บริษัท นอร์ทอีส รับเบอร์ จำกัด (มหาชน)
NORTH EAST RUBBER PUBLIC COMPANY LIMITED
เลขประจำตัวผู้เสียภาษี (TAX ID) : 0107561000242

Tel. : 044-666928-9
Fax. : 044 666212 3
Website. : www.nerubber.com
E-Mail. : ner@nerubber.com

รหัสนโยบายที่ IT001
แก้ไขครั้งที่ 04
มีผลบังคับใช้วันที่ 7 ตุลาคม 2567

นโยบายการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ

1. การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control Policy) เป็นส่วนสำคัญของการรักษาความปลอดภัยในองค์กร โดยมีวัตถุประสงค์เพื่อป้องกันการเข้าถึงข้อมูลและทรัพยากรที่ไม่ได้รับอนุญาต ดังนี้

1.1. ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ก็ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบและผู้บังคับบัญชา ตามความจำเป็นต่อการใช้งาน เท่านั้น

1.2. บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้องขออนุญาตและได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารสายงานที่เกี่ยวข้องเท่านั้น

1.3. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งาน พร้อมจัดให้มีการทบทวนบัญชีและสิทธิ์การใช้งานของผู้ใช้งาน และมีหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

1.3.1. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์
หรือการมอบอำนาจ ดังนี้

1.3.1.1. กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง (User Access Management) เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- แก้ไข
- ไม่มีสิทธิ์

1.3.1.2. กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจให้ เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

1.3.1.3. ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของบริษัทฯ จะต้องลงทะเบียนข้อมูลกับผู้ดูแลระบบที่ได้รับมอบหมาย ยกเว้นการใช้งานในสถานะผู้มาเยือน

*** ในกรณีผู้มาเยือนจะใช้ User สำหรับ ใช้งาน Internet อย่างเดียวที่แยกวง IP สำหรับผู้มาเยือนอย่างเดียว

1.3.2. พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน/แผนก และจัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อ และสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

1.3.3. ดำเนินการแก้ไขข้อมูล สิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากผู้บริหารสายงานหรือผู้บังคับบัญชาของหน่วยงานนั้น

1.3.4. ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อได้รับเอกสารใบแจ้งตรวจสอบพนักงานลาออกของผู้ใช้งานจากฝ่ายบริหารทรัพยากรมนุษย์ ต้องดำเนินการระงับสิทธิ์ภายใน 7 วัน หรือเมื่อเปลี่ยนแปลงตำแหน่งงานต้องดำเนินการภายใน 15 วัน

1.4. ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึก ติดตามการใช้งานระบบสารสนเทศ และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ รวมถึงจัดทำบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศ และการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ฉบับปี 2550 และฉบับปรับปรุงแก้ไขปี 2560 ได้มีการบทบัญญัติที่เกี่ยวข้องกับการเก็บ Log File ไว้ดังนี้ "ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกิน 90 วัน แต่ไม่เกิน 2 ปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้"

1.5. ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกการผ่านเข้า - ออก สถานที่ตั้งของระบบสารสนเทศ (ห้องแม่ข่าย)

1.6. ผู้ดูแลระบบ ต้องจัดพื้นที่บนเครื่องแม่ข่ายให้เหมาะสมแก่ผู้ใช้งาน

1.7. ผู้ดูแลระบบ ต้องทำการสำรองข้อมูลของเครื่องแม่ (Server)

1.8. ผู้ดูแลระบบ ต้องจำกัดการเชื่อมต่อเครื่องคอมพิวเตอร์กับอุปกรณ์สื่อบันทึกข้อมูลต่างๆ เช่น Flash Drive, Smart Phone, External Hard Disk เป็นต้น

1.9. ผู้ดูและระบบ ต้องจัดให้มีการใช้ระบบ Multi-Factor Authentication (MFA) เพื่อเพิ่มความปลอดภัยในการยืนยันตัวตนก่อนเข้าใช้งานโปรแกรมหรือชุดข้อมูลที่สำคัญ เช่น ERP, E-Mail หรือข้อมูลที่ sensitive

1.10. พนักงานหรือผู้ใช้งานต้องได้รับการฝึกอบรมเกี่ยวกับ Cyber Security และวิธีป้องกันรู้จักวิธีป้องกันการโจมตีทางไซเบอร์ เช่น Phishing, Scammer, Spam และ Social Engineering เป็นต้น

1.11. ผู้ดูแลระบบต้องมีการจัดทำแผน Disaster Recovery Plan (DRP) เพื่อให้ครอบคลุมขั้นตอนการฟื้นฟูระบบในกรณีที่เกิดภัยพิบัติหรือการโจมตีทางไซเบอร์

1.12. ผู้ดูแลระบบต้องมีการจัดทำแผน Disaster Recovery Plan (BCP) เพื่อกำหนดแนวทางและขั้นตอนในการดำเนินธุรกิจเมื่อเกิดเหตุการณ์ที่ทำให้ธุรกิจหยุดชะงัก

1.13. ฝ่ายเทคโนโลยีสารสนเทศต้องมีการทบทวนนโยบายฯ เป็นประจำทุกปี หรือทุกครั้งที่มีการเปลี่ยนแปลงเกี่ยวกับเทคโนโลยีหรือระบบใหม่ๆ เพื่อให้มีความมั่นใจว่ามาตรฐานความปลอดภัยที่บริษัทฯ ใช้งานปัจจุบันมีมาตรฐานด้านความปลอดภัยหรือการดำเนินการครอบคุมอย่างมีประสิทธิภาพในการป้องกันหรือดำเนินการ

2.การบริหารจัดการการเข้าถึงเครือข่ายภายในของผู้ใช้งาน (User Access Management)

การบริหารจัดการการเข้าถึงเครือข่ายภายในของผู้ใช้งาน (User Access Management Policy) โดยยึดหลัก Zero Trust Security มีวัตถุประสงค์เพื่อป้องกันการเข้าถึงข้อมูลและทรัพยากรที่ไม่ได้รับอนุญาต เพื่อให้การเข้าถึงข้อมูลเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ และที่สำคัญสามารถตรวจสอบและยืนยันตัวตนของผู้ใช้และอุปกรณ์ทุกครั้งที่มีการเข้าถึงทรัพยากร ไม่ว่าจะอยู่ภายในหรือภายนอกเครือข่ายของบริษัทฯ ดังนี้

2.1. การลงทะเบียนผู้ใช้งาน (User Registration): การกำหนดขั้นตอนการลงทะเบียนผู้ใช้งานใหม่ รวมถึงการตรวจสอบและอนุมัติสิทธิ์การเข้าถึง

2.2. การจัดการบัญชีผู้ใช้งาน (User Account Management): การกำหนดสิทธิ์การเข้าถึงตามบทบาทและหน้าที่ของผู้ใช้งาน รวมถึงการตรวจสอบและทบทวนสิทธิ์การใช้งานอย่างสม่ำเสมอ

2.3. การจัดการรหัสผ่าน (Password Management): การกำหนดนโยบายการตั้งรหัสผ่านที่ปลอดภัย และการเปลี่ยนรหัสผ่านเป็นระยะ

2.4. การควบคุมการเข้าถึงเครือข่าย (Network Access Control): การกำหนดสิทธิ์การเข้าถึงเครือข่ายและทรัพยากรภายในเครือข่ายตามระดับความสำคัญของข้อมูล

2.5. การตรวจสอบและบันทึกการเข้าถึง (Access Monitoring and Logging): การบันทึกและตรวจสอบกิจกรรมการเข้าถึงข้อมูลเพื่อป้องกันการละเมิดความปลอดภัย

2.6. การพิสูจน์ตัวตน (Authentication): ผู้ใช้งานต้องทำการพิสูจน์ตัวตนด้วยชื่อผู้ใช้งานและรหัสผ่านก่อนการเข้าใช้งานเครือข่าย

3.การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control Policy) มีวัตถุประสงค์เพื่อป้องกันการเข้าถึงเครือข่ายไร้สายโดยไม่ได้รับอนุญาต และเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่าย ดังนี้

3.1. การควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ไม่ให้รั่วไหลออกนอกพื้นที่ที่ใช้งานระบบเครือข่ายไร้สายหรือรั่วไหลให้น้อยที่สุด

3.2. การเปลี่ยนค่าเริ่มต้น (Default Settings) ผู้ดูแลระบบต้องทำการเปลี่ยนค่าเริ่มต้นของ SSID (Service Set Identifier) ที่ตั้งค่ามาจากผู้ผลิต เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

3.3. การกำหนด SSID/VLAN แยกระหว่างผู้ใช้งานอินเตอร์เน็ตทั่วไปและผู้ใช้งานที่งานระบบภายในเช่น File Share, Programs, Database, Printer

3.4. การกำหนด IP/VLAN แยกแต่ละอาคารหรือแต่ละชั้น ออกจากกันเพื่อป้องกันการลุกลามของ Virus Computer

3.5. การลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

4.การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities Policy) มีวัตถุประสงค์เพื่อให้ผู้ใช้งานทราบถึงหน้าที่และความรับผิดชอบในการใช้งานระบบสารสนเทศขององค์กร อย่างถูกต้องและปลอดภัย ดังนี้

4.1. การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่หรือแจกจ่ายทำให้ผู้อื่นล่วงรู้

4.2. การกำหนดรหัสผ่าน ต้องมีจำนวนตัวอักขระไม่น้อยกว่า 8 ตัวอักษร โดยประกอบไปด้วยอักษรพิมพ์ใหญ่อย่างน้อย 1 ตัว อักษรพิมพ์เล็กอย่างน้อย 1 ตัว อักษรพิเศษอย่างน้อย 1 ตัว ตัวเลขอย่างน้อย 1ตัว เป็นต้น

4.3. ไม่ใช้ข้อมูลส่วนตัวในการกำหนดรหัสผ่านส่วนบุคคล เช่น ชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว/บริษัทฯ วันเกิด หมายเลขโทรศัพท์ เป็นต้น

4.4. ต้องทำการเปลี่ยนรหัสผ่านทุกๆ 3 เดือน

4.5. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจดจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

4.6. ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

4.7. กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่าน ให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

4.8. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์ หรือระบบสารสนเทศ และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อกหรือเกิดจากความผิดพลาดใดๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันทีโดยปฏิบัติตามแนวทาง ดังนี้

4.8.1 คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบสารสนเทศต้องทำการพิสูจน์ตัวตนทุกครั้ง

4.8.2 การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลและสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

4.9. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลตลอดจนเอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

4.10. ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครองและดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่/เปลี่ยนแปลง/ทำซ้ำหรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บริหารสายงาน/ผู้บังคับบัญชาหรือผู้มีอำนาจอนุมัติ

4.11. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของบริษัทฯ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

4.12. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร ทางบริษัทฯ เคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใด ทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้นตามหลัก PDPA

4.13. ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง/ฟังเพลงและเกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติงาน

4.14. ห้ามใช้ทรัพย์สินของหน่วยงาน ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม/ความมั่นคงของประเทศและกฎหมาย จนทำให้ผู้อื่นได้รับความเสียหาย

4.15. ผู้ใช้งานจะได้รับความเร็วในการใช้งาน Internet ดังต่อไปนี้

User ทั่วไป Upload : 5 Mbs.
Downloads : 5 Mbs.
** 1 user สามารถใช้ได้ 2 อุปกรณ์พร้อมกัน

User สำหรับผู้บริหาร Upload : 10 Mbs.
Downloads : 20 Mbs.
** 1 user สามารถใช้ได้ 10 อุปกรณ์พร้อมกัน

4.16. ผู้ใช้งานจะต้องบันทึกข้อมูลในพื้นที่ ที่ทางบริษัทฯ หรือหน่วยงานจัดให้เท่านั้น

4.17. คอมพิวเตอร์หรือคอมพิวเตอร์โน้ตบุ๊คต้องลงซอฟต์แวร์ป้องกันวัส (Endpoint) จากทางบริษัทฯ จัดหาให้เท่านั้น

5.การบริหารจัดการสินทรัพย์ (Assets Management)

การบริหารจัดการสินทรัพย์ (Asset Management Policy) มีวัตถุประสงค์เพื่อให้การจัดการสินทรัพย์ขององค์กรเป็นไปอย่างมีประสิทธิภาพและสอดคล้องกับเป้าหมายทางธุรกิจ ดังนี้

5.1. ผู้ใช้งานต้องไม่เข้าไปในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ที่เป็นเขตหวงห้าม โดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

5.2. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องควบคุมระบบคอมพิวเตอร์ และเครือข่าย เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

5.3. สำหรับบุคคลภายนอกหรือไม่ใช่เจ้าหน้าที่ที่เกี่ยวข้องเข้าห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายจะต้องมีผู้ดูแลระบบอยู่หรือติดตามเสมอ

5.4. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

5.5. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์ก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

5.6. ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บ ข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive/ Hard disk/ Solid State Drive (SSD)	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐาน การทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย

5.7. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่บริษัทฯ มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยบรรดารายการสินทรัพย์ (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือคืน สินทรัพย์ จะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่ได้รับมอบหมาย

5.8. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่า ทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

5.9. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน๊ตบุ๊ค ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้น ได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารสายงาน/ผู้บังคับบัญชา

5.10. ผู้ใช้งานมีสิทธิ์ใช้สินทรัพย์และระบบสารสนเทศต่างๆที่หน่วยงานจัดเตรียมไว้ให้ใช้งานโดยมีวัตถุประสงค์เพื่อการใช้งานของบริษัทฯ เท่านั้น

5.11. ชุดคอมพิวเตอร์พื้นฐานที่เหมาะสมสำหรับผู้ใช้งานทั่วไป ควรจะประกอบด้วย

OS	: Windows 10 Pro ขึ้นไป
Programs Office	: Microsoft Office Home &Business 2021 ขึ้นไป
CPU	: Intel core i3 gen 12th หรือ Ryzen 3 gen 5th ขึ้นไป
Ram	: DDR4 8 GB ขึ้นไป
SSD	: 240 GB ขึ้นไป
Monitor (จอ)	: 21” ขึ้นไป
UPS (เครื่องสำรองไฟ)	: ต้องสำรองไฟได้อย่างน้อย 5 นาทีขึ้นไป

6.การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing Malwares)

การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and Intellectual Property and Preventing Malwares) มีวัตถุประสงค์เพื่อให้การใช้งานซอฟต์แวร์ในองค์กรเป็นไปอย่างถูกต้องตามกฎหมาย และปลอดภัยจากภัยคุกคามทางไซเบอร์ ดังนี้

6.1. บริษัทฯ ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิด ลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

6.2. ซอฟต์แวร์ (Software) ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการ ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่นๆ ยกเว้นได้รับการอนุญาตจากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

7.การใช้งานอากาศยานซึ่งไม่มีนักบิน (Drone)

การใช้งานอากาศยานซึ่งไม่มีนักบิน (Drone) มีวัตถุประสงค์เพื่อให้การใช้งานโดรนเป็นไปอย่างปลอดภัยและถูกต้องตามกฎหมาย ดังนี้

7.1. การจดทะเบียนและการอนุญาต: ผู้ใช้งานโดรนต้องทำการจดทะเบียนและขออนุญาตใช้งานจากหน่วยงาน
ที่เกี่ยวข้อง เช่น สำนักงานการบินพลเรือนแห่งประเทศไทย (CAAT) และ กสทช. (สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ) เพื่อให้สามารถใช้งานโดรนได้อย่างถูกต้องตามกฎหมาย

7.2. การควบคุมการบิน: การกำหนดพื้นที่และความสูงในการบินโดรน เช่น ห้ามบินในพื้นที่หวงห้ามหรือใกล้สนามบิน และต้องบินในระดับความสูงที่กำหนดไว้

7.3. การรักษาความปลอดภัย: การติดตั้งระบบป้องกันการชนและการควบคุมการบินอัตโนมัติ เพื่อป้องกันอุบัติเหตุและการชนกับสิ่งกีดขวาง

7.4. การอบรมและการรับรอง: ผู้ใช้งานโดรนต้องผ่านการอบรมและได้รับการรับรองจากหน่วยงานที่เกี่ยวข้อง เพื่อให้มีความรู้และทักษะในการใช้งานโดรนอย่างปลอดภัย

7.5. การปฏิบัติตามกฎหมาย: การปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องกับการใช้งานโดรน เช่น พระราชบัญญัติเดินอากาศ พ.ศ. 2497 และประกาศกระทรวงคมนาคม

8.การใช้งานระบบกล้องวงจรปิด

การใช้งานระบบกล้องวงจรปิด (CCTV Policy) มีวัตถุประสงค์เพื่อให้การใช้งานกล้องวงจรปิดเป็นไปอย่างถูกต้องตามกฎหมายและรักษาความปลอดภัยของข้อมูลส่วนบุคคล

8.1. บริษัทฯ ติดตั้งระบบกล้องวงจรปิดเพื่อความปลอดภัยของพนักงานและทรัพย์สิน

8.2. บริษัทฯ ติดตั้งระบบกล้องวงจรปิดเพื่อป้องกันและตรวจสอบเหตุการณ์ที่อาจเกิดขึ้น เช่น การขโมย การทำลายทรัพย์สิน หรืออุบัติเหตุ

8.3. กำหนดพื้นที่ที่ต้องการติดตั้งกล้อง เช่น ทางเข้าหลัก ห้องเก็บของ สถานที่จอดรถ สถานที่ปฏิบัติงาน เป็นต้น

8.4. หลีกเลี่ยงการติดตั้งกล้องในพื้นที่ที่มีความเป็นส่วนตัวสูง เช่น ห้องน้ำ หรือห้องพักพนักงาน

8.5. ระยะเวลาที่จะเก็บข้อมูลจากกล้อง CCTV อย่างน้อย 60 วัน

8.6. สิทธิ์การเข้าถึงข้อมูล

8.6.1. ผู้บริหาร(เจ้าของกิจการ) หรือกรรมการผู้มีสิทธิ์อนุมัติการดำเนินการในบริษัทฯ

8.6.2. ผู้รับผิดชอบที่ได้รับการแต่งตั้งจากประธานเจ้าหน้าที่บริหาร หรือกรรมการผู้มีสิทธิ์อนุมัติการดำเนินการในบริษัทฯ

- เจ้าหน้าที่รักษาความปลอดภัย
- ผู้ดูแลระบบ (ผู้ดูแลระบบ : ฝ่ายเทคโนโลยีสารสนเทศ)

8.6.3. ผู้ได้รับอนุญาตจากผู้บริหาร(เจ้าของกิจการ) หรือกรรมการผู้มีสิทธิ์อนุมัติการดำเนินการในบริษัทฯ

8.6.4. สำหรับบุคคลภายนอก

- เจ้าหน้าที่หน้าที่รัฐ หากมีการขอดูภาพกล้องวงจรปิดเพื่อการสอบสวนจำเป็นต้องมีการร้องขอเป็นลายลักษณ์อักษร
- บุคคลภายนอกทั่วไป หากมีการขอดูภาพกล้องวงจรปิดจำเป็นต้องมีการร้องขอเป็นลายลักษณ์อักษร และใบบันทึกประจำวัน

8.7. แจ้งพนักงานและบุคคลภายนอกเกี่ยวกับการติดตั้ง CCTV ผ่านป้ายหรือประกาศที่เห็นได้ชัดเจน

8.8. ในกรณีที่มีกฎหมายหรือระเบียบที่เกี่ยวข้อง ขอความยินยอมจากพนักงานหรือบุคคลที่เกี่ยวข้องก่อนการติดตั้ง

8.9. การบำรุงรักษาอุปกรณ์ CCTV อย่างสม่ำเสมอเพื่อให้ทำงานได้อย่างมีประสิทธิภาพ

- กรณีบำรุงรักษากำหนดให้มีการบำรุงษาทั้งหมดอย่างน้อยไตรมาสละ 1 ครั้ง
- กรณีอุปกรณ์มีการชำรุด
  - แก้ปัญหาได้เองหากเกิดปัญหาควรแก้ไขทันทีหลังจากทราบการชำรุด
  - หากไม่สามารถแก้ไขได้ด้วยตนเอง ต้องรีบแจ้งทันทีให้ผู้รับเหมาหรือ Outsource เข้ามาแก้ไข

Tel. : 044-666928-9
Fax. : 044-666212-3
Website. : www.nerubber.com
E-Mail. : ner@nerubber.com

9.การใช้ระบบ AI

นโยบายนี้ มีวัตถุประสงค์เพื่อกำหนดแนวทางการใช้งานปัญญาประดิษฐ์ (AI) ในบริษัทฯ เพื่อให้มั่นใจว่าการใช้งาน AI เป็นไปอย่างมีประสิทธิภาพ ปลอดภัย และสอดคล้องกับกฎหมายและจริยธรรม

9.1. บริษัทฯ ต้องจัดให้มีการฝึกอบรมและให้ความรู้เกี่ยวกับการใช้งาน AI กับพนักงาน

9.2. พนักงานหรือผู้ใช้งานต้องได้รับการฝึกอบรมเกี่ยวกับความเสี่ยง และวิธีป้องกันการละเมิดความปลอดภัยจากการใช้งาน AI

9.3. ต้องมีการรายงานผลการตรวจสอบ และปัญหาที่พบจากการใช้งาน AI ให้กับผู้บริหารทราบ

9.4. ต้องมีการทดสอบและประเมินผลกระทบของการใช้งาน AI

จึงประกาศให้ทราบโดยทั่วกัน ณ วันที่ 7 ตุลาคม 2567

ลงชื่อ.....
(นายปริญญา ลีนะธรรม)
รองประธานเจ้าหน้าที่บริหารสายงานพัฒนาองค์กร

ลงชื่อ.....
(นายชูวิทย์ จึงธนสมบูรณ์)
ประธานเจ้าหน้าที่บริหาร