นโยบายความมั่นคงปลอดภัยสารสนเทศ กลุ่มทรู (True Information Security Policy)

1. วัตถุประสงค์

นโยบายความมั่นคงปลอดภัยสารสนเทศฉบับหลักนี้ มีวัตถุประสงค์เพื่อกำหนดแนวทางในการปกป้องคุ้มครองทรัพย์สินสารสนเทศของ บริษัท ทรู คอร์ปอเรชั่น จำกัด (มหาชน), บริษัทย่อย และผู้มีส่วนได้ส่วนเสีย (บุคคลภายนอก, คู่ค้า หรือลูกค้า และสาธารณชน) ภายใต้สภาพแวดล้อมที่มีความปลอดภัย

นโยบายฉบับนี้จัดทำขึ้นเพื่อให้พนักงานของกลุ่มทรูและบริษัทย่อย, หน่วยงานด้านเทคโนโลยีสารสนเทศ (IT), เจ้าของระบบสารสนเทศ และบุคคลอื่นที่มีสิทธิ์ในการใช้งานสิ่งอำนวยความสะดวกของกลุ่มทรูและบริษัทย่อย ได้ทราบถึงหลักการในการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ

เป้าหมายในการปกป้องทรัพย์สินสารสนเทศประกอบด้วย:

- **ทรัพย์สินสารสนเทศ:** จะได้รับการคุ้มครองจากการเข้าถึงโดยไม่ได้รับอนุญาตหรือการนำไปใช้ในทางที่ผิด
- **การรักษาความลับ (Confidentiality):** ของข้อมูลจะได้รับการคุ้มครองอย่างปลอดภัย
- **ความถูกต้องครบถ้วน (Integrity):** ของข้อมูลจะได้รับการดูแลให้มีความสมบูรณ์
- **ความพร้อมใช้งาน (Availability):** ของทรัพย์สินสารสนเทศจะได้รับการดูแลเพื่อให้สามารถให้บริการได้อย่างต่อเนื่อง
- **การบริหารความต่อเนื่องทางธุรกิจ:** กระบวนการวางแผนความต่อเนื่องทางธุรกิจจะได้รับการดูแลอย่างสม่ำเสมอ
- **การปฏิบัติตามกฎระเบียบ:** ปฏิบัติตามข้อกำหนดทางกฎหมาย ข้อบังคับ และพันธะสัญญาอย่างเคร่งครัด
- **ความปลอดภัยรอบด้าน:** รักษาความปลอดภัยทั้งทางกายภาพ, ทางตรรกะ (Logical), สภาพแวดล้อม และระบบการสื่อสาร
- **บทลงโทษ:** การละเมิดนโยบายนี้อาจนำไปสู่การดำเนินการทางวินัยหรือการดำเนินคดีอาญา
- **การทำลายข้อมูล:** เมื่อข้อมูลไม่มีความจำเป็นต้องใช้งานอีกต่อไป จะต้องได้รับการทำลายด้วยวิธีการที่เหมาะสม
- **การรายงานเหตุการณ์:** เหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยสารสนเทศทั้งหมดต้องรายงานต่อหน่วยงานที่ได้รับมอบหมาย และมีการตรวจสอบผ่านช่องทางการบริหารจัดการที่เหมาะสม

ทรัพย์สินสารสนเทศ หมายรวมถึง:

- ระบบสารสนเทศอิเล็กทรอนิกส์ (ซอฟต์แวร์, คอมพิวเตอร์ และอุปกรณ์ต่อพ่วง) ที่เป็นกรรมสิทธิ์ของกลุ่มทรูและบริษัทย่อย ไม่ว่าจะติดตั้งหรือเข้าถึงผ่านเครือข่ายของบริษัทฯ หรือไม่ก็ตาม
- เครือข่ายคอมพิวเตอร์ที่ใช้งานทั้งทางตรงและทางอ้อม
- ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลที่เป็นกรรมสิทธิ์ของกลุ่มทรูและบริษัทย่อย
- วัสดุและเอกสารในรูปแบบกระดาษ
- อุปกรณ์บันทึกอิเล็กทรอนิกส์ (ภาพ, เสียง, ระบบกล้องวงจรปิด)

---

2. นโยบาย (Policy)

กลุ่มทรูและบริษัทย่อยกำหนดให้ผู้ใช้งานทุกคนต้องปฏิบัติหน้าที่ด้วยความระมัดระวังในการใช้งานและดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศ

2.1 ผู้ใช้งานระบบสารสนเทศที่ได้รับอนุญาต

ผู้ใช้งานระบบสารสนเทศของกลุ่มทรูและบริษัทย่อยทุกคนต้องได้รับอนุมัติอย่างเป็นทางการจากหน่วยงาน IT โดยผู้ใช้งานที่ได้รับอนุญาตจะมีอัตลักษณ์ผู้ใช้งาน (User Identity) เฉพาะตัว ห้ามมิให้เปิดเผยรหัสผ่านใดๆ ที่เกี่ยวข้องกับอัตลักษณ์นั้นให้แก่บุคคลอื่นโดยเด็ดขาด ผู้ใช้งานที่ได้รับอนุญาตต้องใช้ความระมัดระวังในการปกป้องข้อมูลของกลุ่มทรูและบริษัทย่อยที่อยู่ในความครอบครอง ข้อมูลความลับ ข้อมูลส่วนบุคคล หรือข้อมูลส่วนตัว ห้ามมิให้มีการคัดลอกหรือเคลื่อนย้ายโดยมิได้พิจารณาถึง:

- การได้รับอนุญาตจากเจ้าของข้อมูล
- ความเสี่ยงที่เกี่ยวข้องกับการสูญหายหรือการตกไปอยู่ในมือของผู้ที่ไม่มีสิทธิ์
- วิธีการรักษาความปลอดภัยของข้อมูลระหว่างการขนส่งและเมื่อถึงปลายทาง

2.2 การใช้งานระบบสารสนเทศอย่างเหมาะสม

การใช้งานระบบสารสนเทศของกลุ่มทรูและบริษัทย่อยโดยผู้ใช้งานที่ได้รับอนุญาต ต้องเป็นไปโดยชอบด้วยกฎหมาย มีความซื่อสัตย์ สุจริต และคำนึงถึงสิทธิและความรู้สึกของผู้อื่น

2.3 เจ้าของระบบ (System Owners)

เจ้าของระบบที่มีหน้าที่รับผิดชอบระบบสารสนเทศ ต้องประสานงานกับหน่วยงาน IT เพื่อให้มั่นใจว่า:

- ระบบได้รับการปกป้องจากการเข้าถึงโดยมิได้รับอนุญาตอย่างเพียงพอ

- มีแผนความต่อเนื่องทางธุรกิจ (BCP) และพร้อมใช้งานเพื่อให้ระบบสารสนเทศทางธุรกิจที่สำคัญมีความพร้อมใช้เสมอ
- ระบบสามารถกู้คืนได้ในกรณีที่เกิดความเสียหายต่อแหล่งข้อมูลหลัก (เช่น ระบบคอมพิวเตอร์ล้มเหลวหรือสูญหาย)
- ข้อมูลได้รับการดูแลให้มีความถูกต้องแม่นยำและมีคุณภาพสูง
- การโอนย้ายข้อมูลความลับผ่านทางเว็บไซต์อินเทอร์เน็ตต้องได้รับการปกป้อง
- เจ้าของระบบต้องใช้เทคนิคการเข้ารหัส (Cryptography) ที่ได้รับอนุมัติเพื่อรักษาความลับและความถูกต้องของข้อมูล
- ระบบถูกพัฒนาขึ้นอย่างปลอดภัยและตรงตามวัตถุประสงค์การใช้งาน
- ข้อมูลอิเล็กทรอนิกส์ รวมถึงข้อมูลส่วนบุคคล ข้อมูลธุรกรรม รายการบันทึกกิจกรรม (Audit Trail) และบันทึกการเข้าถึง (Access Logs) จะต้องจัดเก็บไว้ในระยะเวลาที่เหมาะสมตามกฎหมายที่เกี่ยวข้องและมาตรฐานของกลุ่มทรูเท่านั้น
- บุคคลภายนอกที่เข้าถึงข้อมูลหรือให้บริการแก่กลุ่มทรูและบริษัทย่อย ควรเข้าใจในความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัย

2.4 การปฏิบัติการ (Operations)

หน่วยงาน IT ของแต่ละบริษัทในกลุ่มทรูและบริษัทย่อย รับผิดชอบงานด้านการปฏิบัติการที่เกี่ยวข้องในพื้นที่ความรับผิดชอบของตน โดยต้องมั่นใจว่า:

- การเปลี่ยนแปลงข้อมูลและการตั้งค่าระบบ (Configuration) จะต้องมีการควบคุม
- มีการจัดการและเฝ้าระวังช่องโหว่ (Vulnerabilities) ที่เกี่ยวข้องกับระบบและโครงสร้างพื้นฐาน
- มีแผนกู้คืนระบบจากภัยพิบัติ (DRP) และพร้อมที่จะกู้คืนข้อมูลตามระดับความสำคัญ
- มีการสำรองข้อมูลอิเล็กทรอนิกส์และพร้อมสำหรับการกู้คืน
- มีระบบการพิสูจน์ตัวตนที่เข้มแข็ง (Strong Authentication) เพื่อยืนยันตัวตนผู้ได้รับอนุญาต
- ทรัพย์สินทาง IT ได้รับความปลอดภัยจากการโจรกรรมและความเสียหายทางกายภาพ
- สนับสนุนกิจกรรมด้านการกำกับดูแล IT (IT Governance), การบริหารความเสี่ยง IT และการปฏิบัติตามข้อกำหนด IT

2.5 การควบคุมการเข้าถึง (Access Control)

กลุ่มทรูและบริษัทย่อยยึดหลักการ "การให้สิทธิ์เท่าที่จำเป็น" (Least Privilege) ในการควบคุมการเข้าถึง เพื่อให้มั่นใจว่าเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่มีสิทธิ์เข้าถึงแอปพลิเคชันทางธุรกิจ

ระบบ เครือข่าย และอุปกรณ์คอมพิวเตอร์ โดยมีการกำหนดความรับผิดชอบรายบุคคล และมอบสิทธิ์การเข้าถึงให้เพียงพอต่อการปฏิบัติงานตามหน้าที่ แต่ไม่เกินขอบเขตอำนาจที่ได้รับ

2.6 ข้อมูลส่วนบุคคล (Personal Information)
ข้อมูลส่วนบุคคลต้องได้รับการปกป้องจากการถูกละเมิดหรืออันตรายใดๆ โดยเจ้าหน้าที่ของกลุ่มทรูและบริษัทย่อยที่ได้รับมอบหมายอย่างเป็นทางการเท่านั้น ที่อาจเข้าถึงหรือตรวจสอบข้อมูลส่วนบุคคลที่อยู่ในระบบสารสนเทศของตนได้

2.7 ความมั่นคงปลอดภัยในการสื่อสารและการปฏิบัติการ
มีการใช้แนวทางการป้องกันเชิงลึก (Defence-in-depth) เพื่อปกป้องทรัพย์สินสารสนเทศจากภัยคุกคามที่มีอยู่และที่เกิดขึ้นใหม่ การดำเนินงานด้านความปลอดภัย เช่น การสำรองและกู้คืนข้อมูล, การจัดการการเปลี่ยนแปลง (Change Management), การบริหารการออกระบบ (Release Management) และการวางแผนขีดความสามารถ (Capacity Planning) จะต้องดำเนินการโดยเจ้าหน้าที่ IT ที่มีประสบการณ์ มีการเฝ้าระวังความปลอดภัยเพื่อตรวจจับเหตุการณ์ที่ผิดปกติหรือน่าสงสัย และแจ้งเตือนทีมตอบสนองเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศเพื่อจัดการเหตุการณ์ต่อไป

การเข้าถึงเครือข่ายของกลุ่มทรูและบริษัทย่อยจากระยะไกล (Remote Access) อนุญาตเฉพาะพนักงานที่ได้รับอนุมัติล่วงหน้าและใช้อุปกรณ์ที่บริหารจัดการโดยบริษัทฯ เท่านั้น โดยผ่านโซลูชัน VPN ที่มีการเข้ารหัส ตรวจสอบความปลอดภัยของอุปกรณ์ และรองรับการพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-factor Authentication)

2.8 การละเมิดนโยบาย
บุคคลที่ละเมิดนโยบายนี้จะต้องถูกดำเนินการทางวินัยและดำเนินคดีตามกฎหมาย กลุ่มทรูและบริษัทย่อยจะดำเนินคดีทางกฎหมายกับพนักงานหรือบุคคลภายนอก เพื่อให้มั่นใจว่าระบบสารสนเทศจะไม่ถูกใช้งานโดยบุคคลที่ไม่มีสิทธิ์

---

3. ความเป็นเจ้าของ (Ownership)
ผู้บริหารระดับสูงด้าน IT ของกลุ่มทรูและแต่ละบริษัทย่อย มีหน้าที่รับผิดชอบโดยตรงในการรักษานโยบายนี้ในพื้นที่ที่ตนดูแล หน่วยงาน IT และเจ้าของระบบสารสนเทศทั้งหมดมีหน้าที่รับผิดชอบในการนำนโยบายนี้ไปปฏิบัติและควบคุมให้มีการปฏิบัติตามอย่างเคร่งครัด

---

4. การเปลี่ยนแปลงนโยบายความปลอดภัย

เราอาจปรับปรุงนโยบายความปลอดภัยนี้เป็นครั้งคราวตามแนวปฏิบัติทางด้านความปลอดภัย และการปฏิบัติตามกฎหมายที่เกี่ยวข้อง เราขอสงวนสิทธิ์ในการปรับปรุงนโยบายความปลอดภัยนี้บนเว็บไซต์ของเราโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

*** รายชื่อบริษัทในกลุ่มทรู (LISTS OF TRUE GROUP OF COMPANIES)**

Asia Wireless Communication Co., Ltd., Bangkok Inter Teletech Public Company Limited, BFKT (Thailand) Limited, Chiwiborirak Co., Ltd., Seekone Holding Company Limited, Seekster Co., Ltd., Seekforce Co., Ltd., Cineplex Co., Ltd., WorldPhone Shop Company Limited, TAC Property Company Limited, dtac TriNet Company Limited, DTAC Broadband Company Limited, dtac Accelerate Company Limited, dtac Digital Media Company Limited, TeleAssets Company Limited, Hutchison Wireless MultiMedia Holdings Limited, Internet Knowledge Service Center Co., Ltd., KSC Commercial Internet Co., Ltd., MKSC World Dot Com Co., Ltd., SM True Co., Ltd., True Corporation Public Company Limited, Telecom Asset Management Co., Ltd., Telecom Holding Co., Ltd., Thai News Network (TNN) Co., Ltd., True Digital Group Co., Ltd., True Digital Park Co., Ltd., True Distribution and Sales Co., Ltd., True4U Station Co., Ltd., True Incube Co., Ltd., True Internet Corporation Co., Ltd., True Life Plus Co., Ltd., True Media Solutions Co., Ltd., True Move Co., Ltd.,True Move H Universal Communication Co., Ltd., True Multimedia Co., Ltd., True United Football Club Co., Ltd., True Visions Group Co., Ltd., True Voice Co., Ltd., Gold Palace Investments Limited,Golden Light Co., Ltd., Goldsky Co., Ltd., K.I.N. (Thailand) Co., Ltd., Mediaload Pte. Ltd., Mediaload (Cambodia) Co., Ltd., Mediaload Myanmar Co., Ltd., Two Way PR Co., Ltd. "True Internet Technology (Shanghai) Company Limited ", True Trademark Holdings Company Limited, Crave Interactive Limited, Crave Interactive B.V., Crave Interactive Inc., PT True Digital Indonesia, True Digital Philippines Inc., True Digital Vietnam Joint Stock Company, Zapgroup Inc.