# แนวนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ
# และ นโยบายคุ้มครองข้อมูลส่วนบุคคล
# บริษัท โคโนวานซ์ จำกัด

**หลักการและเหตุผล**

ตามพระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 และประกาศสำนักพัฒนาธุรกรรมทางอิเล็กทรอนิกส์เรื่องมาตรฐานรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการพระชุม พ.ศ. 2563 กำหนดให้ผู้ให้บริการการประชุมผ่านสื่ออิเล็กทรอนิกส์มีแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และ แนวนโยบายการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้ระบบเทคโนโลยีสารสนเทศและระบบควบคุมการประชุมของ **บริษัท โคโนวานซ์ จำกัด** (บริษัทฯ) เป็นไปอย่างเหมาะสมมีประสิทธิภาพมีความมั่นคงปลอดภัย สามารถดำเนินงานได้ และคำนึงถึงการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้น จากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ บริษัทฯจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศและระบบควบคุมการประชุม

**วัตถุประสงค์**

1.1 เพื่อให้มีนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศของบริษัทฯ ให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

1.2 เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและ เครือข่ายคอมพิวเตอร์ของบริษัทฯทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

1.3 เพื่อเป็นกรอบและแนวปฏิบัติในการกำหนดมาตรฐาน ขั้นตอนการปฏิบัติงาน ผู้รับผิดชอบ รวมถึงสิ่งอำนวยความสะดวกด้านคอมพิวเตอร์สำหรับการติดตั้งและใช้งานระบบเพื่อการรักษาความมั่นคงปลอดภัยของสารสนเทศ

1.4 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร พนักงาน เจ้าหน้าที่ ผู้ดูแลระบบและ บุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบ เทคโนโลยีสารสนเทศของบริษัทฯ ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด รวมถึงด้านการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน เป็นนโยบายในการธำรงไว้ ซึ่งความลับ(Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability) รวมถึงกรณีที่เกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายฯ

1.5 เพื่อกำหนดให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ มีแผนเตรียมความพร้อมสำหรับกรณี ฉุกเฉิน และให้สามารถกู้ระบบกลับคืนได้ภายในระยะเวลาที่เหมาะสมตามกฎหมาย เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของระบบควบคุมการประชุมสามารถใช้งานได้เป็นปกติอย่างต่อเนื่อง เหมาะสมและสอดคล้องตามภารกิจ และ เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัทฯ โดนบุกรุก ขโมย ทำลาย แทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่างๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัทฯ

1.6 ด้านการตรวจสอบและประเมินความเสี่ยง เพื่อกำกับแลดูการบริหารระบบสารสนเทศให้เกิดประสิทธิภาพและประสิทธิผลตลอดจนการกำหนดแนวทางการแก้ไขปัญหาและอุปสรรคต่าง ๆ ที่เกิดขึ้น อย่างน้อยปีละ 1 ครั้ง เพื่อทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบัน

**องค์ประกอบของนโยบาย**

นโยบายฯนี้จัดทำขึ้นโดยอาศัยกรอบตามมาตรฐานสากลด้านความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013 และ ISO/IEC 27701:2019 รวมทั้งข้อกำหนดตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ เพื่อใช้เป็นกรอบและแนวปฏิบัติในการป้องกันและรักษาทรัพย์สินด้านสารสนเทศของบริษัทฯจากภาวะคุกคามทุกประเภทที่อาจจะเกิดขึ้นทั้งจากภายในและภายนอกบริษัทฯ โดยเจตนาหรือโดยรู้เท่าไม่ถึงการณ์ซึ่งเป็นแนวนโยบายในภาพรวมเพื่อการจัดการด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศโดยจัดแบ่งสาระสำคัญ ออกเป็น 12 หมวด ประกอบด้วย

หมวด 1 นโยบายความมั่นคงปลอดภัย

หมวด 2 การจัดการสินทรัพย์สารสนเทศ

หมวด 3 การควบคุมการเข้าถึง

หมวด 4 การเข้ารหัสลับข้อมูล

หมวด 5 การสร้างความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

หมวด 6 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน

หมวด 7 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

หมวด 8 การจัดหาพัฒนาและบำรุงรักษาระบบสารสนเทศ

หมวด 9 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

หมวด 10 การบริหารความต่อเนื่องของการดำเนินภารกิจของบริษัท

หมวด 11 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย

หมวด 12 การกำหนดผู้รับผิดชอบ

หมวด 13 การบริหารจัดการความเสี่ยงด้านความปลอดภัยไซเบอร์

**คำนิยาม**

- **บริษัทฯ** หมายถึง บริษัท โคโนวานซ์ จำกัด
- **ผู้บริหารระดับสูง** หมายถึง ผู้มีอำนาจบริหารในระดับสูงของของบริษัท ฯ
- **ผู้จัดการด้านความปลอดภัยสารสนเทศ** (Information Security Manager: ISM) หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของบริษัทฯ ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ
- **ผู้ดูแลระบบ** (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบให้ดูแลใช้งานและบำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ทั้งอุปกรณ์ฮาร์ดแวร์ (hardware) และ ซอฟต์แวร์ (software) และอุปกรณ์ต่อพ่วงที่ประกอบกันขึ้นเป็นระบบคอมพิวเตอร์ ผู้ดูแลระบบจะเป็นผู้ที่ได้รับอนุญาตให้มีอำนาจในการปรับเปลี่ยน เพิ่มเติม แก้ไข ปรับปรุงให้ระบบคอมพิวเตอร์ของบริษัทฯ ทำงานได้อย่างถูกต้อง มีประสิทธิภาพสอดคล้องกับความต้องการทางธุรกิจและมีความปลอดภัย รวมถึงสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีจดหมายอิเล็กทรอนิกส์ (Email Account)
- **เจ้าหน้าที่** หมายถึง ผู้บริหาร พนักงาน ลูกจ้าง และพนักงานจ้างเหมาของบริษัทฯ
- **ระบบคอมพิวเตอร์** (Computer system) หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้ง ฮาร์ดแวร์ (hardware) และซอฟต์แวร์ (software) ทุกขนาด อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสายและไร้สาย วัสดุอุปกรณ์การเก็บรักษา และการถ่ายโอนข้อมูลชนิดต่างๆระบบ Internet และระบบ Intranet รวมถึงอุปกรณ์ไฟฟ้า และสื่อสารโทรคมนาคมต่างๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือคล้ายคลึงกับคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของบริษัทฯ ที่อยู่ระหว่างการติดตั้ง และยังไม่ได้ส่งมอบ หรือของพนักงานที่นำเข้ามาติดตั้ง หรือใช้งานภายในสถานประกอบการของบริษัทฯ

- **ระบบเทคโนโลยีสารสนเทศ** หมายถึง ระบบควบคุมการประชุมของบริษัทฯที่ตั้งอยู่ที่ดาต้าเซ็นเตอร์ภายในประเทศไทย ภายใต้การดูแลของผู้ดูแลระบบ
- **สารสนเทศ** หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปตัวเลข ข้อความ หรือกราฟฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย ละสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆได้
- **ข้อมูล** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
- **ข้อมูลสารสนเทศ (**Information Technology) หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่างๆไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือหรืออุปกรณ์ใดๆ
- **ระบบงาน** หมายถึง การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงานเพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้
- **ระบบปฏิบัติการ** (Operating system) หมายถึง ซอฟแวร์ควบคุมการทำงานของเครื่องคอมพิวเตอร์และจัดสรรการใช้ทรัพยากรระบบซึ่งได้แก่ การจัดการหน่วยความจำ การควบคุมการทำงานของอุปกรณ์ป้อนข้อมูล **(**แป้นพิมพ์/ เมาส์**)** และอุปกรณ์แสดงผล **(**จอภาพ/ เครื่องพิมพ์**)**
- **ระบบเครือข่าย** (Network) หมายถึง ระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ
- **เครื่องคอมพิวเตอร์แม่ข่าย** (Server) หมายถึง เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทำหน้าที่เป็น ศูนย์กลางของการทำงานอาทิจัดเก็บข้อมูลซอฟต์แวร์ สำหรับให้บริการแก่เครื่องคอมพิวเตอร์อื่นๆ หรือควบคุมการทำงานในเครือข่าย
- **สินทรัพย์** หมายถึง สิ่งใดก็ตามที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศที่มีคุณค่าสำหรับบริษัทฯ รวมถึง ฮาร์ดแวร์(Hardware) ซอฟต์แวร์(Software) และข้อมูลภายใต้การดูแลของเจ้าหน้าที่
- **ความมั่นคงปลอดภัยของสารสนเทศ** ( Information security) หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)
- **ความลับ** (Confidentiality) หมายถึง การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้
- **ข้อมูลสำคัญ** หรือ **ข้อมูลที่เป็นความลับ** (Sensitive Information)" หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัทฯ หรือที่บริษัทฯ มีพันธะผูกพันตามข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบธุรกิจ หรือสัญญาซึ่งบริษัทฯ ไม่อาจนำไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์อย่างอื่น นอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัทฯการรั่วไหลของข้อมูลสำคัญหรือข้อมูลที่เป็นความลับดังกล่าวอาจเป็นเหตุให้การดำเนินธุรกิจของบริษัทฯ ต้องหยุดชะงัก ขาดประสิทธิภาพ หรือบริษัทฯเสื่อมเสียชื่อเสียง
- **ความถูกต้องครบถ้วน** (integrity) หมายถึง การรับรองว่าข้อมูลจะไม่ถูกกระทำการใดๆ อันมีผลให้เกิด การเปลี่ยนแปลง หรือแก้ไขโดยผู้ไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม สภาพพร้อมใช้งาน ( availability) หมายถึง การรับรองได้ว่าข้อมูล หรือระบบเทคโนโลยีสารสนเทศ ทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน
- **ความมั่นคงปลอดภัย** (security) หมายถึงกระบวนการ และการกระทำใดๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาระบบคอมพิวเตอร์และข้อมูลสารสนเทศที่เป็นระบบและข้อมูลสำคัญให้พ้นจากความพยายามใดๆทั้งจากภายในและจากบุคคลภายนอกในการเข้าถึงเพื่อโจรกรรมทำลายหรือแทรกแซงการทำงานจนเป็นเหตุให้การดำเนินธุรกิจของบริษัทฯได้รับความเสียหาย
- **เหตุการณ์ด้านความมั่นคงปลอดภัย** ( information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

- **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** ( information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบ ของบริษัทฯถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
- **ความเสี่ยง** หมายถึง โอกาสของทรัพยากรสารสนเทศในการถูกละเมิดการรักษาความปลอดภัยเหตุการณ์หรือการกระทำใดๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหายทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กรทั้งในด้านยุทธศาสตร์ การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้โดยวัดจากผลกระทบ(Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์
- **ความเสี่ยงของระบบสารสนเทศ (**Information System risk) หมายถึง โอกาสที่จะเกิด ข้อผิดพลาด ความเสียหาย การกระทำใดๆ ที่ก่อให้เกิดการสูญเสียหรือทำลายฮาร์ดแวร์(hardware) ซอฟต์แวร์(software) ข้อมูล สารสนเทศหรือความสามารถในการประมวลผลข้อมูลของระบบสารสนเทศ
- **ช่องโหว่** (vulnerability) หมายถึง จุดอ่อนของระบบสารสนเทศที่ทำให้ผู้ไม่ประสงค์ดีเข้าโจมตีระบบทำให้ประสิทธิภาพของการทำงานลดลง
- **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** (access control) หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดย มิชอบเอาไว้ด้วยก็ได้
- **บุคคลภายนอก** หมายถึง บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ
- **ผู้ใช้งาน** (user) หมายถึง พนักงาน ผู้บริหารของบริษัทฯ หรือ ผู้เข้าร่วมประชุมที่ได้รับอนุญาติให้ใช้ระบบการประชุม รวมไปถึงบุคคลภายนอกบริษัทฯที่ได้รับอนุญาตให้มีรหัสเข้าใช้งานในบัญชีรายชื่อผู้สามารถเข้าใช้งาน หรือ/และ มีรหัสผ่านเพื่อเข้าใช้งานอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ
- **รหัสผ่าน** ( password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล ระบบควบคุมการประชุม และระบบเทคโนโลยีสารสนเทศ
- **สิทธิของผู้ใช้งาน** หมายถึงสิทธิทั่วไป สิทธิจำเพาะสิทธิพิเศษและสิทธิอื่นใดที่เกี่ยวข้องกับระบบที่ให้บริการโดยบริษัทฯ
- **มาตรฐาน** (standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
- **ระบบอินเทอร์เน็ต** (internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่าย คอมพิวเตอร์ต่างๆ ของบริษัทฯ เข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
- **จดหมายอิเล็กทรอนิกส์** (Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่าย ที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่ง ข้อมูลชนิดนี้ได้แก่ SMTP, POP3 **และ** IMAP เป็นต้น
- **ข้อมูลส่วนบุคคล** หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถ ระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ เช่น ชื่อ สกุล ที่อยู่ วันเดือนปีเกิด หมายเลขโทรศัพท์ เลขประจำตัวประชาชน เป็นต้น
- **เจ้าของข้อมูล** หมายถึง บุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล
- **บุคคล** หมายถึง บุคคลธรรมดา

# หมวด 1
# นโยบายความมั่นคงปลอดภัย

**<u>วัตถุประสงค์</u>**

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบ เทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอกซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบควบคุมการประชุม

**1. ข้อกำหนดตามกฎหมาย**

ความมั่นคงปลอดภัยด้านสารสนเทศบางประเด็นอาจจะเกี่ยวข้องกับกฎหมายที่ได้มีบัญญัติ มีประกาศและมีผลบังคับใช้ อาทิ

**(1)** กฎหมายธุรกรรมทางอิเล็กทรอนิกส์

**(2)** กฎหมายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

**(3)** กฎหมายลิขสิทธิ

รวมถึงกฎหมาย ระเบียบข้อบังคับอื่นที่เกี่ยวข้องซึ่งใช้บังคับอยู่แล้วในขณะนี้และที่จะได้ออกใช้บังคับต่อไปในภายหน้า

**2. มาตรฐานระดับสากล**

มาตรฐานการรักษาความมั่นคงปลอดภัย ISO/IEC 27001:2013 และ ISO/IEC 27701:2019 จัดเป็นมาตรฐานที่ได้รับการยอมรับจากหลาย ประเทศในการนำไปใช้บริหารจัดการระบบสารสนเทศขององค์กร และเป็นมาตรฐานที่ถูกใช้เป็นพื้นฐานและอ้างอิงประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่องมาตรฐานการรักษาความ**มั่นคง**ปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ **พ.ศ. 2563**

**3. ผู้ได้รับผลกระทบจากนโยบาย**

นโยบายนี้มีผลบังคับกับเจ้าหน้าที่ทุกคนของบริษัท โคโนวานซ์ จำกัด รวมถึงผู้รับสัญญา และผู้เยี่ยมเยือนซึ่งแม้จะมิได้รับการว่าจ้างจากบริษัทฯ แต่มีส่วนเกี่ยวข้องกับการทำงาน หรือสามารถเข้าถึงสารสนเทศของบริษัทฯ

**4. พื้นที่ที่มีผลบังคับใช้**

นโยบายนี้มีผลบังคับใช้กับทุกตำแหน่งพื้นที่ที่สามารถเข้าถึงสารสนเทศและเครือข่ายสารสนเทศของบริษัท โคโนวานซ์ จำกัด ได้ ซึ่งรวมถึงการเรียกใช้งานจากทางบ้าน หรือการเข้าถึงจากระยะไกล และการเชื่อมโยง จากภายนอก

**5. การตรวจสอบและทบทวน**

บริษัทฯต้องกำหนดให้มีผู้บริหารระดับสูงทำหน้าที่กำกับดูแลนโยบายและรับผิดชอบในการตรวจสอบการดำเนินงานตามนโยบายความมั่นคงปลอดภัยของสารสนเทศอย่างสม่ำเสมอและทันเหตุการณ์ โดยให้มีการ ทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุการณ์แปรเปลี่ยนที่สำคัญ บริษัทฯต้องติดตามเพื่อให้มั่นใจว่า นโยบายเหล่านี้มีความเหมาะสม สอดคล้องกับข้อกฎหมายและมาตรฐาน

## หมวด 2
## การจัดการสินทรัพย์สารสนเทศ

**<u>วัตถุประสงค์</u>**

การจัดการสินทรัพย์สารสนเทศ ( Information Asset Management) กำหนดขึ้นเพื่อป้องกันสินทรัพย์ สารสนเทศของบริษัทฯ ให้เกิดความมั่นคงปลอดภัย และสามารถใช้งานสินทรัพย์เหล่านั้นได้อย่างเหมาะสม

**1. หน้าที่ความรับผิดชอบต่อสินทรัพย์สารสนเทศ**

บริษัทฯต้องกำหนดให้มีผู้รับผิดชอบในการจัดทำบัญชีสินทรัพย์สารสนเทศและปรับปรุงข้อมูลให้ถูกต้อง อยู่เสมอ โดยให้ความสำคัญกับสินทรัพย์ที่มีผลต่อการดำเนินภารกิจของบริษัทฯ

**2. การกำจัดสินทรัพย์หรือการนำสินทรัพย์กลับมาใช้งานอีกครั้ง**

โดยให้ทำลายข้อมูลสำคัญในสินทรัพย์ก่อนที่จะกำจัดสินทรัพย์ดังกล่าว รวมถึงมีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในสินทรัพย์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำสินทรัพย์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

## หมวด 3
## การควบคุมการเข้าถึง

**<u>วัตถุประสงค์</u>**

การควบคุมการเข้าถึงระบบสารสนเทศ รวมถึงระบบควบคุมการประชุมโดยกำหนดสิทธิของผู้เข้าถึงบนระบบที่สิทธิที่แตกต่างกันอย่างชัดเจนโดยจัดให้มี เพื่อให้มีความมั่นคงปลอดภัย

- **นโยบายควบคุมการเข้าถึง (**Access Control Policy)

1) มีการกำหนดให้มีการควบคุมการใช้งานข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึง ให้ เข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น โดยปฏิบัติตามวิธีปฏิบัติงานเรื่องการควบคุมการเข้าถึง (Access Control) และวิธีปฏิบัติงานเรื่องการลงทะเบียนใช้งานระบบสารสนเทศ

2) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวน สิทธิ์การเข้าถึงอย่างสม่ำเสมอ โดยปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการทบทวนสิทธิ์การเข้าถึงของ ผู้ใช้งาน (Review of User Access Rights Procedure) ทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาต จากผู้บังคับบัญชาตามความจำเป็นในการใช้งาน

3) ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้

4) ต้องมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ และเฝ้าระวังการละเมิดความปลอดภัย ที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

5) ต้องบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ ของทั้งผู้ที่ได้รับ อนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

6) ต้องกำหนดกฎเกณฑ์ข้อห้ามและบทลงโทษการเข้าถึงข้อมูลและระบบสารสนเทศ

7) การเข้าถึงข้อมูล และระบบสารสนเทศของบริษัทฯ จะกระทำได้ก็ต่อเมื่อได้รับการอนุมัติโดย ผู้บังคับบัญชาของบุคคลนั้น ๆ และสามารถเข้าใช้ข้อมูล และระบบเฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของ บุคคลนั้น ๆ เท่านั้น ความปลอดภัยของข้อมูล และกระบวนการรักษาความลับของข้อมูลถือว่าเป็นส่วน หนึ่งในการกำหนดนโยบาย และขั้นตอนการทำงานของระบบสารสนเทศกระบวนการเหล่านี้หมาย รวมถึงการให้สิทธิ์ และการบริหารจัดการรหัสในการเข้าใช้งาน การก าหนดขอบเขตในการเข้าถึงข้อมูล หรือระบบคอมพิวเตอร์ และอุปกรณ์ที่เก็บข้อมูลประเภทอื่น ๆ การสำรองข้อมูลและการกู้ข้อมูลที่ เสียหายกลับคืนมา

- **การเข้าถึงเครือข่ายและบริการเครือข่าย** (Access to Network and Network Services)

ผู้ใช้งานต้องได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการของเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึง เท่านั้น

1) ต้องควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะ เพื่อรักษาความมั่นคง ปลอดภัยให้แก่ข้อมูลและระบบเทคโนโลยีสารสนเทศ อาทิ

- ใช้งานโปรโตคอลที่มั่นคงปลอดภัยในการบริหารจัดการระบบเครือข่าย อาทิ **Secure Socket Layer (SSL) Simple Network Management Protocol (SNMP)**
- จำกัดการใช้งานเครือข่ายที่ส่งผลกระทบต่อ **Bandwidth** เช่น การรับ-ส่งไฟล์ขนาดใหญ่ ฟังเพลง ออนไลน์ ดูทีวีออนไลน์ หรือ เล่นเกมส์ออนไลน์ ในช่วงเวลาทำการ ยกเว้นกรณีที่ได้รับอนุญาต จาก **ISM**
- ผู้ใช้งานจะต้องสามารถเข้าถึงระบบเครือข่ายและระบบสารสนเทศได้ แต่เพียงบริการที่ได้รับ อนุญาตให้เข้าถึงเท่านั้น

2) ระบบเครือข่ายต้องได้รับการออกแบบและตั้งค่าอย่างเหมาะสม เพื่อรักษาความมั่นคงปลอดภัย ให้แก่ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ

- อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายทั้งหมดต้องได้รับการตั้งค่าให้มีความปลอดภัยและการมีการ ตรวจสอบกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับระบบเครือข่าย
- ระบบสายสัญญาณต้องได้รับมาตรฐานอุตสาหกรรมและได้รับการติดตั้งโดยผู้ที่มีความชำนาญที่ ผ่านการพิจารณาอนุมัติแล้ว
- อุปกรณ์เครือข่าย อาทิ Router, Firewall, Switch, Wireless Access Point ต้องได้รับการตั้งค่า ตามความจำเป็นด้านความมั่นคงปลอดภัยของอุปกรณ์นั้นๆ หรือตามคำแนะนำของบริษัทฯ ด้านความมั่นคงปลอดภัยต่าง ๆ อาทิ SANS Institute หรือ NSA
- IP Address ต้องได้รับการลงทะเบียน แจกจ่ายและบริหารจัดการ
- อุปกรณ์เครือข่ายที่สำคัญ เช่น Router, Core Switch ต้องมีอุปกรณ์สำรองไฟฟ้า (UPS) เสมอ
- การเปลี่ยนแปลงระบบเครือข่ายหรืออุปกรณ์เครือข่ายต้องได้รับการควบคุมโดยปฏิบัติตาม เอกสารวิธีการปฏิบัติงานเรื่อง การจัดการการเปลี่ยนแปลงระบบสารสนเทศ (Change Management )
- ระบบเครือข่ายต้องได้รับการออกแบบหรือตั้งค่าให้ทำงานได้อย่างมีประสิทธิภาพ (Reliable) มี ความยืดหยุ่น (Flexible) รวมถึงสามารถรองรับการขยายตัวและความต้องการใช้งานในอนาคต (Scalable)

3) ข้อตกลงการให้บริการเครือข่ายต้องระบุถึงรายละเอียด และข้อกำหนดเกี่ยวกับการรักษาความ มั่นคงปลอดภัย ระดับการให้บริการ และการบริหารจัดการบริการเครือข่ายทั้งหมด หากบริการเครือข่าย นั้นได้รับการดำเนินการโดยหน่วยงานภายนอก ต้องมีการระบุถึงสิทธิของบริษัทฯ ในการติดตามตรวจสอบ และตรวจประเมินการท างานของหน่วยงานภายนอกด้วย

- **การจัดการการเข้าถึงระบบของผู้ใช้งาน** (User Access Management)

เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ใช้งานสามารถเข้าถึงระบบสารสนเทศได้

1) การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User Registration and De-Registration)

- การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการสำหรับการ ลงทะเบียนผู้ใช้งานใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งระเบียบปฏิบัติสำหรับ การยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป หรือ

เมื่อเปลี่ยนตำแหน่งงานภายในบริษัทฯ เป็นต้น โดย ปฏิบัติตามวิธีปฏิบัติงานเรื่องการควบคุมการเข้าถึง (Access Control) และ วิธีปฏิบัติงาน เรื่องการลงทะเบียนใช้งานระบบสารสนเทศ โดยผู้ใช้งานต้องได้รับการทบทวน และ พิจารณาอนุมัติตามขั้นตอนของบริษัทฯ อย่างเคร่งครัด

2) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning)

- การจัดการสิทธิการเข้าถึงของผู้ใช้งาน ต้องกำหนดให้มีวิธีการในการบริหารจัดการสิทธิการเข้าถึง ทั้งการให้สิทธิและการถอดถอนสิทธิต้องมีระเบียบวิธีการกำหนดไว้สำหรับผู้ใช้งานทุกประเภท

3) การบริหารจัดการสิทธิตามระดับสิทธิการเข้าถึง (Management of Privileged Access Right)

- ต้องกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตาม หน้าที่ที่รับผิดชอบด้วย
- ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ **Log-on** เข้าสู่ระบบสารสนเทศ

4) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of User)

- ต้องมีกระบวนการจัดการ การส่งมอบข้อมูลเพื่อพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นความลับ และการ เก็บรักษาข้อมูลความลับของตัวเอง การส่งมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นข้อมูลลับ
- เจ้าหน้าที่ ต้องปฏิบัติตามวิธีปฏิบัติงานเรื่อง การลงทะเบียนใช้งานระบบสารสนเทศ โดยการส่งมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งาน

5) การทบทวนสิทธิในการเข้าถึงระบบของผู้ใช้งาน (Review of User Access Rights)

- ต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ตามคู่มือการปฏิบัติงาน เรื่องการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights Procedure)

6) การถอนหรือการจัดการสิทธิการเข้าถึง (Removal or Adjustment of Access Rights)

- สิทธิการเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อสารสนเทศและอุปกรณ์ ประมวลผลสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการ จ้าง และต้องได้รับการปรับปรุงให้ถูกต้องอย่างสม่ำเสมอ โดยปฏิบัติงานเรื่องการลงทะเบียนใช้งานระบบ สารสนเทศ
- ต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ ตามคู่มือการปฏิบัติงาน เรื่องการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights Procedure)

- **หน้าที่ความรับผิดชอบของผู้ใช้งาน** (User responsibilities)

เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลที่ใช้ในการพิสูจน์ตัวตน

1) การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information)

การใช้งานและเก็บรักษาข้อมูลการพิสูจน์ตัวตนของผู้ใช้งาน ต้องดำเนินการตามนโยบายหรือวิธี ปฏิบัติขององค์กรสำหรับการใช้งานข้อมูลพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ เช่น

-เก็บรักษา **Username** และ **Password** ต้องเป็นความลับห้ามเปิดเผยให้บุคคลอื่นทราบ

-หลีกเลี่ยงการเก็บบันทึกข้อมูลการตรวจสอบความลับ เว้นแต่สามารถเก็บไว้อย่างปลอดภัย ได้และ เมื่อได้รับข้อมูล **Password** ซึ่งเป็นข้อมูล **Default** ควรมีการแก้ไขทันทีเมื่อเข้าใช้งานระบบ ครั้ง แรก

- **การควบคุมการเข้าถึงระบบ** (System and Application Access Control)

เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาติ

1) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

- ต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน ลบ ได้ เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้ งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

-บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น **Root** หรือ **Administrator** ต้องได้รับการพิจารณามอบหมาย

ให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึง อย่างเหมาะสมกับการทำงานเท่านั้น

-บุคคลภายนอก ต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้าน เทคโนโลยีสารสนเทศและการสื่อสาร (**ICT Security Policy**) ของบริษัทฯ อย่างเคร่งครัด ก่อนที่จะ ได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทฯ

2) ขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure log-on Procedure)

- ต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย โดยกำหนดให้ระบบปฏิเสธ การให้บริการ หากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน 3 ครั้ง

3) ระบบบริหารจัดการรหัสผ่าน (**Password Management System)**

- ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ ผู้ใช้งานระบบเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

4) การใช้โปรแกรมอรรถประโยชน์ (**Use of Privileged Utility Programs)**

-การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

- ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

  - ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
  - ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
  - จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
  - ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ เช่น ผู้ใช้งานระบบ เป็นต้น

5) การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (**Access Control to Program Source Code)**

- ผู้พัฒนาระบบสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึง **Source Code** ของระบบที่ใช้งานจริง หรือให้บริการ เช่น

  - ไม่ควรเก็บ **Source Code** ไว้ในเครื่องที่ใช้งานจริงและต้องเก็บ **Source Code** ไว้ในที่ที่ปลอดภัย
  - ต้องไม่เก็บ **Source Code** ที่อยู่ในระหว่างทำการทดสอบรวมไว้กับ **Source Code** ที่ใช้งานได้จริงแล้ว

## หมวด 4
## การเข้ารหัสลับข้อมูล

**<u>วัตถุประสงค์</u>**

เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และเพื่อป้องการความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ ซึ่งการเข้ารหัสลับรวมถึงข้อมูลระบบควบคุมการประชุม เช่น ข้อมูลการสนทนาและข้อมูลการลงคะแนนของระบบควบคุมการประชุม ทั้งการส่งข้อมูลและการจัดเก็บข้อมูล

**1) นโยบายการใช้มาตรการเข้ารหัสข้อมูล (**Policy on the Use of Cryptographic Controls)

-บริษัทฯ ต้องมีนโยบายการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่ เกี่ยวข้อง

**2) การบริหารจัดการกุญแจในการเข้ารหัสข้อมูล (**Key Management)

-นโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจต้องมีการจัดทำและปฏิบัติตามตลอดวงจรชีวิตของกุญแจโดยบริษัทฯ ควรมีการกำหนดมาตรการในการเก็บ **Key** ที่เป็นข้อมูลลับของแต่ละส่วนข้อมูล

## หมวด 5
## การสร้างความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

**<u>วัตถุประสงค์</u>**

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผล บังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ

**1) การรักษาความปลอดภัยทางกายภาพ**

บริษัทฯต้องกำหนดรายละเอียดของสถานที่และอุปกรณ์ที่จำเป็นต้องมีระบบการป้องกันการเสียหายและการควบคุมการเข้าออกในการรักษาความมั่นคงปลอดภัย อาทิ ห้องดาต้าเซ็นเตอร์ซึ่งเป็นพื้นที่ จัดเก็บเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ด้านเครือข่ายต้องมีระบบรักษาความปลอดภัยและมีการควบคุมการ เข้าถึงอย่างเข้มงวด โดยอนุญาตเฉพาะผู้รับผิดชอบเท่านั้น

**2) การรักษาความปลอดภัยของอุปกรณ์**

อุปกรณ์สำคัญที่ถูกจัดเก็บในห้องดาต้าเซ็นเตอร์ ต้องมีการจัดวางอย่างถูกต้องและมีการป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต การเดินสายเพื่อเชื่อมโยงระหว่างอุปกรณ์ต้องมีป้ายเพื่อบ่งบอกถึงตำแหน่งในการเชื่อมต่อกับอุปกรณ์ และมีการกำหนดแผนการบำรุงรักษาอุปกรณ์อย่างชัดเจนและต่อเนื่อง

## หมวด 6
## ความมั่นคงปลอดภัยสำหรับการดำเนินงาน

**<u>วัตถุประสงค์</u>**

เพื่อกำหนดให้การปฏิบัติงานกับอุปกรณ์ประมวลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

**1) ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ**

บริษัทฯ ต้องกำหนดขั้นตอนการปฏิบัติงานรวมถึงหน้าที่และความรับผิดชอบให้เป็นลายลักษณ์อักษร มีการจัดการการเปลี่ยนแปลงเมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมเกี่ยวกับระบบสารสนเทศโดยต้องมีเอกสารการร้องขอการเปลี่ยนแปลงและเอกสารบันทึกการเปลี่ยนแปลง มีการจัดการขีดความสามารถโดยการติดตามสภาพการใช้งานและการวางแผนการจัดการระบบสารสนเทศ มีการแยกเครื่องมือในการประมวลผลสารสนเทศในการพัฒนาทดสอบและสภาพแวดล้อมในการปฏิบัติงานเพื่อความมั่นคงปลอดภัยของข้อมูล

**2) การป้องกันโปรแกรมที่ไม่ประสงค์ดี**

บริษัทฯต้องจัดให้มีการติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมที่ไม่ประสงค์ดี รวมทั้งโปรแกรมเพื่อป้องกันช่องโหว่ของระบบปฏิบัติการสำหรับระบบงาน หรืออุปกรณ์ของบริษัทฯและกำหนดให้มีระเบียบและขั้นตอนวิธี ปฏิบัติที่เหมาะสม และสนับสนุนให้หน่วยงานภายในที่มีการใช้งานระบบผ่านเครือข่ายของบริษัทฯ ได้ยึดถือและปฏิบัติตาม

**3) การสำรองข้อมูล**

บริษัทฯต้องจัดให้มีการสำรองข้อมูลที่สำคัญโดยต้องกำหนดรูปแบบและวิธีปฏิบัติ รวมทั้งแผนการ สำรองข้อมูลที่เหมาะสมตามลำดับความสำคัญของสารสนเทศของบริษัทฯเพื่อป้องกันการสูญหายอันอาจจะ เกิดขึ้นจากภาวะคุมคาม หรือจากการเกิดภัยพิบัติ โดยต้องกำหนดให้มีผู้รับผิดชอบในการสำรองข้อมูลตามรูปแบบ และแผนการดำเนินการที่กำหนดไว้

**4) การเฝ้าระวังด้านความมั่นคงปลอดภัย**

บริษัทฯต้องมีการเฝ้าระวังระบบที่สำคัญ เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต การปฏิเสธการ ให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ ต้องให้มีการจัดเก็บ ข้อมูลจราจรบนเครือข่ายที่สอดคล้องกับข้อกำหนดตามพระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์ และ ต้องกำหนดขั้นตอนวิธีปฏิบัติในการติดตั้งเวลาของระบบคอมพิวเตอร์กลางให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาในกรณีเกิดเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ของบริษัทฯ

## หมวด 7
## ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

**<u>วัตถุประสงค์</u>**

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน และป้องกันการบุกรุก ผ่านระบบเครือข่ายจากผู้บุกรุกหรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือ การทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของบริษัทฯได้อย่างถูกต้อง การบริหารจัดการด้านการสื่อสารและเครือข่ายคอมพิวเตอร์สารสนเทศ (Communication and Operations Management) ได้กำหนดขึ้น

เพื่อให้การดำเนินงานที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านสารสนเทศ และอุปกรณ์ประมวลผลมีความถูกต้อง เหมาะสม และปลอดภัย ผู้ดูแลระบบและผู้ใช้บริการได้ตระหนักถึงหน้าที่ ความรับผิดชอบด้านการจัดการและการใช้ระบบคอมพิวเตอร์และเครือข่ายสารสนเทศ โดยให้มีส่วนร่วมในการ ช่วยกันป้องกันทรัพยากรและข้อมูลที่มีค่าบริษัทฯให้มีความลับ ความถูกต้อง และมีความ พร้อมใช้งานอยู่เสมอ

**1) การควบคุมการเข้าถึงระบบ**

บริษัทฯต้องมีนโยบายควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร และทบทวนตามระยะเวลาที่กำหนดไว้ โดยพิจารณาให้สอดคล้องกับภารกิจของบริษัทฯ และความมั่นคงปลอดภัย ในการเข้าถึงสินทรัพย์สารสนเทศ

**2) การจัดการการเข้าถึงของผู้ใช้**

บริษัทฯต้องมีการกำหนดมาตรการและแนวปฏิบัติอย่างเป็นระบบเพื่อใช้ในการกำหนดรหัสบัญชีผู้ใช้ สำหรับบุคลากรการจัดการสิทธิในการเข้าใช้ระบบสารสนเทศ การจัดการรหัสผ่าน รวมถึงทบทวนสิทธิการเข้าถึง ของผู้ใช้

**3) หน้าที่ความรับผิดชอบของผู้ใช้งาน**

เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต ผู้ใช้งานต้องให้ความร่วมมือในการปฏิบัติตามมาตรการด้านการ รักษาความปลอดภัยในการเข้าถึงอย่างเคร่งครัด

**4) การควบคุมการเข้าถึงเครือข่าย**

การเข้าถึงเครือข่ายจากภายในบริษัทฯ หรือ การเชื่อมต่อจากภายนอกต้องมีมาตรการควบคุมที่ชัดเจน ต้องผ่านการพิสูจน์ตัวตน และ ตรวจสอบสิทธิตามขั้นตอนอย่างมีประสิทธิภาพ โดยระบบต้องยอมให้เฉพาะผู้ใช้งานที่ ได้รับอนุญาตผ่านเข้าสู่เครือข่าย และใช้บริการได้ตามสิทธิที่กำหนดให้เท่านั้น

**5) การควบคุมการใช้งานระบบสารสนเทศ**

การเข้าถึงระบบสารสนเทศต้องมีการควบคุมการใช้งานสารสนเทศ ซึ่งได้แก่ มีการกำหนดสิทธิในการใช้ งานระบบสารสนเทศ อาทิ เขียน อ่าน ลบ ได้ มีการกำหนดกลุ่มของผู้ใช้ตามความจำเป็นในการปฏิบัติงานได้ มีการ แยกการติดตั้งระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูงไว้ในบริเวณเครือข่ายที่ปลอดภัย

## หมวด 8
## การจัดหาพัฒนาและบำรุงรักษาระบบสารสนเทศ

<u>วัตถุประสงค์</u>

การจัดหาการพัฒนาและการบำรุงรักษาระบบสารสนเทศ ( Information system acquisition, development and maintenance) เป็นหมวดที่กำหนดขึ้นเพื่อให้การพัฒนาและการบำรุงระบบสารสนเทศ ดำเนินการได้โดยสอดคล้องกับนโยบายความมั่นคงปลอดภัยและเพื่อให้เกิดความถูกต้องสมบูรณ์ของข้อมูลในระบบสารสนเทศของบริษัทฯ

**1) ข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศ**

การจัดหาและการพัฒนาระบบสารสนเทศใหม่ หรือ การปรับปรุงจากระบบที่มีอยู่เดิม ต้องมีการวิเคราะห์ และระบุข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศ

**2) การตรวจสอบการประมวลผล**

ระบบสารสนเทศที่พัฒนาขึ้นต้องผ่านการตรวจสอบการประมวลผลทั้งส่วนข้อมูลนำเข้า และผลลัพธ์จากการประมวลผล รวมทั้งต้องมีกลไกในการตรวจจับข้อผิดพลาดและบันทึกไว้เพื่อการตรวจสอบและแก้ไข

**3) การสร้างความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ**

ระบบที่ให้บริการต้องมีการควบคุมการติดตั้งซอฟต์แวร์(software)ลงไปยังระบบที่ให้บริการ มีการป้องกันข้อมูลที่ใช้สำหรับการทดสอบและมีการควบคุมการเข้าถึงซอร์สโค้ด(source code)ของระบบ

**4) การสร้างความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบ**

ในการพัฒนาระบบสารสนเทศต้องมีการกำหนดขั้นตอนวิธีปฏิบัติอย่างเป็นทางการเพื่อใช้ควบคุมการเปลี่ยนแปลงหรือแก้ไข และ

ต้องมีการตรวจสอบการทำงานหลังจากเปลี่ยนแปลงนั้นๆ

**5) การจัดการช่องโหว่ในฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software)**

ฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ต้องได้รับการดูแลอย่างสม่ำเสมอเพื่อให้สามารถทำงานได้เป็นปกติ และต้องมี การปรับปรุงเพื่อปิดช่องโหว่อย่างเหมาะสมตามแนวปฏิบัติที่ได้ผ่านการทดสอบแล้ว

## หมวด 9
## การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

**<u>วัตถุประสงค์</u>**

การดำเนินการกับสถานการณ์ด้านความมั่นคงปลอดภัย (Information security incident management) กำหนดขึ้นเพื่อให้มีระบบการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย และใช้เป็น เครื่องมือที่ช่วยในการตรวจสอบและปรับปรุงแก้ไขระบบให้มีประสิทธิภาพมากยิ่งขึ้น

**หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ**

บริษัทฯ ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยโดยขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระเบียบที่ดี

**การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย**

ผู้ใช้งาน และ บุคคลภายนอก ทุกคนมีหน้าที่ต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัทฯ ให้กับผู้จัดการด้านความปลอดภัยสาระสนเทศ โดยห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยด้วยตกเอง และไม่กระทำการอื่นๆ ที่ถือเป็นข้อห้ามของบริษัทฯ เช่น ที่กฎหมายบัญญัติว่าเป็นความผิด

**การจัดการและแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย**

เมื่อได้รับรายงานเหตุการณ์ผิดปกติ หรือจุดอ่อนด้านความมั่นคงปลอดภัยแล้ว ต้องมีการวิเคราะห์และ ตรวจสอบเพื่อค้นหาที่มาของความผิดปกติ และดำเนินการหาวิธีที่จะใช้ในการป้องกันปัญหาที่อาจจะเกิดขึ้นในอนาคตโดยบริษัทฯควรกำหนดขั้นตอนการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัย อาทิ

- ความล้มเหลวของระบบสารสนเทศ
- ผลกระทบจากซอฟต์แวร์ที่ไม่ประสงค์ดี
- การปฏิเสธการให้บริการ
- การละเมิดความลับและความถูกต้องสมบูรณ์
- การใช้ระบบสารสนเทศผิดวัตถุประสงค์

**การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย**

ผู้จัดการด้านความปลอดภัยสาระสนเทศต้องรวบรวม บันทึก และจัดเก็บ เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้น

และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า รวมถึงจัดเก็บหลักฐานตามกฎ หรือ หลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางศาล หากมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

## หมวด 10

## การบริหารความต่อเนื่องของการดำเนินภารกิจของบริษัท

**<u>วัตถุประสงค์</u>**

การบริหารความต่อเนื่องของการดำเนินภารกิจของบริษัทฯกำหนดขึ้นเพื่อมิให้การดำเนินงานตามภารกิจของบริษัทฯเกิดการติดขัดหรือหยุดชะงัก และป้องกันมิให้การปฏิบัติงานตามภารกิจที่สำคัญของบริษัทฯต้องได้รับผลกระทบ หรือเกิดความเสียหายรุนแรง อันเนื่องจากความผิดพลาดของระบบสารสนเทศ และเพื่อให้ มั่นใจได้ว่าสามารถกู้ระบบคืนได้ในระยะเวลาที่เหมาะสม

**1) กระบวนการวางแผน**

เพื่อให้การดำเนินงานของบริษัทฯเป็นไปอย่างต่อเนื่องนั้น ต้องพิจารณาและให้ความสำคัญกับประเด็น ดังต่อไปนี้

- การจัดลำดับความสำคัญของระบบสารสนเทศ
- การจัดลำดับความสำคัญของผู้ใช้งานหลัก หรือ บริเวณที่ผู้ใช้ปฏิบัติงาน
- ข้อตกลงที่เกี่ยวกับลำดับความเร่งด่วนของการแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย
- การจัดทำเอกสารคู่มือและแผนการดำเนินการ หลังเกิดเหตุการณ์ความเสียหาย

**2) กรอบการวางแผน**

ในการกำหนดแผนการแก้ไขเหตุการณ์ความเสียหายต้องพิจารณาถึงระดับความสำคัญและลำดับก่อนหลังของการจัดการในประเด็นต่างๆอันได้แก่

- ความสูญเสียที่เกิดขึ้นกับพื้นที่ที่ใช้งานหลักภายในอาคาร
- ความสูญเสียที่เกิดขึ้นกับอาคารหลัก
- ความสูญเสียที่เกิดขึ้นกับพื้นที่ปฏิบัติงานหลัก
- ความสูญเสียที่เกิดขึ้นกับส่วนของระบบเครือข่ายหลัก

**3) ความสูญเสียที่เกิดขึ้นกับระบบปฏิบัติการของคอมพิวเตอร์**

<u>ความสูญเสียที่เกิดขึ้นกับบุคลากรหลัก</u>

ในการจัดทำแผนการแก้ไขเหตุการณ์ความเสียหายต้องระบุรายละเอียดในประเด็นดังต่อไปนี้

- ขั้นตอนการปฏิบัติการฉุกเฉินต้องครอบคลุมวิธีปฏิบัติงานที่สามารถดำเนินการได้อย่างฉับไวทันทีเพื่อการแก้ไขและควบคุมสถานการณ์ที่เกิดขึ้น
- กระบวนการทดสอบที่จำเป็นต้องดำเนินการเพื่อให้เกิดความมั่นใจว่าแผนการแก้ไขเหตุการณ์ที่จัดทำไว้นั้นสามารถดำเนินการได้จริง

**4) การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ**

(Implement information security continuity)

- บริษัทฯ ต้องจัดตั้ง ISM บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ ของระบบเทคโนโลยีสารสนเทศ ซึ่งประกอบ
- ISM บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ ต้องจัดทำแผนรองรับ เหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ ที่เป็นลายลักษณ์อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละหนึ่ง1 ครั้ง โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการจัดทำแผนการบริหารความ ต่อเนื่องให้กับธุรกิจ (Business Continuity Plans Development and Execution Procedure)

**5) การตรวจสอบ ทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ**

(Verify, Review and Evaluate information security continuity)

- ISM บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ ต้องกำหนดเวลาการ ทดสอบแผน กำหนดการทดสอบแผนฉุกเฉินที่ชัดเจนรวมถึงกำหนดระยะเวลาที่ใช้ในการทดสอบตั้งแต่เริ่มต้นจนสิ้นสุดกระบวนการทดสอบ
- ISM บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ ต้องกำหนดเหตุการณ์ จำลองที่จะใช้ทดสอบและรายละเอียดในการกำหนดรายละเอียดของเหตุการณ์ จำลอง ควรระบุวัตถุประสงค์ ขอบเขตของระบบงาน หรือกระบวนการทำงานที่เกี่ยวข้องกับการทดสอบแผนทั้งหมดรวมถึงการกำหนดขั้นตอนการทดสอบแผนฉุกเฉิน
- ISM บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ ต้องกำหนดทรัพยากรต่างๆ ที่ใช้ในการทดสอบแผนฉุกเฉินกำหนดผู้รับผิดชอบที่จะทำหน้าที่ควบคุม ประสานงาน และรับผิดชอบในการจัดการทดสอบแผนฉุกเฉิน รวมถึงสถานที่ และอุปกรณ์เครื่องมือต่างๆ และงบประมาณที่ต้องใช้ด้วย
- ISM บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ ต้องกำหนดแผนงาน แนวทาง และระยะเวลาในการทบทวนและปรับปรุงแผนอย่างชัดเจน เพื่อให้แผน นั้นมีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน

**6) การเตรียมอุปกรณ์ประมวลผลสำรอง** (Redundancies)

เพื่อจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ

- สภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนทศ (Availability of information processing facilities) อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอ เพื่อให้ตรงตาม ความต้องการด้านสภาพความพร้อมใช้ที่กำหนด

## หมวด 11

## การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิด

## นโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน (Compliance)

**<u>วัตถุประสงค์</u>**

กำหนดขึ้นเพื่อให้มั่นใจว่าบุคลากรของบริษัทฯรับทราบ และปฏิบัติตามนโยบาย กฎ ระเบียบ ข้อบังคับ รวมทั้งกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ

**1) การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย**

บริษัทฯต้องศึกษาและกำหนดรายการของนโยบาย กฎ ระเบียบ ข้อบังคับ กฎหมาย หรือ สัญญาที่ เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เพื่อให้บุคลากรได้รับทราบทำความเข้าใจ และปฏิบัติตามได้อย่างเคร่งครัด

**2) การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง** (Compliance with Legal and Contractual Requirements)

เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับ รวมทั้งสัญญาต่าง ๆ

- การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

  - บริษัทฯต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือ สัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน
  - เจ้าหน้าที่บริษัทฯ ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตาม รายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยี สารสนเทศและการสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการตรวจสอบกับกฎหมาย IT (W IT CL 02) และมีรายการดังต่อไปนี้เป็นอย่างน้อย
    - นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
    - พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
    - พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
    - พ.ร.ฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์
    - พ.ร.บความมั่นคงปลอดภัยไซเบอร์
    - พ.ร.บคุ้มครองข้อมูลส่วนบุคคล
    - พ.ร.บ. ลิขสิทธิ

  รวมถึงกฎหมาย ระเบียบข้อบังคับอื่นที่เกี่ยวข้องซึ่งใช้บังคับอยู่แล้วในขณะนี้และที่จะได้ออกใช้บังคับต่อไปในภายหน้า

- ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัทฯ ถือเป็น สินทรัพย์ของบริษัทฯ (ยกเว้น ข้อมูลที่เป็นสินทรัพย์ของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร

หรือลิขสิทธิของบุคคลภายนอก) ทั้งนี้บริษัทฯ สามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่างๆตามกฎหมายโดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

- เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ และขอสงวนสิทธิในการตรวจสอบการใช้งานเครื่องคอมพิเตอร์ ระบบ คอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่างๆของบริษัทฯ กำหนดไว้

- บริษัทฯขอสงวนสิทธิในการเข้าถึง ทบทวน และตรวจสอบอีเมลของผู้ใช้งาน โดยไม่จำเป็นต้อง แจ้งให้ทราบล่วงหน้า อย่างไรก็ตามบริษัทฯ จะดำเนินการตรวจสอบดังกล่าวต่อเมื่อมีความ จำเป็นเท่านั้น และจะไม่เปิดเผยข้อมูลใดๆ ของผู้ใช้งาน เว้นแต่เป็นการเปิดเผยตามคำสั่งศาลตามบทบังคับของกฎหมายหรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น

- ห้ามเจ้าหน้าที่บริษัทฯใช้งานสินทรัพย์และระบบเทคโนโลยีสารสนเทศของบริษัทฯ กระทำ การใดๆที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม

- การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใดๆ ออกนอกประเทศ ไม่ขัดต่อ ข้อกฎหมายใดๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ผู้ใช้งานต้อง ปรึกษาผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

**3) การทบทวนความมั่นคงปลอดภัยสารสนเทศ** (Information Security Reviews)

เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ อย่างสอดคล้องกับนโยบายและขั้นตอน ปฏิบัติขององค์กร

- การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)
  - ISM ต้องมีการทบทวน วิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติ ขององค์กร เช่น ทบทวนวัตถุประสงค์ มาตรการ นโยบาย วิธีปฏิบัติงานต่างๆ ให้ถูกต้องและเป็นปัจจุบัน ตามรอบระยะเวลาที่กำหนด เช่น ปีละ 1 ครั้ง หรือทบทวนเมื่อมีการเปลี่ยนแปลง
- การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน (Compliance with Security Policy and Standards)
  - ISMต้องจัดให้มีการตรวจสอบระบบทั้งหมดของหน่วยงานตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและระยะเวลาที่กำหนดไว้
  - ISMต้องมีการตรวจสอบและทบทวนเอกสารนโยบายมาตรการวิธีการปฏิบัติงานรวมถึงแบบฟอร์มที่เกี่ยวเนื่องกันตามระยะเวลาที่กำหนดหรือเมื่อเปลี่ยนแปลง
- การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)
  - ISM ต้องจัดให้มีการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งาน หรือให้บริการอยู่แล้วตาม ระยะเวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่า ระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และ ทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบด้วย

## หมวด 12

## การกำหนดผู้รับผิดชอบ

**<u>วัตถุประสงค์</u>**

การกำหนดผู้รับผิดชอบ กำหนดขึ้นเพื่อ กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรือ อันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตาม แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

**1) การกำหนดผู้รับผิดชอบ**

ผู้จัดการด้านความปลอดภัยสารสนเทศ (ISM) มีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงาน และ เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศ รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติงานอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ ความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัย ของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการ

**2) การฝ่าฝืนระเบียบและการพิจารณาโทษ**

- บริษัทฯจะไม่รับผิดชอบต่อผลของการกระทำที่เกิดขึ้นจากผู้ใช้งานและ /หรือบัญชีของผู้ใช้
- ผู้ใช้งานที่ฝ่าฝืนระเบียบการใช้งานเครือข่ายระบบเทคโนโลยีสารสนเทศของบริษัทฯจะถูกพิจารณาระงับและ/หรือยกเลิกบัญชีผู้ใช้งาน
- เจ้าหน้าที่สารสนเทศจะแจ้งหน่วยงานต้นสังกัดและผู้บริหารบริษัทฯ เพื่อ พิจารณาโทษแก่ผู้ใช้งานที่ฝ่าฝืนระเบียบตามความเหมาะสม

## หมวด 13

## การบริหารจัดการความเสี่ยงด้านความมั่งคงปลอดภัยไซเบอร์

**<u>วัตถุประสงค์</u>**

เพื่อแสดงถึงการยอมรับความเสี่ยงและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์โดยบริษัทฯใช้วิธีการที่สอดคล้องกันในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยรวมถึงมีมาตรการรักษาความมั่นคงปลอดภัยเพื่อปกป้องข้อมูลซึ่งสอดคล้องกับกระบวนการในการระบุและประเมินความเสี่ยง (Risks Identification and Assessment)

- วิธีการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัย (Security Risk Management Methodology)
- การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Management of Cyber Security Incident)
- การบริหารความเสี่ยงกับบุคคลภายนอก (Risk Management with External Parties)

- การกำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Incident response plan) อย่างเป็นลายลักษณ์อักษร และประเมินเหตุการณ์หรือจุดอ่อนของการรักษาความปลอดภัยระบบสารสนเทศ เพื่อพิจารณาระดับความรุนแรงของเหตุการณ์และผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ และต้องจัดให้มีการทดสอบกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

<u>การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ</u>

ต้องสอดคล้องกับนโยบายการบริหารจัดการความเสี่ยงของบริษัทฯและครอบคลุมในเรื่องดังต่อไปนี้

1. การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2. การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
3. การประเมินความเสี่ยง ที่ครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยงและผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง
4. การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้
5. การกำหนดตัวชี้วัดระดับความเสี่ยงรวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดดังกล่าวต่อผู้ที่มีหน้าที่รับผิดชอบเพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

# นโยบายคุ้มครองข้อมูลส่วนบุคคล

**<u>วัตถุประสงค์</u>**

**ขอบเขตของนโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ**

นโยบายคุ้มครองข้อมูลส่วนบุคคลนี้ให้รวมถึงบริการอื่นๆ ทั้งนี้อาจมีการแสดงข้อกำหนดซึ่งเกี่ยวข้องกับนโยบายคุ้มครองข้อมูลส่วนบุคคลเพิ่มเติมในบริการของบริษัทฯ บริษัทฯอาจดำเนินการปรับปรุงหรือแก้ไขนโยบายคุ้มครองข้อมูลส่วนบุคคลเพื่อให้สอดคล้องกับแนวทางการให้บริการและหลักเกณฑ์ของกฎหมายที่มีการเปลี่ยนแปลงไป โดยอาจไม่ได้แจ้งหรือบอกกล่าวให้ทราบล่วงหน้า นโยบายคุ้มครองข้อมูลส่วนบุคคลนี้ยังบังคับใช้กับการใช้บริการทางสื่ออิเล็กทรอนิกส์ ตลอดจน แอปพลิเคชัน (Application) และระบบโปรแกรม (Program) ที่เกี่ยวข้องกับการให้บริการของบริษัทฯ ทั้งที่มีอยู่ในปัจจุบันและที่บริษัทฯอาจจะได้พัฒนาหรือจัดให้มีขึ้นในอนาคต

**การเก็บรวบรวมข้อมูลส่วนบุคคล**

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้กระทำภายใต้วัตถุประสงค์ และเพียงเท่าที่จำเป็นตามกรอบวัตถุประสงค์อันชอบด้วยกฎหมายหรือเพื่อประโยชน์ที่มีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์ในการเก็บรวบรวม โดยต้องแจ้งให้เจ้าของข้อมูลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลดังนี้

- วัตถุประสงค์การเก็บข้อมูล
- ข้อมูลส่วนบุคคลที่ทำการเก็บ
- กรณีที่เจ้าของข้อมูลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายโดยต้องแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบด้วย
- ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจถูกเปิดเผย
- สิทธิของเจ้าของข้อมูล
- เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเมื่อใดก็ได้ ถ้าไม่มีข้อจำกัดสิทธิ

**การใช้งานข้อมูลส่วนบุคคล**

บริษัทฯจะใช้ข้อมูลส่วนบุคคลของท่านในการให้บริการของบริษัทฯตามวัตถุประสงค์ของท่าน และข้อผูกพันตามสัญญาที่เกิดขึ้น เพื่อให้เป็นไปตามกฎหมาย หลักเกณฑ์ และระเบียบต่างๆ ที่เกี่ยวข้อง และเพิ่มประสิทธิภาพในการให้บริการรวมถึงการโฆษณาประชาสัมพันธ์กิจกรรมทางการตลาด ตลอดจนให้คำแนะนำที่เหมาะสมเพื่อให้บริการต่างๆตรงกับความต้องการของท่านหรือตามที่เห็นว่าจะเป็นประโยชน์แก่ท่านในการที่จะได้รับข้อเสนอบริการต่างๆจากบริษัทฯ

**การเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลภายนอก**

บริษัทฯอาจเปิดเผยข้อมูลส่วนบุคคลของท่านแก่ผู้ที่เกี่ยวข้องเพื่อการประกอบธุรกิจและให้บริการ เช่น คู่ค้า ผู้ให้บริการ ผู้ว่าจ้าง หรือตามคำสั่งของหน่วยงานของรัฐที่เกี่ยวข้องหรือตามที่กฎหมายกำหนด

**มาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล**

บริษัทฯใช้ระบบการจัดเก็บข้อมูลส่วนบุคคลและระบบรักษาความปลอดภัยของข้อมูลที่มีมาตรฐานทั้งในด้านเทคโนโลยีและกระบวนการเพื่อให้มั่นใจได้ว่าข้อมูลของท่านจะมีความปลอดภัย อีกทั้งบริษัทฯ ได้จำกัดสิทธิการเข้าถึงข้อมูลส่วนบุคคลของท่าน เพื่อป้องกันไม่ให้ข้อมูลส่วนบุคคลของท่านถูกนำไปใช้ เปิดเผย ทำลาย หรือเข้าถึงโดยไม่ได้รับอนุญาต เพื่อไม่ให้มี การเปลี่ยนแปลงแก้ไขหรือมีบุคคลอื่นใดเข้าถึงข้อมูลนั้นได้โดยมิชอบ อย่างไรก็ตามแม้ว่าบริษัทฯ จะมีมาตรฐานเทคโนโลยีและวิธีการรักษาความปลอดภัยเพื่อช่วยมิให้มีการเข้าสู่ข้อมูลส่วนบุคคลของท่าน ท่านก็ยังคงต้องปกป้องข้อมูลส่วนตัวของตัวท่านเองให้มีความปลอดภัยด้วย โดยปฏิบัติตามคำแนะนำเรื่องความปลอดภัยของข้อมูลส่วนบุคคลในการทำธุรกรรมผ่านสื่ออิเล็กทรอนิกส์ ดังนั้นบริษัทฯจึงขอสงวนสิทธิที่จะปฏิเสธความรับผิดในความเสียหายหรือสูญหายใดๆที่เกิดขึ้นในทุกกรณี

**สิทธิของเจ้าของข้อมูลส่วนบุคคล**

1. สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตน หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลที่ตนไม่ได้ให้ความยินยอมโดยบริษัทฯ ต้องดำเนินการตามคำขอภายใน 30 วันนับแต่วันที่ได้รับคำขอ
2. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลของตนตามที่กฎหมายกำหนด
3. สิทธิขอรับหรือขอให้ส่งหรือโอนย้ายข้อมูลส่วนบุคคลของตนไปยังบุคคลอื่นเพื่อวัตถุประสงค์ของตนเอง เมื่อบริษัทฯ สามารถทำได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ
4. สิทธิขอลบข้อมูลส่วนบุคคลของตนออกจากระบบ หรือขอให้ทำลาย หรือการระงับใช้ หรือการทำให้ข้อมูลส่วนบุคคลของตนเป็นข้อมูลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ เว้นแต่กรณีที่บริษัทฯ ต้องปฏิบัติตามกฎหมายที่เกี่ยวข้องในการเก็บรักษาข้อมูลดังกล่าว

5. สิทธิขอแก้ไขข้อมูลส่วนบุคคลของตนถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด
6. สิทธิในการถอนความยินยอมที่เคยให้ไว้ หรือไม่อนุญาตให้นำข้อมูลส่วนบุคคลไปเก็บรวบรวม ใช้ เปิดเผยเว้นแต่ได้รับยกเว้นตามที่กฎหมายกำหนด
7. สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคลตามที่กฎหมาย

**การทบทวนนโยบายฯ**

บริษัทฯจะทบทวนนโยบายปีละ 1 ครั้ง หรือ กรณีที่กฎหมายมีการเปลี่ยนแปลงแก้ไข

**การบังคับใช้นโยบายคุ้มครองข้อมูลส่วนบุคคล**

ท่านตกลงและรับทราบว่า นโยบายคุ้มครองข้อมูลส่วนบุคคลนี้มีผลบังคับใช้กับข้อมูลส่วนบุคคลของท่านทั้งหมดโดยทันที

**กฎหมายที่ใช้บังคับ**

นโยบายคุ้มครองข้อมูลส่วนบุคคลนี้อยู่ภายใต้การบังคับและตีความตามกฎหมายไทย และศาลไทยเป็นผู้มีอำนาจในการพิจารณาข้อพิพาทใดที่อาจเกิดขึ้น

**การติดต่อบริษัทฯ**

หากผู้ใช้บริการมีคำถามเกี่ยวกับนโยบายคุ้มครองข้อมูลส่วนบุคคลรวมถึงคำขอใดที่จะใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล โปรดแจ้งความประสงค์ ทางอีเมล์ ตามที่อยู่ หรือทางโทรศัพท์ รายละเอียด ดังนี้

**บริษัท โคโนวานซ์ จำกัด**

ที่อยู่ : 32/625 ซอยนวมินทร์135 แขวงนวลจันทร์ เขตบึงกุ่ม กรุงเทพมหานคร-10230

โทรศัพท์: 082-979-4978

E-mail: contact@conovance.com