บริษัท นอร์ทอีส รับเบอร์ จำกัด (มหาชน)
NORTHEAST 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 331
แก้ไขครั้งที่ 03
มีผลบังคับใช้วันที่ 1 กรกฎาคม 2566

นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ

1.การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

1. ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ก็ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบและผู้บังคับบัญชา ตามความจำเป็นต่อการใช้งาน เท่านั้น

2. บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้องขออนุญาตและได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารสายงานที่เกี่ยวข้องเท่านั้น

3. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งาน พร้อมจัดให้มีการทบทวนบัญชีและสิทธิ์การใช้งานของผู้ใช้งาน และมีหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวน สิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

3.1 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

3.1.1 กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง (User Access Management) เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- แก้ไข
- ไม่มีสิทธิ์

3.1.2 กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

3.1.3 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของบริษัทฯ จะต้องลงทะเบียนข้อมูลกับผู้ดูแลระบบที่ได้รับมอบหมาย ยกเว้นการใช้งานในสถานะผู้มาเยือน

***ในกรณีผู้มาเยือนจะใช้ User สำหรับ ใช้งาน Internet อย่างเดียวที่แยกวง IP สำหรับผู้มาเยือนอย่างเดียว

3.2 พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน/แผนก และจัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อ และสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

3.3 ดำเนินการแก้ไขข้อมูล สิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากผู้บริหารสายงานหรือผู้บังคับบัญชาของหน่วยงานนั้น

3.4 ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อได้รับเอกสารใบแจ้งตรวจสอบพนักงานลาออกของผู้ใช้งานจากฝ่ายบริหารทรัพยากรมนุษย์ ต้องดำเนินการระงับสิทธิ์ภายใน 7 วัน หรือเมื่อเปลี่ยนแปลงตำแหน่งงานต้องดำเนินการภายใน 15 วัน

4. ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึก ติดตามการใช้งานระบบสารสนเทศ และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ รวมถึงจัดทำบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศ

3.4 ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อได้รับเอกสารใบแจ้งตรวจสอบพนักงานลาออกของผู้ใช้งานจากฝ่ายบริหารทรัพยากรมนุษย์ ต้องดำเนินการระงับสิทธิ์ภายใน 7 วัน หรือเมื่อเปลี่ยนแปลงตำแหน่งงานต้องดำเนินการภายใน 15 วัน

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

5. ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกการผ่านเข้า-ออก สถานที่ตั้งของระบบสารสนเทศ (ห้องแม่ข่าย)

7. ผู้ดูแลระบบ ต้องจัดพื้นที่บนเครื่องแม่ข่ายให้เหมาะสมแก่ผู้ใช้งาน

8. ผู้ดูแลระบบ ต้องทำการสำรองข้อมูลของเครื่องแม่ (Server)

2.การบริหารจัดการการเข้าถึงเครือข่ายภายในของผู้ใช้งาน (User Access Management)

ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

1. จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานสำหรับระบบเครือข่าย
2. ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งานเพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน
3. ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ
4. ผู้ดูแลระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และได้รับความเห็นชอบให้ใช้งานจากผู้บริหารสายงาน/ผู้จัดการและผู้บังคับบัญชาเท่านั้น

3.การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

1. การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้ รหัสผ่าน (Password)

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

3. ไม่ใช้ข้อมูลส่วนตัวในการกำหนดรหัสผ่านส่วนบุคคล เช่น ชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว/บริษัทฯ วันเกิด หมายเลขโทรศัพท์ เป็นต้น เพราะเป็นข้อมูลที่สามารถรู้ได้อย่างง่ายดาย

***โดยสามารถตรวจสอบความปลอดภัยของรหัสผ่านได้ง่ายๆ ผ่านทางเว็บไซต์

Website : https://www.security.org/how-secure-is-my-password/

4. ต้องทำการเปลี่ยนรหัสผ่านทุกๆ 3 เดือน

5. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจดจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

6. ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

7. กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่าน ให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

8. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศ และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อกหรือเกิดจากความผิดพลาดใดๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันทีโดยปฏิบัติตามแนวทาง ดังนี้

8.1 คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบสารสนเทศต้องทำการพิสูจน์ตัวตนทุกครั้ง

8.2 การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลและสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

9. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

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

11. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของบริษัทฯ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

12. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตาม เห็นสมควร ทางบริษัทฯ เคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใด ทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้นตามหลัก PDPA

13. ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง/ฟังเพลงและเกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติงาน

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

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

16. ผู้ใช้งานจะต้องบันทึกข้อมูลในพื้นที่ ที่ทางบริษัทฯ หรือหน่วยงานจัดให้เท่านั้น

4.การบริหารจัดการสินทรัพย์ (Assets Management)

1. ผู้ใช้งานต้องไม่เข้าไปในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ที่เป็นเขตหวงห้าม โดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

2. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องควบคุมระบบคอมพิวเตอร์ และเครือข่าย เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

3. สำหรับบุคคลภายนอกหรือไม่ใช่เจ้าหน้าที่ที่เกี่ยวข้องเข้าห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย จะต้องมีผู้ดูแลระบบอยู่หรือติดตามเสมอ

4. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจ ส่วนบุคคล

5. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์ก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

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

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

8. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่า ทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

9. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน๊ตบุ๊ค ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้น ได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารสายงาน/ผู้บังคับบัญชา

10. ผู้ใช้งานมีสิทธิ์ใช้สินทรัพย์และระบบสารสนเทศต่างๆที่หน่วยงานจัดเตรียมไว้ให้ใช้งานโดยมีวัตถุประสงค์เพื่อการใช้งานของบริษัทฯ เท่านั้น

11. ชุดคอมพิวเตอร์พื้นฐานที่เหมาะสมสำหรับผู้ใช้งานทั่วไป ควรจะประกอบด้วย

OS	: Windows 11 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
(*** แบตเตอร์รี่ควรเปลี่ยนทุกๆ 1 ปี)	

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

1. ทางบริษัทฯ ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิด ลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

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

6.การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

1. ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ไม่ให้รั่วไหลออกนอกพื้นที่ที่ใช้งานระบบเครือข่ายไร้สายหรือรั่วไหลให้น้อยที่สุด

2. ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน และกำหนดให้ซ่อน SSID (Service Set Identifier) สำหรับใช้งานระบบเครือข่ายภายใน

3. ผู้ดูแลระบบเลือกใช้วิธีการควบคุมชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

4. ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้ง มีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

7.การใช้งานอากาศยานซึ่งไม่มีนักบิน (Drone)

อากาศยานซึ่งไม่มีนักบิน (Drone) จะต้องขึ้นทะเบียนกับ คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ ก่อนนำมาใช้งานเพื่อกิจการของบริษัทฯ และต้องได้รับอนุญาตจากทางผู้บังคับบัญชา เท่านั้น

จึงประกาศให้ทราบโดยทั่วกัน ณ วันที่ 1 กรกฎาคม 2566

ลงชื่อ.....

(นายชูวิทย์ จึงธนสมบูรณ์)

ประธานเจ้าหน้าที่บริหาร