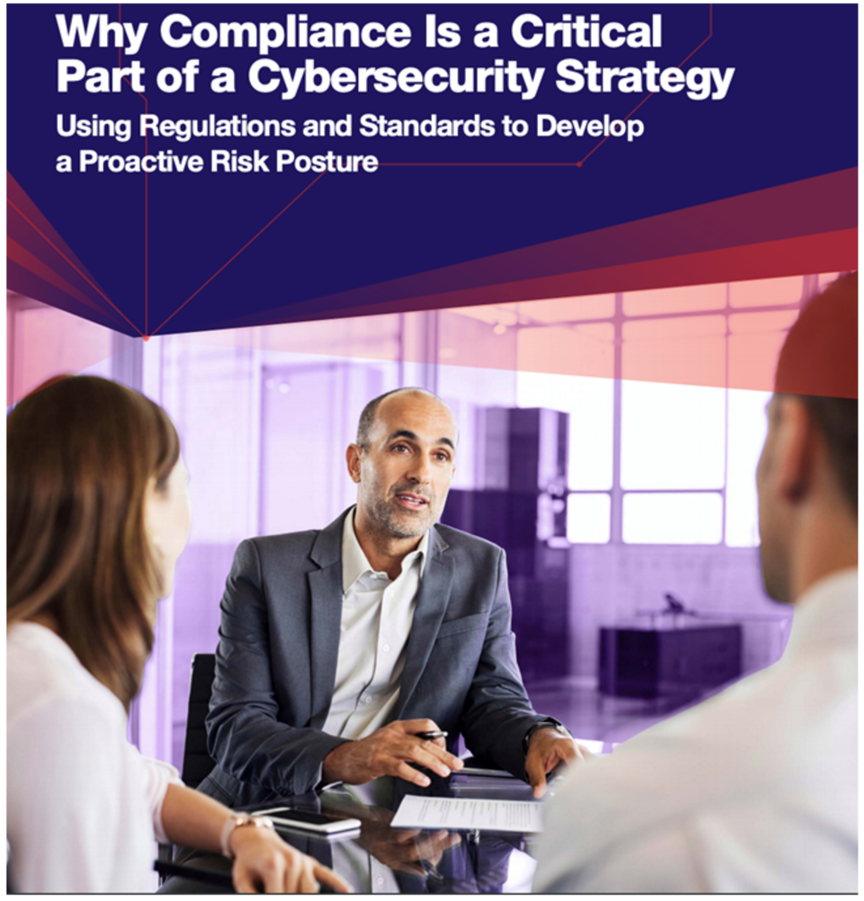
# Full security with NIST




**ISO 27001**

**Information Security Management System**

## NIST Cybersecurity Framework

| IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER |
|---|---|---|---|---|
| Asset Management | Access Control | Anomalies and Events | Response Planning | Recovery planning |
| Business Environment | Awareness and Training | Security Continuous Monitoring | Communications | Improvements |
| Governance | Data Security | Detection Process | Analysis | Communications |
| Risk Assessment | Info. Protection and Procedures | | Mitigation | |
| Risk Management Strategy | Maintenance | | Improvements | |
| Supply Chain Risk Management | Protective Technology | | | |

Reference : Framework for Improving Critical Infrastructure Cybersecurity
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

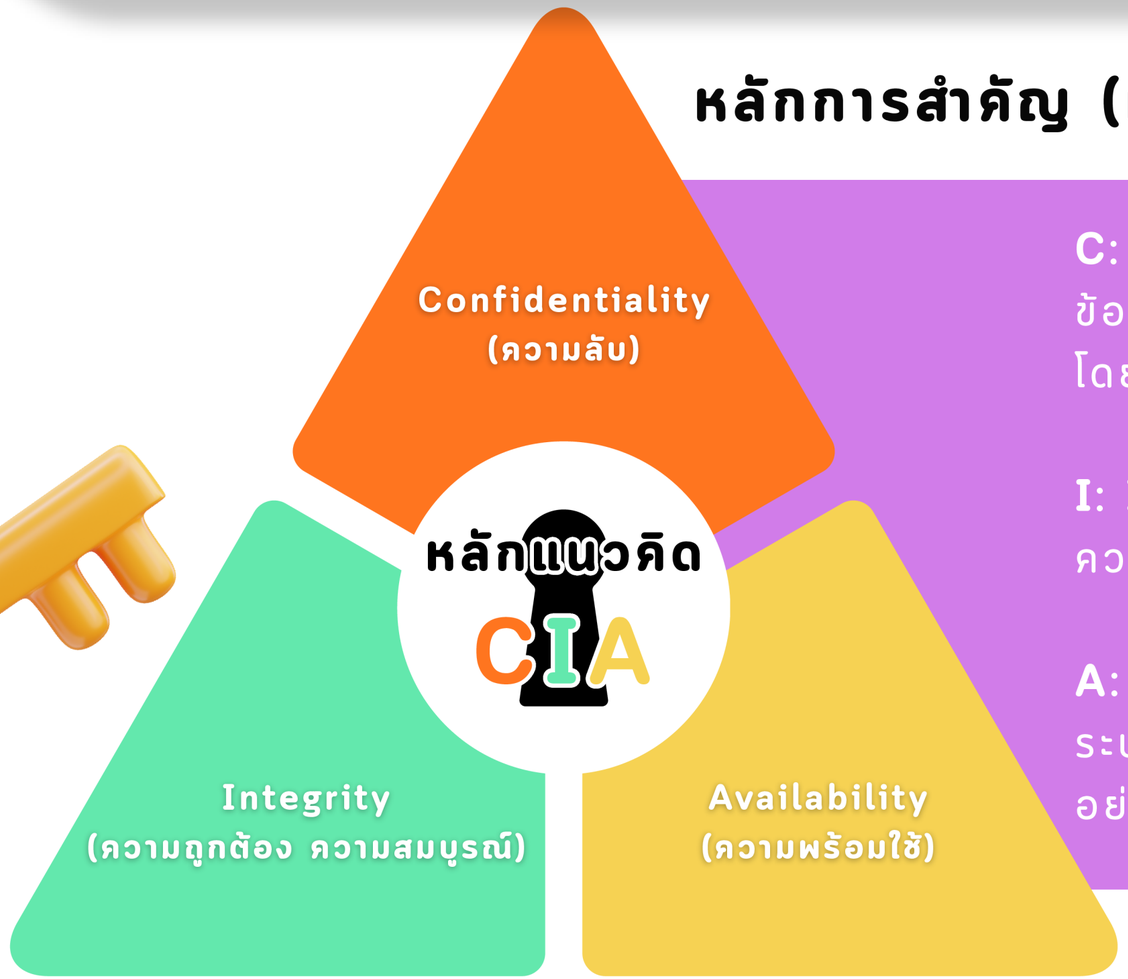
# ป้องกันได้ 100%

# Case จริง

## เว็บไซต์หน่วยงานถูกแฮก

- หน้าเว็บถูกเปลี่ยน
- ข้อมูลรั่วไหล
- หรือถูกฝังมัลแวร์

# นโยบายความมั่นคงปลอดภัยสารสนเทศ
# สำนักงานปลัดกระทรวงอุตสาหกรรม




## หลักการสำคัญ (หัวใจของความมั่นคงปลอดภัย)

**C: Confidentiality**
ข้อมูลและระบบสารสนเทศจะต้องเข้าถึงได้โดยผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น

**I: Integrity**
ความถูกต้องครบถ้วนของข้อมูล

**A: Availability**
ระบบสารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้น

# หน้าที่รับผิดชอบของผู้ใช้งาน (สิ่งที่ต้องทำ)

แนวทางปฏิบัติสำคัญ (ต้องปฏิบัติอย่างเคร่งครัด)

## บัญชีผู้ใช้งานและรหัสผ่าน

- **ใช้บัญชีส่วนตัว**เท่านั้น **ห้ามแชร์**กับผู้อื่น **ห้ามบันทึก**ไว้ในระบบ
- **ตั้งรหัสผ่านให้รัดกุม** (ตัวเล็ก-ใหญ่-ตัวเลข-อักขระ ≥ 8 ตัว)
- **เปลี่ยนรหัสทุก 180 วัน** หรือเมื่อได้รับแจ้งเตือน
- หากใช้รหัสชั่วคราว **ต้องเปลี่ยนภายใน 7 วัน**
- **แจ้งผู้ดูแลระบบทันที**เมื่อเข้าสู่ระบบไม่ได้
- ขออนุญาตก่อนเข้าใช้งานระบบ

## ความปลอดภัยของอุปกรณ์

- **ออกจากระบบ**ทุกครั้งหลังใช้งาน
- ตั้งล็อกหน้าจออัตโนมัติภายใน 15 นาที
- ล็อกเครื่อง / สื่อบันทึกข้อมูลเมื่อไม่ใช้งาน
- **เก็บเอกสารและข้อมูลสำคัญ**ในที่ปลอดภัย
- รับ-ส่งข้อมูลลับต้องเข้ารหัส (SSL / VPN)
- **ตรวจไวรัส**ก่อนใช้สื่อบันทึก (เช่น Flash Drive)
- อัปเดตระบบและโปรแกรมสม่ำเสมอ

## อินเทอร์เน็ต / E-mail / โซเชียล

- **ติดตั้งโปรแกรมป้องกันไวรัส**ก่อนเชื่อมต่ออินเทอร์เน็ต
- **ตรวจไวรัส**ก่อนรับ-ส่งข้อมูลทุกครั้ง
- **ตรวจ e-mail** เป็นประจำ และลบข้อความไม่จำเป็น
- **ตรวจสอบไฟล์แนบก่อนเปิด** โดยเฉพาะ .exe
- ใช้โซเชียลอย่างระมัดระวัง
- หากพบปัญหา **แจ้ง ศทส. ทันที**

## การปฏิบัติงานจากภายนอกหน่วยงาน

- ผู้ปฏิบัติงานจากภายนอก **ต้องปฏิบัติงานในที่ปลอดภัย**
- ต้องขออนุมัติการใช้งานจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อเปิดสิทธิ์ให้ปฏิบัติงานจากภายนอกได้

# ข้อห้ามสำหรับผู้ใช้งาน (สิ่งที่ห้ามทำโดยเด็ดขาด)

## การเข้าถึงและความลับ

- **ห้าม**ใช้บัญชีร่วมกัน หรือบอกรหัสผ่าน
- **ห้าม**ตั้งรหัสผ่านง่าย (เช่น ชื่อ, วันเกิด)
- **ห้าม**เผยแพร่ข้อมูลลับขององค์กร

## ข้อจำกัดในการสื่อสารสาธารณะและเครือข่าย

- **ห้าม**เปิดอีเมล หรือไฟล์แนบจากคนที่ไม่รู้จัก
- **ห้าม**เข้าเว็บไซต์ที่ไม่เหมาะสมหรือผิดกฎหมาย
- **ห้าม**โพสต์ข้อความที่ทำลายชื่อเสียงองค์กร

## การใช้งานที่ไม่ได้รับอนุญาตและผิดกฎหมาย

- **ห้าม**ติดตั้งโปรแกรมหรือใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์
- **ห้าม**ใช้เพื่อความบันเทิง (เกม, หนัง) หรือโหลดบิต
- **ห้าม**ถอนการติดตั้ง Antivirus ที่หน่วยงานจัดหา
- **ห้าม**นำเครื่องส่วนตัวมาเชื่อมต่อระบบเครือข่ายของหน่วยงาน (เว้นแต่ได้รับอนุญาต)
- **ห้าม**ใช้อีเมลของหน่วยงานสมัครเรื่องส่วนตัว

## ข้อจำกัดในการทำงานจากภายนอก

- **ไม่อนุญาต**ให้ปฏิบัติงานจากภายนอกหน่วยงานสำหรับระบบงานที่มีความลับในระดับชั้นลับ ชั้นลับมาก และชั้นลับมากที่สุด
- **ไม่อนุญาต**ให้บุคคลภายนอก (เช่น สมาชิกในครอบครัว) สามารถเข้าถึงระบบสารสนเทศและข้อมูลของหน่วยงานเมื่อปฏิบัติงานจากภายนอก