ISMS Policy

NT Conference

ประวัติการปรับปรุงเอกสาร

Version No	ปรับปรุงโดย	คำอธิบายและเหตุผลในการแก้ไข
1.0	นายพีรพัฒน์ โพธิ์ชนะพันธุ์	ต้นฉบับ
1.1	นายพีรพัฒน์ โพธิ์ชนะพันธุ์	เพิ่มนโยบายการเก็บสำรองข้อมูลสำคัญ เป็นระยะเวลาอย่างน้อย 2 ปี
1.2	นายพีรพัฒน์ โพธิ์ชนะพันธุ์	เพิ่มการตรวจสอบช่องโหว่กรณีมีการเปลี่ยนแปลงระบบอย่างมีนัยยะสำคัญหรือ Major change
1.3	นายพีรพัฒน์ โพธิ์ชนะพันธุ์	เพิ่มการแสดงหลักฐานการทดสอบก่อนการเปลี่ยนแปลงระบบ

สารบัญ

วัตถุประสงค์และขอบเขตของนโยบาย

บริษัท โทรคมนาคมแห่งชาติ จากัด (มหาชน) ได้นำระบบเทคโนโลยีการประชุมทางไกลผ่านระบบเครือข่ายอินเทอร์เน็ตมาให้บริการภายใต้ชื่อ NT Conference เพื่ออำนวยความสะดวกแก่ผู้ใช้บริการ ดังนั้นเพื่อสร้างความมั่นใจแก่ผู้ใช้บริการ จึงกำหนดหลักการของความมั่นคงปลอดภัยของระบบโดยมีองค์ประกอบ ดังนี้

องค์ประกอบ	**คำอธิบาย**
เป็นความลับ (Confidentiality)	ป้องกันการเปิดเผยหรือการแทรกแซงข้อมูลสารสนเทศที่มีความสำคัญระดับสูง (sensitive) จากผู้ที่ไม่ได้รับอนุญาต
มีความสมบูรณ์ (Integrity)	ข้อมูลถูกต้องสมบูรณ์ และไม่ถูกแก้ไขด้วยวิธีการใดๆ โดยที่ไม่ได้รับการอนุญาต
พร้อมใช้ (Availability)	มั่นใจว่าข้อมูลสารสนเทศจะพร้อมใช้ในเวลาที่ต้องการ

เป้าหมายของความมั่นคงปลอดภัยสารสนเทศ

เป็นผู้ให้บริการ ประชุมทางไกลผ่านระบบเครือข่ายอินเทอร์เน็ตที่มีประสิทธิภาพและมีความปลอดภัยสูงสุด แก่หน่วยงานภาครัฐ และเอกชน

นโยบายด้านความมั่นคงปลอดภัยสารสนเทศระบบ NT Conference

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) จัดทำนโยบายนี้เพื่อเป็นส่วนหนึ่งของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ของระบบ NT Conference ในการป้องกันภัยคุกคาม ลดความเสี่ยงจากช่องโหว่และผู้บุกรุก เพื่อให้สารสนเทศมีความปลอดภัย สามารถรักษาความลับและความถูกต้องของข้อมูล และมีความพร้อมในการให้บริการอยู่ในระดับที่ยอมรับได้ โดยนโยบายนี้มีวัตถุประสงค์ ดังนี้

- เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ทำให้การดำเนินธุรกิจมีประสิทธิภาพและประสิทธิผล
- เพื่อเผยแพร่ให้พนักงานและลูกจ้างทุกระดับได้รับทราบและปฏิบัติให้สอดคล้องกับมาตรฐานสากล และถูกต้องตามกฎ ระเบียบของบริษัท

- เพื่อให้มีการดำเนินการที่เหมาะสมและสัมฤทธิ์ผล มีการตรวจสอบและประเมินนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง
- เพื่อสร้างความตื่นตัวให้ผู้บริหาร พนักงานและลูกจ้าง ผู้ดูแลระบบ และหน่วยงานภายนอกที่ปฏิบัติงานให้กับบริษัท ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศ
- เพื่อสามารถจัดสรรและบริหารทรัพยากรต่างๆ ของระบบสารสนเทศได้อย่างมีประสิทธิภาพ
- เพื่อให้เกิดความเชื่อมั่นว่าเมื่อเกิดภัยพิบัติทางธรรมชาติ และเหตุจลาจล ธุรกิจสามารถให้บริการได้อย่างต่อเนื่อง และสามารถกู้คืนได้ตามระยะเวลาที่กำหนดที่ยอมรับได้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท ประกอบด้วยหมวดต่างๆ ดังนี้

1. การบริหารจัดการความเสี่ยง (Risk Management Policy)

1.1 กำหนดให้มีการทำแผนบริหารความเสี่ยงทางด้านความมั่นคงปลอดภัย และให้มีการทบทวนการประเมินความเสี่ยงอย่างน้อย ปีละ 1 ครั้ง

1.2 กำหนดให้มีการประเมินความเสี่ยง เสนอแผนเพื่อดำเนินการบริหารจัดการความเสี่ยงต่อผู้บริหารให้รับทราบและอนุมัติ

1.3 จัดทำรายงานผลการดำเนินการตามแผนการบริหารจัดการความเสี่ยง

2. การบริหารสินทรัพย์

2.1 การจัดหมวดหมู่สินทรัพย์ (Inventory of Assets)

ต้องจัดทำบัญชีสินทรัพย์และแบ่งประเภทให้ชัดเจน ซึ่งรวมถึงบัญชีครุภัณฑ์คอมพิวเตอร์และบัญชีข้อมูลที่เก็บไว้ในสื่อต่าง ๆ ทั้งหมด เพื่อใช้ในการกำหนดมูลค่าสินทรัพย์ระดับความสำคัญและวิธีการป้องกันที่เหมาะสม รวมทั้งต้องระบุผู้เป็นเจ้าของสารสนเทศ (แต่ละชนิด) ตามที่กำหนดไว้ในบัญชีสินทรัพย์

2.2 การตรวจสอบบัญชีสินทรัพย์ (Inventory Check)

ต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ตามระยะเวลาที่กำหนดไว้ตามนโยบาย บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

2.3 การจัดหมวดหมู่ข้อมูลและสารสนเทศ (Data and Information Classification)

2.3.1 ต้องทำการจัดหมวดหมู่ กำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันสารสนเทศของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดย บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) จัดให้มีกระบวนการในการจัดหมวดหมู่ของข้อมูลและสินทรัพย์ เช่น ชั้นลับที่สุด ชั้นลับมากและชั้นลับ การกำหนดแนวทางการแบ่งชั้นความลับของข้อมูล ต้องอยู่ในการควบคุมดูแลและรักษาความปลอดภัยที่เหมาะสมไม่ว่าจะอยู่ในรูปแบบใดก็ตาม

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

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

ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับข้อมูลและสารสนเทศ โดยแยกตามหมวดหมู่ที่กำหนดไว้ มีการส่งมอบและจัดเก็บ ตามขั้นตอนกระบวนการต่าง ๆ ซึ่งประกอบไปด้วย การถ่ายเอกสาร การจัดเก็บ การส่งต่อ การสื่อสารและการทำลาย จะต้องปฏิบัติตามแนวทางปฏิบัติงานที่ได้มีการกำหนดไว้

3. การควบคุมการเข้าถึง (Access Control)

3.1 การควบคุมการเข้าถึงระบบ NT Conference ของผู้ใช้งาน (User Access Management)

3.1.1 การลงทะเบียนผู้ใช้งาน (User Registration) ต้องทำการลงทะเบียนผู้ใช้งานใหม่ เพื่อให้สามารถใช้งานระบบสารสนเทศได้ นอกจากนี้ ต้องมีระเบียบปฏิบัติเพื่อยกเลิกการใช้งานของผู้ใช้งานทันที ในกรณีที่มีการลาออกหรือเปลี่ยนตำแหน่งงานภายในบริษัท

3.1.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege Management) ต้องกำหนดสิทธิการเข้าถึงของผู้ใช้งานในการเข้าถึงระบบและข้อมูลให้เหมาะสมกับการใช้งานและหน้าที่ความรับผิดชอบในการปฏิบัติงาน โดยผู้ใช้งานต้องได้รับการอนุมัติสิทธิให้เสร็จสมบูรณ์ก่อน จึงจะสามารถเข้าใช้งานระบบได้

3.2 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

ต้องจัดให้มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่เหมาะสม โดยต้องมีการสอบทานความเหมาะสมของสิทธิของผู้ใช้งานในการเข้าใช้ข้อมูลอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

4. การเข้ารหัสข้อมูล (Cryptography)

4.1 ระเบียบปฏิบัติงานการควบคุมการเข้ารหัสข้อมูล (Cryptographic Controls)

กำหนดระเบียบปฏิบัติงานการควบคุมการเข้ารหัสข้อมูล (Cryptographic Controls) ที่เป็นมาตราฐานสากลเพื่อป้องกันข้อมูลที่เป็นชั้นความลับ การปลอมแปลง หรือความถูกต้องของข้อมูลสารสนเทศ รวมถึงมาตราฐานการเข้ารหัสลับข้อมูลรับส่งระหว่างเครือข่าย (data-in-transit encryption) และข้อมูลส่วนบุคคลที่ถูกจัดเก็บ (data-at-rest encryption) บนระบบ NT Conference ไม่ให้มีการรั่วไหลออกไปสู่บุคคลภายนอกที่ไม่เกี่ยวข้องหรือมีสิทธิในการเข้าถึงข้อมูล โดยใช้มาตรฐานการเข้ารหัสที่มีความปลอดภัยสากล เช่น SSL/TLS (เวอร์ชั่น 1.2) SHA-256 DTLS(เวอร์ชั่น 1.2) AES 256 เป็นต้น

5. ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

5.1 มาตรฐานในการกำหนดบริเวณที่ต้องมีความมั่นคงปลอดภัยด้านสารสนเทศ (Secure Areas)

5.1.1 ต้องกำหนดพื้นที่ใช้งานระบบสารสนเทศจัดเป็นหมวดหมู่ จัดทำแผนผังติดป้ายประกาศควบคุมการเข้าออกพื้นที่

5.1.2 ติดตั้งระบบรักษาความปลอดภัย เช่น กล้องวงจรปิด ระบบ Access Control

5.2 การควบคุมการเข้าออก (Physical Entry Controls)

5.2.1 ระบุตัวตนผู้ใช้งาน และช่วงเวลาเข้าออกพื้นที่

5.2.2 กำหนดให้ผู้ใช้งานสามารถเข้าออกได้เฉพาะพื้นที่ที่ได้รับอนุญาติเท่านั้น

5.2.3 ผู้ที่มีความจำเป็นต้องเข้าออกพื้นที่ต้องได้รับอนุญาติ และสามารถระบุตัวตน ช่วงเวลาเข้าออกได้

5.3 ความมั่นคงปลอดภัยด้านสารสนเทศสำหรับสำนักงาน ห้องทำงาน และเครื่องมือต่างๆ (Securing Offices, Room and Facilities)

5.3.1 ต้องจัดให้มีมาตรการความมั่นคงปลอดภัยด้านสารสนเทศให้กับสานักงาน ห้องทางาน และเครื่องมือต่าง ประตูหน้าต่างสำนักงานต้องปิดล๊อกกุญแจ หรือมี Access Control ติดตั้งเครื่องปรับอากาศและควบคุมความชื้น

5.3.2 ติดป้ายประกาศ “ห้ามเข้าก่อนได้รับอนุญาต” หรือ “เฉพาะผู้ที่เกี่ยวข้อง” และป้าย “ห้ามถ่ายรูป”

5.3.3 กำหนดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access, Delivery, and Loading Areas)

5.4 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

5.4.1 จัดตั้งเครื่องมือไว้ในที่ที่ปลอดภัย มีการป้องกันภัยที่จะเกิดขึ้นกับอุปกรณ์เหล่านั้น

5.4.2 กำหนดให้มีการบำรุงรักษา ซ่อมแซม ตรวจสอบ เป็นประจำ

5.4.3 การนำอุปกรณ์ไปใช้นอกสถานที่ต้องปฏิบัติตามระเบียบการ ยืม-คืน ของบริษัท

5.5 ระบบกระแสไฟฟ้าสำรอง (Power Supplies) และระบบป้องกันภัย

5.5.1 มีระบบไฟฟ้าสำรองอัตโนมัติ และมีการตรวจสอบ ทดสอบ และซ่อมบำรุงประจำ

5.5.2 มีระบบเดือนภัย เช่น ไฟไหม้ มีระบบดับเพลิง

5.6 การเดินสายไฟฟ้าหลัก (Main Power Cable)

5.6.1 สายไฟฟ้าหลัก กับสายสื่อสัญญาณต้องเดินแยกกันมีระบบป้องกันที่ได้มาตรฐาน

5.6.2 สายไฟฟ้าหลัก และสายสื่อสัญญาณต้องมีการติดตั้งตู้พักสายมีการล๊อกและจำกัดการเข้าถึง

5.6.3 จุดต่อสายสาย ปลั๊กสายไฟต้องเป็นไปตามมาตรฐานที่กำหนด

5.6.4 ติดป้ายบอกแต่ละสายให้ชัดเจน

6. การบริหารการเปลี่ยนแปลง (Change Management)

6.1 จัดทำแผนและ Action Plan พร้อมหลักฐานการทดสอบก่อนการเปลี่ยนแปลงเสนอผู้บริหารในสายงานที่รับผิดชอบอนุมัติแผน เพื่อติดตั้ง ปรับปรุง หรือแก้ไขเปลี่ยนแปลงระบบ และให้หน่วยงานที่รับผิดชอบประเมินผลกระทบด้านความปลอดภัย ก่อนดำเนินการ

6.2 ต้องมีแผนการทำถอยหลังกลับ (Roll Back Plan)

6.3 ต้องปรับปรุงเงื่อนไขการให้บริการต่อหน่วยงานภายนอกเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับหน่วยงานภายนอก

6.4 การปรับปรุง เปลี่ยนแปลงระบบ จากหน่วยงานภายนอก (Supplier, Partner) ต้องทำการประเมินผลกระทบที่จะเกิดขึ้นรวมทั้งจัดทำแผนถอยหลังกลับ (Roll back Plan) ทำ Action Plan เสนอต่อหน่วยงานที่รับผิดชอบก่อน เพื่อให้หน่วยงานที่รับผิดชอบขออนุมัติผู้บริหารในสายงานที่รับผิดชอบในเรื่องดังกล่าว

7. การสำรองข้อมูล (Backup Management)

7.1 ต้องสำรองข้อมูลที่สำคัญ เช่น ข้อมูลการทำงานและการใช้งานของระบบ ข้อมูลส่วนบุคคล เป็นต้น โดยเก็บไว้เป็นระยะเวลาอย่างน้อย 2 ปี

7.2 ต้องมีการทบทวนตารางเวลาการสำรองข้อมูลและทดสอบข้อมูลที่สำรองไว้อย่างอย่างน้อยปีละ 1 ครั้ง เพื่อให้มีความพร้อมในการนำมาใช้งาน

7.3 ต้องมีการสำรองข้อมูลอย่างน้อยวันละ 1 ครั้ง

7.4 ต้องมีการสำรองข้อมูลจัดเก็บไว้อย่างน้อย 3 ชุด

7.5 ข้อมูลที่สำรองไว้ต้องมีการเข้ารหัสโดยใช้เทคโนโลยีที่เหมาะสมเพื่อป้องกันการเปิดเผยข้อมูล

8. การบริหารจัดการเครือข่าย (Network Management)

8.1 ระบบเครือข่ายภายใน หน่วยงาน มีแนวทางปฏิบัติดังนี้

8.1.1 ปิด Service Ports ที่ไม่จำเป็น และไม่ใช้ค่า Default Username และ Default Password

8.1.2 การเชื่อมโยงเครือข่ายเพื่อใช้งานระบบต่าง ๆ จะสามารถกระทำได้ต่อเมื่อได้รับอนุญาตจากผู้ดูแลรับผิดชอบ

8.1.3 ต้องมีแผนดำเนินการบำรุงรักษาและปรับปรุงเครือข่ายอย่างต่อเนื่อง

8.1.4 แยกเครือข่ายที่ใช้งานทั่วไป กับเครื่องข่ายที่มีความสำคัญออกจากกัน

8.1.5 ต้องติดตั้งอุปกรณ์ป้องกันเครือข่าย รวมถึงการติดตั้งซอฟแวร์ หรืออื่นๆ ที่เกี่ยวข้องกับการป้องกันเครือข่าย

8.1.6 ติดตั้งอุปกรณ์ หรือระบบเพื่อติดตามเฝ้าระวังสิ่งผิดปกติ (Log Monitoring and Management)

8.1.7 ผู้ดูแลระบบจะต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น

8.2 ระบบ Remote Access

8.2.1 ต้องมีนโยบายเชื่อมต่อผ่าน VPN (Virtual Private Network) กรณีมีการเชื่อมต่อจากภายนอก หรือจากระยะไกล (Remote)

8.2.2 อุปกรณ์ RAS (Remote Access Server) ต้องไม่ใช้ค่า Default Community, Default Password , Default Password

8.3 อุปกรณ์ Server

8.3.1 ต้องไม่เปิดเผย OS Version, Service Port, IP Address และ Service Patch Version ให้บุคคลที่ไม่เกี่ยวข้องทราบ

9. การตอบโต้ต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดและการทำงานที่บกพร่องของระบบสารสนเทศ (Responding to Security Incidents and Malfunctions)

9.1 กำหนดให้มีการตรวจสอบช่องโหว่ทางเทคนิค เพื่อหาช่องโหว่ที่อาจจะเกิดขึ้นกับระบบอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือกรณีที่มีการเปลี่ยนแปลงระบบอย่างมีนัยยะสำคัญหรือ Major change

9.2 ดำเนินการปรับปรุง Patch อย่างสม่ำเสมอเพื่อป้องกันช่องโหว่ของระบบ NT Conference

9.3 ผู้ปฏิบัติงาน หรือผู้ใช้งานเมื่อพบเห็นเหตุการณ์ด้านความมั่นคงปลอดภัย หรือจุดอ่อน ช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ต้องรายงานสิ่งที่เกิดขึ้นให้แก่ผู้รับผิดชอบหรือผู้ดูแลระบบทราบโดยเร่งด่วน

9.4 กำหนดขั้นตอนปฏิบัติและหน้าที่ความรับผิดชอบ เพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

9.5 ผู้ดูแลระบบต้องจัดทำบันทึกเหตุการณ์ วิธีการแก้ไข เพื่อเรียนรู้เหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

9.6 ต้องดำเนินการเก็บรวบรวมหลักฐานพยาน เพื่อใช้อ้างอิงในการวิเคราะห์ สืบสวนหรือเป็นหลักฐานในกระบวนการทางศาล โดยมีระยะเวลาตามกฎหมาย (เช่น 90 วัน หรือ 1ปี เป็นต้น)

9.7 ผู้บริหารและผู้ดูแลรับผิดชอบต้องร่วมกันวิเคราะห์ความเสี่ยง และประเมินสถานการณ์การบุกรุก/ละเมิด/ระบาด ที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบ NT Conference อย่างน้อยปีละ 1 ครั้ง

10. การบริหารความต่อเนื่องในการดำเนินงาน (Business Continuity Management) BCM

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ได้ตั้งคณะทำงานแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ซึ่งประกอบไปด้วยตัวแทนจากหน่วยงานเจ้าของข้อมูล เจ้าของระบบงาน หน่วยงานที่ดูแลระบบเครือข่าย เป็นต้น เข้าร่วมเป็นคณะทำงานฯ ซึ่งระบบ NT Conference เป็นอีกหนึ่งระบบที่บรรจุในแผน BCM ของบริษัท

10.1 กระบวนการหลักในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ประกอบด้วยหัวข้อหลัก ดังนี้

10.1.1 การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis)

10.1.2 การประเมินความเสี่ยงและการควบคุม (Risk Analysis &Control)

10.1.3 การวางกลยุทธ์สำหรับแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ (IT Contingency Plan Strategy Development)

10.1.4 การพัฒนาแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ (IT Contingency Plan Development)

10.1.5 การประชาสัมพันธ์และการฝึกอบรม

10.1.6 การทดสอบ ปรับปรุงแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

10.2 นโยบายการดำเนินการตามแผน BCM

10.2.1 กำหนดให้มีการทบทวนและทดสอบแผนอย่างน้อยปีละ 1 ครั้ง

10.2.2 ต้องปรับปรุง เปลี่ยนแปลงแผนเมื่อมีการเปลี่ยนโครงสร้างองค์กร

10.3 แนวทางปฏิบัติของการสำรองข้อมูลและการกู้คืนข้อมูล

10.3.1 เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลและสารสนเทศ ผู้ใช้งานควรปฏิบัติตามนโยบายการสำรองข้อมูลและการกู้คืนข้อมูล

11. การปฏิบัติตามข้อกำหนด (Compliance)

มีวัตถุประสงค์มีเพื่อป้องกัน หลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ มีแนวทางปฏิบัติดังนี้

11.1 กำหนดให้หน่วยงานด้านกฎหมาย ระบุข้อกำหนดทางด้านกฎหมาย ระเบียบปฏิบัติ สัญญาหรือข้อกำหนดต่างๆ ด้านเทคโนโลยีสารสนเทศ และด้านอื่นๆ ที่เกี่ยวข้องกับธุรกิจของบริษัท และให้มีผู้ดูแล ติดตาม และปรับปรุงข้อกำหนดดังกล่าว อย่างน้อยปีละ 1 ครั้ง

11.2 สื่อสาร สร้างการรับรู้ และให้เกิดความตระหนักสำหรับนโยบายทางด้านความมั่นคงปลอดภัยข้อมูลสารสนเทศของบริษัท และการปฏิบัติตามกฎหมาย ข้อบังคับ ไม่ละเมิดลิขสิทธิ์ และทรัพย์สินทางปัญญา

11.3 ผู้ดูแลระบบ ต้องจัดให้มีวิธีการป้องกันข้อมูลส่วนตัวของพนักงานและลูกจ้าง เช่น ข้อมูลในไปรษณีย์อิเล็กทรอนิกส์ ข้อมูลในระบบบริหารงานบุคคล เป็นต้น

11.4 กำหนดให้มีวิธีการป้องกันข้อมูลส่วนตัวและให้ผู้ดูแลระบบศึกษาและปฏิบัติตามมาตรการการเข้ารหัสข้อมูล (Cryptographic Control)

11.5 ผู้ใช้งานต้องไม่ทำการแก้ไขเปลี่ยนแปลง หรืออนุญาตให้ผู้ที่ไม่ได้รับอนุญาตทำการแก้ไขเปลี่ยนแปลงซอฟต์แวร์หรืออุปกรณ์ประมวลผลสารสนเทศในเครื่องที่ตนรับผิดชอบ

11.6 การเปลี่ยนแปลงระบบคอมพิวเตอร์ ฮาร์ดแวร์ อุปกรณ์ และสื่อที่ใช้ในการจัดเก็บข้อมูล จะต้องได้รับอนุมัติจากหัวหน้าหน่วยงานที่ดูแลระบบเป็นลายลักษณ์อักษร เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและการแก้ไขโดยไม่ได้ตั้งใจ ซึ่งอาจมีผลต่อการหยุดชะงักของธุรกิจ หรือการเปิดเผยข้อมูลโดยไม่ได้รับการอนุญาต

12. นโยบายการกำจัดอุปกรณ์และการนำกลับมาใช้ใหม่

12.1 เพื่อให้มีความมั่นใจว่า ข้อมูลที่มีความสำคัญในอุปกรณ์นั้นได้ถูกทำลายก่อนที่จะนำอุปกรณ์ดังกล่าวกลับมาใช้ใหม่ และข้อมูลสำคัญไม่ถูกเปิดเผยแก่บุคคลภายนอก

12.2 กำหนดนโยบายและวิธีปฏิบัติการทำลายและการนำอุปกรณ์กลับมาใช้ใหม่โดยให้มีการทำบันทึกการขอนำอุปกรณ์กลับมาใช้ใหม่หรือทำลาย และต้องมีการอนุมัติจากผู้บริหารที่เกี่ยวข้อง

12.3 ก่อนนำอุปกรณ์ที่ต้องการนำกลับมาใช้ใหม่ หรือทำลาย ให้ทำการทำลายข้อมูลที่อยู่ในสื่อบันทึกดังกล่าว

12.4 หากมีความจำเป็นต้องจัดส่งให้หน่วยงานภายนอกซ่อมแซม ให้ผู้ดูแลระบบดำเนินการสำรองข้อมูลที่สำคัญลงในสื่อบันทึกข้อมูลและทำลายข้อมูลดังกล่าวออกจากอุปกรณ์ก่อนที่จะจัดส่งต่อไป

12.5 ต้องมีการบันทึกรายการซ่อมบำรุงอุปกรณ์ว่ามีอุปกรณ์ชิ้นใดถูกส่งซ่อม เมื่อใด จัดส่งให้ใคร และใครเป็นผู้ดำเนินการ ขอบเขตงานในการซ่อมแซมหรือบำรุงรักษา การซ่อมแซมเสร็จสิ้นเมื่อใด และเวลาที่ได้รับของคืนเมื่อใด

12.6 หากการซ่อมแซมมีความจำเป็นต้องกำหนดสิทธิ์การเข้าถึง เมื่อซ่อมแซมเสร็จต้องยกเลิกหรือลบสิทธิ์ในการเข้าถึงที่ให้แก่ช่างเทคนิค

13. นโยบายการจัดเก็บและตรวจสอบข้อมูลจราจรอิเล็กทรอนิกส์

13.1 ต้องมีการจัดเก็บ เฝ้าระวัง ตรวจสอบข้อมูลจราจรอิเล็กทรอนิกส์ (Log) ที่เกี่ยวข้องกับการการใช้งานบริการ NT Conference เช่น Access log, Event log และ Activity Log เป็นต้น

13.2 ต้องมีการกำหนดระยะเวลาการจัดเก็บข้อมูล Log ต่างๆ เป็นระยะเวลาอย่างน้อย 1 ปี

13.3 ต้องมีการจัดระดับชั้นข้อมูล Log รวมถึงมาตรการการจัดการข้อมูล Log

13.4 ต้องมีการตรวจสอบและวิเคราะห์ข้อมูล Log อย่างน้อยปีละ 1 ครั้ง

14. การบทบทวนนโยบาย

14.1 บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) จะทำการทบทวนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศระบบ NT Conference และ นโยบายด้านการคุ้มครองข้อมูลส่วนบุคลเป็นประจำทุกปี อย่างน้อยปีละ 1 ครั้ง หรือกรณีที่กฎหมายมีการเปลี่ยนแปลงแก้ไขไปเป็นอย่างอื่น