# คู่มือการรักษาความปลอดภัยของข้อมูล

สังกัด

ชื่อ-สกุล

ข้อมูลสำหรับติดต่อด้านระบบข้อมูล

ชื่อฝ่าย

ข้อมูลสำหรับติดต่อ – –

ข้อมูลสำหรับติดต่อ – –

# นโยบายด้านการรักษาความปลอดภัยของข้อมูลขั้นพื้นฐาน

เราตระหนักถึงความสำคัญของการรักษาความปลอดภัยของข้อมูลตามปรัชญาของ AEON ที่ว่า “แสวงหาสันติภาพ เคารพผู้อื่น และช่วยเหลือชุมชนท้องถิ่นโดยมีลูกค้าเป็นจุดเริ่มต้น” และปกป้องข้อมูลสำคัญจากภัยคุกคามต่างๆ รวมทั้งสนับสนุนชีวิตประจำวันที่วางใจได้และอุดมสมบูรณ์ นอกจากนี้เราถือว่าข้อมูลต่างๆ ของ AEON เป็นสินทรัพย์สำคัญเพื่อพัฒนากิจกรรมทางธุรกิจและสร้างมูลค่าเพิ่ม และเราจะจัดการข้อมูลอย่างถูกต้องและปลอดภัย สร้างความสัมพันธ์ที่ไว้วางใจกันอย่างแท้จริงกับผู้คนที่เกี่ยวข้องกับ AEON เช่น ลูกค้า ชุมชนท้องถิ่น บริษัทคู่ค้า และผู้ถือหุ้นทุกท่าน และเพื่อให้บรรลุเรื่องดังกล่าวเราจึงระบุนโยบายการรักษาความปลอดภัยของข้อมูลขั้นพื้นฐานไว้ในฐานะแนวทางเพื่อให้พนักงานทั้งหมดที่สังกัดใน AEON ตระหนักถึงการรักษาความปลอดภัยของข้อมูลในระดับสูงและปฏิบัติตาม

จัดทำเมื่อวันที่ 1 กันยายน 2019
AEON Co., Ltd.

# การดำเนินการด้านการรักษาความปลอดภัยของข้อมูล

## AEON จะดำเนินกิจกรรมดังต่อไปนี้เพื่อเคร่งครัดในนโยบายการรักษาความปลอดภัยของข้อมูลขั้นพื้นฐาน

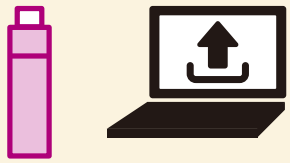
(1) เราจะสร้างระบบเพื่อบำรุงรักษาและปรับปรุงการรักษาความปลอดภัยของข้อมูลอย่างต่อเนื่อง
(2) เราจะกำหนดและปฏิบัติตามระเบียบเพื่อรักษาความปลอดภัยของข้อมูล
(3) เราจะดำเนินการประเมินความเสี่ยงอย่างเหมาะสมและใช้มาตรการที่เหมาะสมและสมเหตุสมผลเพื่อปกป้องข้อมูล
(4) เราจะให้ความรู้ด้านการรักษาความปลอดภัยของข้อมูลที่เหมาะสมแก่พนักงาน ฯลฯ เพื่อยกระดับความตระหนักรู้
(5) เราจะปฏิบัติตามบทบัญญัติ ข้อบังคับ และสัญญาทั้งหมดกับลูกค้า บริษัทคู่ค้า และพนักงาน จากนั้นจัดการข้อมูลอย่างเหมาะสม
(6) เราจะสร้างระบบที่รับมือได้อย่างรวดเร็วและมีประสิทธิภาพโดยเตรียมพร้อมเมื่อเกิดอุบัติเหตุและเหตุการณ์ด้านการรักษาความปลอดภัยของข้อมูล
(7) ในการจ้างงานภายนอก เราจะพยายามคงระดับการรักษาความปลอดภัยของข้อมูลให้เท่าเทียมหรือสูงกว่าของ AEON
(8) เราจะควบคุมผลกระทบจากภัยพิบัติและการโจมตีทางไซเบอร์ ฯลฯ ให้เหลือน้อยที่สุดผ่านกิจกรรมการรักษาความปลอดภัยของข้อมูล รวมทั้งมุ่งมั่นในการดำเนินธุรกิจอย่างต่อเนื่อง
(9) เราจะดำเนินการตรวจสอบและตรวจติดตามกิจกรรมข้างต้นตามกำหนดเวลาและไม่ตามกำหนดเวลา รวมทั้งมุ่งมั่นในการปรับปรุงอย่างต่อเนื่อง
(10) หากฝ่าฝืนนโยบายขั้นพื้นฐานนี้และกฎระเบียบในบริษัทเกี่ยวกับการรักษาความปลอดภัยของข้อมูล เราจะลงโทษตามกฎระเบียบการทำงาน

# กฎการรักษาความปลอดภัยขั้นพื้นฐาน

## ข้อห้าม

ใช้อุปกรณ์อื่น
นอกเหนือจาก
ที่บริษัทให้ยืม

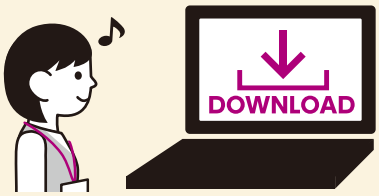

นำอุปกรณ์สื่อสาร
ของบริษัทออกไป
โดยไม่ได้รับอนุญาต



เช่น) แฟลชไดรฟ์ USB

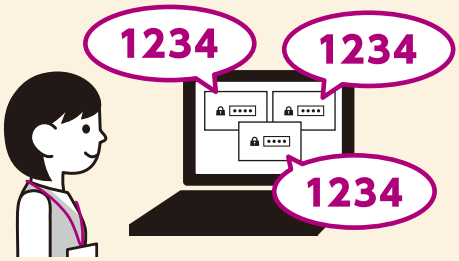
ใช้สื่อบันทึกข้อมูล
ภายนอกโดยไม่
ได้ยื่นขอล่วงหน้า


เข้าดูอินเทอร์เน็ตส่
วนตัวในเวลางาน

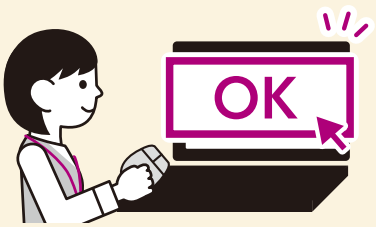



ใช้ซอฟต์แวร์หรือบ
ริการที่ไม่ได้รับอนุญาต

## ข้อควรระวัง



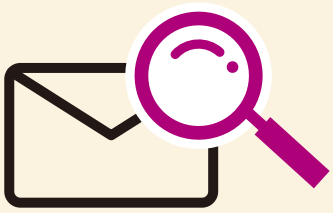

ใช้รหัสผ่านเดิมซ้ำๆ




คลิก OK ง่ายๆ
โดยที่ไม่ได้ตรวจสอบ

# เมื่อใช้อีเมล

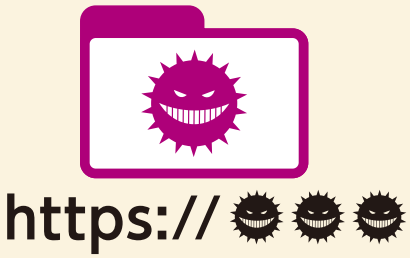
## ข้อควรระวังเมื่อรับอีเมล



ตัวอย่างที่ถูกต้อง)
○○@AEONpeople.biz

ตรวจสอบว่าที่อยู่อีเม
ลผู้รับถูกต้องหรือไม่

ไม่ตอบกลับหรือส่ง
ต่อโดยไม่ระมัดระวัง




ไม่เปิดไฟล์หรือลิงก์
ที่น่าสงสัย

## ข้อควรระวังเมื่อส่งอีเมล


ตรวจสอบรายละเอียด
และผู้รับอย่างละเอียด

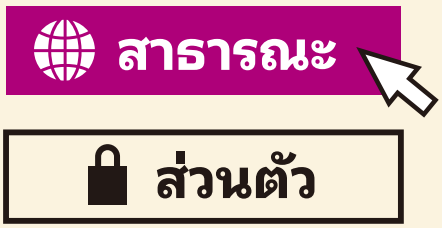

ใช้รหัสผ่านไฟล์กับข้
อมูลที่เป็นความลับ

# เมื่อทำงานระยะไกล (ทำงานนอกบริษัท)

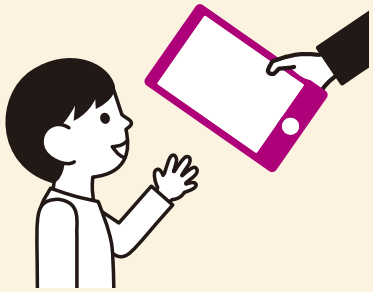
## ข้อห้าม

ฟรีไวไฟ

เชื่อมต่อ Wi-Fi สาธารณะ



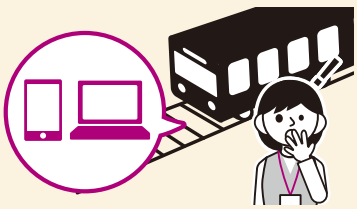

เปิดเผยเอกสาร/ข้อมูลที่บันทึกภาพไว้ด้วยความประมาทเลินเล่อต่อสาธารณะ



ใช้งานอุปกรณ์ที่ยืมมาในครอบครัว

## ข้อควรระวัง


ล็อกหน้าจอด้วยรหัสผ่านเมื่อไม่อยู่ที่โต๊ะทำงาน



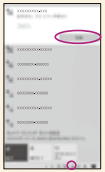
ถืออุปกรณ์สื่อสารไว้ใกล้ตัวเมื่อเดินทาง

**สำคัญ** จะทำอย่างไรถ้าคอมพิวเตอร์ติดไวรัส! ขั้นตอนการรับมือ

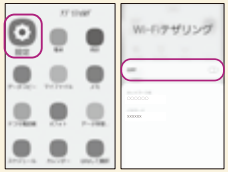
การรับมือเบื้องต้น

## ขั้นแรก ให้ตัดการเชื่อมต่อจากเครือข่ายโดยเร็ว!

ถอดสาย LAN ออก



ตัดการเชื่อมต่อ Wi-Fi



ปิดการใช้งานการแชร์อินเทอร์เน็ตจากสมาร์ตโฟน

**วิธีสุดท้าย** OFF! **ให้ปิดเครื่อง**

รายงานอุบัติเหตุ

## รายงานบริษัทโดยเร็ว

**รายงาน**
**ติดต่อ**
**และปรึกษา**

อย่าพยายามแก้ปัญหาด้วยตัวเอง!
ถ้าติดต่อใครไม่ได้ ให้รอโดยไม่ตื่นตระหนก
จนกว่าจะติดต่อได้!

รักษาสถานะปัจจุบัน

## รักษาสถานะปัจจุบันไว้เพื่อตรวจสอบ

**ไม่ใช้งานคอมพิวเตอร์** *โดยหลักการแล้วจะไม่ปิดเครื่อง

# รายงานสถานการณ์เช่นนี้ทันที

รายงานไปยังข้อมูลสำหรับติดต่อฉุก
เฉินทันทีถ้าเกิดเหตุต่อไปนี้

## อาการที่ผิดปกติของคอมพิวเตอร์

รีสตาร์ตซ้ำๆ
หลายครั้ง

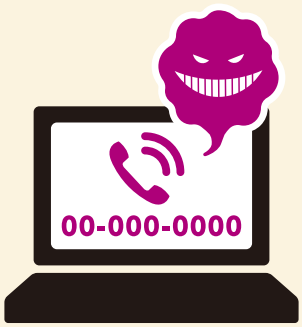

ข้อความที่ไม่คุ้นเ
คยปรากฏขึ้น

ไม่สามารถปิด
หน้าต่างได้

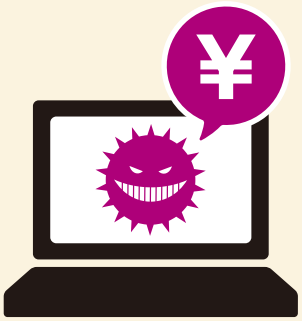
ไฟล์ถูกเข้ารหัสและ
ไม่สามารถเปิดได้

ข้อมูลที่บันทึกไว้สูญหาย
/เสียหาย

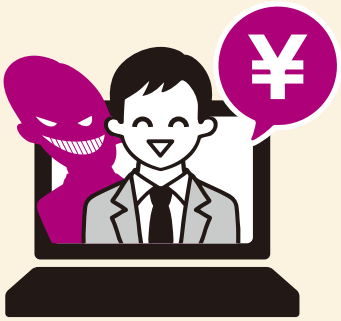
## ได้รับการติดต่อจากบุคคลที่สามที่มีเจตนาร้าย




หมายเลขโทรศัพ
ท์ปรากฏขึ้นและเร่งใ
ห้ติดต่อ



เรียกร้องเงินเพื่อแก้
ไขให้คืนสภาพเดิม



แอบอ้างเป็นบริ
ษัทคู่ค้าและเรียกร้
องให้จ่ายเงิน

# ขั้นตอนการรายงาน

## ตรวจพบการเกิดเหตุขัดข้อง

แต่ละธุรกิจ แต่ละบริษัท และสาขา

บริษัทบำรุงรักษาและดำเนินการระบบ

ฝ่ายกิจการทั่วไปของแต่ละบริษัท

AEON Smart Technology Co., Ltd.

ฝ่ายระบบของแต่ละบริษัท (รวมถึงการเงิน)

## รายงานเหตุขัดข้อง (ทำความเข้าใจสถานการณ์)

วางแผน ICT ของ AEON Co., Ltd.
(สำนักงานรักษาความปลอดภัย)ฝ่ายกิจการทั่วไป

**แจ้ง**

## ตรวจสอบผลกระทบ (ทำความเข้าใจผลกระทบ)

สมาชิกที่จัดการและแก้ไขวิกฤต

จัดตั้งหน่วยงานแก้ไขตามสถานการณ์

ผู้จัดการสาขา, ผู้จัดการแผนก หัวหน้างานระบบ

**แจ้ง**

**แจ้ง**

ประธานบริษัท, ผู้รับผิดชอบระบบของแต่ละบริษัท ฝ่ายที่เกี่ยวข้องใน AEON Co., Ltd.

ประธานกรรมการ, ประธานบริษัท, รองประธานบริษัท, กรรมการผู้บริหาร

ดำเนินการแก้ไข

30 นาที

30 นาที