

บริษัท โพรเอ็น คอร์ป จำกัด (มหาชน)

นโยบายการกำกับดูแล การบริหารจัดการ และรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท โพรเอ็น คอร์ป จำกัด (มหาชน) เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและจากการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่ บริษัท โพรเอ็น คอร์ป จำกัด (มหาชน) และบริษัทย่อย และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และกฎหมายอื่นที่เกี่ยวข้องได้ บริษัท โพรเอ็น คอร์ป จำกัด (มหาชน) จึงเห็นสมควรกำหนดนโยบายการกำกับดูแล การบริหารจัดการ และรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังต่อไปนี้

1. ประกาศนี้เรียกว่า “ประกาศ บริษัท โพรเอ็น คอร์ป จำกัด (มหาชน) เรื่อง นโยบายการกำกับดูแล การบริหารจัดการ และรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ”
2. บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือขัดแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน
3. นโยบายการกำกับดูแล การบริหารจัดการ และรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ของ บริษัท โพรเอ็น คอร์ป จำกัด (มหาชน) มีวัตถุประสงค์ดังต่อไปนี้
 - 3.1 เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของ บริษัท โพรเอ็น คอร์ป จำกัด (มหาชน) ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล
 - 3.2 เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับใน บริษัท โพรเอ็น คอร์ป จำกัด (มหาชน) และบริษัทย่อย ได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด
 - 3.3 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีการปฏิบัติให้ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับ บริษัท โพรเอ็น คอร์ป จำกัด (มหาชน) และบริษัทย่อย ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านด้านสารสนเทศของ บริษัท โพรเอ็น คอร์ป จำกัด (มหาชน) และบริษัทย่อย ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะทบทวนนโยบายปีละ 1 ครั้ง
4. นโยบายการกำกับดูแล การบริหารจัดการ และรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ของ บริษัท โพรเอ็น คอร์ป จำกัด (มหาชน) กำหนดประเด็นสำคัญ ดังต่อไปนี้
 - 4.1 การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ
 - 4.1.1 การควบคุมการเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล ที่คำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ โดยมีข้อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง และสิทธิในการใช้งาน เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
 - 4.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและ ป้องกันการเข้าถึงจากผู้ไม่ได้รับอนุญาต ต้องลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนด



รหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่ได้รับอนุญาตเท่านั้นที่จะสามารถเข้าใช้งานระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ตลอดจนบริหารจัดการสิทธิในการเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับ ต้องทบทวนสิทธิในการใช้งานและตรวจสอบการละเมิดความปลอดภัยอย่างสม่ำเสมอ

4.1.3 การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิในการเข้าถึงเครือข่ายให้ผู้ที่เข้าใช้งาน และต้องพิสูจน์ยืนยันตัวตน (Authentication) ของผู้ใช้งานก่อนเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยตามที่ บริษัท โปรเอ็น คอร์ป จำกัด (มหาชน) จัดสรรไว้ และออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อให้การควบคุมและป้องกันภัยคุกคามเป็นไปอย่างมีระบบและมีประสิทธิภาพ

4.1.4 การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิให้ผู้ที่เข้าใช้งาน และต้องพิสูจน์ยืนยันตัวตน (Authentication) ของผู้ใช้งานก่อนเข้าใช้งาน ต้องระงับการใช้งานเมื่อผู้ใช้งานไม่ใช้งานอย่างต่อเนื่องตามระยะเวลาที่กำหนด เพื่อจำกัดเวลาในการเชื่อมต่อระบบสารสนเทศ (Session Time-Out) กำหนดมาตรการในการใช้งานโปรแกรมมัลแวร์ประเภทต่างๆ เพื่อไม่ให้ละเมิดลิขสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดี

4.1.5 การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิการเข้าถึงระบบ

4.1.6 เทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่างๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (Email) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่างๆ โดยต้องให้สิทธิเพื่อการปฏิบัติงานในหน้าที่เท่านั้น และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

4.2 การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานโดยคัดเลือกระบบสารสนเทศที่สำคัญเรียงลำดับความจำเป็นจากมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมในกรณีฉุกเฉินหรือในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์อย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

4.3 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดการตรวจสอบภายในของหน่วยงาน (Internal Audit) หรือการตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Audit) อย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติและต่อเนื่อง

5. ต้องกำหนดการแบ่งประเภทและลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

6. ผู้บริหารระดับสูงของ บริษัท โปรเอ็น คอร์ป จำกัด (มหาชน) มีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศ ให้การสนับสนุนและกำหนดทิศทางการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่ชัดเจน รวมทั้งมีการ



มอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใดๆ

7. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นไปตามแนวปฏิบัติตามระเบียบคู่มือปฏิบัติงาน
8. นโยบายการกำกับดูแล การบริหารจัดการ ได้ผ่านการทบทวนและเห็นชอบจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 1/2568 วันที่ 25 กุมภาพันธ์ 2568 และให้มีผลใช้บังคับตั้งแต่วันที่ 26 กุมภาพันธ์ 2568 เป็นต้นไป



(นายกิตติพันธ์ ศรีบัวเอี่ยม)
ประธานเจ้าหน้าที่บริหาร

