องติดตั้งอุปกรณ์ ซอฟต์แวร์ระบบ การเข้ารหัสข้อมูลอัตโนมัติ หรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ
- ผู้ดูแลระบบจะต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น

2.5.1.2 ระบบ Remote Access อุปกรณ์ Remote Access Server (RAS) ที่ติดตั้งใช้งานใน Remote Area หรือเพื่อการทำงานกับหน่วยงานภายนอก ได้แก่ Remote Access Server (RAS), Remote VPN, Remote Router มีข้อปฏิบัติดังนี้

- อุปกรณ์ RAS จะต้องทำ Harden และบันทึกการทำ Configuration Set up ของอุปกรณ์ RAS ทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง
- เมื่อเสร็จสิ้นการทดสอบการใช้งานอุปกรณ์ RAS แล้วให้ลบ User/Password ที่ใช้ในงานทดสอบทันที
- อุปกรณ์ RAS ที่สามารถ Management ทาง Remote Terminal ได้จะต้องไม่มีค่า Default Community, Default Username และ Default Password

2.5.1.3 อุปกรณ์ Server อุปกรณ์ Server ที่ติดตั้งเพื่อการทำงานภายใน บริษัท กสท โทรคมนาคม จำกัด (มหาชน) มีข้อปฏิบัติดังนี้

- ผู้ดูแลระบบต้องไม่ใช้ Default Username/Default Password

- ต้องทำ Hardening และบันทึกการทำ Configuration Set up ของอุปกรณ์ Server และจัดทำเป็นเอกสารทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง
- ให้เปิด Service Port ที่จำเป็นเท่านั้น ส่วน Port ที่ไม่ใช้งานให้ปิดทั้งหมดและต้องมีการบันทึกการติดตั้ง Service Patch ทุกครั้ง
- ต้องไม่เปิดเผย OS Version, Service Port, IP Address และ Service Patch Version ให้บุคคลที่ไม่เกี่ยวข้องทราบ
- เมื่อจบการใช้งานที่ Console ต้อง Logoff User นั้นโดยทันที
- ผู้ดูแลระบบต้องสำรองข้อมูลและระบบปฏิบัติการอย่างน้อยเดือนละครั้ง และทดสอบการสำรองข้อมูลอย่างน้อยปีละ 2 ครั้ง โดยสอดคล้องกับความสำคัญของระบบ

2.5.2 ผู้ดูแลระบบ ต้องบริหารจัดการความมั่นคงปลอดภัยในเครือข่าย ซึ่งมีแนวทางปฏิบัติดังนี้

2.5.2.1 ห้ามนำอุปกรณ์เครือข่ายมาติดตั้งกับระบบเครือข่ายของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) โดยไม่รับอนุญาตจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ

2.5.2.2 ห้ามผู้ใช้งานเครือข่ายกระทำการใด ๆ ที่รบกวนระบบเครือข่าย เช่น การเปิดใช้งาน Service DHCP เพื่อเชื่อมต่อเข้ากับระบบเครือข่ายของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เอง

2.6 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit Logging)

ให้บันทึกกิจกรรมการใช้งานของผู้ใช้งาน การปฏิเสธการให้บริการของระบบ และเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้ ซึ่งประกอบด้วย

2.6.1 User ID

2.6.2 วัน เวลา และรายละเอียดที่สำคัญ เช่น การเข้าระบบและการออกจากระบบ

2.6.3 ระบุเครื่องปลายทาง หรือที่ตั้ง(ถ้ามี)

2.6.4 บันทึกของการพยายามเข้าสู่ระบบทั้งสำเร็จและไม่สำเร็จหรือล้มเหลว

2.6.5 บันทึกของการพยายามเข้าสู่ข้อมูลและทรัพยากรทั้งสำเร็จและไม่สำเร็จหรือลืมเห

2.6.6 การเปลี่ยนค่า Config ของระบบ

2.6.7 การใช้สิทธิพิเศษ เช่น Administrator หรือ Root

2.6.8 การใช้ยูทิลิตี้และซอฟต์แวร์ประยุกต์ของระบบ

2.6.9 การเข้าถึงไฟล์และชนิดของการเข้าถึง

2.6.10 Network Address และ Protocol

2.6.11 สัญญาณเตือนที่เพิ่มขึ้นโดยระบบการเข้าถึงหรือควบคุมการใงานสารสนเทศ

2.6.12 การทำงานและไม่ทำงานของระบบการป้องกัน เช่น ระบบป้องกันไวรัส และ IDS

2.7 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of Log Information)

เพื่อตรวจสอบการใช้งานสินทรัพย์สารสนเทศอย่างสม่ำเสมอ โดยต้องมีการประเมินความเสี่ยงและปฏิบัติตามที่กฎหมายกำหนด มีแนวทางปฏิบัติดังนี้

2.7.1 การระบุตัวตนในการเข้าถึง ประกอบด้วย

2.7.1.1 User ID

2.7.1.2 วัน เวลา และรายละเอียดที่สำคัญ

2.7.1.3 ชนิดของเหตุการณ์

2.7.1.4 การเข้าถึงไฟล์

2.7.1.5 ซอฟต์แวร์หรือยูทิลิตี้ที่ใช้

2.7.2 การดำเนินการเกี่ยวกับสิทธิของผู้ใช้งาน

2.7.2.1 การใช้บัญชีผู้ใช้งานแบบสิทธิพิเศษ เช่น Administrator ,Root หรือ Supervisor

2.7.2.2 การเริ่มต้นและหยุดของระบบ

2.7.2.3 อุปกรณ์ที่นำมาเชื่อมต่อ

2.7.3 การพยายามเข้าถึงของผู้ที่ไม่มีสิทธิ

2.7.3.1 การล้มเหลวหรือยกเลิกของผู้ใช้งาน

2.7.3.2 การล้มเหลวหรือยกเลิกการกระทำที่เกี่ยวกับข้อมูลหรือทรัพยากรอื่น ๆ

2.7.3.3 การฝ่าฝืนนโยบายการเข้าถึงและการแจ้งเตือนของ Network Gateway และ Firewall

2.7.3.4 การแจ้งเตือนของ IDS

2.8 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of Log Information)

เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต จึงควรพิจารณาเรื่องดังต่อไปนี้

2.8.1 การเปลี่ยนแปลงชนิดของข้อความที่ถูกบันทึก

2.8.2 Log ที่ถูกแก้ไขหรือถูกลบ

2.8.3 ความจุของพื้นที่ในการจัดเก็บ Log ที่ไม่เพียงพอ ทำให้ไม่สามารถจัดเก็บ Log ได้

2.8.4 ระยะเวลาในการจัดเก็บและการ Backup Log

2.9 การบันทึกเหตุการณ์ข้อผิดพลาด (Fault Logging)

การบันทึกเหตุการณ์ข้อผิดพลาดต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร ดังนี้

2.9.1 ทบทวน Log ที่ผิดพลาด เพื่อความมั่นใจว่าความผิดพลาดนั้นได้มีการตัดสินใจที่ดีแล้ว

2.9.2 ทบทวนปริมาณ Log ที่มีการแก้ไข เพื่อความมั่นใจว่ามีการควบคุมที่เข้มงวดและกระทำไปตามสิทธิที่ได้รับ

2.10 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock synchronization)

การตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงาน โดยการตั้งเวลาด้วย Network Time Protocol หรือ NTP ไปยังเซิร์ฟเวอร์ที่ให้บริการข้อมูลเวลาอย่างน้อยที่เป็น Stratum 1 ให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ถูกบุกรุก โดยสามารถอ้างอิงผู้ให้บริการดังต่อไปนี้

2.10.1 ภายใน กสท

การตั้งเวลาของเครื่อง Server และเครื่องคอมพิวเตอร์ทุกเครื่องใน บริษัท กสท โทรคมนาคม จำกัด (มหาชน) โดยการตั้งเวลาด้วย Network Time Protocol (NTP) ไปยัง Server ที่ให้บริการขอมูลเวลา คือ

2.10.1.1 clock1.cattelecom.com หรือ 10.9.1.19

2.10.1.2 clock2.cattelecom.com หรือ 172.16.9.91

2.10.2 ภายในประเทศไทย

2.10.2.1 สถาบันมาตรวิทยาแห่งชาติ เครื่อง time1.nimt.or.th หรือ 203.185.69.60

2.10.2.2 กรมอุทกศาสตร์ กองทัพเรือ เครื่องเซิร์ฟเวอร์ time.navy.mi.th หรือ 118.175.67.83

2.10.2.3 ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทยหรือ ThaiCERT เครื่องเซิร์ฟเวอร์ clock.thaicert.org หรือ 203.185.129.186 หรือ 203.185.129.187

2.10.3 ในต่างประเทศ

National Institute of Standards and Technology ประเทศสหรัฐอเมริกา เครื่องเซิร์ฟเวอร์ time.nist.gov หรือ 192.43.244.18

หมวด 8
การบริหารจัดการสถานะการณ์ด้านการมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident Management)

1. วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคลองและได้ผลในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

2. การตอบโต้ต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดและการทำงานที่บกพร่องของระบบสารสนเทศหรือซอฟท์แวร์ (Responding to Security Incidents and Malfunctions)

เพื่อลดความเสียหายจากเหตุการณ์ละเมิดความมั่นคงปลอดภัยและระบบทำงานบกพร่อง เช่น ไวรัสคอมพิวเตอร์แพร่กระจาย ระบบถูกบุกรุก เป็นต้น และให้บุคลากรใน บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้เรียนรู้จากประสบการณ์ความเสียหายดังกล่าว มีแนวทางปฏิบัติดังนี้

2.1 หากผู้ใช้งานพบเห็นเหตุการณ์ด้านความมั่นคงปลอดภัย (Reporting Information Security Events) และ/หรือจุดอ่อน ช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (ReportingInformation Security Weaknesses) และ/หรือการทำงานที่บกพร่องหรือการทำงานผิดปกติของซอฟต์แวร์ (Reporting Software Malfunctions) ผู้ใช้งานต้องรายงานสิ่งที่เกิดขึ้นให้แก่ผู้รับผิดชอบหรือผู้ดูแลระบบทราบโดยเร่งด่วน

2.2 ในกรณีที่ไม่สามารถติดต่อผู้ดูแลระบบได้ ให้รายงานกับผู้บังคับบัญชาตามลำดับขั้น และรายงานให้หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ทราบด้วย

2.3 ผู้ดูแลระบบต้องร่วมกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ประเมินขอบเขต (Scope) และความรุนแรง (Severity) ของปัญหา หากพบว่าเป็นปัญหาที่จะมีผลกระทบในวงกว้าง รุนแรง หรือมีผลต่อชื่อเสียงของบริษัท จะต้องรายงานให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบโดยด่วน เพื่อหาแนวทางแก้ไขและป้องกันไม่ให้เกิดในครั้งต่อไป

3. การบริหารจัดการและการปรับปรุงแก้ไขต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Management of Information Security Incidents and Improvements)

เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ควรยึดหลักปฏิบัติดังต่อไปนี้

3.1 กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

หัวหน้าหน่วยงานที่มีระบบงานที่สำคัญ เช่น ERP, HR, EIS, MIS, Billing, CRM เป็นต้น ต้องมีการกำหนดหน้าที่ความรับผิดชอบและกำหนดขั้นตอนปฏิบัติ เพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด และขั้นตอนดังกล่าวต้องมีความรวดเร็วได้ผล และมีความเป็นระบบระเบียบที่ดี

3.2 การเรียนรู้จากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Learning from Security Incidents)

3.2.1 ผู้ดูแลระบบต้องบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย จุดอ่อน ช่องโหว่ ภัยคุกคามหรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไข เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

3.2.2 ผู้ดูแลระบบต้องจัดทำ สรุปรายงานเหตุการณ์การละเมิดความมั่นคงปลอดภัยให้ผู้บังคับบัญชาและหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ อย่างน้อยเดือนละ 1 ครั้ง

3.2.3 หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ และหน่วยงานดูแลรับผิดชอบด้านบริหารความเสี่ยง ต้องร่วมกันวิเคราะห์ความเสี่ยง และประเมินสถานการณ์การบุกรุก/ละเมิด/ระบาด ที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศทุก 6 เดือน

3.3 การเก็บรวบรวมหลักฐาน (Collection of Evidence)

3.3.1 หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ต้องดำเนินการให้หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญ เช่น ERP, HR, EIS, MIS, Billing, CRM เป็นต้น ให้มีการรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในการวิเคราะห์ สืบสวนหรือเป็นหลักฐานในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

3.3.2 หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่า ได้ปฏิบัติตามข้อกำหนดทางด้านกฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล ระเบียบ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) และกฎหมาย (เช่น 90 วัน หรือ 1 ปี เป็นต้น)

3.3.3 หัวหน้าหน่วยงานดูแลรับผิดชอบด้านกฎหมายและหน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องศึกษากฎเกณฑ์ที่เกี่ยวข้อง เช่น ถ่อยแถลงในกฎหมายแพ่งหรืออาญา ซึ่งระบุถึงลักษณะของหลักฐานที่ต้องเก็บรวบรวมมา เพื่อใช้ในการดำเนินการทางกฎหมายกับผู้กระทำผิด เป็นต้น

3.3.4 หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องศึกษาถึงลักษณะของหลักฐานที่มีความสมบูรณ์และมีคุณภาพ เพื่อสามารถนำไปใช้ในกระบวนการของศาลได้

4. การรายงานเหตุการณ์น่าสงสัย

4.1 ผู้ใช้งานมีหน้าที่รับผิดชอบในการรายงานเหตุการณ์ทันทีที่สงสัยว่าเป็นเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล

4.2 ถ้าหากพบเหตุการณ์ที่น่าสงสัยให้ทำการรายงานต่อผู้ดูแลระบบ หรือหัวหน้าหน่วยงานทันที เช่น เหตุการณ์ต่อไปนี้

4.2.1 พบว่ารหัสผ่านส่วนบุคคลของตนถูกล็อค โดยไม่ทราบสาเหตุ

4.2.2 เวลาการเข้าใช้งานระบบครั้งล่าสุด (Last Logon Time) ที่ผิดปกติ

4.2.3 พบหลักฐานหรือสิ่งผิดสังเกตในเครื่องคอมพิวเตอร์ของตน เช่น มีไฟล์ที่ไม่รู้จัก การเปลี่ยนแปลงของค่าต่าง ๆ

4.2.4 มีการไม่ปฏิบัติตามขั้นตอนความมั่นคงปลอดภัย

4.2.5 พบหรือคาดว่าระบบงานจะมีปัญหาด้านความปลอดภัยของข้อมูล

4.2.6 พบหรือคาดว่าข้อมูลในระบบจะถูกทำลาย แก้ไข หรือลบทิ้ง

4.2.7 มีความพยายามที่จะเข้าใช้อย่างระบบอย่างผิดวิธี ไม่ว่าจะสำเร็จหรือไม่

4.2.8 การให้บริการของระบบเกิดการชะงัก หรือไม่สามารถให้บริการ

4.2.9 เกิดการละเมิดสิทธิเข้าไปใช้งานระบบเพื่อประมวลผลหรือจัดเก็บข้อมูล

4.2.10 การแก้ไขค่าความปลอดภัยในระบบ เช่น Hardware, Software หรือ Firmware โดยผู้ใช้งานไม่ทราบ

หมวด 9
การบริหารความต่อเนื่องในการดำเนินงาน
(Business Continuity Management)

1. วัตถุประสงค์

เพื่อให้การดำเนินธุรกิจของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เป็นไปอย่างต่อเนื่อง นโยบายนี้เป็นส่วนหนึ่งของการสนับสนุนแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ และหน่วยงานที่รับผิดชอบระบบและข้อมูลจะต้องปฏิบัติอย่างเคร่งครัด เพื่อทำให้การดำเนินธุรกิจของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เป็นไปอย่างมีประสิทธิภาพประสิทธิผล และอย่างต่อเนื่อง

2. คำแถลงนโยบาย

2.1 ขั้นตอนเตรียมการของแผนรองรับเหตุการณ/ฉุกเฉิน

2.1.1 บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ต้องจัดตั้งคณะทำงานแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ซึ่งประกอบไปด้วยตัวแทนจากหน่วยงานเจ้าของข้อมูล เจ้าของระบบงาน หน่วยงานที่ดูแลระบบเครือข่าย เป็นต้น

2.1.2 คณะทำงานจะต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ที่เป็นลายลักษณ์อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละหนึ่งครั้ง

2.1.3 กระบวนการหลักในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ต้องประกอบด้วยหัวข้อหลัก ดังนี้

- การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis)
- การประเมินความเสี่ยงและการควบคุม (Risk Analysis &Control)
- การวางกลยุทธ์สำหรับแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ (IT Contingency Plan Strategy Development)
- การพัฒนาแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ (IT Contingency Plan Development)
- การประชาสัมพันธ์และการฝึกอบรม
- การทดสอบ ปรับปรุงแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

2.1.4 แนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ควรพิจารณาดังนี้

- การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการดำเนินธุรกิจและการให้บริการของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)
- การตอบสนองต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย เช่น กำหนดแนวทางการควบคุม การแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น
- การดำเนินการเพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง เช่น การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น
- การกลับคืนสู่การทำงานปกติ เพื่อให้ธุรกิจของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) กลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น

2.2 แนวทางปฏิบัติของการสำรองข้อมูลและการกู้คืนข้อมูล

เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลและสารสนเทศ ผู้ใช้งานควรปฏิบัติตามนโยบายการสำรองข้อมูล การกู้คืน และรักษาความลับของข้อมูล

2.3 แนวทางปฏิบัติของการเก็บรักษาข้อมูลและสารสนเทศ

2.3.1 เจ้าของข้อมูลเป็นผู้จัดเก็บรักษาข้อมูลเกี่ยวกับระบบ ซึ่งได้แก่ ข้อมูลเกี่ยวกับระบบปฏิบัติการ (OS) ระบบเครือข่าย และซอฟต์แวร์ระบบงาน (ทั้ง Source Code และ Executable Files) โดยให้เป็นไปตามความต้องการที่เจ้าของข้อมูลในระบบนั้นกำหนด จำนวนครั้งและระยะเวลาในการเก็บรักษาข้อมูลดังกล่าวต้องสอดคล้องกับการประเมินความเสี่ยงของข้อมูลนั้น ๆ ด้วย

2.3.2 ก่อนที่จะมีการปรับปรุงหรือเปลี่ยนแปลงระบบ หน่วยงานที่รับผิดชอบต้องทำการสำรองข้อมูลของระบบทุกครั้ง

2.3.3 ถ้าการสำรองข้อมูลถูกดำเนินการที่เซิร์ฟเวอร์หรือเครื่องคอมพิวเตอร์หลัก (Host) และเป็นข้อมูลของระบบงานที่สำคัญจะต้องเพิ่มจำนวนครั้งในการสำรองข้อมูลของเซิร์ฟเวอร์นั้นด้วย

2.3.4 ข้อมูลและสารสนเทศที่มีความสำคัญมากต้องการดำเนินธุรกิจของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) จะต้องทำการสำรองข้อมูลไว้ทุกวัน และข้อมูลสำรองดังกล่าวต้องมีการจัดเก็บไว้นอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลักอย่างเหมาะสม โดยตรวจสอบให้แน่ใจว่าสถานที่นั้นมีความปลอดภัย

2.3.5 ระบบข้อมูลที่สำคัญทั้งหมดของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ควรมีระบบการประมวลผลสำรอง ระบบเครือข่ายสำรอง เพื่อป้องกันการพึ่งพาระบบหลักเพียงระบบเดียว ในกรณีที่ระบบหนึ่งไม่สามารถทำงานได้ สามารถใช้งานอีกระบบหนึ่งได้ทันทีเพื่อให้ธุรกิจหลักของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ดำเนินต่อไปได้

2.3.6 ข้อมูลและสารสนเทศที่ถูกจัดประเภทเป็นข้อมูลธรรมดา ซึ่งไม่ส่งผลกระทบต่อการดำเนินกิจการของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) จำนวนครั้งในการสำรองข้อมูลนั้นขึ้นอยู่กับการพิจารณาของเจ้าของข้อมูล และข้อมูลดังกล่าวจะถูกนำไปจัดเก็บในสถานที่ ๆ มีความปลอดภัย

หมวด 10
การปฏิบัติตามข้อกำหนด
(Compliance)

1. วัตถุประสงค์

เพื่อเป็นแนวทางในการปฏิบัติสำหรับการใช้งานซอฟต์แวร์ของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) และของบุคคลที่สามซึ่งมีการนำมาใช้ภายใน บริษัท กสท โทรคมนาคม จำกัด (มหาชน) รวมถึงเรื่องของการอนุญาตให้ใช้ซอฟต์แวร์ตามกฎหมายและข้อกำหนดในการใช้ซอฟต์แวร์ของผู้ใช้งาน และผู้ที่เกี่ยวข้องกับ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

2. การระบุข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมาย (Identification of applicable legislation)

หน่วยงานดูแลรับผิดชอบด้านกฎหมาย ต้องระบุข้อกำหนดทางด้านกฎหมาย ระเบียบปฏิบัติ และสัญญาว่าจ้าง รวมทั้งสัญญาที่ทำกับหน่วยงานภายนอก ที่เกี่ยวข้องกับการดำเนินงานหรือธุรกิจของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ต้องบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร และปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอรวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว

3. การป้องกันข้อมูลส่วนตัวและการเข้ารหัส มีแนวทางการปฏิบัติดังนี้

3.1 ผู้ดูแลระบบ ต้องจัดให้มีวิธีการป้องกันข้อมูลส่วนตัวของพนักงานและลูกจ้าง เช่น ข้อมูลในไปรษณีย์อิเล็กทรอนิกส์ ข้อมูลในระบบบริหารงานบุคคล เป็นต้น เพื่อใช้เป็นหลักฐานอ้างอิงในทางกฎหมายในกรณีที่มีข้อพิพาทกัน

3.2 ผู้ดูแลระบบ ต้องศึกษาและปฏิบัติตามข้อกำหนดหรือกฎหมายของประเทศ เกี่ยวกับการเข้ารหัสข้อมูล รวมทั้งเมื่อจำเป็นต้องโยกย้ายข้อมูลที่เข้ารหัสไว้ หรืออุปกรณ์ หรือเครื่องมือหรือระบบที่ใช้ในการเข้ารหัสข้อมูลไปยังอีกประเทศหนึ่ง ให้ศึกษาและปฏิบัติตามข้อกำหนดหรือกฎหมายของประเทศนั้นด้วย

4. การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of Misuse of Information Processing Facilities)

4.1 อุปกรณ์ประมวลผลสารสนเทศของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) มีไว้เพื่อใช้ในกิจการของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เท่านั้น ยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

4.2 อุปกรณ์ประมวลผลสารสนเทศที่ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เช่ามาใช้งาน ต้องกำหนดให้มีหน่วยงานระดับผู้จัดการฝ่ายขึ้นไปเป็นผู้รับผิดชอบ และหน่วยงานที่เช่า จะต้องจัดทำบัญชีรายการของอุปกรณ์ประมวลผลสารสนเทศที่เช่ามาใช้งาน และให้ส่งสำเนาดังกล่าวให้หน่วยงานที่รับผิดชอบในการจัดการข้อมูลและสินทรัพย์ของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) (ตามคำสั่งของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ที่ 11/2554 หรือคำสั่งอื่นที่มาทดแทนคำสั่งดังกล่าว)

4.3 หัวหน้าหน่วยงานแต่ละหน่วยงาน ต้องกำหนดให้มีการป้องกันสินทรัพย์และอุปกรณ์ของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เช่น Notebook, Mobile Phone เมื่อถูกนำไปใช้งานนอกสำนักงาน โดยต้องปฏิบัติตามระเบียบในการใช้งานการยืม-คืน

4.4 ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่าง ๆ เมื่อมีการเปลี่ยนแปลง เพื่อใช้เป็นข้อมูลในการควบคุมสินทรัพย์ของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

4.5 ผู้ใช้งานต้องไม่ทำการแก้ไขเปลี่ยนแปลง หรืออนุญาตให้ผู้ที่ไม่ได้รับอนุญาตทำการแก้ไขเปลี่ยนแปลงซอฟต์แวร์หรืออุปกรณ์ประมวลผลสารสนเทศในเครื่องที่ตนรับผิดชอบ

4.6 ไม่อนุญาตให้ผู้ใช้งานติดตั้งซอฟต์แวร์หรืออุปกรณ์ในเครื่องของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) การเปลี่ยนแปลงระบบคอมพิวเตอร์ ฮาร์ดแวร์ อุปกรณ์ และสื่อที่ใช้ในการจัดเก็บข้อมูลจะต้องได้รับอนุมัติจากหัวหน้าหน่วยงานที่ดูแลระบบงานนั้น ๆ เป็นลายลักษณ์อักษร เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและการแก้ไขโดยไม่ได้ตั้งใจ ซึ่งอาจมีผลต่อการหยุดชะงักของธุรกิจหรือการเปิดเผยข้อมูลโดยไม่ได้รับการอนุญาต

4.7 อุปกรณ์ประมวลผลสารสนเทศจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนขั้นต่ำเป็นอย่างน้อยโดยการใส่รหัสผ่านตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

4.8 อุปกรณ์ประมวลผลสารสนเทศควรมีกระบวนการเพื่ออัพเดทระบบป้องกันซอฟต์แวร์ไม่พึงประสงค์ตามนโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

5. การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด (Regulation of Cryptographic Controls)

หน่วยงานต่าง ๆ ซึ่งเป็นเจ้าของข้อมูล ต้องใช้มาตรการการเข้ารหัสข้อมูล (Cryptographic controls) ตามที่ได้กำหนดในนโยบายการพัฒนาระบบสารสนเทศ

6. การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย (Compliance with security policies and standards)

หัวหน้าหน่วยงานแต่ละหน่วยงาน ต้องกำหนดให้ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

7. มาตรการการตรวจประเมินระบบสารสนเทศ (Information systems audit controls)

หัวหน้าหน่วยงานที่ดูแลระบบงานสำคัญหรือระบบสารสนเทศที่มีข้อมูลความลับของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เช่น ERP, HR, EIS, MIS, Billing, CRM เป็นต้น ต้องวางแผนการตรวจประเมินระบบทั้งหมด โดยการตรวจประเมินที่จะดำเนินการ จะต้องมีผลกระทบต่อระบบและกระบวนการดำเนินงานของ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) น้อยที่สุด

8. การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of information systems audit fools)

หน่วยงานดูแลรับผิดชอบด้านตรวจสอบภายใน หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ และหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ต้องร่วมกันหาทางป้องกันซอฟต์แวร์ที่ใช้ในการตรวจประเมินระบบ มิให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิดหรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้น ๆ