

## นโยบายและแนวปฏิบัติด้านการใช้เทคโนโลยีสารสนเทศ การสื่อสาร และการรักษาความปลอดภัยของสารสนเทศ

คณะกรรมการบริษัทกำหนดกรอบการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่สอดคล้องกับความต้องการของกิจการ รวมทั้งดูแลให้มีการนำเทคโนโลยีสารสนเทศมาใช้ในการเพิ่มโอกาสทางธุรกิจและพัฒนาการดำเนินงาน การบริหารความเสี่ยง เพื่อให้กิจการสามารถบรรลุวัตถุประสงค์และเป้าหมายหลักของกิจการ

### แนวปฏิบัติ

1. การใช้งานระบบสารสนเทศของบริษัทต้องเป็นไปเพื่อการดำเนินธุรกิจของบริษัทเท่านั้น ซึ่งระบบสารสนเทศถือเป็นทรัพย์สินของบริษัท ผู้ใช้มีอาชญากรรมความเป็นส่วนตัว (Privacy) ได้ และต้องหลีกเลี่ยงการใช้ระบบสารสนเทศที่ไม่เกี่ยวข้องกับงานของบริษัท
2. บุคลากรของบริษัทต้องปฏิบัติตามนโยบายความปลอดภัยสารสนเทศ (Information Security Policy) และมาตรฐานความปลอดภัยสารสนเทศ (Information Security Standard) ตลอดจนกฎหมายระเบียบ ข้อบังคับ นโยบายต่างๆ ที่เกี่ยวข้องอย่างเคร่งครัด
3. บริษัทส่งเสริมให้บุคลากรของบริษัทใช้สื่ออินเทอร์เน็ตเพื่อประโยชน์ในการทำงาน บุคลากรของบริษัทต้องใช้สื่ออินเทอร์เน็ตและระบบคอมพิวเตอร์เท่าที่จำเป็นและเป็นประโยชน์ต่อการทำงาน ไม่กระทำการในทางที่จะก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์และอินเทอร์เน็ตของบริษัท ไม่กระทำการที่เป็นการรบกวนระบบคอมพิวเตอร์และอินเทอร์เน็ตของผู้อื่นในสำนักงาน ไม่ใช้ระบบคอมพิวเตอร์ของบริษัทเผยแพร่ข้อมูลที่ไม่เหมาะสมในทางศีลธรรม ขนบธรรมเนียม และจารีตประเพณี หรือละเมิดกฎหมาย เช่น การสร้างความเสียหายแก่ชื่อเสียงและทรัพย์สิน การมีไว้ซึ่งสื่อลามกอนาจาร การ Forward mail ที่เป็นการรบกวน สร้างความรำคาญหรือที่เป็นการโฆษณาสินค้าธุรกิจและบริการ นอกเหนือจากสินค้าและบริการของบริษัท และการส่ง Spam mail เป็นต้น
4. เจ้าของข้อมูลสารสนเทศต้องกำหนดระดับชั้นความลับสารสนเทศให้เหมาะสมกับข้อมูลที่ได้อ้างอิงข้อมูลจากมาตรฐานความปลอดภัยสารสนเทศ (Information Security Standard) โดยในการจัดแบ่งระดับชั้นความลับ ให้พิจารณาถึงความจำเป็นที่ต้องปกป้องข้อมูลดังกล่าวในทางธุรกิจและผลกระทบหากข้อมูลรั่วไหลหรือถูกแก้ไข ข้อบังคับและกฎหมาย ข้อผูกมัดในสัญญา ทั้งนี้ระดับชั้นความลับสามารถเปลี่ยนแปลงได้โดยขึ้นอยู่กับการตัดสินใจของเจ้าของข้อมูลนั้น
5. บุคลากรของบริษัทที่พบเหตุฉุกเฉินซึ่งอาจกระทบการดำเนินธุรกิจและเสถียรภาพของระบบสารสนเทศ หรือพบเห็นช่องโหว่ (Vulnerability) ของระบบทั้งเชิงเทคนิคและการดำเนินงานหรือสิ่งนี้อาจสร้างความเสี่ยงให้กับบริษัทต้องแจ้งหน่วยงานที่รับผิดชอบดูแลโดยเร็ว

6. บุคลากรของบริษัทต้องใช้โปรแกรมคอมพิวเตอร์ที่มีลิขสิทธิ์ถูกต้อง หากจำเป็นต้องติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมเพื่อการปฏิบัติงาน ให้ติดต่อหน่วยงานที่ดูแลงานด้านเทคโนโลยีสารสนเทศของบริษัท ห้ามติดตั้ง และใช้งานโปรแกรมคอมพิวเตอร์ที่ลิขสิทธิ์ไม่ถูกต้องในสำนักงานโดยเด็ดขาด
7. บุคลากรของบริษัทต้องเก็บรักษารหัสผ่านสำหรับเข้าระบบคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ต่างๆ ของบริษัทเป็นความลับ เพื่อป้องกันไม่ใ้บุคคลอื่นเข้าถึงสารสนเทศของบริษัท
8. กรณีที่บริษัทอนุญาตให้มีการว่าจ้างลูกจ้างชั่วคราว นักศึกษาฝึกงาน ตลอดจนหน่วยงาน บริษัท ผู้ขาย คู่ค้า คู่สัญญา ที่ปรึกษาลูกค้าของบริษัท บุคคลที่มีใช้พนักงานของบริษัทเข้าใช้ระบบสารสนเทศของบริษัท ผู้บังคับบัญชาในสายงานต้องควบคุมการใช้ระบบสารสนเทศของบุคคลดังกล่าวให้เป็นไปตามกฎระเบียบ ข้อบังคับ นโยบายต่างๆ ของบริษัท และต้องรับผิดชอบต่อความเสียหายที่อาจจะเกิดขึ้นกับบริษัทจากการใช้ระบบสารสนเทศนั้น
9. บุคลากรของบริษัทต้องให้ความร่วมมือในการตรวจสอบ ควบคุม และการดำเนินการใดๆ เพื่อความปลอดภัยในการใช้ระบบสารสนเทศของบริษัท