

# นโยบายการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศ

บริษัท เอ็น.ดี. รับเบอร์ จำกัด (มหาชน)  
N.D. Rubber Public Company Limited



(นายชัยสิทธิ์ สัมฤทธิวิธินา)

กรรมการผู้จัดการ

ผู้อนุมัติ

## นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

### นโยบายการใช้ Internet, E-mail (IT-Internet)

1. ในเวลาทำงานอนุญาตให้ใช้อินเทอร์เน็ตได้เฉพาะเว็บไซต์ที่ได้รับอนุญาตหรือเว็บไซต์ที่เกี่ยวข้องกับงานเท่านั้น
2. Password (รหัสผ่าน) เข้าสู่ระบบ E-mail ต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร ต้องมีอักษรตัวพิมพ์เล็กตัวพิมพ์ใหญ่และตัวเลข
3. ควรเปลี่ยน Password ใหม่ ทุกๆ 90 วัน
4. ห้ามใช้ E-mail ของพนักงานไปใช้ลงทะเบียนในเรื่องส่วนตัวบน Internet เช่น ใช้ E-mail ลงประกาศขายสินค้าบน Internet เป็นต้น
5. สำหรับหน่วยงาน หรือบุคคลภายนอก ที่มีความจำเป็นต้องใช้งานระบบเครือข่าย Internet ต้องได้รับอนุญาตจาก IT หรือผู้ที่เกี่ยวข้องก่อนทุกครั้ง ตามเอกสารแจ้งในใบขอดำเนินการด้าน IT

### นโยบายการป้องกัน Virus ด้วย Sophos Antivirus

1. ผู้ใช้ระบบทุกท่านจะถูกติดตั้ง Sophos Antivirus พร้อม Update Pattern
2. ผู้ใช้ระบบทุกท่านสามารถสั่ง Scan Virus ได้ที่ Local Drive เท่านั้น
3. บริษัทฯ ไม่อนุญาตให้นำสื่อบันทึกภายนอก มาใช้งานกับเครื่องคอมพิวเตอร์ของบริษัทฯ เพื่อป้องกัน Virus
4. เมื่อผู้ใช้ระบบติด Virus ควรทำการติดต่อ IT Helpdesk ที่เบอร์ 110 ทันที
5. แผนก IT ดำเนินการสื่อสารให้ความรู้เกี่ยวกับการป้องกัน Virus

### นโยบายการใช้รหัสผ่าน (IT-Password)

นโยบายการตั้งรหัสผ่านเพื่อเข้าใช้งานคอมพิวเตอร์กำหนดเป็นดังนี้

1. สำหรับระบบปฏิบัติการ รหัสผ่านมีความยาวไม่น้อยกว่า 8 ตัวอักษร ซึ่งประกอบด้วยตัวอักษรพิมพ์เล็กพิมพ์ใหญ่และตัวเลข เช่น It123456 , Admin678 ยกเว้นอักขระพิเศษ เช่น @, #, \$, % เป็นต้น
2. รหัสผ่านมีอายุ 90 วัน และรหัสผ่านไม่สามารถนำมาใช้ซ้ำได้ 5 ครั้งติดต่อกัน
3. รหัสผ่านต้องเป็นแบบ Shadowed (\*) (ไม่สามารถแสดงหรือพิมพ์ออกมาได้)
4. รหัสผ่านเริ่มต้น จะถูกเปลี่ยนแปลงทันทีเมื่อส่งมอบถึงมือผู้ใช้ (ผู้ใช้งาน Login ครั้งแรก)
5. รหัสผ่านเริ่มต้นที่ติดมากับระบบ รวมถึงบัญชีผู้ใช้ที่ไม่ได้ใช้ จะต้องถูกล็อกไม่ให้นำไปใช้งานได้
6. การใส่รหัสผ่านสามารถใส่ผิดได้ 3 ครั้งถ้าเกินชื่อผู้ใช้จะถูกล็อกจนกว่าจะแจ้งให้เจ้าหน้าที่ IT ปลดล็อกให้

### นโยบาย การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (IT-PC)

1. พนักงานไม่มีสิทธิ์ที่จะติดตั้งโปรแกรมใดๆ ลงบนเครื่องคอมพิวเตอร์ด้วยตนเอง โปรแกรมใดๆ ที่จำเป็นต้องใช้เพื่อทำงาน หรือกิจกรรมอื่นใด จะต้องแจ้งในใบขอดำเนินการด้าน IT และได้รับอนุมัติจากหัวหน้างานแล้วเจ้าหน้าที่ IT จะทำการติดตั้งโปรแกรมให้ตามที่ได้รับอนุมัติ
2. ในกรณีที่พนักงานใช้โปรแกรมอื่นใดนอกเหนือจากที่ได้รับอนุญาตและประกาศอย่างเป็นทางการแล้ว หากมีปัญหาเกิดขึ้น เช่นปัญหาด้านลิขสิทธิ์ หรือความเสียหายอื่นใดที่อาจเกิดขึ้นได้ พนักงานผู้นั้นจะต้องรับผิดชอบค่าใช้จ่าย และความเสียหายที่เกิดขึ้นแต่เพียงผู้เดียว
3. ไม่เก็บไฟล์รูปภาพ สื่อวิดีโอ หรือไฟล์อื่นใด ที่ขัดกับหลักกฎหมาย ศีลธรรม และจริยธรรมอันดีงาม ไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล หากมีปัญหาเกิดขึ้น เช่น ปัญหาทางด้านลิขสิทธิ์ หรือความเสียหายอื่นใด ที่อาจเกิดขึ้นได้ พนักงานผู้นั้นจะต้องเป็นผู้รับผิดชอบค่าใช้จ่าย และความเสียหายที่เกิดขึ้นแต่เพียงผู้เดียว
4. ให้ Lock เครื่องคอมพิวเตอร์หรือ Log off ออกจากเครื่องทุกครั้งที่ถูกออกจากโต๊ะ ไม่ปล่อยให้ผู้อื่นสามารถใช้เครื่องคอมพิวเตอร์ได้ในขณะที่พนักงานไม่อยู่ ถ้าไม่ปฏิบัติตาม หากมีผู้อื่นเข้าไปใช้งานแล้วเกิดความเสียหายใดๆ ก็ตาม User ที่ Log in ค้างไว้จะต้องเป็นผู้รับผิดชอบเสมือนได้ใช้งานด้วยตัวเอง
5. ปิดหน้าจอทุกครั้งที่ไม่ได้นั่งทำงานต่อเนื่อง และปิดเครื่องคอมพิวเตอร์และจอคอมพิวเตอร์ก่อนกลับบ้านทุกครั้ง

### นโยบายการทำงานของผู้ดูแลระบบ (IT-ADMIN)

1. ทำการทดสอบก่อนที่จะติดตั้งโปรแกรม หรือปรับปรุงค่าบางอย่างบนระบบงานจริง
2. ไม่ทิ้งแผ่นดิสก์ แผ่นซีดี ไว้บนเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้
3. Log off ออกจากระบบทุกครั้งหลังจากใช้หน้าจอเครื่องคอมพิวเตอร์เม่่าข้าย

### นโยบายการป้องกันการโจมตีระบบ (IT-Intrusion Detection Policy)

1. การบันทึกการเข้าสู่ระบบ ของระบบปฏิบัติการ ต้องเปิดใช้งานและไม่สามารถแก้ไขข้อมูลใน log ได้
2. ฟังก์ชันการแจ้งเตือนและการบันทึกข้อมูล Log ของไฟล์ Antivirus จะต้องเปิดการใช้งาน
3. Log file การใช้งานอินเทอร์เน็ต ตาม พ.ร.บ.คอมพิวเตอร์ 2560 ต้องเก็บอย่างน้อย 90 วัน

### นโยบายการเก็บสำรองข้อมูล (DATA-BACKUP)

1. ทำการเก็บสำรองข้อมูลเอกสาร ไฟล์งานต่างๆ ของผู้ใช้งาน ใน Map-Drive ต่อไปนี้คือ public folder อย่างน้อย 3 วัน และข้อมูลที่เก็บใน Drive C:, D:, E: อย่างเช่น my document, desktop เป็นต้น จะไม่ได้รับการสำรองข้อมูลหากข้อมูลในส่วนนี้สูญหาย ทาง IT จะทำการกู้ข้อมูลให้ ด้วยโปรแกรม กู้ข้อมูลที่เหมาะสม แต่จะไม่รับประกันว่าข้อมูลที่กู้จะได้กลับมาครบถ้วน หรืออาจไม่ได้เลย

2. หากผู้ใช้งานทำข้อมูลสูญหาย สามารถแจ้ง IT ด้วยการมาแจ้งด้วยตนเอง เท่านั้น เพื่อจะได้สอบถามถึงปัญหา และตำแหน่งที่เก็บข้อมูลเดิมก่อนจะสูญหาย และจะกู้คืนข้อมูลดังกล่าวให้ทันทีที่ได้รับแจ้ง
3. อุปกรณ์บันทึกข้อมูลสำรอง ควรอยู่ในตำแหน่งที่ปลอดภัย หรือควรมีที่ติดตั้งมากกว่า 1 ที่ติดตั้ง เพื่อความปลอดภัย

#### **นโยบายการบำรุงรักษาอุปกรณ์ IT (IT-Maintenance)**

1. หากเจ้าหน้าที่ IT พบว่าอุปกรณ์ IT มีปัญหาด้าน Hardware และประเมินความสะอาดด้วยสายตา แล้วพบว่าสกปรก หรือพบว่าอาจก่อให้เกิดปัญหาต่อการใช้งานในอนาคต จะต้องทำความสะอาดหรือป้องกันปัญหาที่จะเกิดขึ้นถึงแม้อุปกรณ์ชิ้นนั้นจะยังใช้งานได้ก็ตาม
2. จัดทำแผนการบำรุงรักษาทั้งระบบ รวมถึง Hardware และ Software อย่างสม่ำเสมอทุกๆ 4 เดือน โดยการตรวจดูตรวจทางกายภาพ บางอย่างไม่สามารถทำความสะอาดได้ ส่วน Software ต้องสอบถามจากทำใช้งานของ User แทนตามเอกสาร Checklist