บริษัท เทิร์นคีย์ คอมมูนิเคชั่น เซอร์วิส จำกัด (มหาชน)

TURNKEY COMMUNICATION SERVICES PUBLIC COMPANY LIMITED

นโยบายเทคโนโลยีสารสนเทศ

(Information Technology Policy)

P-EXC-014

นโยบายเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อเป็นการกำหนดนโยบายการควบคุม การรักษาความปลอดภัย และการใช้งานเทคโนโลยีสารสนเทศ ของบริษัท เทิร์นคีย์ คอมมูนิเคชั่น เซอร์วิส จำกัด (มหาชน) (“บริษัทฯ”) ให้เกิดการใช้งานอย่างมีประสิทธิภาพภายใต้มาตรฐานการรักษาความปลอดภัยและปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไขเพิ่มเติม

ขอบเขต

กำหนดนโยบาย ระเบียบ มาตรฐาน การปฏิบัติงาน และมาตรการรักษาความปลอดภัย ให้ครอบคลุมการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ทั้งด้านผู้ดูแลระบบ และผู้ใช้งาน ประกอบด้วย

ภาคที่ 1 การควบคุมและจัดการเทคโนโลยีสารสนเทศ
เพื่อใช้เป็นระเบียบ หรือ วิธีปฏิบัติของพนักงานในแผนกเทคโนโลยีสารสนเทศ

ภาคที่ 2 การใช้งานเทคโนโลยีสารสนเทศ
เพื่อเป็นแนวปฏิบัติในการใช้งานเทคโนโลยีสารสนเทศของพนักงานในบริษัทฯ

ภาคที่ 1 การควบคุมและจัดการเทคโนโลยีสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทฯ มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถให้บริการแก่พนักงานผู้ใช้งานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาการถูกคุกคามจากภัยต่าง ๆ จึงกำหนดให้มีการควบคุม และการจัดการเทคโนโลยีสารสนเทศ เพื่อเป็นมาตรฐานและแนวปฏิบัติของพนักงานทุกคนในแผนกเทคโนโลยีสารสนเทศ ดังนี้

- การมอบหมายหน้าที่ความรับผิดชอบ
- การควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์
- การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- การรักษาความปลอดภัยเทคโนโลยีสารสนเทศ
- การควบคุมการพัฒนาระบบสารสนเทศ
- การสำรองข้อมูลระบบสารสนเทศ
- การรองรับเหตุฉุกเฉิน
- การแก้ไขปัญหา และการรายงาน

การมอบหมายหน้าที่ความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดแนวทางในการแต่งตั้งผู้ดูแลระบบ และมอบหมายความรับผิดชอบที่เกี่ยวข้องกับการเข้าถึงและควบคุมระบบเทคโนโลยีสารสนเทศขององค์กรให้เป็นไปอย่างมีระบบ โปร่งใส และสอดคล้องกับนโยบายที่เกี่ยวข้อง

แนวทางปฏิบัติ

1. การแต่งตั้งผู้ดูแลระบบ หัวหน้าสายงานด้านเทคโนโลยีสารสนเทศจะเป็นผู้พิจารณาและเสนอชื่อผู้ดูแลระบบ พร้อมกำหนดหน้าที่ความรับผิดชอบอย่างชัดเจน
2. การอนุมัติจากผู้บริหาร การแต่งตั้งและมอบหมายหน้าที่ควรได้รับการอนุมัติจากผู้บริหารที่มีอำนาจเพื่อให้แน่ใจว่าบทบาทหน้าที่มีความเหมาะสมและตรวจสอบได้
3. การจัดทำและทบทวนหน้าที่งาน (Job Description) ควรจัดทำคำอธิบายหน้าที่งานของบุคลากรในสายงาน IT และดำเนินการปรับปรุงข้อมูลให้ทันสมัยอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับโครงสร้างงานและเทคโนโลยีที่เปลี่ยนแปลง
4. การสื่อสารบทบาทอย่างชัดเจน ผู้ที่ได้รับมอบหมายบทบาทในการดูแลระบบควรได้รับการชี้แจงถึงหน้าที่ ขอบเขต และสิทธิ์ในการเข้าถึงระบบอย่างชัดเจนจากหัวหน้าสายงาน
5. การดำเนินงานนอกเหนือสิทธิ์ที่ได้รับมอบหมาย ในกรณีที่จำเป็น เช่น การแก้ไขปัญหาเร่งด่วน หรือการเข้าถึงจากระยะไกล (Remote Access) ควรมีการขออนุมัติล่วงหน้า และรายงานผลการดำเนินงานให้ผู้ดูแลทราบ
6. การใช้บริการจากภายนอก หากจำเป็นต้องจ้างหน่วยงานภายนอกในการจัดการหรือสนับสนุนด้านเทคโนโลยี ควรพิจารณาคุณสมบัติ ความน่าเชื่อถือ และแนวทางความปลอดภัยที่ชัดเจนก่อนเริ่มดำเนินการ

การควบคุมการเข้าออกศูนย์คอมพิวเตอร์

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงห้องศูนย์คอมพิวเตอร์อย่างเหมาะสม โดยจำกัดเฉพาะผู้มีหน้าที่เกี่ยวข้อง และป้องกันความเสี่ยงจากการสูญเสียหรือความเสียหายที่อาจเกิดกับระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศขององค์กร

แนวทางปฏิบัติ

1. พื้นที่ศูนย์คอมพิวเตอร์ควรมีระบบควบคุมการเข้า-ออก (Access Control) เช่น ระบบบัตรอิเล็กทรอนิกส์, ระบบสแกนลายนิ้วมือ หรือเทคโนโลยียืนยันตัวตนอื่นที่เหมาะสม โดยระบบควรสามารถบันทึกประวัติการเข้า-ออกได้
2. ควรกำหนดสิทธิ์ในการเข้าถึงไว้เฉพาะบุคลากรที่มีความรับผิดชอบโดยตรงต่อการปฏิบัติงานภายในพื้นที่ดังกล่าว และผ่านการอนุมัติจากผู้มีอำนาจที่เกี่ยวข้อง

3. ควรมีการจัดเก็บข้อมูลของผู้ได้รับสิทธิ์เข้าถึงอย่างเหมาะสม เช่น รายชื่อผู้มีสิทธิ์, หมายเลขบัตร, หรือวิธีการยืนยันตัวตน ทั้งนี้การจัดเก็บควรดำเนินการอย่างปลอดภัยตามมาตรฐานที่เกี่ยวข้อง
4. ควรมีการตรวจสอบบันทึกการเข้า-ออกของพื้นที่ศูนย์คอมพิวเตอร์เป็นระยะ เพื่อให้สามารถตรวจพบการใช้งานที่ไม่เหมาะสมหรือผิดปกติได้โดยเร็ว
5. ในกรณีที่มีความจำเป็นต้องให้บุคคลภายนอกเข้าพื้นที่ศูนย์คอมพิวเตอร์ เช่น การติดตั้งหรือซ่อมบำรุงระบบ ควรมีขั้นตอนขออนุญาตล่วงหน้า พร้อมระบุรายละเอียด เช่น วัตถุประสงค์ ระยะเวลา และผู้ประสานงาน โดยการเข้าถึงควรอยู่ภายใต้การควบคุมของเจ้าหน้าที่ที่ได้รับมอบหมาย

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ ในการเพิ่ม แก้ไขปรับปรุง เพื่อให้มีการควบคุมและตรวจสอบการปฏิบัติงานให้มีความถูกต้อง และไม่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศของบริษัทฯ

แนวทางปฏิบัติ

1. การเปิดและจัดการบัญชีผู้ใช้งาน ควรกำหนดให้เป็นไปตามกระบวนการที่ได้รับอนุมัติจากผู้มีอำนาจและสอดคล้องกับบทบาทหน้าที่ของผู้ใช้งาน
2. การยกเลิกหรือปิดบัญชีผู้ใช้งาน ควรดำเนินการระงับหรือปิดบัญชีผู้ใช้งานภายในระยะเวลาที่เหมาะสม พร้อมจัดเก็บบันทึกการดำเนินการไว้
3. การควบคุมการเข้าถึงระบบงานคอมพิวเตอร์ การเข้าถึงระบบงานควรจำกัดเฉพาะผู้ที่ได้รับมอบหมายหรือได้รับอนุมัติอย่างเป็นทางการ และไม่ควรโอนสิทธิ์การใช้งานให้บุคคลอื่นโดยไม่ได้รับอนุญาต
4. การควบคุมการเข้าถึงระบบฐานข้อมูล การเข้าถึงระบบฐานข้อมูลควรจำกัดเฉพาะบุคลากรที่ได้รับการแต่งตั้งอย่างชัดเจน และมีหลักฐานประกอบการอนุมัติที่สามารถตรวจสอบย้อนหลังได้
5. การควบคุมการเข้าถึงอุปกรณ์เครือข่าย การเข้าถึงหรือปรับเปลี่ยนอุปกรณ์เครือข่ายควรอยู่ภายใต้การควบคุมของผู้มีอำนาจ พร้อมจัดเก็บบันทึกและข้อมูลการเปลี่ยนแปลงอย่างเหมาะสม
6. การควบคุมการเข้าถึงโดยบุคคลภายนอก การอนุญาตให้บุคคลภายนอกเข้าถึงระบบหรือพื้นที่ควบคุมควรดำเนินการผ่านกระบวนการขออนุมัติล่วงหน้า และมีการกำกับดูแลการปฏิบัติงานอย่างรอบคอบ
7. การเข้าถึงระบบจากภายนอก (Remote Access) การเข้าถึงระบบจากภายนอกควรดำเนินการผ่านช่องทางที่ปลอดภัย เช่น VPN ที่ได้รับการรับรอง พร้อมควบคุมระยะเวลาและตรวจสอบการใช้งานอย่างสม่ำเสมอ

การรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีเสารสนเทศ มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถให้บริการได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ

แนวทางปฏิบัติ

1. การรักษาความปลอดภัยทางกายภาพและสิ่งแวดล้อม พื้นที่ควบคุมระบบควรมีมาตรการดูแลอุณหภูมิความชื้น อัคคีภัย และการบำรุงรักษาอุปกรณ์ เพื่อให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพและปลอดภัย
2. การรักษาความปลอดภัยระบบคอมพิวเตอร์ การกำหนดสิทธิ์และการใช้รหัสผ่านควรอยู่ภายใต้การควบคุมอย่างเป็นระบบ โดยคำนึงถึงความสอดคล้องกับหน้าที่และการจัดการในกรณีฉุกเฉิน
3. การรักษาความปลอดภัยระบบเครือข่าย การติดตั้ง ปรับเปลี่ยน หรือเข้าถึงระบบเครือข่ายควรได้รับอนุญาตและควบคุมผ่านกระบวนการที่ปลอดภัยและสามารถตรวจสอบย้อนหลังได้
4. การป้องกันความปลอดภัยของระบบฐานข้อมูล การดำเนินการกับกระบวนการ Batch Job ควรมีการควบคุม ตรวจสอบ และรายงานอย่างเหมาะสม เพื่อป้องกันความผิดพลาดที่อาจกระทบต่อฐานข้อมูล
5. การป้องกันการบุกรุก ควรใช้ระบบป้องกันไวรัสที่สามารถอัปเดตอัตโนมัติ และมีการตรวจสอบความพร้อมของระบบอย่างสม่ำเสมอ
6. การดำเนินการด้านซอฟต์แวร์ การใช้งานซอฟต์แวร์ควรเป็นไปตามลิขสิทธิ์ ถูกต้องตามกฎหมาย มีการสำรองข้อมูลก่อนปรับปรุงระบบ และจัดทำบันทึกอย่างเหมาะสม
7. การกำหนดนโยบายรหัสผ่าน ควรกำหนดรหัสผ่านให้มีความซับซ้อน ปรับเปลี่ยนตามระยะเวลา และควบคุมบัญชีผู้ใช้งานเพื่อป้องกันการเข้าถึงโดยมิชอบ
8. การบันทึกประวัติการใช้งานอินเทอร์เน็ต ควรมีระบบบันทึกและตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้ภายในองค์กร เพื่อใช้เป็นข้อมูลอ้างอิงในกรณีจำเป็น

การควบคุมการพัฒนาระบบสารสนเทศ

วัตถุประสงค์

กำหนดกระบวนการพัฒนา และปรับปรุงระบบสารสนเทศของบริษัทฯ และวิธีการควบคุมให้ได้ระบบสารสนเทศที่ตรงตามวัตถุประสงค์ และมีการทำงานที่ครบถ้วนถูกต้องสามารถตรวจสอบได้

แนวทางปฏิบัติ

1. การเริ่มต้นพัฒนาและปรับปรุงระบบ ควรแยกสภาพแวดล้อมการทำงานอย่างชัดเจน และเริ่มต้นจากการวิเคราะห์ความต้องการที่ได้รับการอนุมัติจากผู้มีอำนาจ

2. การพัฒนาระบบภายใน ควรดำเนินการตามวงจร SDLC โดยจัดทำเอกสารประกอบทดสอบในระบบแยก และได้รับอนุมัติอย่างเป็นทางการก่อนใช้งานจริง
3. การจัดหา Software ควรพิจารณาความเหมาะสมและความคุ้มค่า พร้อมเอกสารเสนอฟังก์ชันและงบประมาณเพื่อประกอบการอนุมัติ
4. การพัฒนาโดยหน่วยงานภายนอก การว่าจ้างหน่วยงานภายนอกพัฒนาระบบควรมีเอกสารข้อกำหนดที่ชัดเจน และผ่านกระบวนการประเมินผลและควบคุมคุณภาพตามขั้นตอน
5. การควบคุมหน่วยงานภายนอก ผู้พัฒนาภายนอกควรส่งมอบเอกสารและผลการทดสอบที่ครบถ้วน และการนำระบบขึ้นใช้งานจริงต้องได้รับการตรวจสอบและอนุมัติร่วมกัน
6. การติดตั้งระบบในกรณีพิเศษ การติดตั้งหรือเข้าถึงระบบ Production โดยบุคคลภายนอกต้องได้รับอนุญาตล่วงหน้าและมีการบันทึกการดำเนินงานอย่างเป็นทางการ
7. การควบคุมการโอนข้อมูล (Data Conversion) การโอนย้ายข้อมูลควรตรวจสอบความถูกต้องก่อนและหลังการโอน เพื่อให้ข้อมูลในระบบใหม่ตรงกับข้อมูลต้นทางที่ตรวจสอบได้
8. การตรวจรับระบบ ควรดำเนินการทดสอบระบบตามแผนและผ่านการรับรองผลร่วมกับผู้ใช้งาน พร้อมจัดทำบันทึกเวอร์ชันและอนุมัติอย่างเป็นทางการก่อนเริ่มใช้งาน

การสำรองข้อมูลระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดแนวทางการสำรองและเรียกคืนข้อมูลสารสนเทศให้มีความปลอดภัย เชื่อถือได้ และพร้อมใช้งานเมื่อเกิดเหตุการณ์ไม่คาดคิด

แนวทางปฏิบัติ

1. การจัดทำแนวทางการสำรองข้อมูล ควรมีการจัดทำและปรับปรุงคู่มือการสำรองและเรียกคืนข้อมูลอย่างสม่ำเสมอ โดยครอบคลุมระบบที่สำคัญทั้งหมด
2. การสำรองข้อมูลประจำวัน ควรดำเนินการตามแผนงานที่ชัดเจน โดยอัตโนมัติหรือกึ่งอัตโนมัติเพื่อความต่อเนื่องและสม่ำเสมอ
3. การตรวจสอบผลการสำรอง ควรมีการตรวจสอบผลการสำรองทุกครั้ง พร้อมบันทึกผลและรายงานปัญหาให้ผู้มีอำนาจทราบ
4. การจัดเก็บข้อมูลสำรอง ควรจัดเก็บทั้งในรูปแบบกายภาพและแบบคลาวด์ โดยมีพื้นที่จัดเก็บสำรองนอกสถานที่ (Off-Site) เพื่อรองรับเหตุการณ์ไม่คาดคิด
5. การขนย้ายข้อมูลสำรอง ควรอยู่ภายใต้การควบคุมด้วยระบบบันทึกและลงชื่อรับ-ส่งที่สามารถตรวจสอบย้อนหลังได้
6. การทดสอบการเรียกคืนข้อมูล ควรมีการทดสอบการเรียกคืนข้อมูลตามรอบระยะเวลาที่กำหนด และบันทึกผลการทดสอบเพื่อยืนยันความพร้อมของระบบสำรอง

7. การเรียกคืนข้อมูลจากผู้ใช้งาน การเรียกคืนข้อมูลตามคำร้องขอควรผ่านการอนุมัติอย่างเป็นทางการและดำเนินการภายใต้การควบคุมของฝ่ายที่รับผิดชอบ
8. กรณีเกิดปัญหาในการเรียกคืนข้อมูล หากเกิดปัญหาในการเรียกคืนข้อมูล ควรดำเนินการแจ้งผู้มีอำนาจทันที พร้อมใช้แผนสำรองเพื่อรองรับสถานการณ์ฉุกเฉิน

การรองรับเหตุฉุกเฉิน

วัตถุประสงค์

เพื่อกำหนดแนวทางการฟื้นฟูระบบเทคโนโลยีสารสนเทศให้สามารถกลับมาใช้งานได้โดยเร็ว เมื่อเกิดเหตุฉุกเฉินที่ส่งผลให้ระบบหยุดชะงัก

แนวทางปฏิบัติ

1. การเตรียมข้อมูลสำคัญเพื่อรองรับเหตุฉุกเฉิน ควรจัดเตรียมข้อมูลที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ เช่น ผังเครือข่าย รายการอุปกรณ์ และแผนภาพระบบงาน เพื่อใช้ประกอบการฟื้นฟูระบบเมื่อเกิดเหตุไม่คาดคิด
2. การฟื้นฟูระบบงานหลัก (เช่น ระบบ ERP) เมื่อระบบงานหลักหยุดทำงาน ควรประสานผู้เกี่ยวข้องโดยเร็ว วางแผนร่วมกัน และดำเนินการกู้คืนระบบตามลำดับขั้นตอนภายใต้การควบคุมที่ได้รับอนุมัติ
3. การกู้คืนข้อมูลจากข้อมูลสำรอง (ระบบหลัก) การกู้คืนข้อมูลต้องผ่านการอนุมัติ ตรวจสอบความสมบูรณ์ของข้อมูลสำรอง และประสานทีมที่เกี่ยวข้องในการดำเนินการอย่างปลอดภัย
4. การจัดทำรายงานหลังฟื้นฟูระบบ ควรจัดทำรายงานสรุปเหตุการณ์ สาเหตุ วิธีการแก้ไข ระยะเวลาหยุดชะงัก และแนวทางป้องกันไม่ให้เกิดซ้ำ
5. การฟื้นฟูระบบงานอื่นๆ (Non-ERP Applications) ระบบงานทั่วไปที่หยุดทำงานควรได้รับการตรวจสอบโดยเร็ว และดำเนินการแก้ไขตามประเภทของปัญหาโดยประสานผู้ดูแลหรือผู้พัฒนาระบบที่เกี่ยวข้อง
6. การกู้คืนข้อมูลจากระบบงานอื่นๆ ก่อนกู้คืนข้อมูลจากระบบอื่น ต้องได้รับอนุมัติ ตรวจสอบความถูกต้องของข้อมูลสำรอง และดำเนินการภายใต้แผนที่ปลอดภัย
7. การรายงานเหตุการณ์ในระบบงานอื่นๆ เมื่อระบบกลับมาใช้งานได้ ควรจัดทำรายงานเหตุการณ์ในรูปแบบเดียวกับระบบหลัก เพื่อใช้เป็นข้อมูลอ้างอิงและปรับปรุงแผนรองรับเหตุฉุกเฉินในอนาคต

การแก้ไขปัญหาและการรายงาน

วัตถุประสงค์

เพื่อกำหนดขั้นตอนการรับเรื่อง แก้ไขปัญหา และรายงานผลอย่างมีระบบ โปร่งใส และสามารถตรวจสอบได้

แนวทางปฏิบัติ

1. การรับเรื่องและดำเนินการเบื้องต้น เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่รับแจ้งปัญหา ตรวจสอบเบื้องต้น และดำเนินการแก้ไขตามขอบเขตความรับผิดชอบ หรือส่งต่อให้ผู้เชี่ยวชาญที่เกี่ยวข้อง
2. การประสานงานและขอคำปรึกษา หากไม่สามารถแก้ไขปัญหาได้ภายในหน่วยงาน ควรประสานผู้บังคับบัญชาหรือผู้เชี่ยวชาญที่เกี่ยวข้อง และอาจพิจารณาใช้บริการจากภายนอกหากมีความจำเป็น
3. การบันทึกและรายงานผลการแก้ไข ต้องจัดเก็บบันทึกการรับแจ้งปัญหา วิธีการแก้ไข และผลการดำเนินงานอย่างเป็นระบบ พร้อมสรุปรายงานเสนอผู้มีอำนาจเป็นรายเดือน
4. กรณีมีผลกระทบรุนแรง หากปัญหาที่เกิดขึ้นส่งผลกระทบในระดับสำคัญต่อการดำเนินงานขององค์กร ต้องรายงานให้ผู้บริหารระดับสูงทราบโดยทันที
5. การวิเคราะห์และป้องกันการเกิดซ้ำ ปัญหาที่เกิดซ้ำควรถูกนำมาวิเคราะห์สาเหตุเชิงระบบ เพื่อจัดทำแนวทางป้องกันและปรับปรุงกระบวนการในระยะยาว
6. กรณีเร่งด่วนหรือข้ามขั้นตอนการร้องขอ หากจำเป็นต้องดำเนินการแก้ไขโดยเร่งด่วนโดยยังไม่สามารถทำตามขั้นตอนปกติได้ เจ้าหน้าที่สามารถขออนุมัติเฉพาะกิจและดำเนินการเอกสารย้อนหลังให้สมบูรณ์โดยเร็วที่สุด

ภาคที่ 2 นโยบายการใช้งานเทคโนโลยีสารสนเทศ

เพื่อเป็นแนวปฏิบัติในการใช้งานเทคโนโลยีสารสนเทศของพนักงานทุกคนในบริษัทฯ ประกอบด้วย

- การควบคุมการใช้งานเทคโนโลยีสารสนเทศ
- การใช้เครื่องคอมพิวเตอร์
- การใช้ระบบเครือข่ายคอมพิวเตอร์ และบัญชีผู้ใช้งาน
- การใช้จดหมายอิเล็กทรอนิกส์
- การใช้ระบบอินเตอร์เน็ต
- การดูแลรักษาข้อมูลในเครื่องคอมพิวเตอร์
- การป้องกันไวรัสคอมพิวเตอร์
- การใช้งานปัญญาประดิษฐ์ (AI) ภายในองค์กร

การควบคุมการใช้งานเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อให้พนักงานรับทราบ และเข้าใจวิธีการใช้งานเทคโนโลยีสารสนเทศที่บริษัทฯ ได้จัดสรรให้

แนวทางปฏิบัติ

กำหนดวัตถุประสงค์ ขอบเขตและวิธีการใช้เทคโนโลยีสารสนเทศอย่างถูกต้องและมีประสิทธิภาพภายใต้ข้อบังคับของกฎหมาย และมาตรฐานความปลอดภัยที่บริษัทฯ กำหนดไว้ และแจ้งให้พนักงานรับทราบ

1. ควรใช้งานระบบคอมพิวเตอร์และเครือข่ายขององค์กรเพื่อสนับสนุนการทำงาน และหลีกเลี่ยงการใช้งานที่ไม่เกี่ยวข้องกับองค์กร
2. หากมีความจำเป็นต้องใช้อุปกรณ์ส่วนตัวร่วมกับระบบขององค์กร ควรแจ้งและขอคำแนะนำจากผู้ที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ
3. ผู้ใช้งานควรตระหนักและปฏิบัติตามแนวทางที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศขององค์กร และเคารพข้อกำหนดด้านความปลอดภัยของข้อมูล
4. บุคคลภายนอกที่เข้ามาทำงานภายในองค์กรควรได้รับคำแนะนำเกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรอย่างเหมาะสม
5. องค์กรอาจดำเนินการตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศตามความเหมาะสม หากพบเหตุที่อาจส่งผลต่อความปลอดภัยหรือประสิทธิภาพการทำงาน
6. ควรจัดให้มีช่องทางสำหรับติดต่อผู้ดูแลระบบสารสนเทศ เพื่อขอรับความช่วยเหลือหรือคำแนะนำในการใช้งานระบบต่าง ๆ

การใช้เครื่องคอมพิวเตอร์

วัตถุประสงค์

เพื่อให้พนักงานรับทราบวิธีการจัดสรร และการใช้งานคอมพิวเตอร์

แนวทางปฏิบัติ

1. การจัดสรรเครื่องคอมพิวเตอร์ให้แก่พนักงาน ควรเป็นไปตามความเหมาะสมของหน้าที่งาน โดยผ่านการพิจารณาของผู้มีอำนาจที่เกี่ยวข้อง
2. พนักงานไม่ควรนำเครื่องคอมพิวเตอร์ส่วนตัวหรืออุปกรณ์จัดเก็บข้อมูลแบบพกพาเข้ามาใช้งานภายในองค์กร เว้นแต่ได้รับอนุญาต
3. เครื่องคอมพิวเตอร์ควรใช้เพื่อสนับสนุนการปฏิบัติงานตามภารกิจขององค์กรเท่านั้น ไม่ควรจัดเก็บหรือใช้งานโปรแกรมหรือเนื้อหาที่ไม่เหมาะสม ผิดกฎหมาย หรือเกี่ยวข้องกับการละเมิดลิขสิทธิ์
4. ในกรณีที่มีการใช้เครื่องคอมพิวเตอร์ในลักษณะที่อาจก่อให้เกิดความเสียหายทางกฎหมาย ผู้ใช้งานควรรับผิดชอบตามที่กฎหมายกำหนด
5. ไม่ควรปรับเปลี่ยนหรือติดตั้งระบบปฏิบัติการ หรือโปรแกรมที่มีลิขสิทธิ์ โดยไม่ได้รับอนุญาต
6. ไม่ควรติดตั้งหรือดัดแปลงอุปกรณ์ฮาร์ดแวร์เพิ่มเติม โดยไม่ได้รับการเห็นชอบจากผู้ที่เกี่ยวข้อง
7. พนักงานควรดูแลเครื่องคอมพิวเตอร์ให้อยู่ในสภาพดี พร้อมใช้งานอยู่เสมอ หากเกิดความเสียหายจากการใช้งานที่ไม่เหมาะสม องค์กรอาจพิจารณาให้ผู้ใช้งานร่วมรับผิดชอบตามความเหมาะสม

การใช้ระบบเครือข่ายคอมพิวเตอร์ และบัญชีผู้ใช้งาน

วัตถุประสงค์

จัดสรรบัญชีผู้ใช้งานให้พนักงานใช้งานระบบเครือข่ายคอมพิวเตอร์ ได้ตามหน้าที่ของพนักงานแต่ละคน

แนวทางปฏิบัติ

1. พนักงานควรเก็บรักษาบัญชีผู้ใช้งานและรหัสผ่านเป็นความลับ และควรเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ
2. ไม่ควรใช้บัญชีผู้ใช้งานร่วมกัน หรือเปิดเผยรหัสผ่านแก่ผู้อื่น
3. การใช้งานระบบ ERP และระบบอื่น ๆ ควรเป็นไปตามแนวทางที่องค์กรกำหนด
4. หากต้องการเปิดหรือปิดบัญชีผู้ใช้งาน ควรดำเนินการผ่านช่องทางที่องค์กรกำหนด หรือแจ้งผู้มีหน้าที่เกี่ยวข้อง
5. พนักงานที่ได้รับสิทธิ์เข้าใช้งานระบบต่าง ๆ ควรให้ความระมัดระวังในการใช้งาน และรักษาข้อมูลการเข้าถึงอย่างเหมาะสม
6. ระบบเครือข่ายขององค์กรควรได้รับการดูแล ควบคุม และจัดสรรโดยองค์กร ตามลักษณะงานและสภาพแวดล้อมที่เหมาะสม
7. พนักงานควรหลีกเลี่ยงการอนุญาตให้บุคคลภายนอกเข้าถึงระบบเครือข่ายขององค์กรโดยไม่ได้รับอนุญาต และไม่ควรติดตั้งอุปกรณ์เครือข่ายส่วนตัวภายในพื้นที่ขององค์กร

8. ไม่ควรเข้าไปปรับเปลี่ยนคำสั่งหรือข้อมูลใด ๆ บนอุปกรณ์เครือข่าย เว้นแต่ได้รับมอบหมายหรือได้รับอนุญาตจากผู้มีอำนาจ
9. ควรหลีกเลี่ยงการกระทำใด ๆ ที่อาจส่งผลให้ระบบเครือข่ายทำงานผิดปกติหรือหยุดชะงัก
10. หากจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบเครือข่ายเพื่อการทำงาน ควรมีขั้นตอนการขออนุญาตและบันทึกการเข้าถึงอย่างเหมาะสม

การใช้จดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

เพื่อให้พนักงานใช้จดหมายอิเล็กทรอนิกส์ของบริษัทฯ ได้อย่างมีประสิทธิภาพ

แนวทางปฏิบัติ

1. ระบบอีเมลขององค์กรจัดไว้สำหรับการใช้งานที่เกี่ยวข้องกับภารกิจขององค์กรเท่านั้น
2. การขอเปิดหรือปิดบัญชีอีเมลควรดำเนินการผ่านแบบฟอร์มหรือช่องทางที่องค์กรกำหนด โดยได้รับการอนุมัติจากผู้มีสิทธิ์
3. ควรใช้ภาษาสุภาพในการสื่อสาร และหลีกเลี่ยงการส่งข้อมูลที่ไม่ถูกต้อง ก่อให้เกิดความเสียหาย หรือกระทบต่อบุคคลอื่น
4. ห้ามส่งเนื้อหาที่ไม่เหมาะสม เช่น ภาพหรือข้อความที่เกี่ยวข้องกับสื่ออนาจาร หรือเนื้อหาละเมิดจริยธรรม
5. การส่งข้อมูลผ่านอีเมลควรอยู่ภายใต้กรอบของกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์
6. ไม่ควรส่งอีเมลโดยไม่แสดงชื่อหรือระบุตัวตนของผู้ส่งอย่างชัดเจน
7. ควรจำกัดขนาดของอีเมลและไฟล์แนบให้ไม่เกิน 20 MB เพื่อให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพ
8. หากมีความจำเป็นต้องส่งไฟล์ขนาดใหญ่เกิน 20 MB เป็นประจำ ควรแจ้งขออนุมัติหรือขอใช้บริการผ่านช่องทางที่องค์กรกำหนด

การใช้ระบบอินเตอร์เน็ต

วัตถุประสงค์

เพื่อส่งเสริมให้พนักงานสามารถใช้งานระบบอินเตอร์เน็ตขององค์กรได้อย่างมีประสิทธิภาพ ปลอดภัย และอยู่ภายใต้กรอบกฎหมายและจริยธรรมที่เหมาะสม

แนวทางปฏิบัติ

1. สนับสนุนการใช้งานเพื่อการทำงานอินเตอร์เน็ตที่องค์กรจัดสรรมีวัตถุประสงค์ เพื่อสนับสนุนการปฏิบัติงาน การสืบค้นข้อมูล และการพัฒนาทักษะของพนักงานในบริบทของการทำงาน

2. เคารพกฎหมายและจริยธรรม การใช้งานอินเตอร์เน็ตควรอยู่ภายใต้ขอบเขตของกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 รวมถึงไม่กระทำการใดๆ ที่อาจขัดต่อศีลธรรม หรือส่งผลกระทบในเชิงลบต่อผู้อื่น
3. การระบุตัวตนและการรักษาความปลอดภัย ควรใช้งานอินเตอร์เน็ตผ่านบัญชีผู้ใช้งานที่องค์กรกำหนด โดยรักษารหัสผ่านอย่างปลอดภัย และปฏิบัติตามแนวทางการใช้งานเครือข่ายขององค์กรอย่างเคร่งครัด
4. ความเหมาะสมในการใช้ทรัพยากรขององค์กร ควรหลีกเลี่ยงการนำที่อยู่อีเมลขององค์กรไปใช้สมัครบริการหรือเว็บไซต์ที่ไม่เกี่ยวข้องกับการปฏิบัติงาน เพื่อป้องกันการละเมิดความเป็นส่วนตัวหรือความเสี่ยงจากภัยคุกคามภายนอก
5. การจัดเก็บข้อมูลการใช้งาน องค์กรอาจมีการจัดเก็บประวัติการใช้งานอินเตอร์เน็ตเพื่อวัตถุประสงค์ด้านความปลอดภัยและการตรวจสอบย้อนหลังตามที่กฎหมายกำหนด
6. การเชื่อมต่ออุปกรณ์ภายนอก การเชื่อมต่ออุปกรณ์ส่วนตัวหรืออุปกรณ์ที่ไม่ได้รับการรับรองจากองค์กรเข้าสู่เครือข่ายอินเตอร์เน็ต ควรได้รับการพิจารณาและอนุมัติล่วงหน้าจากผู้มีอำนาจที่เกี่ยวข้อง เพื่อรักษาความมั่นคงปลอดภัยของระบบโดยรวม

การดูแลรักษาข้อมูลในเครื่องคอมพิวเตอร์

วัตถุประสงค์

เพื่อส่งเสริมให้พนักงานมีแนวทางในการจัดเก็บ สำรอง และใช้งานข้อมูลอย่างปลอดภัย เป็นระบบ และลดความเสี่ยงจากการสูญหายหรือรั่วไหลของข้อมูลที่สำคัญ

แนวทางปฏิบัติ

1. ความระมัดระวังในการเผยแพร่ข้อมูล ข้อมูลภายในองค์กรควรถูกใช้งานและเผยแพร่ภายใต้ดุลยพินิจและการอนุมัติที่เหมาะสม โดยเฉพาะในกรณีที่ต้องให้ข้อมูลแก่บุคคลภายนอก ควรดำเนินการตามขั้นตอนและอำนาจของแต่ละส่วนงานอย่างรอบคอบ
2. การใช้พื้นที่จัดเก็บข้อมูลร่วม (Share Drive) องค์กรอาจจัดสรรพื้นที่เก็บข้อมูลกลาง (Share Drive) สำหรับใช้งานร่วมกันในแต่ละแผนก โดยผู้ใช้งานสามารถแจ้งความต้องการเพิ่มเติมได้ผ่านแบบฟอร์มมาตรฐานขององค์กร
3. การบริหารพื้นที่จัดเก็บข้อมูล ผู้ใช้งานควรจัดระเบียบข้อมูลและบริหารพื้นที่ในระบบจัดเก็บร่วมอย่างมีประสิทธิภาพ และหลีกเลี่ยงการเก็บไฟล์ส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับงานไว้ในพื้นที่สาธารณะ
4. การสำรองข้อมูล แนะนำให้พนักงานสำรองข้อมูลที่สำคัญไว้อย่างสม่ำเสมอ ไม่ว่าจะเป็นในอุปกรณ์ภายในเครื่อง (Drive C:/D:) หรือในสื่อเก็บข้อมูลที่ปลอดภัย เช่น Share Drive หรืออุปกรณ์สำรองภายนอก ทั้งนี้ ควรพิจารณาใช้วิธีสำรองข้ามไดรฟ์ เพื่อป้องกันความเสียหายจากฮาร์ดแวร์
5. ระบบสำรองข้อมูลขององค์กร ระบบเซิร์ฟเวอร์ขององค์กรอาจมีการสำรองข้อมูลอัตโนมัติในช่วงเวลาที่กำหนด เพื่อเพิ่มความมั่นใจในความปลอดภัยของข้อมูลร่วม

6. การรักษาความปลอดภัยของอุปกรณ์ เครื่องคอมพิวเตอร์พกพา เช่น Notebook ที่องค์กรจัดสรร อาจติดตั้งระบบรักษาความปลอดภัยล่วงหน้า เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต โดยควรหลีกเลี่ยงการเปลี่ยนแปลงการตั้งค่าดังกล่าว
7. การจัดการไฟล์สำคัญและความลับ สำหรับไฟล์ที่มีลักษณะเป็นข้อมูลความลับ เช่น ด้านบัญชี การเงิน หรือข้อมูลกลยุทธ์ทางธุรกิจ ควรมีการเข้ารหัส (Encrypt) และกำกับข้อความแสดงความเป็นความลับ เพื่อความรัดกุมในการจัดการ
8. การใช้งานอุปกรณ์พกพาและการถ่ายโอนข้อมูล ในกรณีที่จำเป็นต้องนำข้อมูลไปใช้นอกสถานที่ เช่น USB Drive แนะนำให้เข้ารหัสไฟล์ก่อนนำออก และควรใช้ซอฟต์แวร์ที่องค์กรแนะนำ เพื่อความปลอดภัย
9. การควบคุมการนำข้อมูลออกนอกระบบ การเผยแพร่ข้อมูลผ่านอุปกรณ์เก็บข้อมูลพกพา บริการ Cloud หรือช่องทางโซเชียลมีเดีย ควรอยู่ภายใต้การอนุมัติและนโยบายที่ชัดเจนขององค์กร เพื่อหลีกเลี่ยงการรั่วไหลโดยไม่ตั้งใจ
10. การใช้อุปกรณ์พกพาในระบบขององค์กร หากมีความจำเป็นต้องใช้อุปกรณ์พกพาส่วนตัวเชื่อมต่อกับคอมพิวเตอร์ขององค์กร ควรแจ้งและขออนุมัติจากผู้ดูแลระบบ หรือหัวหน้างานที่เกี่ยวข้อง โดยทั่วไปอาจกำหนดให้ใช้งานได้ในระยะเวลาจำกัด เช่น 90 วัน ก่อนที่ระบบจะทำการปิดสิทธิ์เชื่อมต่ออัตโนมัติ

การป้องกันไวรัสคอมพิวเตอร์

วัตถุประสงค์

เพื่อส่งเสริมให้พนักงานใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างต่อเนื่อง ปลอดภัย และลดความเสี่ยงต่อความเสียหายที่อาจเกิดขึ้นกับข้อมูล ระบบงาน และอุปกรณ์จากภัยคุกคามทางไซเบอร์ เช่น ไวรัส มัลแวร์ หรือการโจมตีจากแหล่งที่ไม่ปลอดภัย

แนวทางปฏิบัติ

1. ระบบป้องกันไวรัสขององค์กร ระบบป้องกันไวรัสที่ใช้งานภายในองค์กรได้รับการออกแบบให้สามารถอัปเดตฐานข้อมูลไวรัสผ่านเครือข่ายโดยอัตโนมัติทุกครั้งที่เปิดเครื่อง ผู้ใช้งานจึงควรอนุญาตให้โปรแกรมทำงานตามปกติ เพื่อให้ระบบได้รับการป้องกันอย่างมีประสิทธิภาพอยู่เสมอ
2. การจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์ แนะนำให้จัดเก็บข้อมูลสำคัญไว้ใน Drive D: ซึ่งแยกจากระบบปฏิบัติการใน Drive C: เพื่อลดความเสี่ยงหากเกิดการโจมตีหรือมีไวรัสแทรกซึมเข้าสู่ระบบ
3. หลีกเลี่ยงเว็บไซต์ที่มีความเสี่ยง ผู้ใช้งานควรหลีกเลี่ยงการเข้าถึงเว็บไซต์ที่มีเนื้อหาหรือพฤติกรรมที่อาจก่อให้เกิดความเสี่ยง เช่น เว็บไซต์ลามกอนาจาร, การพนัน, เกมที่ไม่ผ่านการรับรอง หรือเว็บไซต์ที่ผิดกฎหมาย เพื่อป้องกันมัลแวร์และภัยคุกคามอื่นๆ

4. ระมัดระวังการดาวน์โหลดข้อมูลจากเว็บไซต์ ควรพิจารณาอย่างรอบคอบก่อนตอบรับคำเชิญให้ดาวน์โหลดไฟล์หรือเปิดลิงก์จากแหล่งที่ไม่รู้จักหรือไม่น่าเชื่อถือ เพื่อหลีกเลี่ยงไฟล์ที่อาจแฝงมัลแวร์หรือไวรัส
5. การจัดการอุปกรณ์ที่ไม่ใช่ทรัพย์สินขององค์กร หากมีความจำเป็นต้องดำเนินการใดๆ กับอุปกรณ์ที่ไม่ใช่ทรัพย์สินของบริษัท เช่น การล้างระบบ (Format) หรือเชื่อมต่ออุปกรณ์ภายนอก ควรขอคำแนะนำหรือได้รับการอนุมัติจากผู้ดูแลระบบหรือผู้บริหารที่เกี่ยวข้องก่อนดำเนินการ เพื่อรักษาความปลอดภัยโดยรวมของระบบไอที

การใช้งานปัญญาประดิษฐ์ (AI) ภายในองค์กร

วัตถุประสงค์

เพื่อเป็นแนวทางในการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (AI) ภายในองค์กรอย่างมีความรับผิดชอบ โปร่งใส และสอดคล้องกับจริยธรรมและกฎหมายที่เกี่ยวข้อง รวมถึงเพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้น และส่งเสริมความเชื่อมั่นจากพนักงาน ลูกค้า และผู้มีส่วนเกี่ยวข้อง

แนวทางปฏิบัติ

1. ขอบเขตการใช้งาน AI แนวทางนี้ครอบคลุมถึงบุคลากรทุกระดับ รวมถึงบุคคลภายนอกที่ได้รับอนุญาตให้ใช้ AI ในระบบขององค์กร โดยรวมถึงซอฟต์แวร์ แพลตฟอร์ม และบริการ AI ทั้งที่พัฒนาโดยองค์กรเองหรือมาจากแหล่งภายนอก
2. การเคารพสิทธิส่วนบุคคล การใช้งาน AI ควรหลีกเลี่ยงพฤติกรรมที่ละเมิดสิทธิส่วนบุคคล หรืออาจสร้างผลกระทบทางลบต่อองค์กร หรือบุคคลอื่น ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจก็ตาม
3. การตัดสินใจที่สำคัญ การใช้ AI ในการตัดสินใจในประเด็นที่มีผลกระทบสูง เช่น การคัดเลือกบุคลากรหรือการทำสัญญา ควรได้รับการตรวจสอบโดยผู้รับผิดชอบโดยตรงก่อนเสมอ
4. การใช้ AI อย่างโปร่งใส ควรหลีกเลี่ยงการนำ AI ไปใช้ในลักษณะที่บิดเบือนข้อมูล สร้างข้อมูลเท็จหรือทำให้เกิดความเข้าใจผิด ไม่ว่าด้วยเหตุผลใด
5. การปกป้องข้อมูลและความลับ ผู้ใช้งานควรหลีกเลี่ยงการเปิดเผยข้อมูลภายใน อัลกอริทึมหรือกลไกการทำงานของระบบ AI ที่เป็นทรัพย์สินทางปัญญาหรือข้อมูลสำคัญขององค์กร รวมถึงข้อมูลของบุคคลภายนอก
6. การตรวจสอบก่อนนำ AI ไปใช้งานจริง ควรมีการทดสอบความถูกต้อง ความปลอดภัย และอคติที่อาจแฝงอยู่ในระบบก่อนนำ AI ไปใช้จริง โดยเฉพาะในงานที่เกี่ยวข้องกับการตัดสินใจหรือข้อมูลสำคัญ
7. การคุ้มครองข้อมูลส่วนบุคคล (PDPA) การใช้งาน AI ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ควรได้รับความยินยอมจากเจ้าของข้อมูล และปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด
8. ความรู้และการฝึกอบรม ผู้ที่พัฒนาและใช้งาน AI ควรได้รับการอบรมหรือทำความเข้าใจเกี่ยวกับหลักจริยธรรม แนวปฏิบัติ และความเสี่ยงที่เกี่ยวข้องกับการใช้งาน AI อย่างสม่ำเสมอ

9. ช่องทางการแจ้งข้อกังวล องค์กรควรมีช่องทางที่ชัดเจนสำหรับการรับฟังข้อคิดเห็นหรือข้อร้องเรียนเกี่ยวกับการใช้งาน AI จากทั้งพนักงานและลูกค้า
10. การปรับปรุงและดูแลระบบ AI ระบบ AI ควรได้รับการตรวจสอบและปรับปรุงอย่างต่อเนื่อง เพื่อให้ทันสมัย ลดความเสี่ยง และเพิ่มประสิทธิภาพในการใช้งาน
11. การรักษาสิทธิ์ในการใช้งานระบบ AI ควรหลีกเลี่ยงการถ่ายโอนหรือเปิดสิทธิ์การใช้งาน AI ขององค์กรให้บุคคลภายนอกที่ไม่ได้รับอนุญาตโดยตรง และควรใช้ด้วยความระมัดระวัง หากเกิดความเสียหายผู้เกี่ยวข้องอาจต้องรับผิดชอบตามความเหมาะสม

นโยบายเทคโนโลยีสารสนเทศฉบับนี้อนุมัติโดยที่ประชุมคณะกรรมการบริหาร ครั้งที่ 11/2568 เมื่อวันที่ 3 พฤศจิกายน 2568 และให้มีผลบังคับใช้ตั้งแต่วันที่ 3 พฤศจิกายน 2568

- สยาม เตียวตรานนท์ -
(นายสยาม เตียวตรานนท์)
กรรมการผู้จัดการ / ประธานกรรมการบริหาร