



# หลักการ "DO" และ "DON'T" การควบคุมด้าน IT (INFORMATION TECHNOLOGY)

## "DO"

1. ตั้งนโยบายความปลอดภัย
2. อัปเดตซอฟต์แวร์และระบบอย่างสม่ำเสมอ
3. ใช้การเข้ารหัสทั้งในขณะส่งและจัดเก็บข้อมูล
4. กำหนดสิทธิ์การเข้าถึงให้เฉพาะเจาะจงและเหมาะสม
5. ทำการสำรองข้อมูลอย่างสม่ำเสมอและทดสอบการกู้คืนข้อมูลเพื่อให้มั่นใจว่าข้อมูลสำคัญจะไม่สูญหาย
6. ใช้เครื่องมือการตรวจสอบและเฝ้าระวังระบบเพื่อระบุและตอบสนองต่อภัยคุกคามอย่างรวดเร็ว
7. การฝึกอบรมแก่พนักงาน เกี่ยวกับวิธีการป้องกันภัยคุกคามด้าน IT และสร้างความตระหนักในด้านความปลอดภัย
8. ทดสอบระบบอย่างสม่ำเสมอเพื่อค้นหาช่องโหว่และความเสี่ยง



## "DON'T"

1. อย่าใช้รหัสผ่านที่ง่าย
2. อย่าเพิกเฉยต่อการอัปเดต
3. อย่าปล่อยให้ข้อมูลสำคัญไม่ถูกเข้ารหัส
4. อย่าละเลยการสำรองข้อมูล
5. อย่าทิ้งระบบโดยไม่มี การป้องกัน
6. อย่าละเลยการตรวจสอบและเฝ้าระวังระบบอย่างสม่ำเสมอ
7. อย่าทำการติดตั้งซอฟต์แวร์จากแหล่งที่ไม่เชื่อถือได้
8. อย่าประมาทการฝึกอบรมพนักงานเกี่ยวกับความปลอดภัยทาง IT เพราะมนุษย์ยังเป็นจุดอ่อนที่สำคัญ



การปฏิบัติตามหลักการเหล่านี้สามารถช่วยลดความเสี่ยงด้าน IT และเพิ่มความปลอดภัยของข้อมูลในองค์กรได้อย่างมาก

THANK  
you