นโยบายการรักษาความปลอดภัยให้กับระบบสารสนเทศขององค์กร ของบริษัท ไอที ซิตี้ จำกัด (มหาชน)

ด้วยบริษัท ไอที ซิตี้ จำกัด (มหาชน) ให้ความสำคัญกับการใช้คอมพิวเตอร์ และความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศจึงได้มีการปรับปรุงเนื้อหาระเบียบดังกล่าวอย่างต่อเนื่อง เพื่อเป็นแนวทางในการใช้งานที่เหมาะสมสอดคล้องกับเจตนารมณ์ของบริษัทและเพื่อให้สอดคล้องกับกฎหมายประกาศพระราชบัญญัติต่าง ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์และลักษณะการประกอบกิจการของบริษัทโดยให้ใช้ “ระเบียบการใช้คอมพิวเตอร์ และความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ”

ดังนั้น บริษัทจึงขอให้พนักงานทุกท่านปฏิบัติตามข้อกำหนดในระเบียบดังกล่าว อย่างเคร่งครัด โดยเฉพาะอย่างยิ่ง ในส่วนที่เกี่ยวกับการห้ามติดตั้งโปรแกรมอื่นนอกเหนือจากที่บริษัทได้จัดหาไว้ให้ รวมถึงห้ามกระทำการใด ๆ อันเป็นการละเมิดลิขสิทธิ์ของผู้อื่น

หมวดที่ 1

บททั่วไป

1.1 ระเบียบนี้จัดทำขึ้นสำหรับพนักงาน และ/หรือบุคคลอื่นที่บริษัทอนุญาตให้เข้าใช้งานคอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศของบริษัทเพื่อใช้ในการดำเนินงานที่เกี่ยวข้องกับกิจการของบริษัทเท่านั้น

1.2 ให้กรรมการผู้อำนวยการ หรือผู้บริหารที่มีหน้าที่ตามที่ได้รับมอบหมาย เป็นผู้กำหนดหลักเกณฑ์และวิธีการปฏิบัติเพิ่มเติมได้ตามความจำเป็น แต่ต้องไม่ขัดหรือแย้งกับระเบียบฉบับนี้

1.3 นิยาม

บริษัท	หมายถึง	บริษัท ไอที ซิตี้ จำกัด (มหาชน)
พ.ร.บ.	หมายถึง	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562
ข้อมูล	หมายถึง	สิ่งที่สื่อความหมาย หรือข้อความที่มีความหมายและมีความสำคัญที่มีค่าควรจะเก็บไว้เพื่อจะได้นำมาใช้ในโอกาสต่อไป ซึ่งอาจเป็นตัวอักษร ตัวเลข รูปภาพ หรือสัญลักษณ์ใด ๆ เช่น รายงาน บันทึก รูปแบบของโปรแกรม ชุดคำสั่งซอฟต์แวร์ เอกสารรายละเอียดการออกแบบ ระบบ ฐานข้อมูลต่าง ๆ แผนหรือกลยุทธ์ทางธุรกิจวิธีการ เทคนิค กรรมวิธี รายชื่อลูกค้า คู่ค้า สัญญาต่าง ๆ ใบเสนอราคา งบประมาณบริษัท งบประมาณโครงการ ประมาณการรายได้-รายจ่าย เป็นต้น หรือสิ่งที่สื่อความหมายอื่นใด ไม่ว่าการสื่อความหมายนั้นจะผ่านวิธีการใด และไม่ว่าจะจัดเก็บไว้ในรูปแบบใด

ข้อมูลคอมพิวเตอร์	หมายถึง	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
ข้อมูลอันเป็นความลับ	หมายถึง	ข้อมูลของบริษัท ข้อมูลของลูกค้า หรือข้อมูลของคู่ค้า ที่พนักงานได้รับทราบอันเนื่องจากการเป็นพนักงานของบริษัทหรือสามารถเข้าถึงในฐานะพนักงานของบริษัท
ระบบเทคโนโลยีสารสนเทศ	หมายถึง	ระบบงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ที่มาช่วยในการสร้างข้อมูลสารสนเทศ ให้สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา การควบคุม และการติดต่อสื่อสารซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ สื่อสังคมออนไลน์ ที่สามารถสื่อสารกันได้โดยผ่านเครือข่ายอินเทอร์เน็ต ฯลฯ
Instant Messaging Software	หมายถึง	โปรแกรมที่ใช้ติดต่อ โต้ตอบระหว่างบุคคลได้ทันทีผ่านระบบเครือข่าย เช่น Line, Facebook, Messenger, Whatsapp เป็นต้น
ระบบข้อมูล	หมายถึง	ระบบงานโปรแกรมคอมพิวเตอร์ของบริษัทที่ทำงานเกี่ยวข้องในการเก็บนำเข้า จัดการประมวลผลเผยแพร่ และแสดงผล ข้อมูลสารสนเทศ เพื่อสนับสนุนกลไกการทำงานของบริษัท
ระบบคอมพิวเตอร์	หมายถึง	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
ผู้ดูแลระบบ	หมายถึง	พนักงานที่มีหน้าที่รับผิดชอบในการดูแลรักษาคอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์ และ/หรือได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการพัฒนา แก้ไขดูแลระบบข้อมูลและโปรแกรมต่าง ๆ ที่ใช้งานอยู่ในบริษัท และ/หรือหน่วยงานอื่นใดที่มีหน้าที่รับผิดชอบในการดูแลคอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศโดยตรง

หมวดที่ 2

ข้อปฏิบัติการใช้งานคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศ

2.1 พนักงานต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่บริษัทได้ประกาศให้ทราบ รวมถึงปฏิบัติตามกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด ทั้งนี้ การใช้งานระบบเทคโนโลยีสารสนเทศที่นอกเหนือจากที่บริษัทจัดไว้ให้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบก่อน และหากพบว่ามีการใช้งานโดยไม่ได้รับอนุญาต ผู้ดูแลระบบสามารถตัดการใช้งานออกจากระบบเครือข่ายได้ทันที

2.2 การใช้งานคอมพิวเตอร์

(1) การ Login เข้าสู่ระบบคอมพิวเตอร์เครือข่ายของบริษัท พนักงานต้องใช้ Username ของตนเองในการ Login ทุกครั้ง โดย Password ให้ถือเป็นความลับ ห้ามเปิดเผยให้ผู้อื่นทราบโดยเด็ดขาด หรือ Login ให้ผู้อื่นใช้งาน หากเกิดความเสียหายใด ๆ ขึ้น ในระบบที่เกิดจากการใช้งานของ Username ใด พนักงานที่เป็นเจ้าของ Username นั้น ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น ทั้งนี้ การเปิดเผย Password ให้บุคคลอื่นทราบถือเป็นความผิดทางวินัยอย่างร้ายแรง

(2) พนักงานจะต้องไม่ใช้โปรแกรมคอมพิวเตอร์ เพื่อช่วยในการจำรหัสผ่านอัตโนมัติ

(3) พนักงานทุกคนต้องตั้งระบบการล็อกคอมพิวเตอร์อัตโนมัติหลังจากไม่ได้ใช้งานนานเกิน 15 นาที

(4) พนักงานไม่มีสิทธิในการแก้ไขกำหนดค่าต่าง ๆ (Configuration) คอมพิวเตอร์ด้วยตนเอง เช่น Computer Name IP Address ระดับสิทธิการเข้าถึง เป็นต้น

(5) พนักงานไม่มีสิทธิติดตั้ง แก้ไข ลบหรือถอดถอนโปรแกรมในคอมพิวเตอร์ด้วยตนเอง หากมีโปรแกรมที่จำเป็นเฉพาะทางให้ทำการร้องขอผ่านผู้มีอำนาจอนุมัติ และส่งคำขอดังกล่าวให้แผนกเทคโนโลยีสารสนเทศ (IT) เพื่อดำเนินการตามขั้นตอนต่อไป

(6) พนักงานมีสถานะเป็นผู้รับผิดชอบคอมพิวเตอร์ (ตามที่บริษัทได้ขึ้นทะเบียนไว้) และมีหน้าที่ระมัดระวังความปลอดภัยในการใช้คอมพิวเตอร์

(7) พนักงานพึงใช้คอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศของบริษัทอย่างมีประสิทธิภาพไม่ดาวน์โหลดและอัพโหลดข้อมูลหรือสิ่งอื่นใดที่ไม่เกี่ยวข้องกับงาน หรือกิจการของบริษัท

(8) อุปกรณ์คอมพิวเตอร์ ระบบเทคโนโลยีสารสนเทศและข้อมูลต่าง ๆ ให้ถือเป็นทรัพย์สินของบริษัท พนักงานไม่ควรใช้คอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศเพื่อประโยชน์ส่วนตัว

(9) พนักงานควรใช้ระบบเทคโนโลยีสารสนเทศและอุปกรณ์สื่อสารอื่น ๆ ที่บริษัทจัดให้ เช่น อุปกรณ์คอมพิวเตอร์ โทรศัพท์ โทรสาร โทรศัพท์มือถือ อย่างมีจิตสำนึกและรับผิดชอบ โดยคำนึงถึงประโยชน์ของบริษัทเป็นหลัก

(10) หากพนักงานมีความจำเป็นที่จะต้องนำข้อมูลส่วนตัวมาเก็บไว้ที่คอมพิวเตอร์ของบริษัท ควรกระทำด้วยความระมัดระวัง ในกรณีที่เกิดความเสียหายใด ๆ พนักงานจะต้องเป็นผู้รับผิดชอบความเสียหายนั้นเอง

(11) การใช้ Instant Messaging Software ใด ๆ ในระบบเทคโนโลยีสารสนเทศของบริษัท ให้ใช้เพื่อการติดต่อเกี่ยวกับการทำงานเท่าที่จำเป็น และควรปิดการแจ้งเตือน (Notification) ทุกรูปแบบ เพื่อไม่เป็นการรบกวนการทำงานของตนเองและผู้อื่น

2.3 การป้องกันไวรัส

(1) การนำอุปกรณ์เก็บข้อมูลใด ๆ เช่น Thump Drive, External Hard disk, CD, DVD เป็นต้น มาใช้งานกับคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศของบริษัท พนักงานต้องสแกน (Scan) อุปกรณ์เหล่านั้นก่อนทุกครั้ง เพื่อกำจัดและป้องกันการแพร่กระจายไวรัส

(2) พนักงานมีหน้าที่ตรวจสอบ Antivirus Pattern File ของเครื่องตนเอง ให้เป็น Version ล่าสุดเสมอ โดยสามารถขอคำแนะนำจากผู้ดูแลระบบได้

(3) เพื่อความปลอดภัยในการใช้คอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศ กรณีพนักงานพบไวรัสจะต้องแจ้งให้ผู้ดูแลระบบดำเนินการกำจัดไวรัสโดยเร็ว

(4) พนักงานพึงให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบในการตรวจสอบระบบความปลอดภัยของคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศ รวมทั้งปฏิบัติตามคำแนะนำที่เกี่ยวข้องกับความปลอดภัยที่บริษัทกำหนด

2.4 การใช้อินเทอร์เน็ต

(1) การใช้งานระบบทุกอย่างที่เกี่ยวกับอินเทอร์เน็ตของพนักงานจะถูกบันทึกไว้ในระบบของบริษัท

(2) ควรใช้อินเทอร์เน็ตในการแสวงหาข้อมูลและความรู้ที่เป็นประโยชน์ต่อการปฏิบัติงาน และจะต้องหลีกเลี่ยงเว็บไซต์ที่ผิดกฎหมาย หรือละเมิดศีลธรรมอันดีงาม

2.5 การใช้อีเมล

(1) พนักงานต้องใช้อีเมลบริษัทเพื่อการติดต่อเรื่องงานเท่านั้น และต้องไม่กระทำการใดที่ก่อให้เกิดความเสียหายต่อบริษัท

(2) ห้ามมิให้พนักงานส่งอีเมล แบบกระจายถึงพนักงานทุกคนที่ไม่เกี่ยวข้องโดยไม่จำเป็น

(3) พนักงานพึงใช้ข้อความที่สุภาพชนทั่วไปใช้ในข้อความที่ส่งไปถึงบุคคลอื่น

(4) ห้ามมิให้พนักงานนำอีเมลบริษัท ไปใช้สมัครหรือบอกรับสมาชิกใด ๆ เป็นการส่วนตัว

2.6 การจัดเก็บไฟล์ข้อมูล

(1) พนักงานจะต้องทำการเก็บไฟล์ข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการทำงานของบริษัทไว้บนพื้นที่ที่บริษัทจัดเตรียมไว้ให้ (“Drive กลาง”) และพนักงานพึงลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจาก Drive กลาง เพื่อเป็นการประหยัดพื้นที่บน Drive กลาง

(2) พนักงานที่มีหน้าที่รับผิดชอบโดยตรง หรือได้รับมอบหมายจากบริษัท มีสิทธิในการเข้าถึงและส่งต่อข้อมูลหรืออีเมลบนคอมพิวเตอร์ทุกเครื่องของบริษัท รวมถึงคอมพิวเตอร์ที่ต่อเข้ากับระบบเครือข่ายคอมพิวเตอร์ของบริษัท และมีสิทธิหน้าที่ในการติดตั้ง ตรวจสอบ แก้ไข ปัญหาใด ๆ ที่เกิดจากการใช้งานคอมพิวเตอร์ของบริษัท หรือการใช้งานคอมพิวเตอร์ที่ต่อเข้ากับระบบเครือข่ายคอมพิวเตอร์ของบริษัทได้ตลอดเวลา

2.7 การดูแลรักษาคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศ

(1) ดูแลรักษาอุปกรณ์ให้อยู่ในสภาพดี และพร้อมใช้งานรวมถึงใช้คอมพิวเตอร์เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามสัญญาจ้าง รวมถึงการปฏิบัติหน้าที่อื่นตามที่บริษัทได้กำหนดเท่านั้น

(2) ใช้อุปกรณ์และระบบคอมพิวเตอร์ เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามสัญญาจ้าง รวมถึงการปฏิบัติหน้าที่อื่นตามที่บริษัทได้ร้องขอเท่านั้น

(3) ใช้อุปกรณ์ในการเชื่อมต่อระบบคอมพิวเตอร์ ระบบปฏิบัติการ และแอปพลิเคชั่น รวมถึงการขออนุญาตใช้งาน หรือเข้าถึงข้อมูลตามวิธีการ ประกาศ ระเบียบ และนโยบายรวมถึงปฏิบัติตามกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด

(4) ห้ามพนักงานนำคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศของบริษัทให้ผู้อื่นยืมใช้และห้ามนำไปใช้ในกิจกรรมที่บริษัทไม่ได้กำหนด หรือในกิจกรรมที่อาจก่อให้เกิดความเสียหายต่อบริษัท

(5) พนักงานมีหน้าที่ตรวจสอบสภาพความพร้อมใช้ของคอมพิวเตอร์ อุปกรณ์ที่เกี่ยวข้อง และโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์หรือไม่

2.8 การปฏิบัติงานภายนอกบริษัท

(1) พนักงานมีหน้าที่รับผิดชอบในการดูแล และป้องกันคอมพิวเตอร์พกพาที่ได้รับ โดยพนักงานต้องล็อก เมื่อไม่ได้ใช้งานภายในบริษัท และต้องไม่วางอุปกรณ์ไว้ในที่สาธารณะโดยไม่มีคนดูแล

(2) พนักงานต้องระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ และต้องมีการควบคุมเครือข่ายที่ใช้ในการเข้าสู่ระบบอย่างรัดกุมรวมถึงควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว

(3) การเข้าสู่ระบบระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ พนักงานต้องแสดงหลักฐาน ระบุเหตุผล และความจำเป็นในการดำเนินงานอย่างเพียงพอ รวมถึงต้องได้รับอนุมัติจากผู้มีอำนาจอนุมัติตลอดจนต้องพิสูจน์ตัวตนผ่านระบบเทคโนโลยีสารสนเทศที่บริษัทกำหนด

หมวดที่ 3

การใช้คอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศที่ต้องใช้ด้วยความระมัดระวังเป็นพิเศษ

บริษัทไม่มีนโยบายสนับสนุนให้พนักงานใช้คอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศกระทำการเผยแพร่ส่งต่อข้อมูลด้วยตนเอง และ/หรือให้ความร่วมมือ ยินยอม รู้เห็นเป็นใจในการกระทำความผิดดังต่อไปนี้

3.1 การใช้งาน Freeware หรือ Shareware ใด ๆ ที่ไม่มีการทดสอบความเข้ากันได้กับระบบของบริษัท หรืออาจมี Adware หรือ Spyware ติดมาด้วย

3.2 การใช้งานเครื่องมือของบุคคลที่สามใด ๆ ที่อาจส่งผลให้ระบบ และ/หรือทรัพย์สินของบริษัทไม่สามารถทำงานได้เป็นปกติ หรืออาจก่อให้เกิดความเสียหายต่อบริษัท

3.3 ส่ง นำเข้า เผยแพร่ หรือแสดงข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือนำข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นโดยทุจริต หรือโดยหลอกลวง หรือน่าจะก่อให้เกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจหรือโครงสร้างพื้นฐานของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

3.4 ส่ง นำเข้า เผยแพร่ หรือแสดงข้อมูลเข้าสู่ระบบคอมพิวเตอร์อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้าย หรือมีลักษณะลามก หรือขัดต่อศีลธรรมอันดีของประชาชน ซึ่งประชาชนทั่วไปอาจเข้าถึงได้

3.5 นำภาพของผู้อื่นที่เกิดจากการสร้าง การตัดต่อ การเติม หรือการดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือด้วยวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย

3.6 กระทำหรือดำเนินการใด ๆ โดยมิชอบโดยใช้อุปกรณ์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์ซึ่งอาจก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศ หรือข้อมูลอื่นที่เกี่ยวข้องของบริษัทหรือบุคคลอื่น หรือกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของประเทศ

3.7 ใช้อุปกรณ์หรือเชื่อมต่อระบบคอมพิวเตอร์ เพื่อแสดงความเห็นหรือเข้าร่วมกิจกรรมที่อาจก่อให้เกิดความเสียหายต่อบริษัท ภาพลักษณ์ของบริษัท หรือชื่อเสียงของบริษัท หรือในลักษณะที่ก่อให้เกิดความเข้าใจคลาดเคลื่อนไปจากความเป็นจริง

3.8 ใช้อุปกรณ์หรือเชื่อมต่อระบบคอมพิวเตอร์ เพื่อเข้าเว็บไซต์การพนัน การประมูลสิ่งผิดกฎหมาย หรือเว็บไซต์ที่ขัดต่อกฎหมาย หรือศีลธรรมอันดีของประชาชน

3.9 ใช้อุปกรณ์หรือเชื่อมต่อระบบคอมพิวเตอร์เพื่อกระทำการอื่นใดอันถือว่าเป็นความผิดตามกฎหมายใด ๆ ที่ใช้บังคับอยู่ในปัจจุบัน รวมถึงที่ได้มีการแก้ไขเพิ่มเติมหรือประกาศใช้บังคับใหม่ในอนาคต

หมวดที่ 4

การใช้คอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศจะต้องได้รับอนุมัติ

การใช้คอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศกระทำการดังต่อไปนี้ จะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจอนุมัติในหน่วยงานทุกครั้ง

4.1 การขอสิทธิ์ในการเข้าถึง Folder ใด ๆ บน Server ซึ่งพนักงานนั้นไม่มีสิทธิ์มาก่อน

4.2 การขอ Track Transaction ของอีเมล อินเทอร์เน็ตของพนักงานท่านอื่น

4.3 การขอเพิ่มอีเมล Group และการขอเพิ่มสมาชิกของอีเมล Group รวมทั้งการขอเพิ่มอีเมลเพื่อใช้งานเฉพาะด้าน

4.4 การนำโปรแกรมคอมพิวเตอร์ อุปกรณ์อื่นใดจากภายนอกเข้ามาใช้งานหรือเชื่อมต่อกับคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศรวมถึงการปรับแต่งอุปกรณ์ ฮาร์ดแวร์ หรือติดตั้งอุปกรณ์ใด ๆ ที่นอกเหนือจากอุปกรณ์มาตรฐานที่บริษัท ติดตั้งให้จะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจอนุมัติ

4.5 การทำซ้ำ ดัดแปลง เผยแพร่ต่อสาธารณชน ให้เช่าต้นฉบับ หรือสำเนางานซึ่งโปรแกรมคอมพิวเตอร์ของบริษัทจะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจอนุมัติ

4.6 พนักงานมีหน้าที่ดูแลรักษาคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศที่อยู่ในความรับผิดชอบของตนเอง ให้ใช้งานได้อย่างปกติ และถูกต้องตามกฎระเบียบของบริษัท

4.7 ห้ามมิให้ดาวน์โหลดและอัพโหลดไฟล์ทุกประเภทที่ไม่เกี่ยวข้องต่อการปฏิบัติงานหรือดำเนินธุรกิจใด ๆ ของบริษัท โดยโปรแกรมมาตรฐานที่สามารถติดตั้งได้ภายในต้องเป็นโปรแกรมลิขสิทธิ์เท่านั้น เว้นแต่กรณีโปรแกรมประเภทซอฟต์แวร์ฟรีที่สนับสนุนระบบการทำงาน วัตถุประสงค์ และธุรกิจของบริษัท สามารถติดตั้งได้ แต่จะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจอนุมัติ

หมวดที่ 5
ข้อห้ามในการใช้คอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศ

เพื่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท และเพื่อป้องกันการกระทำความผิดตามกฎหมาย ห้ามพนักงานกระทำการดังต่อไปนี้

5.1 ห้ามนำคอมพิวเตอร์ และ/หรืออุปกรณ์แบบพกพา (Mobile Device) ส่วนตัว เข้ามาเชื่อมต่อกับระบบเครือข่ายของบริษัท

5.2 ห้ามเปิดไฟล์ใด ๆ ที่ไม่รู้จัก หรือไม่ทราบแหล่งที่มาแน่ชัด ไม่ว่าจะรับมาจากทางใดก็ตาม เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นจากการเปิดไฟล์ดังกล่าว

5.3 ห้ามพนักงานเข้าถึงระบบหรือข้อมูลที่ไม่ได้รับอนุญาต หรือไม่ได้มีไว้สำหรับตนโดยมิชอบ

5.4 ห้ามพนักงานที่ล่วงรู้มาตรการป้องกัน หรือวิธีการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ของผู้อื่นนำข้อมูลที่ล่วงรู้ไปใช้โดยมิชอบ และ/หรือทำให้เกิดความเสียหายแก่บริษัทและผู้อื่น

5.5 ห้ามพนักงานใช้อีเมลของบริษัทในการส่งต่อข้อความที่เป็นการกล่าวร้าย ทำให้เสื่อมเสีย หรือข้อความที่หยาบคาย ลามก ข่มขู่ ก่อกวน หรือสร้างความรำคาญให้กับผู้อื่น

5.6 ห้ามทำการใด ๆ อันเป็นการละเมิดลิขสิทธิ์ของผู้อื่น เช่น ใช้ทำซ้ำ หรือเผยแพร่ ซึ่งซอฟต์แวร์ รูปภาพ บทความ หนังสือเป็นต้น

5.7 ห้าม Share Drive จากเครื่องของตนเองให้กับบุคคลภายนอก

5.8 ห้ามพนักงานเปลี่ยนแปลง คัดลอก ทำซ้ำ ลบทิ้ง ทำลาย หรือเปิดเผยข้อมูลอันเป็นความลับแก่บุคคลภายนอก

5.9 ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในคอมพิวเตอร์ของบริษัทหรือนอกเหนือจากที่บริษัทได้จัดไว้ให้ กรณีมีความจำเป็นต้องติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงเพิ่มเติม ให้แจ้งผู้ดูแลระบบเป็นผู้ดำเนินการเท่านั้น

5.10 ห้ามพนักงานใช้คอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศเพื่อการดังต่อไปนี้

(1) การกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

(2) การกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

(3) การค้าหรือการแสวงหาผลกำไร หรือผลประโยชน์ส่วนตัว

(4) การแสดงความเห็นในเรื่องที่เกี่ยวข้องกับการดำเนินงานของบริษัทไปยังที่อยู่เว็บไซต์ (Website) ใด ๆ ในลักษณะที่จะก่อให้เกิด หรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง หรือก่อให้เกิดความเสียหายแก่บริษัทหรือบุคคลอื่น

(5) การกระทำอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของบริษัท หรือบุคคลอื่น

(6) การกระทำเพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้ที่มีสิทธิในข้อมูลดังกล่าว

(7) การรับส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายแก่บริษัท เช่น การรับส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับส่งข้อมูลที่ได้รับจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น เป็นต้น

(8) การขัดขวาง หรือการทำให้คอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศของบริษัท ไม่สามารถใช้งานได้ตามปกติ

(9) การกระทำอื่นใดที่อาจขัดต่อผลประโยชน์ของบริษัท หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่บริษัท

หมวดที่ 6

การใช้งานสื่อสังคมออนไลน์

6.1 การใช้งานสื่อสังคมออนไลน์ทั่วไป

(1) เมื่อมีการกล่าวถึงบริษัท ตราสินค้า การดำเนินธุรกิจ รวมถึงการเปิดเผย เผยแพร่ ข้อมูลที่มีส่วนเกี่ยวข้องกับบริษัท ผ่านสื่อสังคมออนไลน์ให้พนักงานพึงตระหนักและระมัดระวังการสื่อสารโดยใช้เนื้อหา บทความ ข้อความ รูปภาพ ภาพนิ่ง ภาพเคลื่อนไหว ความเห็นที่เผยแพร่บนสื่อสังคมออนไลน์หรือสื่อใด ๆที่สามารถเข้าถึงได้โดยสาธารณะ อันอาจส่งผลกระทบต่อภาพลักษณ์ของบริษัท และ/หรือทำให้บริษัทได้รับความเสียหาย

(2) พนักงานต้องใช้ความระมัดระวัง ในการสื่อสารข้อเท็จจริงผ่านสื่อสังคมออนไลน์ ที่อาจนำไปสู่การโต้แย้งที่รุนแรง โดยเฉพาะเรื่องเกี่ยวกับ สถาบันกษัตริย์ การเมือง เชื้อชาติ และศาสนา เป็นต้น

(3) การเผยแพร่ รูปภาพ ข้อมูลและแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ อันเป็นการละเมิดกฎหมาย จริยธรรมและจรรยาบรรณทางธุรกิจ ในลักษณะที่ก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความจริง หรือก่อให้เกิดความเสียหายต่อภาพลักษณ์ หรือชื่อเสียงของบริษัท หรืออาจเกิดความเสียหายอย่างร้ายแรงแก่ทรัพย์สินของบริษัท

6.2 การใช้งาน Official Account ผ่านสื่อสังคมออนไลน์

(1) ห้ามพนักงานเปิด และ/หรือใช้ Official Account ใด ๆ ที่เกี่ยวข้องหรือสื่อถึงบริษัท โดยไม่ได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

(2) พนักงานที่มีหน้าที่รับผิดชอบเปิด และ/หรือใช้ Official Account ของบริษัท เพื่อเป็นช่องทางในการเผยแพร่ข้อมูลอย่างเป็นทางการ จะต้องกรอกแบบฟอร์มของบริษัท โดยเสนอต่อผู้มีอำนาจอนุมัติทั้งนี้ เมื่อมีการเปิดและ/หรือใช้ Official Account แล้วพนักงานผู้รับผิดชอบต้องมีการแจ้ง Username และ Password ให้ผู้ดูแลระบบทราบ

(3) ห้ามโพสต์ข้อความบนสื่อสังคมออนไลน์ โดยใช้ Official Account ของบริษัท พาดพิง หรืออ้างอิงถึงบุคคลที่สาม หรือหมิ่นประมาท หรือก่อให้เกิดความเสียหายแก่ผู้อื่น หรือกระทำการใดที่เป็นความผิดตามกฎหมาย

(4) ห้ามนำ Official Account ไปใช้ อ้างอิง เปิดเผย รวมถึงการใช้ hashtag (#) ข้อความอื่นใดที่เกี่ยวข้องกับสินค้าและบริการของบริษัทอันอาจก่อให้เกิดความเสียหายต่อภาพลักษณ์ของบริษัท

หมวดที่ 7

ข้อปฏิบัติสำหรับผู้ดูแลระบบ

7.1 ผู้ดูแลระบบมีหน้าที่ควบคุม ดูแลบำรุงรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ กรณีพบความผิดปกติเกิดขึ้นในระบบ หรือในกรณีพบว่ามีการใช้งานไม่ถูกต้อง ไม่ตรงกับวัตถุประสงค์ของบริษัท หรือละเมิดข้อตกลงการใช้งาน ผู้ดูแลระบบมีอำนาจระงับการใช้เพื่อป้องกันความเสียหายได้

7.2 ผู้ดูแลระบบต้องไม่เข้าถึงข้อมูลซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และต้องไม่เปิดเผยข้อมูลที่ตนได้รับมาจากหรือเนื่องจากการปฏิบัติหน้าที่ให้แก่บุคคลหนึ่งบุคคลใดทราบ

7.3 ผู้ดูแลระบบมีหน้าที่จัดเก็บข้อมูลจราจรคอมพิวเตอร์ โดยถือปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

7.4 ผู้ดูแลระบบมีหน้าที่ควบคุมดูแลซอฟต์แวร์ และโปรแกรมต่าง ๆ ที่ติดตั้งบนคอมพิวเตอร์ ให้ถูกต้องตามลิขสิทธิ์ของซอฟต์แวร์ตลอดจนควบคุมการติดตั้งซอฟต์แวร์ และโปรแกรมต่าง ๆ ลงในระบบโดยไม่ให้กระทบ หรือไม่ได้ก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศของบริษัท

7.5 ผู้ดูแลระบบมีหน้าที่พัฒนา ปรับปรุง บำรุงรักษา และต้องกำหนดขั้นตอนการปฏิบัติงาน เพื่อให้มั่นใจว่าในการใช้งานข้อมูลสารสนเทศซอฟต์แวร์ที่พัฒนา และที่ครอบครองมีความถูกต้อง สอดคล้องกับกฎหมาย และข้อกำหนดเงื่อนไขต่าง ๆ ที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด

7.6 ผู้ดูแลระบบมีหน้าที่ควบคุมการใช้งาน และต้องตรวจสอบซอฟต์แวร์อย่างสม่ำเสมอ เช่น การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ การเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์

7.7 กำหนดให้มีการตรวจสอบคอมพิวเตอร์ของบริษัท เพื่อตรวจดูรายการซอฟต์แวร์ในคอมพิวเตอร์ และเพื่อให้แน่ใจว่าคอมพิวเตอร์ทุกเครื่องมีใบอนุญาต หรือการใช้งานสำหรับซอฟต์แวร์ลิขสิทธิ์อย่างถูกต้องตามกฎหมาย

หมวดที่ 8

การฝ่าฝืน และไม่ปฏิบัติตาม
ระเบียบการใช้คอมพิวเตอร์ และความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

7.1 หากพนักงาน ฝ่าฝืนข้อห้ามของระเบียบฉบับนี้ ถือเป็นความผิดอย่างร้ายแรง และบริษัทจะดำเนินการลงโทษทางวินัยตามหลักเกณฑ์การลงโทษทางวินัยของบริษัท และต้องถูกดำเนินคดีทางกฎหมายในทางแพ่งเพื่อติดตามเรียกร้องค่าเสียหาย รวมถึงถูกบังคับโทษในทางอาญาจนกว่าคดีจะถึงที่สุด

7.2 หากมีการตรวจพบความผิดจากการที่พนักงานใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ และ/หรือการละเมิดทรัพย์สินทางปัญญาใด ๆ จะถือเป็นความรับผิดชอบของพนักงานเองโดยทางบริษัทมิได้มีส่วนรับผิดชอบใด ๆ ทั้งสิ้น

7.3 ในกรณีที่พนักงานอนุญาตให้ผู้อื่นใช้คอมพิวเตอร์ที่อยู่ในความรับผิดชอบของตน พนักงานจะต้องรับผิดชอบหากเกิดความเสียหายต่อคอมพิวเตอร์นั้น ๆ รวมถึงความเสียหายอื่น ๆ ที่เกี่ยวข้องกับข้อมูลและสารสนเทศภายในบริษัท

7.4 หากข้อกำหนดและเงื่อนไขที่กำหนดในระเบียบฉบับนี้มีข้อความขัดหรือแย้งกับข้อกำหนดและเงื่อนไขที่กำหนดในความตกลงอื่นที่พนักงานผูกพันอยู่ก่อนแล้วนั้น ให้ถือเอาข้อกำหนดและเงื่อนไขของระเบียบฉบับนี้มีผลใช้บังคับ แต่หากข้อกำหนดและเงื่อนไขที่กำหนดในระเบียบฉบับนี้มีข้อความขัดหรือแย้งกับเงื่อนไขที่บริษัทกำหนดให้ระเบียบฉบับนี้มีผลใช้บังคับ

7.5 ระเบียบฉบับนี้มีผลผูกพันตลอดไป แม้ว่าพนักงานได้สิ้นสุดสถานะการเป็นพนักงานของบริษัทแล้ว และพนักงานทราบดีว่าหากไม่ปฏิบัติตามระเบียบฉบับนี้ บริษัทอาจได้รับความเสียหาย และบริษัทมีสิทธิได้รับการเยียวยาความเสียหายเต็มจำนวนตามความเสียหายที่เกิดขึ้นจากการกระทำดังกล่าว รวมถึงการเยียวยาอื่นตามกฎหมาย อีกทั้งบริษัทมีสิทธิสั่งห้ามไม่ให้พนักงานกระทำการอย่างใดอย่างหนึ่ง และ/หรือสั่งให้ปฏิบัติตามระเบียบฉบับนี้

นโยบายนี้ให้มีผลตั้งแต่วันที่ 10 ตุลาคม 2565 เป็นต้นไป

ประกาศ ณ วันที่ 10 ตุลาคม 2565

นายโสภณ อิงค์ธเนศ

กรรมการผู้อำนวยการ

บริษัท ไอที ซิตี้ จำกัด (มหาชน)