นโยบายการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศ

บริษัท เอ็น.ดี. รับเบอร์ จำกัด (มหาชน)

N.D. Rubber Public Company Limited

“นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ”

บริษัท เอ็น.ดี.รับเบอร์ จำกัด (มหาชน) “บริษัทฯ” และบริษัทในเครือ มีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดวิธีดำเนินการเพื่อใช้เป็นแนวปฏิบัติ และป้องการการสูญหาย รวมทั้งป้องกันความเสียหาย ทั้งทางด้าน Software และ Hardware เมื่อเกิดเหตุกรณีฉุกเฉินด้าน IT โดยมีรายละเอียดดังนี้

นโยบายการใช้ Internet, E-mail (IT-Internet)

1. ในเวลาทำงานอนุญาตให้ใช้อินเตอร์เน็ตได้เฉพาะเว็บไซท์ ที่ได้รับอนุญาตหรือเว็บไซท์ ที่เกี่ยวข้องกับงานเท่านั้น
2. Password (รหัสผ่าน) เข้าระบบ E-mail ต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร ต้องมีอักษรตัวพิมพ์เล็กตัวพิมพ์ใหญ่และตัวเลข โดยฝ่าย IT จะเป็นผู้กำหนดรหัสผ่านพร้อมกับติดตั้ง Outlook ให้ผู้ใช้งานเท่านั้น
3. ห้ามใช้ E-mail ของพนักงานไปใช้ลงทะเบียนในเรื่องส่วนตัวบน Internet เช่น ใช้ E-mail ลงประกาศขายสินค้าบน Internet เป็นต้น
4. สำหรับหน่วยงาน หรือบุคคลภายนอก ที่มีความจำเป็นต้องใช้งานระบบเครือข่าย Internet ต้องได้รับอนุญาต จาก 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. แผนกIT ดำเนินการสื่อสารให้ความรู้เกี่ยวกับการป้องกันVirus

นโยบายการใช้รหัสผ่าน (IT-Password)

รหัสผ่านของแต่ละระบบต้องกำหนดดังนี้

1. สำหรับระบบปฏิบัติการ รหัสผ่านมีความยาวไม่น้อยกว่า 8 ตัวอักษร ซึ่งประกอบด้วยตัวอักขระพิมพ์เล็กพิมพ์ใหญ่และตัวเลข 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 จะต้องถูกล็อคไม่ใช้นำไปใช้งานได้
6. การใส่รหัสผ่านสามารถใส่ผิดได้ 5 ครั้งถ้าเกินชื่อผู้ใช้จะถูกล็อคจนกว่าจะแจ้งให้เจ้าหน้าที่ IT ปลดล็อคให้

นโยบาย การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (IT- Computer/ Laptop)

1. พนักงานไม่มีสิทธิ์ที่จะติดตั้งโปรแกรมใดๆ ลงบนเครื่อง Computer/ Laptop ด้วยตนเอง โปรแกรมใดๆ ที่จำเป็นต้องใช้เพื่อทำงาน หรือกิจกรรมอื่นใด จะต้องแจ้งในใบขอดำเนินการด้าน IT และได้รับอนุมัติจากหัวหน้างาน แล้วเจ้าหน้าที่ IT จะทำการติดตั้งโปรแกรมให้ตามที่ได้รับการอนุมัติ
2. ในกรณีที่พนักงานใช้โปรแกรมอื่นใดนอกเหนือจากที่ได้รับอนุญาตและประกาศอย่างเป็นทางการแล้ว หากมีปัญหาเกิดขึ้น เช่นปัญหาด้านลิขสิทธิ์ หรือความเสียหายอื่นใดที่อาจเกิดขึ้นได้ พนักงานผู้นั้นจะต้องรับผิดชอบค่าใช้จ่าย และความเสียหายที่เกิดขึ้นแต่เพียงผู้เดียว
3. ไม่เก็บไฟล์รูปภาพ สื่อวิดีโอ หรือไฟล์อื่นใด ที่ขัดกับหลักกฎหมาย ศีลธรรม และจริยธรรมอันดีงาม ไว้บนเครื่อง Computer/ Laptop ส่วนบุคคล หากมีปัญหาเกิดขึ้น เช่น ปัญหาทางด้านลิขสิทธิ์ หรือความเสียหายอื่นใด ที่อาจเกิดขึ้นได้ พนักงานผู้นั้นจะต้องเป็นผู้รับผิดชอบค่าใช้จ่าย และความเสียหายที่เกิดขึ้นแต่เพียงผู้เดียว
4. ให้ Lock เครื่องคอมพิวเตอร์หรือ Log off ออกจากเครื่องทุกครั้งที่ลุกออกจากโต๊ะ ไม่ปล่อยให้ผู้อื่นสามารถใช้เครื่อง Computer/ Laptop ได้ในขณะที่พนักงานไม่อยู่ ถ้าไม่ปฏิบัติตาม หากมีผู้อื่นเข้าไปใช้งานแล้วเกิดความเสียหายใด ๆ ก็ตาม User ที่ Log in ค้างไว้จะต้องเป็นผู้รับผิดชอบเสมือนได้ใช้งานด้วยตัวเอง
5. ปิดหน้าจอทุกครั้งที่ไม่ได้นั่งทำงานต่อเนื่อง และปิดเครื่อง Computer/ Laptop และจอ Computer/ Laptop ก่อนกลับบ้านทุกครั้ง

<u>นโยบายการทำงานของผู้ดูแลระบบ (IT-ADMIN)</u>

1. ทำการทดสอบก่อนที่จะติดตั้งโปรแกรม หรือปรับปรุงค่าบางอย่างบนระบบงานจริง
2. ไม่ทิ้งแผ่นดิสก์ แผ่นซีดี ไว้บนเครื่อง Computer/ Laptop เมื่อไม่ได้ใช้
3. Log off ออกจากระบบทุกครั้งหลังจากใช้หน้าจอเครื่อง Computer/ Laptop แม่ข่าย

<u>นโยบายการป้องกันการจู่โจมระบบ (IT-Intrusion Detection Policy)</u>

1. การบันทึกการเข้าสู่ระบบ ของระบบปฏิบัติการ ต้องเปิดใช้งานและไม่สามารถแก้ไขข้อมูลใน log ได้
2. ฟังก์ชั่นการแจ้งเตือนและการบันทึกข้อมูล Log ของไฟล์ Antivirus จะต้องเปิดการใช้งาน
3. Log file การใช้งานอินเตอร์เน็ต ตาม พ.ร.บ.คอมพิวเตอร์ 2560 ต้องเก็บอย่างน้อย 90 วัน
4. เปิดฟังก์ชั่นFire wall features : APT Blocker และ Gateway Antivirus เพื่อป้องกันการโจมตี

<u>นโยบายการเก็บสำรองข้อมูล (DATA-BACKUP)</u>

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

<u>นโยบายการบำรุงรักษาอุปกรณ์ไอที (IT-Maintenance)</u>

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

นโยบายทบทวนสิทธิ์ (Review Policy)

ต้องมีการตรวจสอบและทบทวนสิทธิ์การใช้งานของระบบอย่างน้อย 1 ครั้ง/ปี

นโยบายการจัดลำดับความสำคัญของข้อมูล (Data Share Policy)

นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดแนวทางในการจัดการและปกป้องข้อมูลของบริษัทอย่างเหมาะสม เพื่อป้องกันการรั่วไหลของข้อมูลที่อาจก่อให้เกิดความเสียหายต่อบริษัท โดยการจัดลำดับความสำคัญของข้อมูลจะช่วยให้บริษัทสามารถกำหนดมาตรการรักษาความปลอดภัยที่เหมาะสมกับข้อมูลแต่ละประเภทได้

SL1 = ***ข้อมูลลับที่สุด Secret*** หมายถึง ข้อมูลที่ไม่สามารถเปิดเผยได้ ต้องมีการจำกัดสิทธิ์การเข้าถึง หากถูกเปิดเผยโดยไม่ได้รับอนุญาตจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

SL2 = ***ข้อมูลลับ Confidential*** หมายถึง ข้อมูลที่ไม่ควรเปิดเผย ต้องกำหนดสิทธิ์เข้าถึงได้เฉพาะบางกลุ่มเท่านั้น หากถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียต่อบริษัท

SL3 = ***ข้อมูล ใช้ภายใน Internal Use*** หมายถึง ข้อมูลที่จัดทำขึ้นใช้ภายในองค์กร และควรมีการควบคุมการใช้ข้อมูล ซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต

SL4 = ***ข้อมูลเปิดเผยได้ Public*** หมายถึง ข้อมูลที่สามารถเปิดเผยได้แก่บุคคลทั่วไปโดยไม่ก่อให้เกิดความเสียหายกับบริษัท

นโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศฉบับนี้ ได้ผ่านการพิจารณาและเห็นชอบจากคณะกรรมการบริษัท ในการประชุมคณะกรรมการบริษัท ครั้งที่ 4/2569 เมื่อวันที่ 14 พฤษภาคม 2569

(DATO' Alex Kang Pang Kiang)

ประธานกรรมการบริษัท

บริษัท เอ็น.ดี. รับเบอร์ จำกัด (มหาชน)