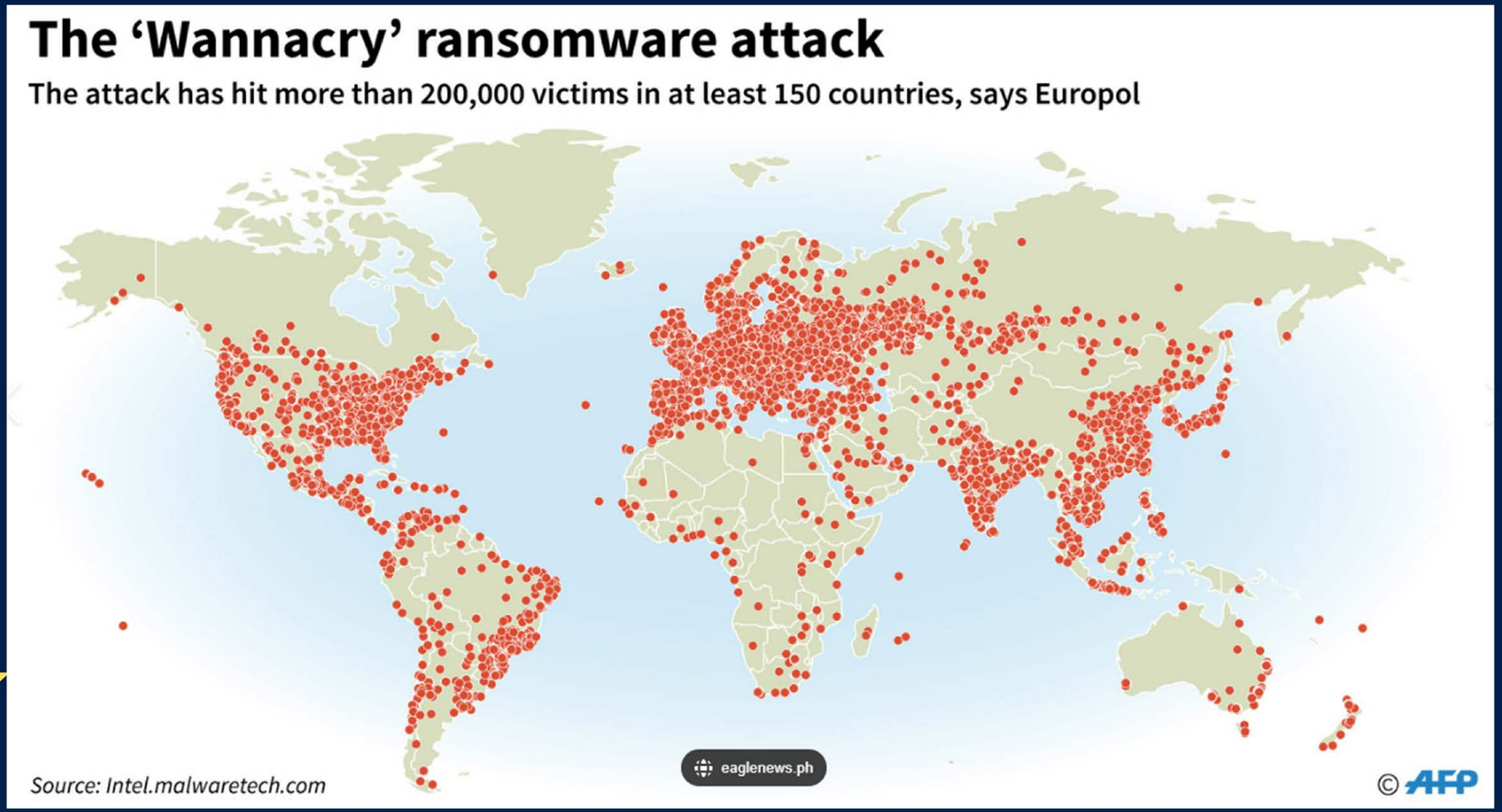
PDPA
ในงานรังสีเทคนิค

YUDTHAPHON VICHIANIN, PH.D.

AGENDA

- Possible causes of data risks
- Principles of Information Security
- Hats in Information Security
- International Standard for Information Security Management Systems
- Techniques for Integrity and Confidentiality
- How to securely delete files
- Health Information & Related Laws

ATTACKS


The ‘Wannacry’ ransomware attack
The attack has hit more than 200,000 victims in at least 150 countries, says Europol
Source: Intel.malwaretech.com
eaglenews.ph
© AFP

https://www.khaosod.co.th/special-stories/news_...

รพ.สระบุรี โดนปล่อยไวรัสเรียกค่าไถ่ 63,000 ล้านบาท ป่วนระบบล่ม!

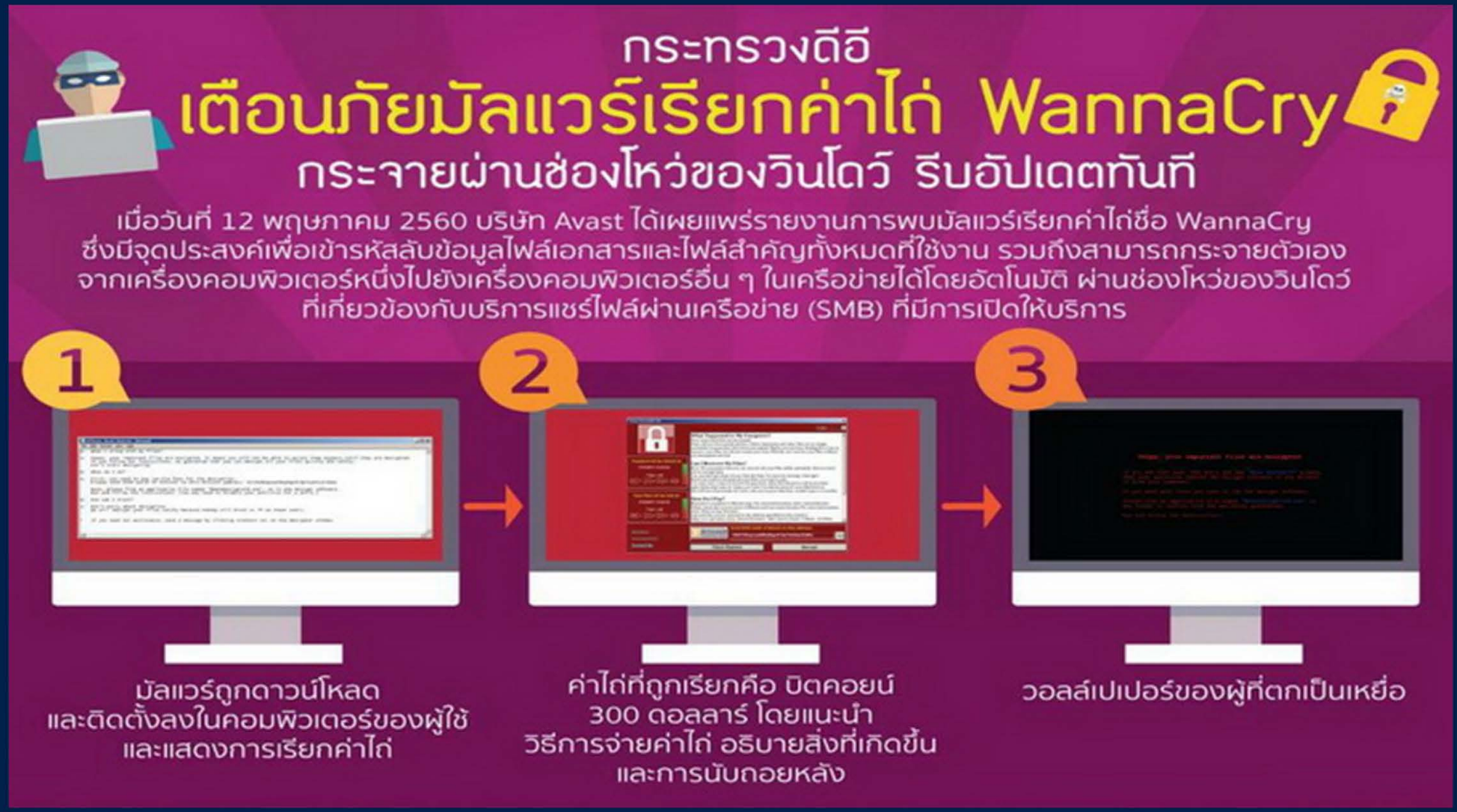
เด่นออนไลน์

9 ก.ย. 2563 - 09:58 น.

Jarinya Jupanich
1h ·

@ตอนนี้คอม รพ สระบุรีถูกโจมตีด้วยransomware เรียกค่าไถ่ด้วยเงินจำนวนหนึ่ง แลกกับข้อมูล ตอนนี้คอมรพ ใช้งานอะไรไม่ได้เลย ดูข้อมูลต่างๆของคนไข้ไม่ได้
@วันนี้ไปตรวจ opdเช้า แต่เสร็จ4โมงเย็น เนื่องจากติดขัดทุกอย่าง ตั้งแต่ห้องบัตร ห้องเจาะเลือดที่เจาะแล้ว ต้องรอprint labมาแปะในOpd เจ้าหน้าที่ต้องวิ่งไปเอาlabเป็นระยะ
@ห้องตรวจ ที่ปกติก็แน่นอยู่แล้ว ยิ่งหนัก แต่ที่หนักใจคือประวัติอะไรไม่รู้ ที่พิมพ์ไว้ในคอมคือละเอียดมาก อันนี้จำได้คร่าวๆ ต้องถามคนไข้หมดเป็นโรคอะไร ใช้ยาอะไร?? ถ้าคนไข้เอาถุงยามาก็พอบอกได้ แต่อันนี้ส่วนใหญ่80% ไม่ได้เอายาเดิมมา ต้องเอาเม็ดยามาถามคนไข้ รวมถึงวิธีการทาน ใช้เวลามากเพราะกลัวerrorด้วย จากนั้นต้องใช้ระบบmanualเขียนยาเป็น10ตัว ตรวจผ่านไปแต่ละคนด้วยความยากลำบาก ที่น่าสงสารสุดคือคนไข้ค่ะ มาเช้าแต่ได้กลับเย็น ดีที่ผู้ป่วยส่วนใหญ่เข้าใจ เห็นใจ รพ ว่าตอนนี้ทุกคน ทุกแผนกลำบากหมด รพ โกลาหล คนไข้ล้น ประมาณ4-5โมงเย็น opd medยังหนาแน่น
@อยากขอความช่วยเหลือจากผู้รู้ถึงวิธีแก้ มีวิธีได้fileคืนมั้ย เพราะ รพ back up fileไม่ถึงปัจจุบัน ถึงแค่ปี 2558(ถ้าไม่จ่ายเงินโจร fileข้อมูลหายมหาศาล)
@ใครมีญาติที่จะมา รพ สระบุรีช่วยแจ้งข้อมูล และให้นำยาเดิมครั้งสุดท้ายมาด้วยค่ะ


Wanna Decryptor 1.0
Ooops, your files have been encrypted!
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files for free. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
How Do I Pay?
Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28
Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
QR Code
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1
Copy
Check Payment
Decrypt


กระทรวงดีอี
เตือนภัยมัลแวร์เรียกค่าไถ่ WannaCry
กระจายผ่านช่องโหว่ของวินโดว์ รีบอัปเดตทันที
เมื่อวันที่ 12 พฤษภาคม 2560 บริษัท Avast ได้เผยแพร่รายงานการพบมัลแวร์เรียกค่าไถ่ชื่อ WannaCry
ซึ่งมีจุดประสงค์เพื่อเข้ารหัสลับข้อมูลไฟล์เอกสารและไฟล์สำคัญทั้งหมดที่ใช้งาน รวมถึงสามารถกระจายตัวเอง
จากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายได้โดยอัตโนมัติ ผ่านช่องโหว่ของวินโดว์
ที่เกี่ยวข้องกับบริการแชร์ไฟล์ผ่านเครือข่าย (SMB) ที่มีการเปิดให้บริการ
1
2
3
มัลแวร์ถูกดาวน์โหลด
และติดตั้งลงในคอมพิวเตอร์ของผู้ใช้
และแสดงการเรียกค่าไถ่
ค่าไถ่ที่ถูกเรียกคือ บิตคอยน์
300 ดอลลาร์ โดยแนะนำ
วิธีการจ่ายค่าไถ่ อธิบายสิ่งที่เกิดขึ้น
และการนับถอยหลัง
วอลล์เปเปอร์ของผู้ที่ตกเป็นเหยื่อ

CYBERSECURITY STATISTICS & FACTS FOR 2022

- **85%** of cybersecurity breaches are caused by human error. (Verizon)
- **94%** of all malware is delivered by email. (CSO Online)
- Ransomware attacks happen every **10 seconds**. (InfoSecurity Group)
- **71%** of all cyberattacks are financially motivated (followed by intellectual property theft, and then espionage). (Verizon)
- The annual global cost of cybercrime is estimated to be **$10.5 trillion** by 2025. (Cybersecurity Ventures)

F-35 fighter jets face greater threats from cyber-attacks than from enemy missiles

Source: Interesting Engineering

The cybersecurity industry is estimated to be worth over $400 billion by 2027

Source: Ce Pro

Over 80% of cybersecurity events involve phishing attacks

Source: CSO Online

Google discovered over 2.1 million phishing sites as of January 2021

Source: Tessian

ความปลอดภัยในระบบคอมพิวเตอร์

ความลับ (Confidentiality)

เพื่อให้มั่นใจว่าข้อมูลจะเข้าถึงได้เฉพาะผู้มีสิทธิ์เท่านั้น

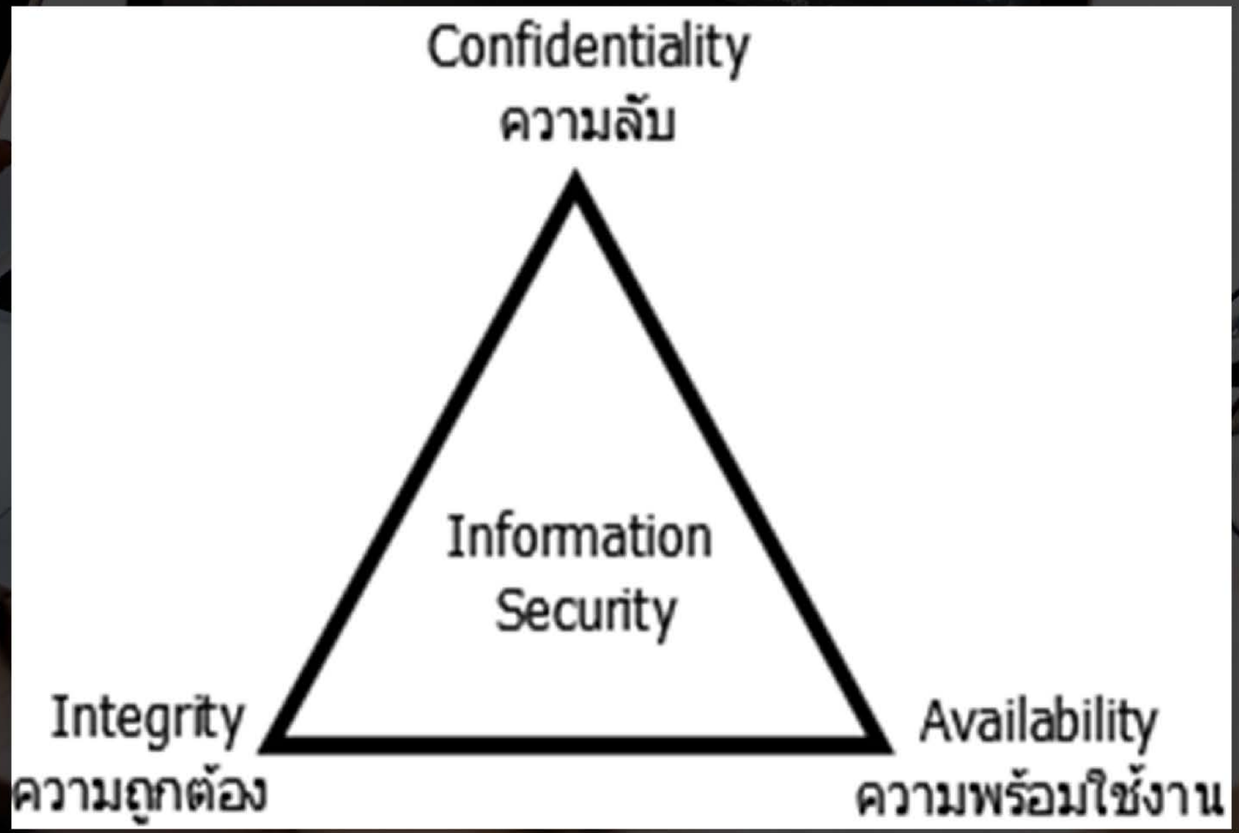
ความถูกต้อง (Integrity)

เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องครบถ้วน สมบูรณ์ โดยข้อมูลจะถูกเปลี่ยนแปลงได้เฉพาะผู้มีสิทธิ์เท่านั้น

ความพร้อมในการใช้งาน (Availability)

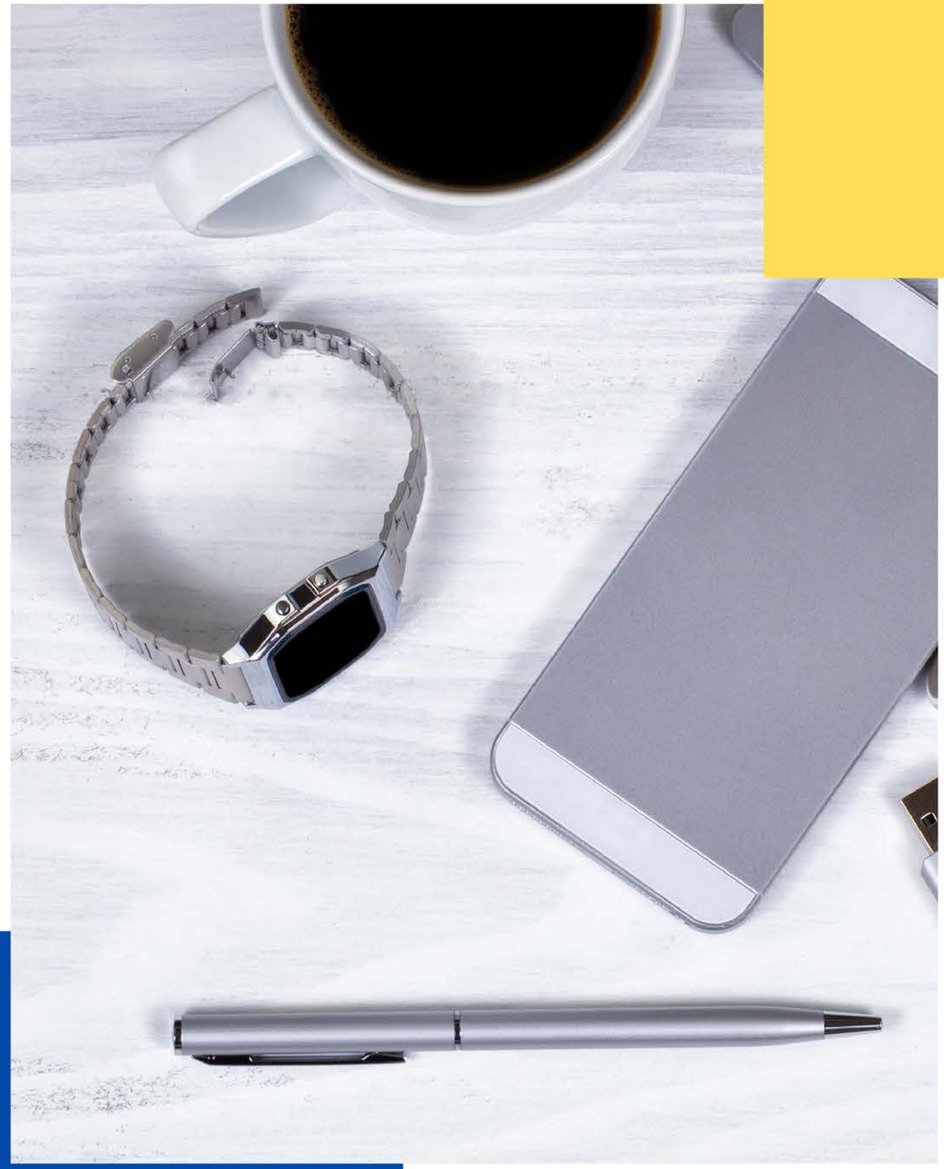
เพื่อให้มั่นใจได้ว่าผู้มีสิทธิ์สามารถเข้าถึงบริการหรือข้อมูลได้ตามต้องการ

Information Security



เข้าใจความเสี่ยง

- ความเสี่ยง (Risk) คือความเป็นไปได้ที่จะสูญเสียทรัพยากร ในรูปแบบต่าง ๆ เช่น ทรัพย์สิน ข้อมูล ชื่อเสียง เป็นต้น
- ด้านการดำเนินงานขององค์กรเช่นแผนกรังสีวิทยาสิ่งสำคัญคือความต่อเนื่อง ในการให้บริการต่าง ๆ ในแผนก
- ส่วนของสารสนเทศความสำคัญจะเกี่ยวข้องกับการทำงานของระบบและตัวข้อมูลในระบบนั้นๆ เช่น ข้อมูลรายการถ่ายภาพของผู้ป่วยใน RIS หรือข้อมูลภาพถ่ายทางรังสีที่เก็บใน PACS
- ส่วนของผู้รับบริการสิ่งที่สำคัญคือการได้รับบริการที่ทันท่วงที มีความถูกต้อง และเก็บรักษาข้อมูลส่วนตัวอย่างเหมาะสม
- ความเสี่ยงจะขึ้นอยู่กับหลายมิติในการพิจารณา ดังนั้นจึงไม่ใช่ความรับผิดชอบของใครเพียงคนใดคนหนึ่งเท่านั้น หากแต่จะต้องมีการจัดการที่เหมาะสม เนื่องจากผลกระทบสามารถส่งผลได้ในหลายมิติขององค์กร



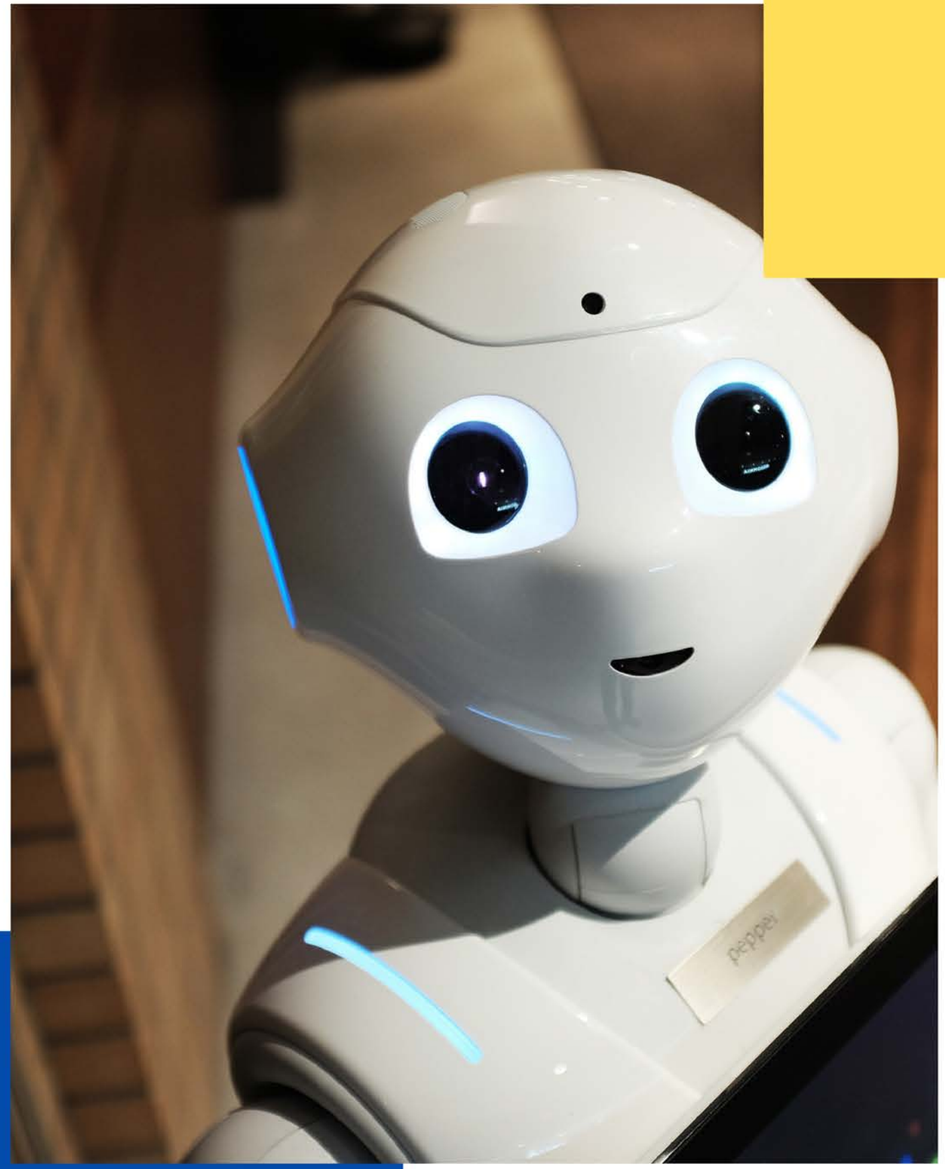
ช่องโหว่

•ช่องโหว่ (Vulnerability) จะมีความหมายในแง่จุดอ่อนที่อาจถูกใช้ในการโจมตีโดยผู้ไม่หวังดี อาจเป็นทางคอมพิวเตอร์ เครือข่าย รวมถึงด้านกายภาพเช่น บุคคล ข้อมูล หรือทรัพย์สิน

•ตัวอย่างประตูหรือหน้าต่างในบ้าน หากเปิดทิ้งไว้โดยไม่ได้รับการดูแล ก็อาจเป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกก่อให้เกิดความเสียหายต่อทรัพย์สินได้

•ส่วนทางคอมพิวเตอร์จะหมายถึงช่องทางที่จะสามารถเจาะเข้ามาโดยไม่ได้รับอนุญาต เข้ามาทำลาย ขโมยข้อมูล หรือทำให้ระบบไม่สามารถให้บริการได้

•ทางการบริหารงานบุคคล เช่นพนักงานที่ถูกเลิกจ้างอาจใช้ช่องทางการเข้าใช้งานระบบแบบปกติ ผ่านบัญชีผู้ใช้และรหัสผ่านที่ยังไม่ได้ถูกยกเลิก เพื่อเข้ามาทำลายข้อมูลหรือคัดลอกข้อมูลผู้ป่วยหรือข้อมูลองค์กรออกไปได้ เป็นต้น



ภัยคุกคาม

•ภัยคุกคาม (Threat) เป็นปัจจัยภายนอกที่ส่งผลกระทบก่อให้เกิดผลเสียต่อทรัพยากร ทรัพย์สิน ข้อมูล ชื่อเสียง ของหน่วยงานหรือองค์กร มีหลากหลายประเภทเช่น

•ภัยคุกคามจากบุคคลภายนอกองค์กร เช่นการเจาะระบบจากผู้ไม่หวังดี การโจรกรรม การโจมตีแบบวิศวกรรมสังคม (Social engineering) หรือปฏิบัติการทางจิตวิทยาการหลอกถามข้อมูล เป็นต้น

•ภัยคุกคามจากบุคคลภายในองค์กร เช่นการแก้แค้น การขโมยข้อมูล การทำงานผิดพลาดโดยไม่ตั้งใจ เป็นต้น

•ภัยคุกคามจากภัยธรรมชาติ เช่นน้ำท่วม ไฟไหม้ แผ่นดินไหว ฟ้าผ่า เป็นต้น

•ภัยคุกคามจากสภาวะแวดล้อม ความชื้น ฝุ่นละออง สารเคมี ความร้อน การรั่วซึม การใช้งานอย่างไม่เหมาะสม เป็นต้น

ภัยคุกคาม

•พนักงาน เป็นผู้ที่สามารถเข้าถึงระบบสารสนเทศในแผนกรังสีได้โดยตรง มีความรู้เกี่ยวกับระบบปัจจุบัน
•พนักงานเก่า เป็นผู้ที่มีความรู้เกี่ยวกับระบบ อาจยังไม่ได้ถูกยกเลิกสิทธิ์ในการใช้งานระบบ
•แฮคเกอร์ เป็นผู้ที่มีแรงจูงใจในการเข้าถึงข้อมูลหรือบริการผ่านช่องโหว่ที่มีอยู่ได้
•คู่แข่งหรือศัตรู เป็นกลุ่มที่ต้องการทราบข้อมูลขององค์กร อาจต้องการสร้างความได้เปรียบทางการค้าเป็นต้น

ภัยคุกคาม

- พนักงาน เป็นผู้ที่สามารถเข้าถึงระบบสารสนเทศในแผนกรังสีได้โดยตรง มีความรู้เกี่ยวกับระบบปัจจุบัน
- พนักงานเก่า เป็นผู้ที่มีความรู้เกี่ยวกับระบบ อาจยังไม่ได้ถูกยกเลิกสิทธิ์ในการใช้งานระบบ
- แฮคเกอร์ เป็นผู้ที่มีแรงจูงใจในการเข้าถึงข้อมูลหรือบริการ ผ่านช่องโหว่ที่มีอยู่ได้
- คู่แข่งหรือศัตรู เป็นกลุ่มที่ต้องการทราบข้อมูลขององค์กร อาจต้องการสร้างความได้เปรียบทางการค้า เป็นต้น

การประเมินความเสี่ยง

Risk analysis

เป็นการวิเคราะห์ความเสี่ยง หรือการคำนวณความเสี่ยง (Risk calculation) เป็นการเตรียมการกับภัยคุกคาม จุดอ่อน รวมถึงผลกระทบที่อาจเกิดขึ้นทั้งด้านความเสียหายของข้อมูล การหยุดทำงานของระบบ หรือแม้กระทั่งชื่อเสียงขององค์กร

ความเสี่ยงต่อองค์กรโดยรวม

เป็นความเสี่ยงในด้านต่าง ๆ ที่อาจจะเกิดขึ้นได้ เช่นเครื่องแม่ข่ายชำรุด ไฟฟ้าดับ อัคคีภัย ระบบเครือข่ายขัดข้อง ซึ่งควรมีการศึกษาและเตรียมการรับผลกระทบ

ความเสี่ยงที่ต้องป้องกัน

เป็นความเสี่ยงที่ได้มีการสำรวจและศึกษา รวมถึงจัดลำดับความสำคัญและให้น้ำหนักผลกระทบที่อาจเกิดขึ้น และให้ค่าความน่าจะเป็นในแต่ละความเสี่ยง เพื่อเตรียมแผนรองรับความเสี่ยงที่จำเป็นต้องป้องกัน

มักเป็นความเสี่ยงที่มีโอกาสเกิดขึ้นได้สูง มีความสำคัญต่อกระบวนการทำงานและมีผลกระทบเป็นวงกว้าง เช่นในแผนกรังสีวินิจฉัย ความเสี่ยงดังกล่าวอาจเป็นเรื่องของระบบเครือข่ายขัดข้อง RIS หรือ PACS หยุดทำงาน ดังนั้นต้องเตรียมแผนการรองรับในกรณีเหล่านี้เป็นต้น

การประเมินความเสี่ยง ด้านภัยคุกคามทางคอมพิวเตอร์

- การประเมินความเสี่ยงระดับระบบ (System-level vulnerability assessment) เป็นการประเมินเพื่อหาจุดอ่อนรวมถึงช่องโหว่ของระบบคอมพิวเตอร์แต่ละเครื่องที่ใช้งานภายในแผนก
- การประเมินความเสี่ยงระดับเครือข่าย (Network-level risk assessment) เป็นการประเมินความเสี่ยงต่อเหตุการณ์ที่อาจเกิดผลกระทบหรือภัยคุกคามของระบบคอมพิวเตอร์รวมถึงระบบเครือข่ายภายในแผนกหรือภายในโรงพยาบาล
- การประเมินความเสี่ยงระดับองค์กร (Organization-level risk assessment) เป็นการประเมินความเสี่ยงในภาพรวมขององค์กรเพื่อระบุภัยคุกคามขององค์กรโดยตรง
-

การคำนวณความเสี่ยง
RISK CALCULATION)

- เป็นการคำนวณผลกระทบเป็นตัวเงิน เพื่อใช้ประกอบการตัดสินใจในการดำเนินการแก้ไขหรือเลือกวิธีในการยับยั้งผลกระทบดังกล่าว โดยพิจารณาองค์ประกอบดังนี้
- ค่าเสียหายต่อปี หรือ ALE (Annual loss expectancy) เป็นจำนวนเงินที่คาดว่าจะเป็นค่าที่เสียหายต่อปี
- ค่าเสียหายต่อครั้ง หรือ SLE (Single loss expectancy) เป็นจำนวนเงินที่คาดว่าจะเป็นค่าที่เสียหายต่อครั้ง
- โอกาสที่จะเกิดต่อปี หรือ ARO (Annualized rate of occurrence) เป็นโอกาสที่คาดว่าจะเกิดขึ้นต่อปี

- ค่าเสียหายต่อปี (ALE) = ค่าเสียหายต่อครั้ง (SLE) x โอกาสที่จะเกิดต่อปี (ARO)

การคำนวณความเสี่ยง
RISK CALCULATION)

ค่าความเสียหายของแพ็กส์เนื่องจากกระแสไฟฟ้ากระชากที่อาจเกิดขึ้นกับเครื่องแม่ข่าย (SLE) เท่ากับ 15,000 บาทต่อครั้ง โดยโอกาสที่จะเกิดขึ้น (ARO) ประมาณ 10 ครั้งต่อปี โดยจะคำนวณ ALE ได้เป็น

ALE = 15,000 x 10 = 150,000 บาท

การจัดการความเสี่ยง (RISK TREATMENT)

การหลีกเลี่ยงความเสี่ยง (RISK AVOIDANCE)

เป็นการหลีกเลี่ยงความเสี่ยงที่อาจเกิดขึ้นโดยปรับเปลี่ยนกระบวนการที่ทำให้เกิดความเสี่ยงหรือผลกระทบ เช่นมาตรการงดการใช้งานช่องเสียบ USB เพื่อหลีกเลี่ยงการติดไวรัสหรือข้อมูลรั่วไหล ในเครื่องคอมพิวเตอร์ในแผนกรังสีที่เกี่ยวข้องกับคลินิกเป็นต้น

การโอนความเสี่ยง (RISK TRANSFER)

เป็นการถ่ายโอนความเสี่ยงให้ผู้อื่นรับผิดชอบแทน เช่น การซื้อประกันการบำรุงรักษาระบบรายปีของเครื่อง CT MRI หรือ PACS เป็นต้น อย่างไรก็ตามระบบก็ยังมีโอกาสเสียหายเช่นเดิม แต่จะมีผู้รับผิดชอบในการแก้ไขและค่าใช้จ่ายที่เกิดขึ้นแทน

การจัดการความเสี่ยง (RISK TREATMENT)

การลดความเสี่ยง (RISK REDUCTION)

เป็นการหาวิธีในการควบคุม จัดการ แก้ไข เพื่อลดโอกาสของความเสี่ยงให้อยู่ในระดับที่รับได้ เช่นติดตั้งซอฟต์แวร์ป้องกันไวรัส จัดอบรมให้กับผู้ใช้งานในแผนก เป็นต้น

การป้องปรามความเสี่ยง (RISK DETERRENCE)

เป็นการลดโอกาสในการตกเป็นเป้าของการโจมตี เช่น การติดกล้องวงจรปิด การติดป้ายเตือน การเพิ่มแสงสว่างในบริเวณต่าง ๆ การประกาศนโยบายและกฎหมายพร้อมบทลงโทษที่ชัดเจนให้ผู้ใช้งานระบบทราบ เป็นต้น

การยอมรับความเสี่ยง (RISK ACCEPTANCE)

เป็นการยอมรับความเสี่ยงนั้นๆ เมื่อพิจารณาแล้วว่าไม่คุ้มค่าหรือไม่สามารถทำได้ในทางปฏิบัติ เช่นมูลค่าการแก้ไขหรือป้องกันควบคุม สูงกว่ามูลค่าของข้อมูลหรืออุปกรณ์ ทรัพย์สินที่จะปกป้อง

การลดความเสี่ยง

การควบคุมทางกายภาพ (PHYSICAL CONTROL)

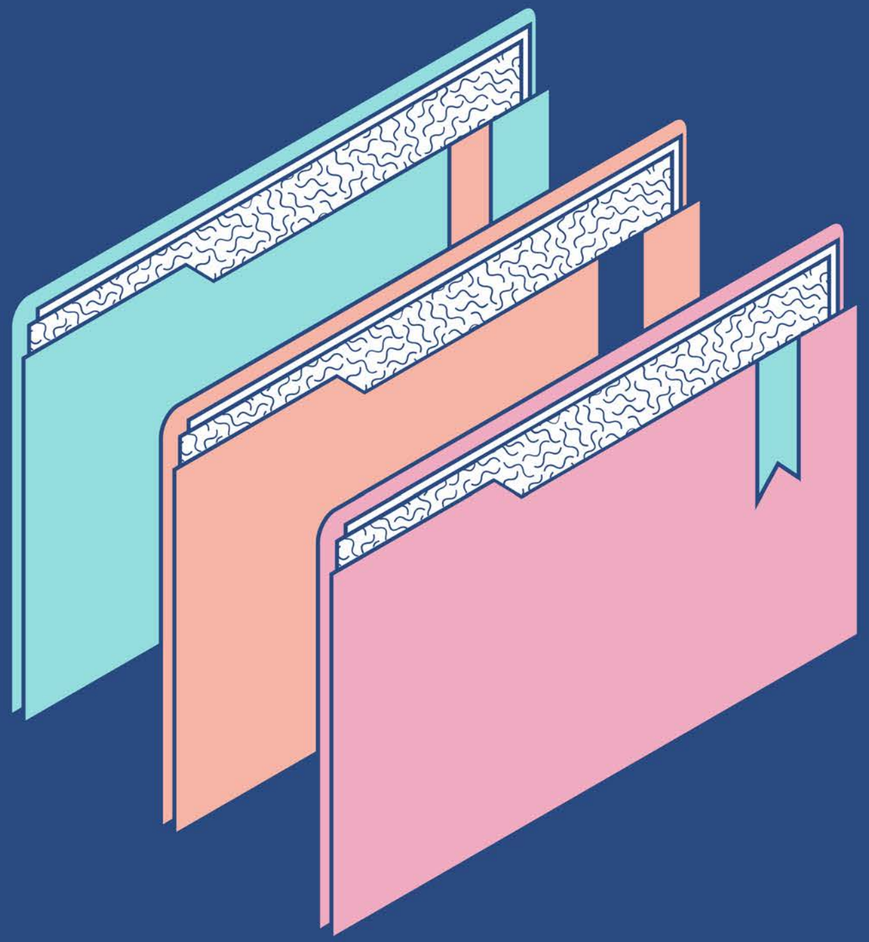
เป็นการจัดการปรับปรุงระบบทางกายภาพให้มีความเหมาะสม เช่นการจัดแบ่งพื้นที่ที่มีความสำคัญออกจากส่วนทำงานปกติ (zoning) การควบคุมการเข้าออกพื้นที่สำคัญ (access control) การจัดระเบียบการจัดวางอุปกรณ์และการเดินสายสัญญาณให้เป็นระบบเป็นต้น

การควบคุมทางด้านเทคนิค (TECHNICAL CONTROL)

เช่นการใช้ซอฟต์แวร์ช่วยในการควบคุม ตรวจสอบ แจ้งเตือนด้านความปลอดภัย เช่นซอฟต์แวร์ป้องกันไวรัส การเข้ารหัสข้อมูลที่สำคัญ การใช้อุปกรณ์ไฟร์วอลล์ (Firewall) ในการควบคุมการใช้งานทรัพยากรบนเครือข่าย

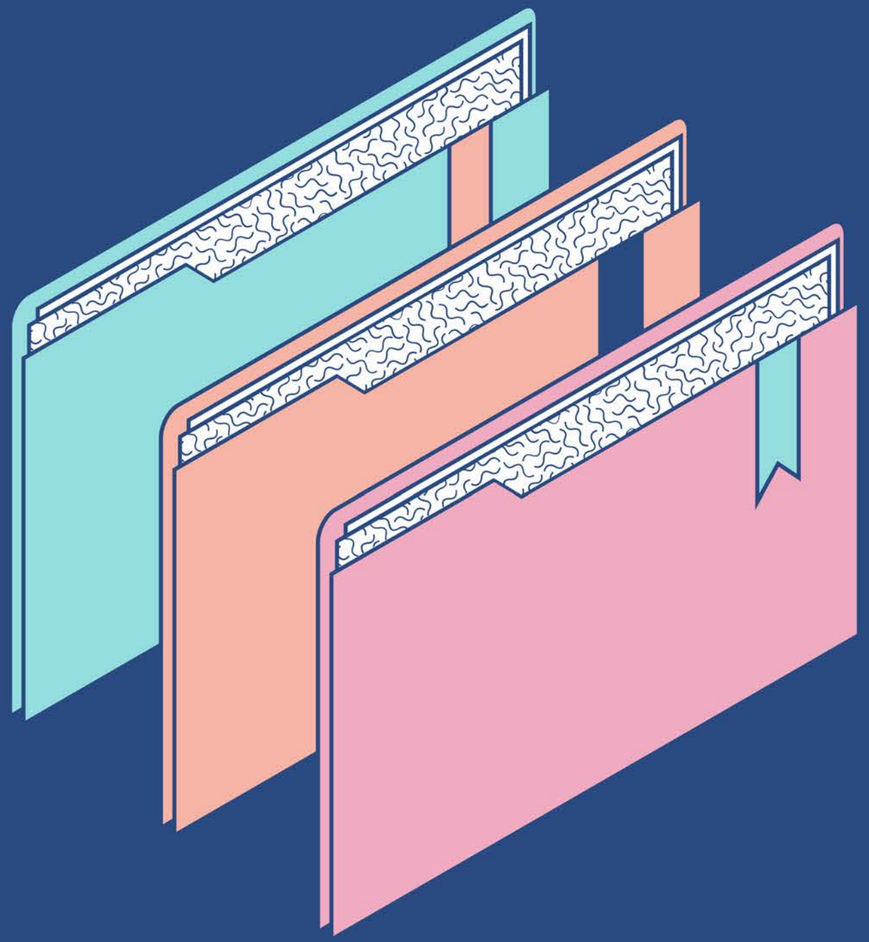
การควบคุมด้านการบริหาร (MANAGEMENT CONTROL)

เป็นการจัดให้มีนโยบาย แนวทางปฏิบัติงาน กฎระเบียบ การอบรมบุคลากร รวมถึงแนวทางในการจัดจ้างบุคคลภายนอกที่เข้ามาปฏิบัติงานภายในองค์กร เป็นต้น



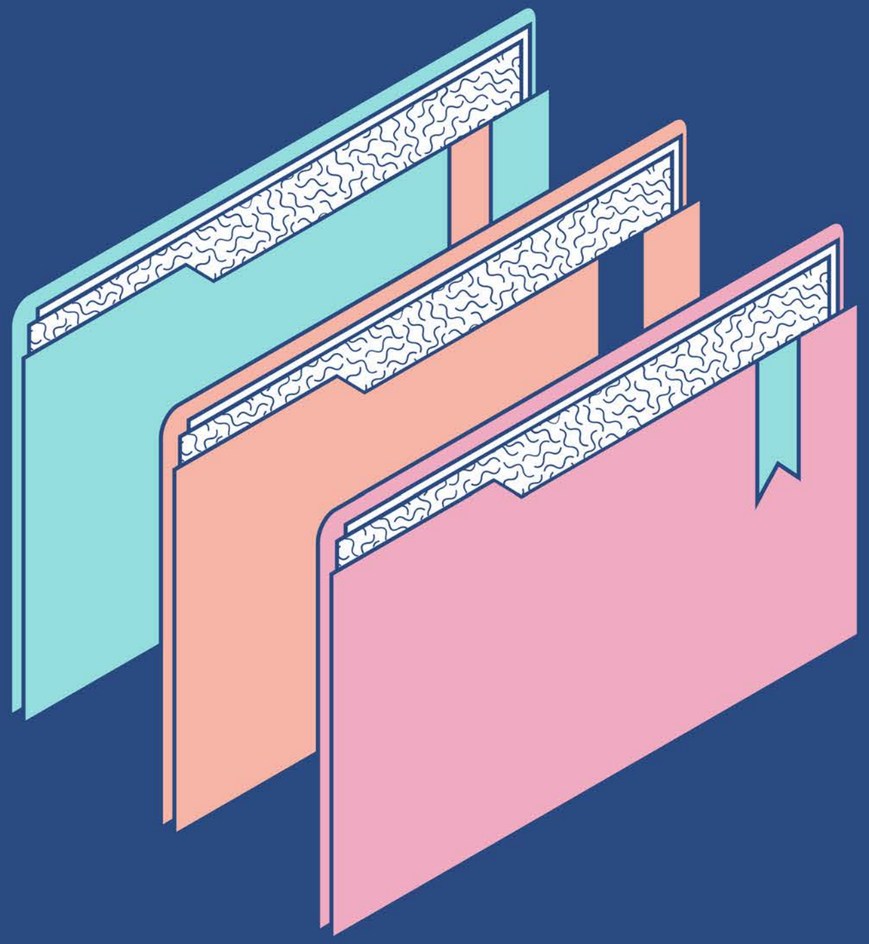
แนวทางการป้องกันภัยคุกคามข้อมูลรังสีวิทยาระยะไกล (ด้านระบบ)

- เปิดใช้งานและปรับปรุงซอฟต์แวร์รักษาความปลอดภัยให้เป็นปัจจุบันทันสมัยอยู่เสมอ หากเป็นอุปกรณ์เคลื่อนที่เช่น โน้ตบุคคอมพิวเตอร์ แทบเล็ต ไม่ควรเชื่อมต่อกับเครือข่ายไร้สายที่ไม่รู้จัก
- ตรวจสอบให้แน่ใจว่าซอฟต์แวร์ป้องกันภัยบนเว็บครอบคลุมการป้องกันอีเมล์และแจ้งเตือนการส่งผ่านข้อมูลเข้าและออกจากเครื่องของผู้ใช้งานในเวลาจริง



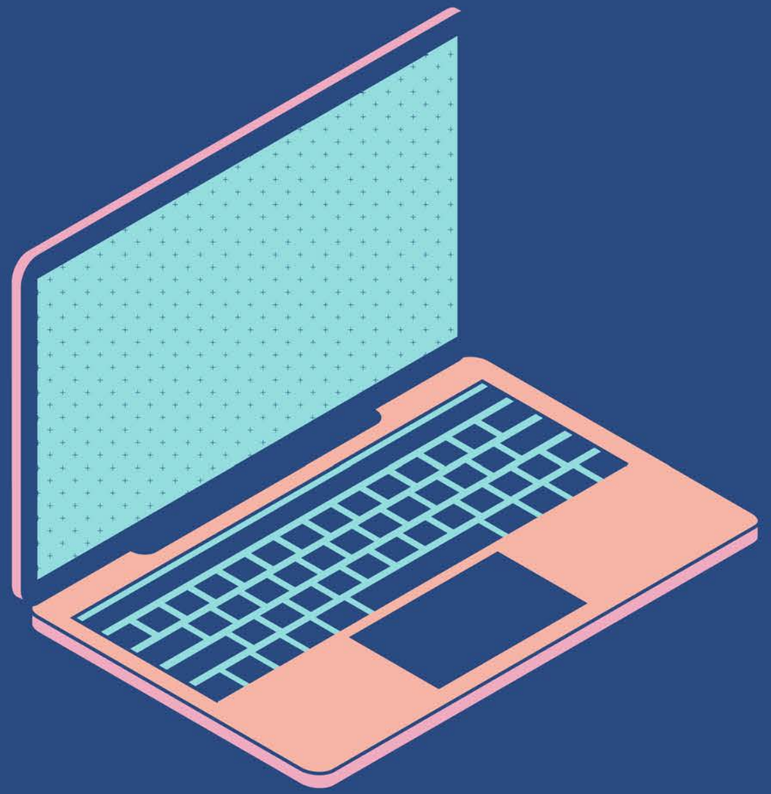
แนวทางการป้องกันภัยคุกคามข้อมูลรังสีวิทยาระยะไกล (ด้านระบบ)

- หากใช้งานเครื่องที่เป็นระบบปฏิบัติการ Windows ให้เปิดใช้งาน Automatic update และติดตั้งโปรแกรมปรับปรุงใหม่ๆ ทันทีที่พร้อมใช้งาน
- ในการเชื่อมต่อเครือข่ายภายนอกโรงพยาบาลเช่นเครือข่ายอินเทอร์เน็ต ควรปรับใช้เทคโนโลยีเช่น การป้องกันโดยการตรวจสอบชื่อเสียงที่สามารถวัดระดับความปลอดภัยและความน่าเชื่อถือของเว็บไซต์ก่อนเข้าชม



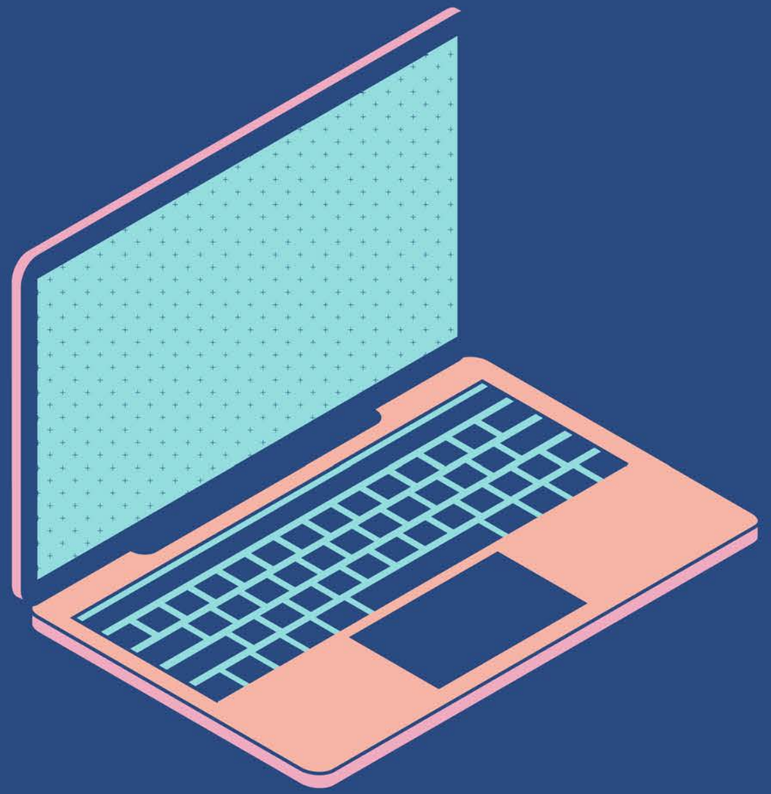
แนวทางการป้องกันภัยคุกคามข้อมูลรังสีวิทยาระยะไกล (ด้านนโยบาย)

- ไม่ใช้บัญชีการใช้งานระบบร่วมกัน
- ไม่ควรใช้รหัสผ่านเดียวกันหลายระบบ
- ไม่บอกรหัสผ่านให้ผู้อื่นทราบ แม้กระทั่งผู้ที่อ้างว่าเป็นผู้ดูแลระบบ
- ไม่จดหรือบันทึกรหัสผ่าน
- ไม่ส่งรหัสผ่านโดยใช้โทรศัพท์ อีเมล์ หรือการส่งข้อความผ่านระบบอินเทอร์เน็ต (Instant messaging)
- ออกจากระบบ (Log-out) เมื่อไม่ใช้งาน
- เปลี่ยนรหัสผ่านเสมอ โดยใช้รหัสผ่านที่แตกต่างกันหลายชุด ตามวงรอบ
- เช่น ทุก 90 วัน จนครบ 5 ชุด



การใช้รหัสผ่านที่ปลอดภัย

- •ใช้ความยาวที่เหมาะสมตั้งแต่ 7 ตัวอักษรขึ้นไป
- •มีการผสมกันระหว่างตัวอักษรตัวใหญ่เล็ก
- •ใช้ตัวเลขในรหัสผ่าน 1-2 ตัว
- •ใช้อักษรพิเศษเช่น % & ! @
- •หลีกเลี่ยงการใช้คำที่บรรจุในพจนานุกรม
- •หลีกเลี่ยงการใช้วันที่ ทะเบียนรถ เบอร์โทรศัพท์ หรือข้อมูลอื่นที่เกี่ยวข้องกับเจ้าของบัญชี
- •หลีกเลี่ยงการใช้คำย่อหน่วยงาน หรือชื่อหน่วยงาน



https://www.dinopass.com/

Malware

เวิร์ม (Worm) มีคุณสมบัติพิเศษคือสามารถแพร่กระจายตัวเองได้อัตโนมัติอย่างรวดเร็ว ไปยังเครื่องอื่นๆ ผ่านทางเครือข่าย สามารถทำลายหรือทำอันตรายให้กับระบบ

ใช้ช่องทางการสื่อสารหรือแบนด์วิธของเครือข่ายให้เครือข่ายช้า แฝงตัวเข้ามารอร่วมในการโจมตีแบบปฏิเสธการให้บริการ DoS (Denial of Service) เป้าหมายที่ระบุไว้

เวิร์มบางประเภทอาศัยช่องโหว่ของบริการ (Service) ของวินโดวส์ แล้วใช้ข่องทางการเชื่อมต่อไปยังเครือข่ายของระบบเพื่อแพร่กระจายตัวเอง

แต่ถ้ามีการอัพเดทระบบปฏิบัติการวินโดวส์เสมอหรือใช้ ไฟร์วอลล์ปิดกั้นช่องทางการเชื่อมต่อที่เวิร์มใช้ก็จะหยุดการโจมตีหรือแพร่กระจายได้

Malware

ไวรัส (Virus) เป็นโปรแกรมที่สามารถติดต่อจากไฟล์หนึ่งไปยังอีกไฟล์หนึ่งภายในระบบเดียวกันได้ หรือจากเครื่องหนึ่งไปยังเครื่องอื่นผ่านการแฝงตัวไปกับไฟล์หรือโปรแกรม

สามารถทำลายฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล โดยเมื่อคอมพิวเตอร์หรือโฮสต์รันโปรแกรมส่วนที่เป็นไวรัสก็จะทำงานด้วยเช่นกัน ทำให้แพร่กระจายไปยังเครื่องอื่น

บางครั้งสามารถสร้างชุดคำสั่งใหม่เพื่ออำพรางหรือซ่อนตัว

Malware

โปรแกรมหลอกลวงหรือโฮคส์ (Hoaxes) เป็นโปรแกรมที่มีวัตถุประสงค์ให้ผู้ใช้ทำบางอย่าง โดยอาจไม่มีวัตถุประสงค์ร้าย นอกจากแค่ต้องการหลอกเท่านั้น

สแกมส์ (Scams) เป็นการใช้ช่องทางการสื่อสาร โดยผู้ไม่หวังดีจะหลอกให้คนอื่นช่วยเหลือ โดยใช้อีเมล์ในการหลอกให้เปิดเผยข้อมูลส่วนตัว เช่น บัญชีธนาคาร หมายเลขบัตรเครดิต แล้วนำข้อมูลนี้ไปใช้ก่ออาชญากรรมต่อไป

ฟิชชิง (Phishing) หรือ แบรนด์สปู๊ฟฟิง (Brand spoofing) เช่น อาชญากรปลอมตัวเป็นตัวแทนจากบริษัทผู้ให้บริการ PACS แล้วขอบัญชีผู้ใช้และรหัสผ่าน เป็นต้น

Malware

สปายแวร์ (Spyware) เป็นโปรแกรมที่เสมือนเป็นโปรแกรมที่ดีแต่เบื้องหลังแอบทำกิจกรรมที่ไม่ได้รับการยินยอมจากผู้ใช้งานเช่น เก็บข้อมูลส่วนตัวของผู้ใช้ เช่นข้อมูลบัตรเครดิต ข้อมูลบัญชีธนาคาร หรือปรับเปลี่ยนการตั้งค่าในเครื่อง เช่นเปลี่ยนหน้าที่อยู่ของโปรแกรมเว็บเบราเซอร์ซึ่งสร้างความรำคาญในการทำงาน

แอดแวร์ (Adware) เป็นโปรแกรมโฆษณาสินค้าที่จะเปิดหน้าต่างใหม่ขึ้นมา บางครั้งอาจรวมอยู่กับโปรแกรมที่ให้ใช้งานได้ฟรี และฝังตัวอยู่ เนื่องจากได้รับความยินยอมจากผู้ใช้ ซึ่งบางครั้งสามารถสร้างความรำคาญและทำให้ประสิทธิภาพในการทำงานของผู้ใช้และเครื่องลดลง

Malware

อินเทอร์เน็ตคุกกี้ เป็นไฟล์แบบข้อความ (Text file) ที่เว็บไซต์ได้สร้างไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้เพื่อบันทึกข้อมูลพฤติกรรมของผู้ใช้ คุกกี้เป็นเครื่องมือที่ถูกกฎหมายสำหรับเก็บข้อมูลของผู้ใช้งานเว็บไซต์

อย่างไรก็ตามมีบางเว็บไซต์ได้พยายามเขียนโปรแกรมเพื่อรวบรวมข้อมูลต่าง ๆ ที่อยู่ในคุกกี้ เพื่อสืบทราบพฤติกรรมของผู้ใช้งานว่าใช้งานเว็บไซต์ไหนบ้างโดยไม่แจ้งให้ผู้ใช้ทราบ

การเฝ้าระวัง (Monitoring)

การปฏิบัติตามนโยบาย เป็นการบังคับใช้มาตรการรักษาความปลอดภัยให้เป็นไปตามนโยบาย

โดยอาจจะใช้การตรวจสอบ Log โดยเจ้าหน้าที่ทำด้วยมือในกรณีที่หน่วยงานมีจำนวนเครื่องไม่มากหรือใช้ซอฟต์แวร์จัดการแบบอัตโนมัติก็ได้

ตัวอย่างเช่นการตรวจสอบ log ในเครื่องแม่ข่าย PACS, RIS รวมถึง Database ที่เกี่ยวข้องด้วย เพื่อดูข้อผิดพลาดต่าง ๆ ที่เกิดขึ้น

การพิสูจน์ทราบตัวตน (Authentication)

การพิสูจน์ทราบตัวตน (Authentication) เป็นการตรวจสอบผู้ใช้ที่ต้องการลงชื่อเข้าใช้งานหรือล็อกอิน (Log in) ระบบคอมพิวเตอร์หรือเครือข่าย และตรวจสอบการเข้าไปยังส่วนสงวนหรือต้องห้าม

ระบบการพิสูจน์ตัวตนอาจใช้ชื่อผู้ใช้ร่วมกับรหัสผ่าน หรือ สมาร์ทการ์ด หรือไบโอเมติกเช่นการแสกนลายนิ้วมือ ระบบจดจำใบหน้า เป็นต้น

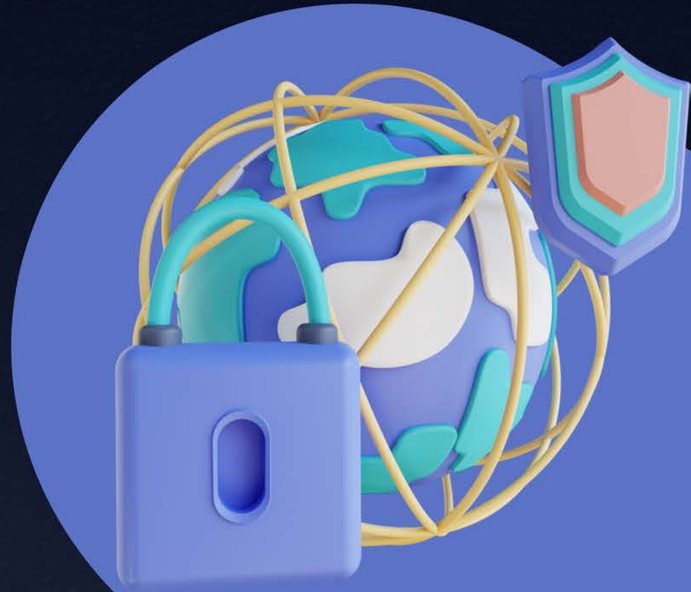
ทุกระบบที่ใช้งานควรมีระบบการพิสูจน์ตัวตน เช่น RIS, PACS รวมไปถึง Workstation ต่าง ๆ ในแผนกรังสีวิทยา

ระบบตรวจจับการบุกรุก (Intrusion Detection System)

- ระบบตรวจจับการบุกรุก หรือ IDS (Intrusion Detection System) เป็นระบบตรวจจับและแจ้งเตือนภัยบนเครือข่าย
- ทำหน้าที่คล้ายสัญญาณกันขโมยสำหรับตรวจจับแจ้งเตือนเมื่อมีการบุกรุกเข้าสู่ระบบเครือข่ายหรือระบบคอมพิวเตอร์โดยผู้ไม่หวังดี
- สามารถตั้งโซนส่วนที่สงวนและส่วนใช้งานปกติได้ ระบบตรวจจับการบุกรุกที่รู้จักกันดีคือซอฟต์แวร์ป้องกันไวรัสซึ่งควรติดตั้งในทุกเครื่อง ทั้งในเครื่องโมดาลabตี้ต่าง ๆ เครื่อง Workstation และ Diagnostic workstation ของแพทย์ รวมถึงเครื่องแม่ข่าย PACS RIS และ Database ด้วย

IDS แบ่งออกเป็น 2 ประเภทคือ

- Host-based IDS สำหรับตรวจจับการบุกรุกเข้ามาในเครื่องคอมพิวเตอร์
- Network-based IDS สำหรับตรวจจับการบุกรุกเข้ามาในเครือข่าย

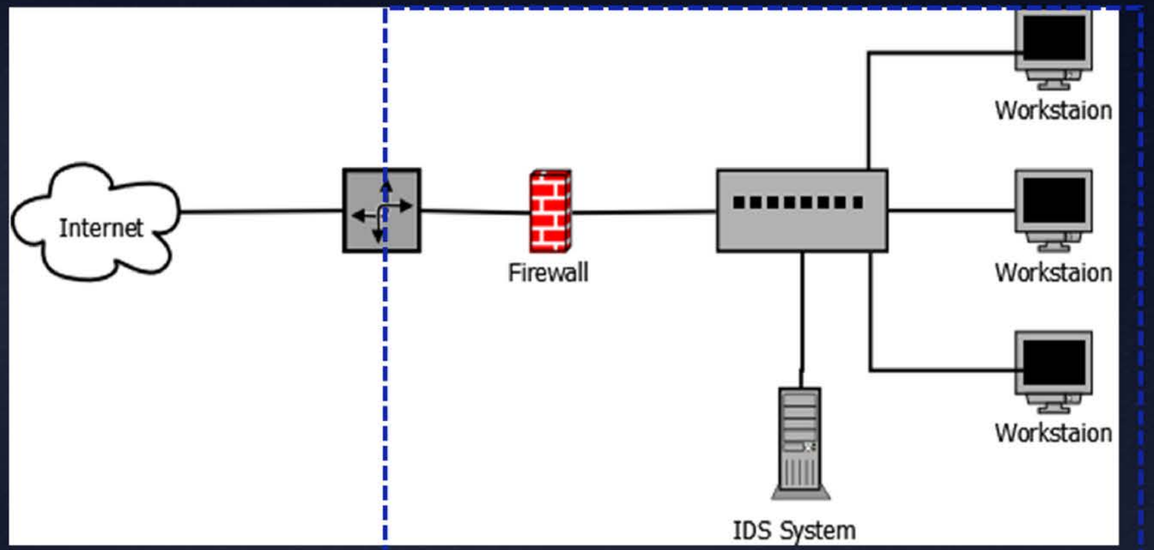


Firewall

ไฟร์วอลล์ (Firewall) เป็นอุปกรณ์ที่ทำหน้าที่ตรวจสอบการเข้าถึงทรัพยากรของระบบจากภายนอก ซึ่งจำเป็นต้องติดตั้งคั่นกลางระหว่างอินเทอร์เน็ตกับเครือข่ายภายใน โดยจะต้องกำหนดขนาดและประสิทธิภาพการทำงานของไฟร์วอลล์ให้เหมาะสมกับปริมาณข้อมูลในเครือข่าย

ไฟร์วอลล์ทำงานโดยการตั้งกฎหรือ Rules

- ปิดกั้นการเชื่อมต่อ (Block connection)
- อนุญาตการเชื่อมต่อ (Allow connection)
- อนุญาตการเชื่อมต่อเฉพาะที่ตรวจสอบแล้วปลอดภัย



VPN (Virtual Private Network)

เครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) เป็นเทคโนโลยีที่ช่วยในการเชื่อมต่อเครื่องคอมพิวเตอร์จากภายนอกองค์กรเข้าสู่เครือข่ายภายในองค์กรโดยอาศัยเครือข่ายสาธารณะเช่น อินเทอร์เน็ต ซึ่งการเชื่อมต่อแบบปกติมีความเสี่ยงจากภัยคุกคามเช่น ข้อมูลรั่วไหลหรือถูกดักจับข้อมูลระหว่างทาง

•

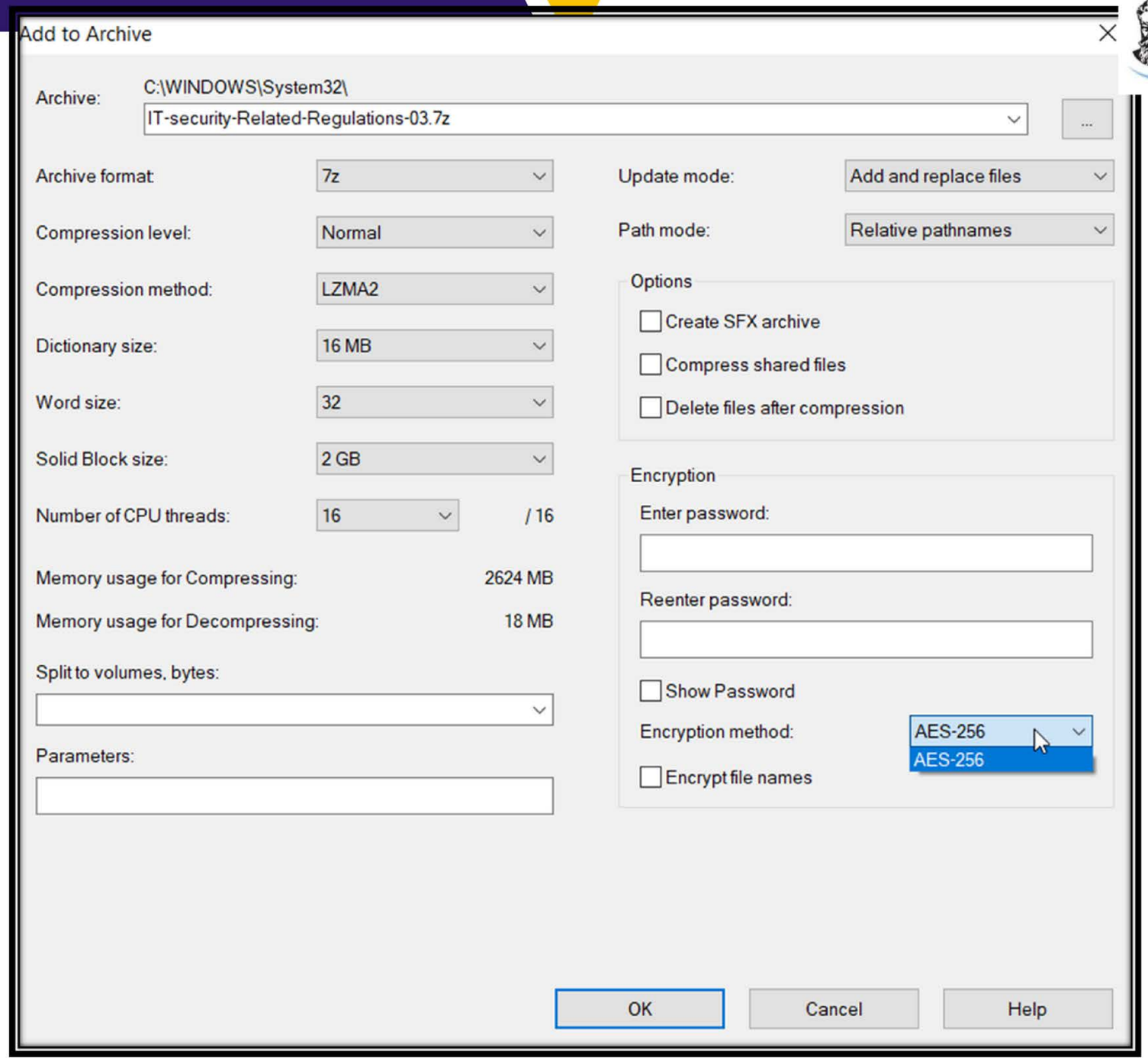
เพื่อเพิ่มความปลอดภัยในการเชื่อมต่อเครื่องจากภายนอกเข้ามาในเครือข่ายจึงจำเป็นต้องมีการเข้ารหัสข้อมูลในการเชื่อมต่อ เพื่อทำให้เฉพาะเครื่องต้นทางและปลายทางเท่านั้นที่จะสามารถอ่านข้อมูลได้อย่างถูกต้อง

การเข้ารหัสข้อมูล (ENCRYPTION)

การเข้ารหัสข้อมูล (Encryption) เป็นการปกป้องความลับ (Confidentiality) และความถูกต้องของข้อมูล ทั้งในระหว่างการรับส่ง หรือในการเก็บไฟล์ในอุปกรณ์บันทึกข้อมูล โดยใช้อัลกอริทึม (Algorithms) ต่าง ๆ

AES (Advanced Encryption Standard) แบบที่ใช้กุญแจขนาดต่าง ๆกันตั้งแต่ 128, 192, 256, 512, 1024, 2048 บิต ซึ่งเป็นที่ยอมรับโดยรัฐบาลในด้านความปลอดภัยและการทำงานที่รวดเร็ว และเป็นตัวเลือกในการเข้ารหัสข้อมูลในหน่วยงานรัฐบาลสหรัฐอเมริกาตั้งแต่ปี 2001

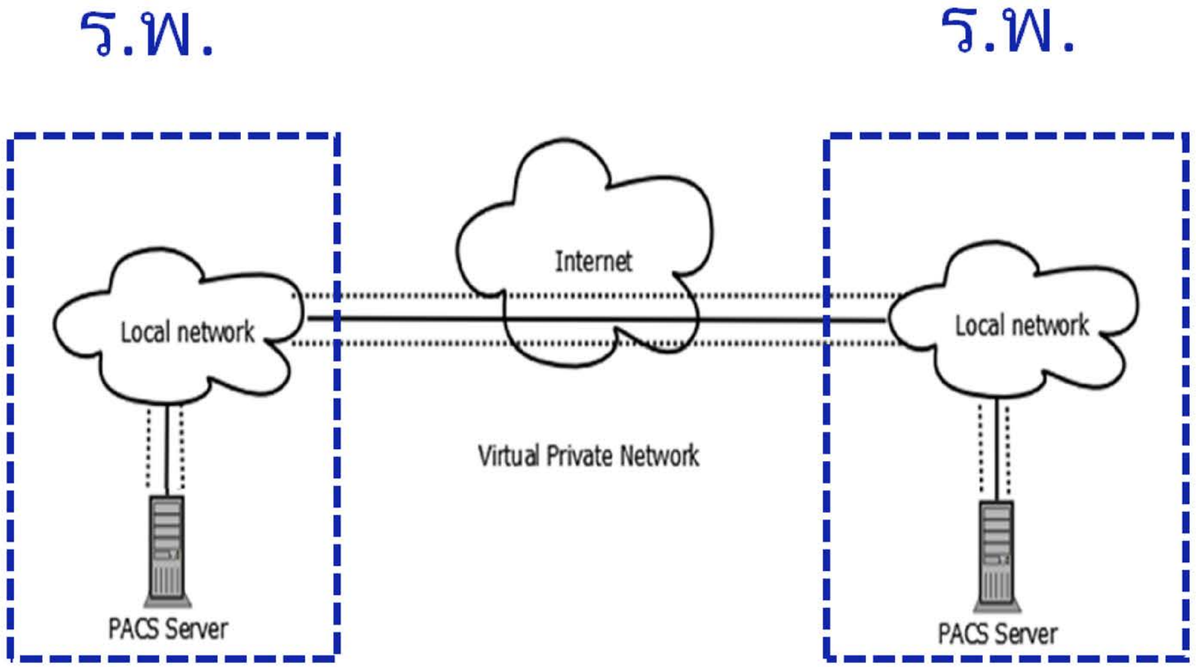
RSA (Rivest–Shamir–Adleman) ใช้กุญแจขนาด 1024 ถึง 2048 บิต


Add to Archive
Archive:
C:\WINDOWS\System32\
IT-security-Related-Regulations-03.7z
...
Archive format:
7z
Compression level:
Normal
Compression method:
LZMA2
Dictionary size:
16 MB
Word size:
32
Solid Block size:
2 GB
Number of CPU threads:
16
/ 16
Memory usage for Compressing:
2624 MB
Memory usage for Decompressing:
18 MB
Split to volumes, bytes:
Parameters:
Update mode:
Add and replace files
Path mode:
Relative pathnames
Options
Create SFX archive
Compress shared files
Delete files after compression
Encryption
Enter password:
Reenter password:
Show Password
Encryption method:
AES-256
AES-256
Encrypt file names
OK
Cancel
Help

O'REILLY® TEAMS INDIVIDUALS FEATURES BLOG CONTENT SPONSORSHIP

As in Recipe 12.3, we will use IPSec Transport mode and a GRE tunnel for this encrypted router-to

```
Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#crypto key pubkey-chain rsa
Router1(config-pubkey-chain)#addressed-key 172.16.2.1
Router1(config-pubkey-key)#address 172.16.2.1
Router1(config-pubkey-key)#key-string
Enter a public key as a hexidecimal number ....
Router1(config-pubkey)#30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181
Router1(config-pubkey)#EA33B519 0CD95EFF EDFD4723 BED73640 97981CC0 1FC83FBF 5C6DF97C
Router1(config-pubkey)#C5FE959D 1E055002 83B92EF4 35B69545 C3217E5F E0C32A73 44FD2373
Router1(config-pubkey)#75598BE0 B4A4E7B2 3C318C2D 3BF3B192 8B71D8C9 A1E0F929 0E84BDAD
Router1(config-pubkey)#BC425170 400BD26A 319E632F 4E9649F5 BA7ADA40 5A94B09C 05F8414E
Router1(config-pubkey)#quit
Router1(config-pubkey-key)#exit
Router1(config-pubkey-chain)#exit

Router1(config)#crypto isakmp policy 100
Router1(config-isakmp)#encryption aes 256
Router1(config-isakmp)#authentication rsa-encr
Router1(config-isakmp)#group 2
Router1(config-isakmp)#exit
Router1(config)#crypto ipsec transform-set TUNNEL-TRANSFORM ah-sha-hmac esp-aes 256
Router1(cfg-crypto-trans)#mode transport
Router1(cfg-crypto-trans)#exit
Router1(config)#
```



SITE-TO-SITE VPN (ROUTER CONFIGURATION)

การรักษาความปลอดภัยทางกายภาพ (Physical security)

การออกแบบสภาวะแวดล้อมที่ปลอดภัย (Safe environmental design) สำหรับระบบสารสนเทศทางรังสีที่ติดตั้งศูนย์ข้อมูลของ RIS, PACS

1.หลีกเลี่ยงการติดตั้งที่ชั้นบนสุดเนื่องจากหากมีอัคคีภัยจะเข้าถึงได้ยาก
2.หลีกเลี่ยงชั้นใต้ดินเนื่องจากปัญหาเรื่องน้ำท่วมและความชื้นจากชั้นดิน
3.ไม่ควรอยู่ใกล้สถานที่สาธารณะที่มีคนพลุกพล่าน
4.ควรอยู่ใจกลางของอาคารเพื่อหลีกเลี่ยงภัยธรรมชาติ

การรักษาความปลอดภัยทางกายภาพ (Physical security)

สำหรับส่วนที่เป็นห้องศูนย์ข้อมูลควรพิจารณาติดตั้งระบบต่าง ๆ ต่อไปนี้เพื่อเป็นแนวทางในการรักษาความปลอดภัย

1.ระบบไฟฟ้าสำรองฉุกเฉิน
2.ระบบควบคุมการเข้าออก เช่น เครื่องสแกนลายนิ้วมือ
3.ระบบควบคุมสภาวะแวดล้อมเช่นเครื่องปรับอากาศ เครื่องควบคุมความชื้น เครื่องกรองอากาศ
4.ระบบแจ้งเตือนภัยอัตโนมัติ
5.ระบบป้องกันอัคคีภัย

การจัดอบรม (Training)

เจ้าหน้าที่: ควรมีการอบรมเจ้าหน้าที่ เพื่อให้สามารถทำความเข้าใจและทราบความสำคัญของการรักษาความปลอดภัย ข้อมูลสำคัญและความลับขององค์กร ให้ความร่วมมือในการปกป้องข้อมูลของผู้รับบริการ ผู้ป่วย และข้อมูลภายในองค์กรไม่ให้เกิดการรั่วไหล

ผู้ดูแลระบบ: ควรได้รับความรู้และเทคนิคใหม่ๆ เพื่อให้ก้าวทันเทคโนโลยี และรูปแบบภัยคุกคามใหม่

นักพัฒนาซอฟต์แวร์: เป็นการอบรมนักพัฒนาซอฟต์แวร์ในด้านการออกแบบและเขียนโปรแกรมให้ปลอดภัย จากเทคนิคการเจาะระบบในรูปแบบต่าง ๆ

ผู้บริหาร: ควรได้รับรายงานและความก้าวหน้าเกี่ยวกับโครงการติดตั้งระบบรักษาความปลอดภัย ผลที่ได้จากการวิเคราะห์หรือประเมินสถานการณ์ ความเสี่ยง ภัยคุกคามโดยเป็นรายงานสรุป

Principles of Information Security

HIPAA	REGULATES HEALTH CARE PROVIDERS' COLLECTION AND DISCLOSURE OF SENSITIVE HEALTH INFORMATION
COPPA	REGULATES ONLINE COLLECTION AND USE OF INFORMATION OF CHILDREN
GLBA	REGULATES FINANCIAL INSTITUTIONS' USE OF NONPUBLIC PERSONAL INFORMATION
FCRA	REGULATES THE COLLECTION AND USE OF DATA CONTAINED IN CONSUMER CREDIT REPORTS
FTC ACT	PROHIBITS "UNFAIR OR DECEPTIVE ACTS OR PRACTICES"

Management & Policy
Regulations & Laws

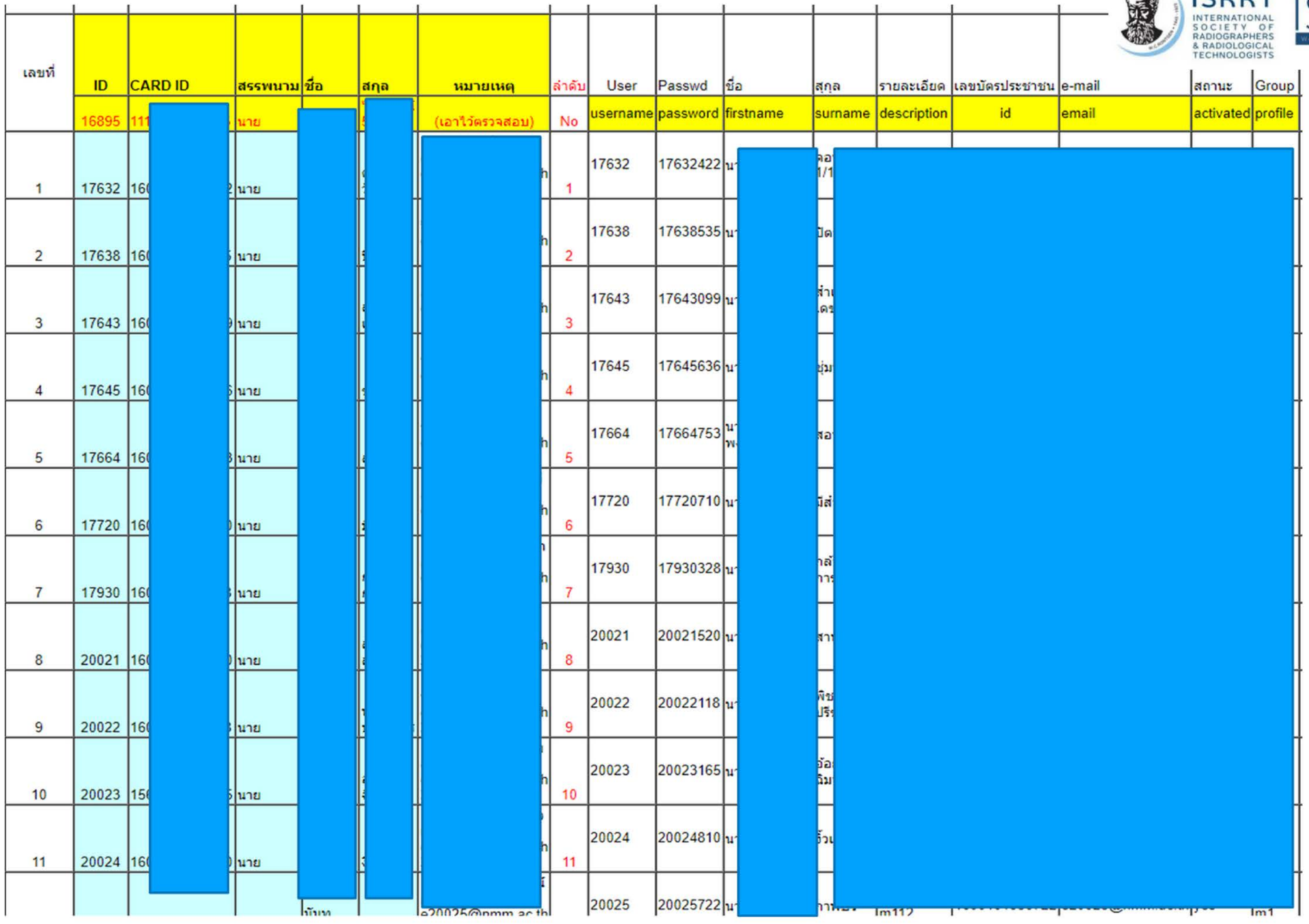
HTTPS://WWW.SECURITYMADESIMPLE.ORG/CYBERSECURITY-BLOG/WHAT-ARE-THE-3-PRINCIPLES-OF-INFORMATION-SECURITY

Attack MAP - example https://www.digitalattackmap.com/

https://www.exploit-db.com › google-hac... ▾ แปลหน้านี้

Google Hacking Database (GHDB)

The GHDB is an index of search queries (we call them dorks) use
information, intended for pentesters and security researchers.

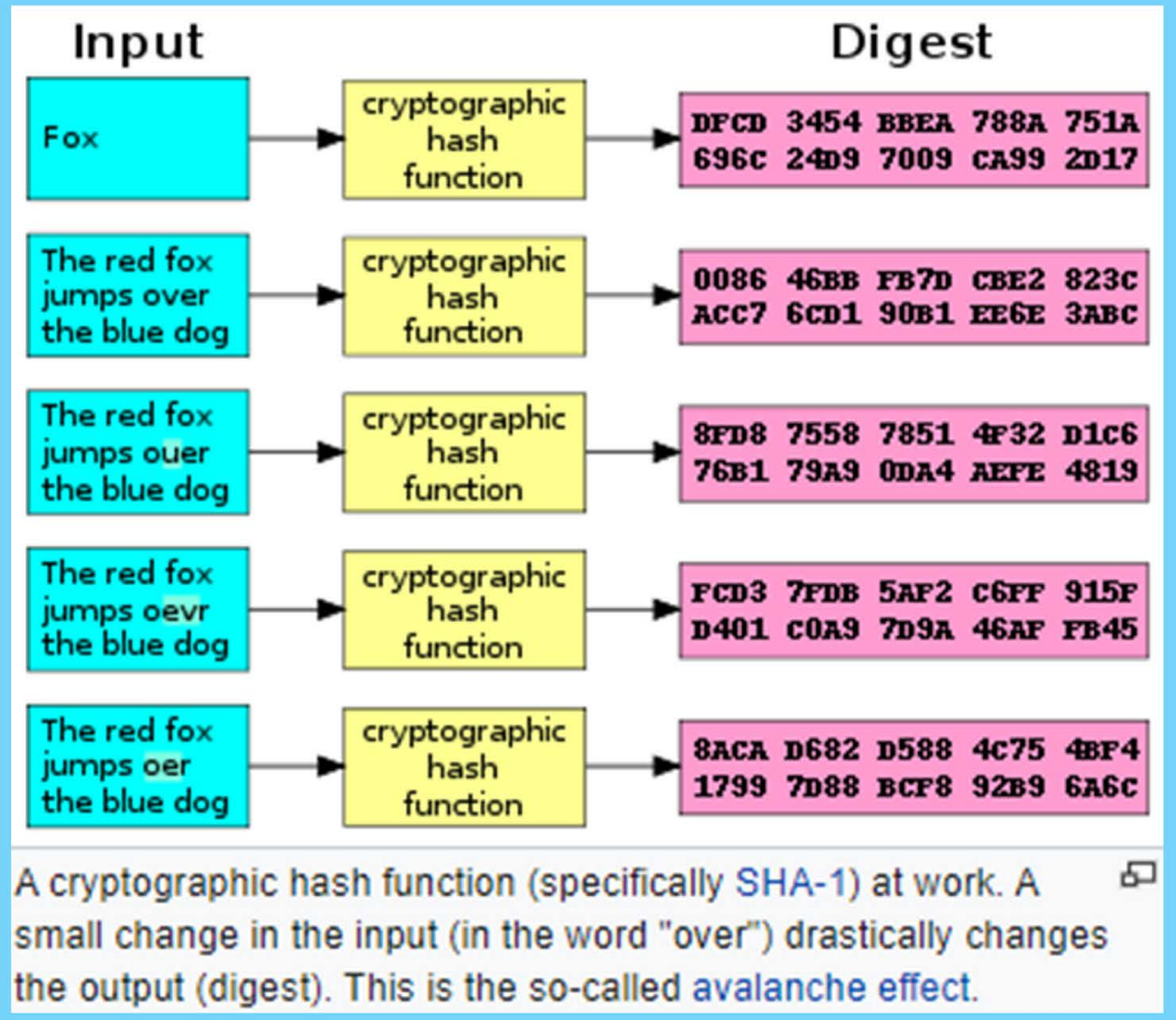


เลขที่	ID	CARD ID	สรรพนาม	ชื่อ	สกุล	หมายเหตุ	ลำดับ	User	Passwd	ชื่อ	สกุล	รายละเอียด	เลขบัตรประชาชน	e-mail	สถานะ	Group
	16895	111	นาย			(เอาไว้ตรวจสอบ)	No	username	password	firstname	surname	description	id	email	activated	profile
1	17632	160	นาย				1	17632	17632422							
2	17638	160	นาย				2	17638	17638535							
3	17643	160	นาย				3	17643	17643099							
4	17645	160	นาย				4	17645	17645636							
5	17664	160	นาย				5	17664	17664753							
6	17720	160	นาย				6	17720	17720710							
7	17930	160	นาย				7	17930	17930328							
8	20021	160	นาย				8	20021	20021520							
9	20022	160	นาย				9	20022	20022118							
10	20023	156	นาย				10	20023	20023165							
11	20024	160	นาย				11	20024	20024810							
								20025	20025722							

TECHNIQUES FOR INTEGRITY AND CONFIDENTIALITY

A hash function is any function that can be used to map data of arbitrary size to fixed-size values.

The values returned by a hash function are called hash values, hash codes, digests, or simply hashes.



A cryptographic hash function (specifically SHA-1) at work. A small change in the input (in the word "over") drastically changes the output (digest). This is the so-called avalanche effect.

HTTPS://EN.WIKIPEDIA.ORG/WIKI/CRYPTOGRAPHIC_HASH_FUNCTION

CRYPTOGRAPHIC HASH ALGORITHMS: EXAMPLES

- MD5
- SHA-1
- SHA-2
- SHA-3

- SHA-256
- SHA-384
- SHA-512

- MD5: MD5 produces a digest of 128 bits (16 bytes)
- SHA-1: SHA-1 produces a hash digest of 160 bits (20 bytes)
- SHA-2: SHA-224 has an output size of 224 bits (28 bytes), SHA-256, 32 bytes; SHA-384, 48 bytes; and SHA-512, 64 bytes
- SHA-3: SHA-3 provides the same output sizes as SHA-2: 224, 256, 384, and 512 bits

Server: localhost » Database: [redacted] » Table: [redacted]

Browse | Structure | SQL | Search | Insert | Export | Import | More

Showing rows 0 - 0 (1 total, Query took 0.0001 seconds.)

```
SELECT * FROM `tbl_users`
```

Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

Show all | Number of rows: 25 Filter rows: Search this table

+ Options

	id	name	pass	email	status
Edit Copy Delete	1	t[redacted]	e10adc3949ba59abbe56e057f20f883e	[redacted]@gmail.com	approved

Check all *With selected:* Edit Copy Delete Export

Show all | Number of rows: 25 Filter rows: Search this table

EXAMPLES

JOHN DOE

USER INFORMATION

PASSWORD (MD5)

E10ADC3949BA59ABBE56E057F20F883E

JOHN DOE

JOHNDOE@GMAIL.COM

JOHNDOE

E10ADC3949BA59ABBE56E057F20F883E

EXAMPLES

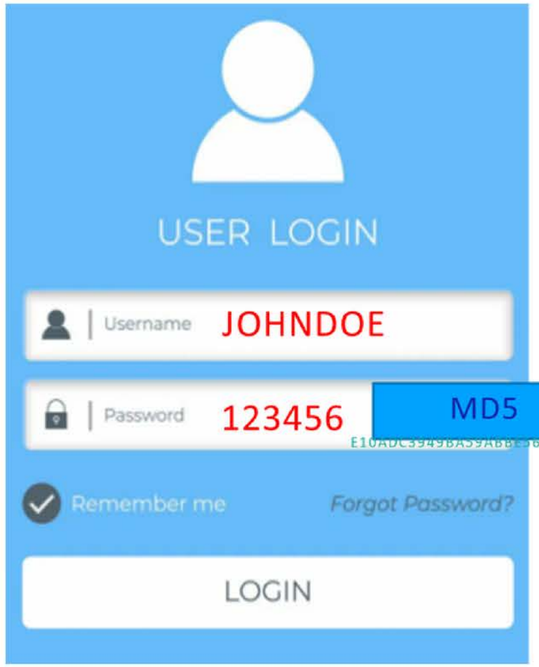
REAL PASSWORD IS NEVER SAVED IN THE DATABASE, ONLY THE HASH VALUE OF THE PASSWORD IS SAVED

JOHN DOE

JOHNDOE@GMAIL.COM

JOHNDOE

E10ADC3949BA59ABBE56E057F20F883E



MD5

E10ADC3949BA59ABBE56E057F20F883E

MATCHED !!!
USER FOUND
LOG-IN TO SYSTEM

USER NAME

MD5

HOW TO SECURELY DELETE FILES

File allocation table

File name	Creation Time	First cluster	Length
A	T1	1	2
B	T2	3	4
C	T3	7	5
D	T4	...	...
E	T5	...	...

File on disk

00	1	2	3	4	5	6	7	8	9	10
10	A	A	B	B	B	B	C	C	C	C
20	C	D	D	E	E	E	E			

HOW TO SECURELY DELETE FILES

File allocation table

File name	Creation Time	First cluster	Length
A	T1	1	2
B Deleted	T2	3	4
C	T3	7	5
D	T4	...	...
E	T5	...	...

*Marked as Deleted

Undeleting possible

File on disk

File content is still on the device

00	1	2	3	4	5	6	7	8	9	10
10	A	A	B	B	B	B	C	C	C	C
20	C	D	D	E	E	E	E			

Press: shift + delete (do not put into the recycle bin)

DATA ERASURE

Clearing

Clearing is the removal of sensitive data from storage devices in such a way that there is assurance that the data may not be reconstructed using normal system functions or software file/data recovery utilities. The data may still be recoverable, but not without special laboratory techniques.

Clearing is typically an administrative protection against accidental disclosure within an organization. For example, before a hard drive is re-used within an organization, its contents may be cleared to prevent their accidental disclosure to the next user.

DATA ERASURE

Purging

Purging or sanitizing is the physical rewrite of sensitive data from a system or storage device with the intent that the data cannot be recovered.

Purging, proportional to the sensitivity of the data, is generally done before releasing media beyond control, such as before discarding old media, or moving media to a computer with different security requirements.

DATA ERASURE

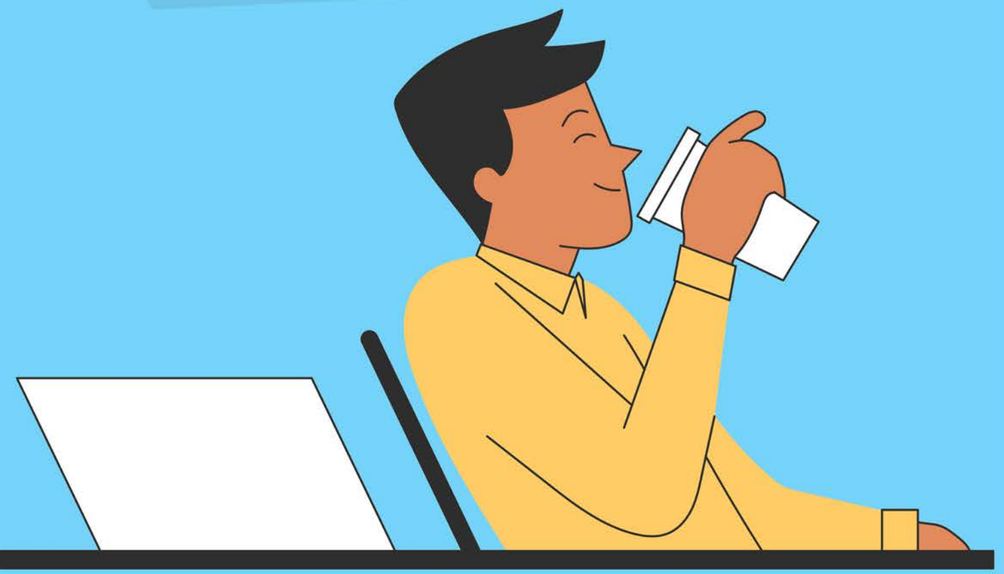
Destruction

The storage media is made unusable for conventional equipment. Effectiveness of destroying the media varies by medium and method.

Depending on recording density of the media, and/or the destruction technique, this may leave data recoverable by laboratory methods.

Conversely, destruction using appropriate techniques is the most secure method of preventing retrieval.

- PURGING
- DATA CLEARING
- DATA WIPING
- DATA DESTRUCTION



A software-based method of overwriting the data that aims to completely destroy all electronic data residing on a hard disk drive or other digital media by using zeros and ones to overwrite data onto all sectors of the device

Overwriting Standard	Date	Overwriting Rounds	Pattern
U.S. Navy Staff Office Publication NAVSO P-5239-26[13]	1993	3	A character, its complement, random
U.S. Air Force System Security Instruction 5020[14]	1996	3	All zeros, all ones, any character
Peter Gutmann's Algorithm	1996	1 to 35	Various, including all of the other listed methods
Bruce Schneier's Algorithm[15]	1996	7	All ones, all zeros, pseudo-random sequence five times
U.S. DoD Unclassified Computer Hard Drive Disposition[16]	2001	3	A character, its complement, another pattern
German Federal Office for Information Security[17]	2004	2–3	Non-uniform pattern, its complement
Communications Security Establishment Canada ITSG-06[18]	2006	3	All ones or zeros, its complement, a pseudo-random pattern
NIST SP-800-88[19]	2006	1	?
U.S. National Industrial Security Program Operating Manual (DoD 5220.22-M)[12]	2006	?	?
NSA/CSS Storage Device Declassification Manual (SDDM)[20]	2007	0	?
Australian Government ICT Security Manual 2014 – Controls[21]	2014	1	Random pattern (only for disks larger than 15 GB)
New Zealand Government Communications Security Bureau NZSIT 402[22]	2008	1	?
British HMG Infosec Standard 5, Baseline Standard[23]	?	1	Random Pattern
British HMG Infosec Standard 5, Enhanced Standard	?	3	All ones, all zeros, random
NIST SP-800-88 Rev. 1[24]	2014	1	All zeros

EXAMPLE

File allocation table

File name	Creation Time	First cluster	Length
A	T1	1	2
B Deleted	T2	3	4
C	T3	7	5
D	T4	...	...
E	T5	...	...

*Deleted and overwritten

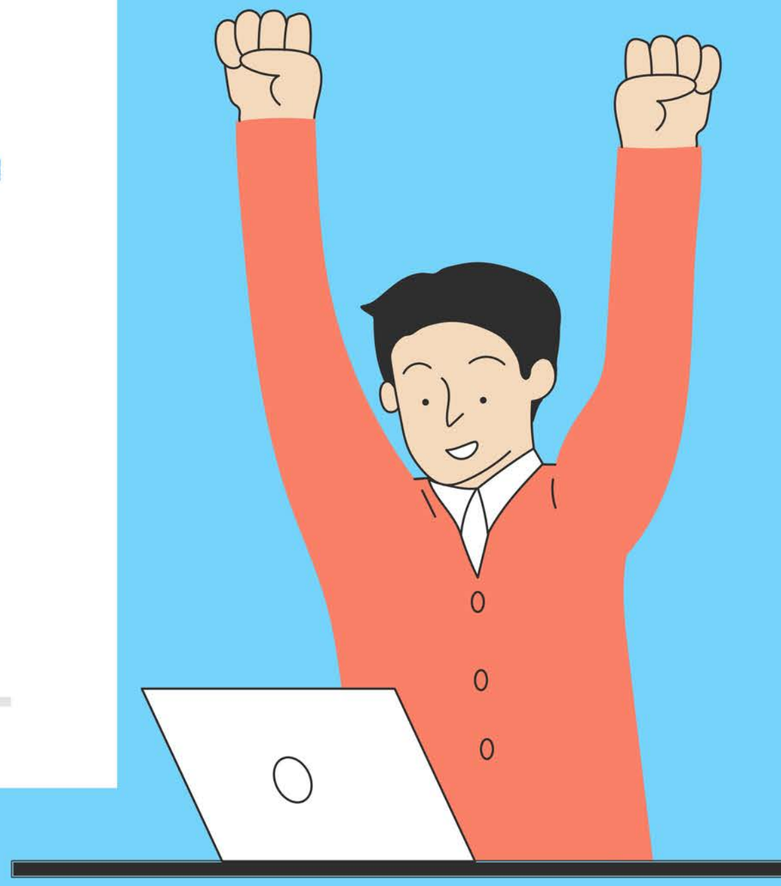
File on disk

File content is overwritten depending on standards

00	1	2	3	4	5	6	7	8	9	10
10	A	A	0	0	0	0	C	C	C	C
20	C	D	D	E	E	E	E			

File Shredder Software (clearing + purging)

File Shredder is a desktop application for shredding (destroying) unwanted files beyond recovery



List of data-erasing software

From Wikipedia, the free encyclopedia

This is a list of utilities for performing data erasure.

Name	Developer	Licensing	Operating system required to run
BleachBit	Andrew Ziem and contributors	GNU General Public License	Windows, Linux
CCleaner	Piriform	Trialware	Windows, OS X
Darik's Boot and Nuke (DBAN)	Darik Horn	GNU General Public License	OS independent, based on Linux
dd[4][5]		Same as host OS	Unix
Disk Utility	Apple	Commercial proprietary software	OS X
Eraser	Heidi Computers Limited	GNU GPL v3	Windows
HDDerase	University of California, San Diego	Freeware	OS independent, based on DOS
hdparm	Mark Lord	BSD license	Linux
nwipe	Martijn van Brummelen	GNU GPL v2	Linux
Parted_Magic	Patrick Verner, Parted Magic LLC	uses mostly GPL components with published source, a few proprietary components, and fee for media/download[10][11]	OS independent, based on Slackware Linux
shred	GNU Project	GNU GPL v3	Unix
ShredIt	Mireth Technology, Burningthumb Software	Trialware	Windows, OS X
srm	Dirk Jagdmann	MIT License[15]	Unix
Zeero		Proprietary software	Tru64 UNIX

DARIK'S BOOT AND NUKE

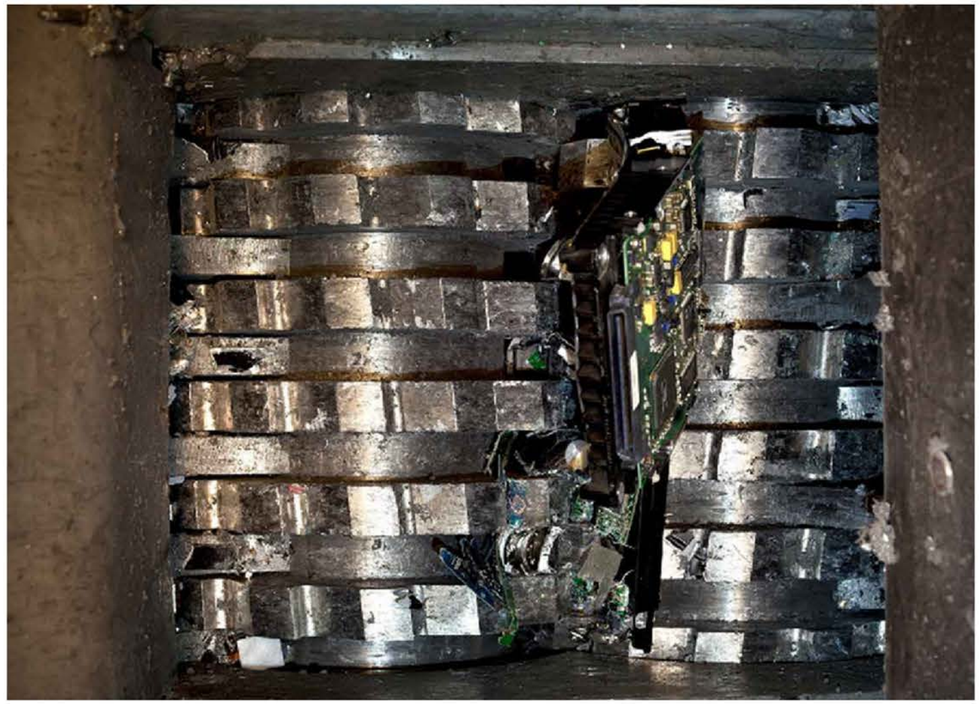
https://dban.org/

DARIK'S BOOT AND NUKE

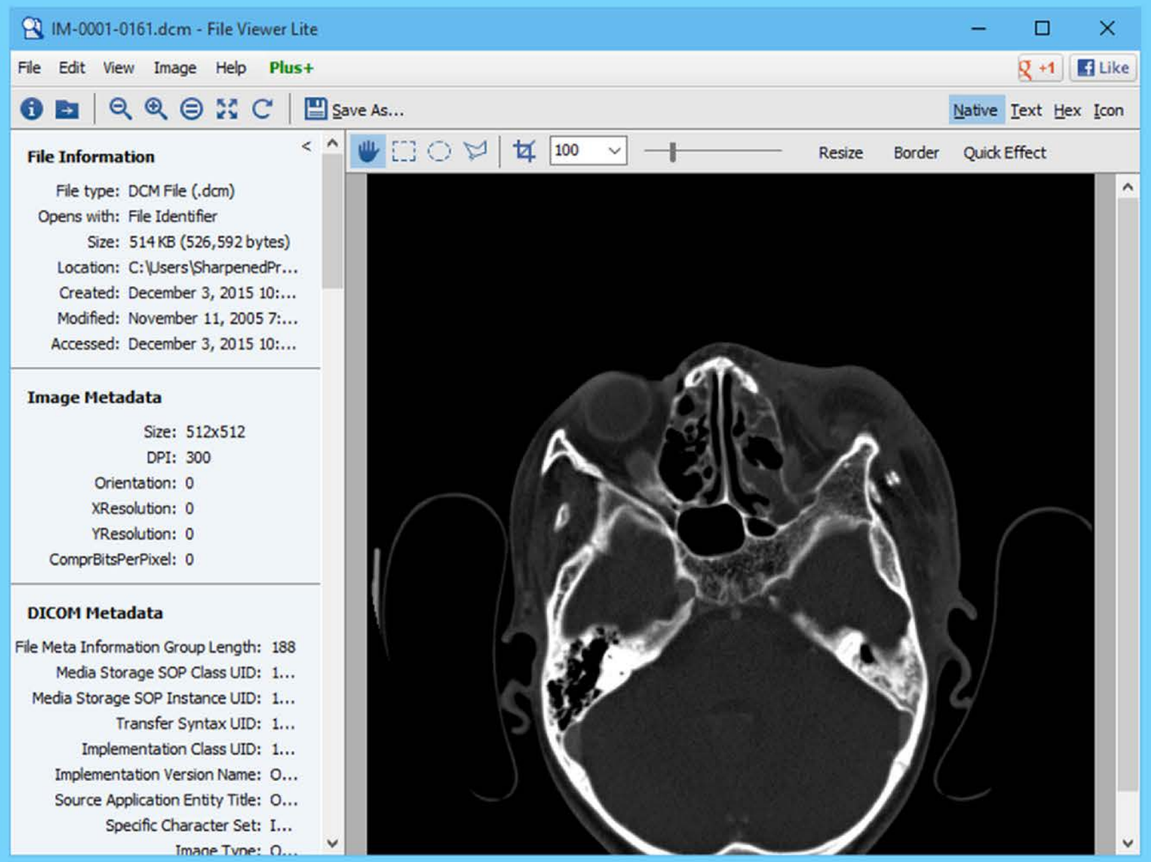
https://dban.org/


```
Darik's Boot and Nuke

 Warning: This software irrecoverably destroys data.

 This software is provided without any warranty; without even the implied
 warranty of merchantability or fitness for a particular purpose. In no event
 shall the software authors or contributors be liable for any damages arising
 from the use of this software.  This software is provided "as is".

 http://www.dban.org/

 * Press the F2 key to learn about DBAN.
 * Press the F3 key for a list of quick commands.
 * Press the F4 key for troubleshooting hints.
 * Press the ENTER key to start DBAN in interactive mode.
 * Enter autonuke at this prompt to start DBAN in automatic mode.

boot: _
```

DESTRUCTION



DICOM ANONYMIZING



General:

TAG	Name	Value
0002, 0012	Implementation Class UID	modified
0002, 0013	Implementation Class UID	"DICOMLIBRARY-100"
0002, 0016	Source Application Entity Title	"DICOMLIBRARY"
0002, 0100	Private Information Creator UID	empty
0002, 0102	Private Information	empty

UID Anonymity:

TAG	Name	Value
0002, 0003	Media Storage SOP Instance UID	unique
0008, 0018	SOP Instance UID	unique

Patient Anonymization:

TAG	Name	Value
0010, 0010	Patient's Name	"Anonymized^^"
0010, 0020	Patient ID	"0"
0010, 0021	Issuer of Patient ID	empty
0010, 0022	Type of Patient ID	empty
0010, 0030	Patient's Birth Date	empty
0010, 0032	Patient's Birth Time	empty
0010, 0050	Patient's Insurance Plan Code Sequence	removed
0010, 0101	Patient's Primary Language Code Sequence	removed
0010, 0102	Patient's Primary Language Code Modifier Sequence	removed
0010, 1000	Other Patient IDs	empty
0010, 1001	Other Patient Names	empty
0010, 1002	Other Patient IDs Sequence	removed
0010, 1005	Patient's Birth Name	empty
0010, 1040	Patient's Address	empty
0010, 1050	Insurance Plan Identification (RET)	empty
0010, 1060	Patient's Mother's Birth Name	empty
0010, 1080	Military Rank	empty
0010, 1081	Branch of Service	empty
0010, 1090	Medical Record Locator	empty
0010, 2150	Country of Residence	empty
0010, 2152	Region of Residence	empty
0010, 2154	Patient's Telephone Numbers	empty
0010, 2160	Ethnic Group	empty
0010, 2180	Occupation	empty
0010, 21b0	Additional Patient History	empty
0010, 21c0	Pregnancy Status	empty
0010, 21d0	Last Menstrual Date	empty
0010, 21f0	Patient's Religious Preference	removed
0010, 2202	Patient Species Code Sequence	removed
0010, 2203	Patient's Sex Neutered	empty
0010, 2293	Patient Breed Code Sequence	removed
0010, 2294	Breed Registration Sequence	removed
0010, 2295	Breed Registration Number	empty
0010, 2296	Breed Registry Code Sequence	removed
0010, 2297	Responsible Person	empty
0010, 2298	Resp	
0010, 2299	Resp	

Study Anonymity:

TAG	Name	Value
0020, 0010	Study ID	"1"
0008, 0050	Accession Number	empty
0032, 000a	Study Status ID (RET)	empty
0032, 000c	Study Priority ID (RET)	empty
0032, 0012	Study ID Issuer (RET)	empty
0032, 0032	Study Verified Date (RET)	empty
0032, 0033	Study Verified Time (RET)	empty
0032, 0034	Study Read Date (RET)	empty
0032, 0035	Study Read Time (RET)	empty
0032, 1000	Scheduled Study Start Date (RET)	empty
0032, 1001	Scheduled Study Start Time (RET)	empty
0032, 1010	Scheduled Study Stop Date (RET)	empty
0032, 1011	Scheduled Study Stop Time (RET)	empty
0032, 1020	Scheduled Study Location (RET)	empty
0032, 1021	Scheduled Study Location AE Title (RET)	empty
0032, 1030	Reason for Study (RET)	empty
0032, 1031	Requesting Physician Identification Sequence	removed
0032, 1032	Requesting Physician	empty
0032, 1033	Requesting Service	empty
0032, 1040	Study Arrival Date (RET)	empty
0032, 1041	Study Arrival Time (RET)	empty
0032, 1050	Study Completion Date (RET)	empty
0032, 1051	Study Completion Time (RET)	empty
0032, 1055	Study Component Status ID (RET)	empty
0032, 1060	Requested Procedure Description	empty
0032, 1064	Requested Procedure Code Sequence	removed
0032, 1070	Requested Contrast Agent	empty
0032, 4000	Study Comments	empty
0040, 2008	Order Entered By	empty
0040, 2009	Order Enterer's Location	empty
0040, 2010	Order Callback Phone Number	empty

Visit Anonymity:

TAG	Name	Value
0008, 0080	Institution Name	empty
0008, 0081	Institution Address	empty
0008, 0082	Institution Code Sequence	removed
0008, 0090	Referring Physician's Name	empty
0008, 0092	Referring Physician's Address	empty
0008, 0094	Referring Physician's Telephone Numbers	empty
0008, 0096	Referring Physician Identification Sequence	removed
0008, 0116	Responsible Organization	empty
0008, 1048	Physician(s) of Record	empty
0008, 1049	Physician(s) of Record Identification Sequence	removed
0008, 1050	Performing Physician's Name	empty
0008, 1052	Performing Physician Identification Sequence	removed
0008, 1060	Name of Physician(s) Reading Study	empty
0008, 1062	Physician(s) Reading Study Identification Sequence	removed
0008, 1070	Operators' Name	empty
0008, 1072	Operator Identification Sequence	removed
0038, 0010	Admission ID	empty
0038, 0011	Issuer of Admission ID	empty
0038, 0016	Route of Admissions	empty
0038, 001a	Scheduled Admission Date (RET)	empty
0038, 001b	Scheduled Admission Time (RET)	empty
0038, 001c	Scheduled Discharge Date (RET)	empty
0038, 001d	Schedul	
0038, 001e	Schedul	
0038, 0020	Admittin	
0038, 0021	Admittin	
0038, 0030	Dischar	
0038, 0032	Dischar	
0038, 0040	Dischar	
0038, 0044	Dischar	
0038, 0300	Current	
0038, 0400	Patient'	
0038, 0500	Patient	

Procedure Anonymity:

TAG	Name	Value
0040, 0001	Scheduled Station AE Title	empty
0040, 0006	Scheduled Performing Physician's Name	empty
0040, 000b	Scheduled Performing Physician Identification Sequence	removed
0040, 0010	Scheduled Station Name	empty
0040, 0011	Scheduled Procedure Step Location	empty
0040, 0012	Pre-Medication	empty
0040, 0241	Performed Station AE Title	empty
0040, 0242	Performed Station Name	empty
0040, 0243	Performed Location	empty
0040, 0296	Billing Item Sequence	removed

Results Anonymity:

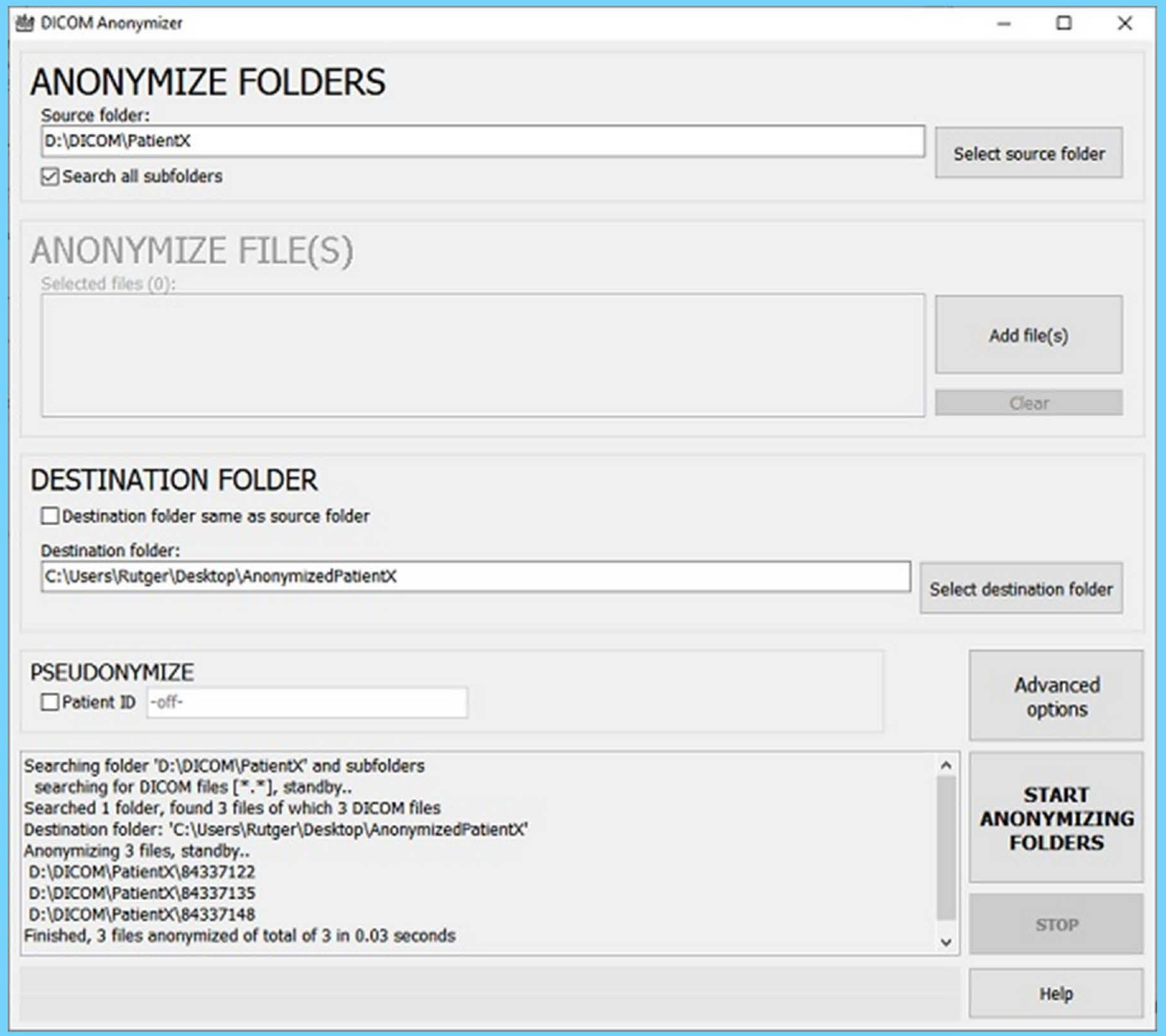
TAG	Name	Value
4008, 0042	Results ID Issuer (RET)	empty

Interpretation Anonymity:

TAG	Name	Value
4008, 010c	Interpretation Author (RET)	empty
4008, 0114	Physician Approving Interpretation (RET)	empty
4008, 0119	Distribution Name (RET)	empty
4008, 011a	Distribution Address (RET)	empty

Equipment Anonymity:

TAG	Name	Value
0008, 0070	Manufacturer	empty
0008, 1010	Station Name	empty
0008, 1040	Institutional Department Name	empty
0008, 1090	Manufacturer's Model Name	empty
0018, 1000	Device Serial Number	empty
0018, 1016	Secondary Capture Device Manufacturer	empty
0018, 1017	Hardcopy Device Manufacturer	empty
0018, 1018	Secondary Capture Device Manufacturer's Model Name	empty
0018, 1019	Secondary Capture Device Software Version(s)	empty
0018, 101a	Hardcopy Device Software Version	empty
0018, 101b	Hardcopy Device Manufacturer's Model Name	empty
0018, 1020	Software Version(s)	empty
0018, 1200	Date of Last Calibration	empty
0018, 1201	Time of Last Calibration	empty
0018, 700c	Date of Last Detector Calibration	empty
0018, 700e	Time of Last Detector Calibration	empty
0018, 7010	Exposures on Detector Since Last Calibration	empty
0018, 7011	Exposures on Detector Since Manufactured	empty

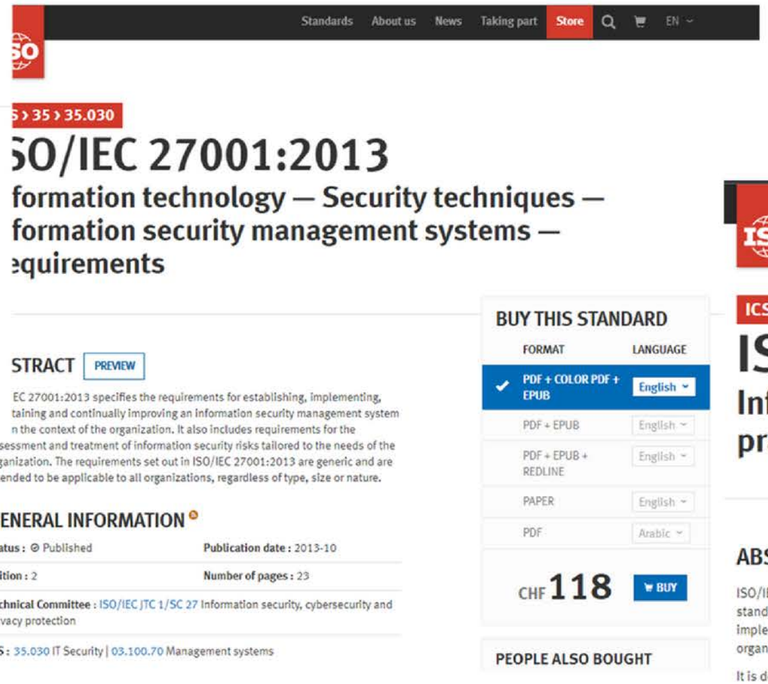


ISRRT INTERNATIONAL SOCIETY OF RADIOGRAPHERS & RADIOLOGICAL TECHNOLOGISTS

ISRRT World Congress Bangkok 2022

DICOM ANONYMIZER

International Standard for Information Security Management Systems

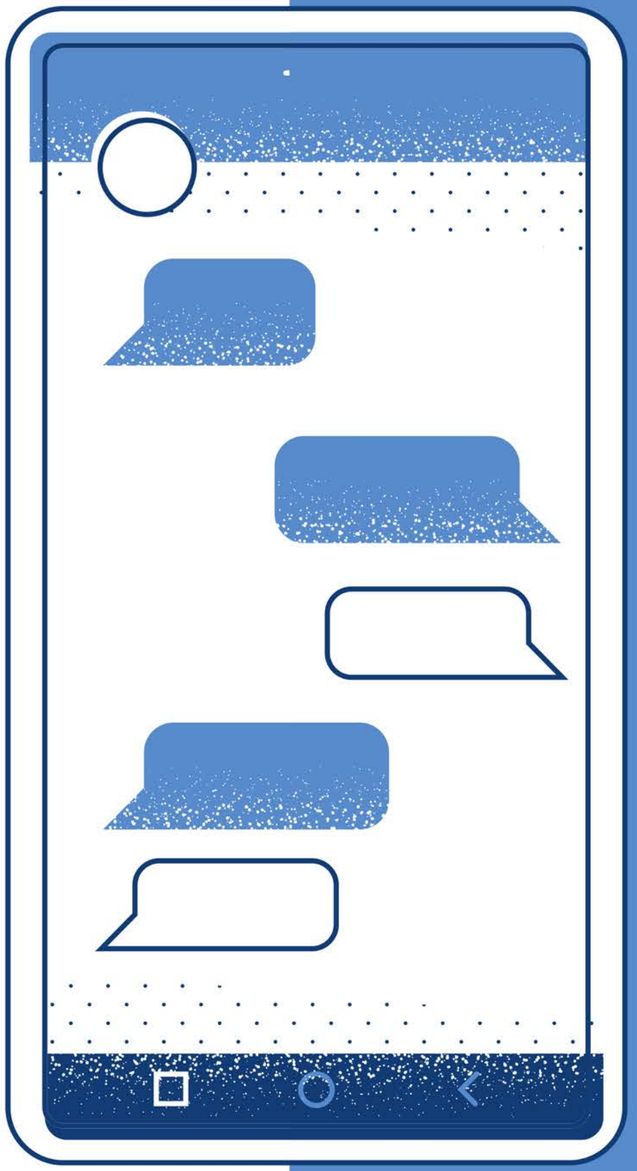


What is an Information Security Management System?

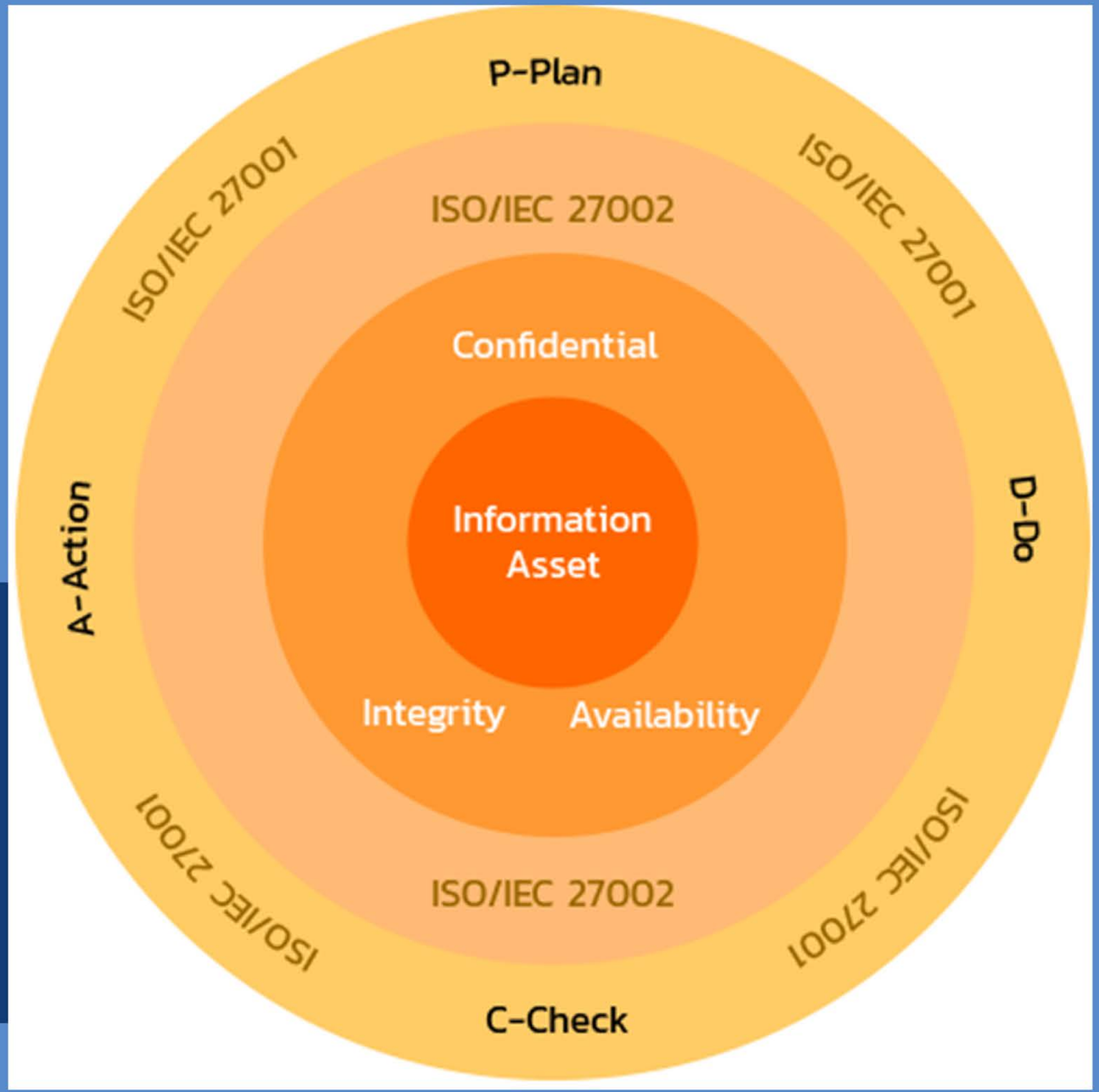
ISO27001 (or to give its proper name, ISO/IEC 27001) is the international standard for Information Security Management Systems (ISMS)

An ISMS is a set of processes that together help an organization to manage their information security by assessing their risks and taking action to reduce them.

The management system is simply a set of things you must do to keep on top of your information security



- **Information security policy** – what are your rules on keeping your subject data secure?
- **Objectives** – what are you trying to do with your data?
- **Risk assessment and treatment** – what could go wrong like subject data leak and how can you stop it?
- **Roles and responsibilities** – who does what in your research?
- Competence – does everyone have the skills they need to work with the data?
- **Awareness training** – does everyone in your research team know about information security?
- **Monitoring and measuring** – quantifying what's going on accessing and using your subject data.
- **Internal audit** – independent checks that it's all happening as it should with your data.
- **Management review** – keeping everything in your subject data use under control.


P-Plan
ISO/IEC 27001
ISO/IEC 27002
Confidential
Information Asset
Integrity
Availability
D-Do
C-Check
A-Action

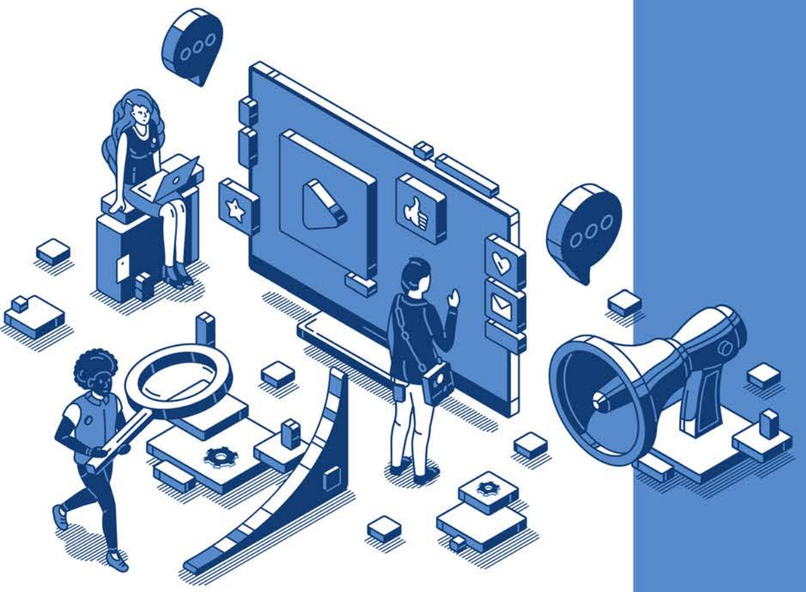
Health Information & Related Laws

http://office.cpd.go.th/itc/index.php/info-organization/law-it/computer-act

พระราชบัญญัติคอมพิวเตอร์

รายละเอียด	PDF
ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563	
พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563	
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	
พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560	
พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	
พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ฉบับที่ 4 พ.ศ. 2562	
พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ฉบับที่ 3 พ.ศ. 2562	
พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ฉบับที่ 2 พ.ศ. 2551	
พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 (แก้ไขเพิ่มเติม พ.ศ. 2551)	
พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	

Personal Data Protection Act B.E. 2562 (2019)



- PDPA ย่อมาจาก Personal Data Protection Act B.E. 2562 (2019)
- เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดยกฎหมาย PDPA Thailand (พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล)
- ประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562
- ปัจจุบันได้ถูกเลื่อนให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565
- คุ้มครองและให้สิทธิที่เราควรมีต่อข้อมูลส่วนบุคคลของเราเองได้
- สร้างมาตรฐานของบุคคลหรือนิติบุคคล ในการเก็บข้อมูลส่วนบุคคล, รวบรวมข้อมูลส่วนบุคคล, ใช้ข้อมูลส่วนบุคคล หรือเพื่อการเปิดเผยข้อมูลส่วนบุคคลก็ตาม
- ซึ่งบทลงโทษของ PDPA สำหรับผู้ที่ไม่ปฏิบัติตามนั้น มีทั้งโทษทางแพ่ง โทษทางอาญา และโทษทางปกครอง

Personal Data Protection Act B.E. 2562 (2019)

- เจ้าของข้อมูลส่วนบุคคล (Data Subject) คือ บุคคลที่ข้อมูลสามารถระบุไปถึงได้

- ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เช่น รพ หรือ แผนกต่างๆ ใน รพ

- ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล อาจให้ผู้อื่น ดำเนินการตามคำสั่ง เช่น จ้าง บริษัท มาดำเนินการ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพุทธศักราช 2562

เรื่องที่แพทย์ควรรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพุทธศักราช 2562 โดย ดร.ปริญญา หอมเอนก จัดโดย แพทยสภา (คณะอนุกรรมการพิจารณาแนวทางการดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

https://www.facebook.com/thaimedcouncil/videos/740771093217660

เรื่อง "ข้อควรรู้สำหรับแพทย์เกี่ยวกับพระราชบัญญัติข้อมูลส่วนบุคคล พ.ศ.2562" ครั้งที่ 2 ฝ่ายจริยธรรมและกฎหมาย แพทยสภา ณ ห้องประชุมแพทยสภา ชั้น 14 อาคารสภาวิชาชีพ ซอยสาธารณสุข 8 กระทรวงสาธารณสุข นนทบุรี

https://www.facebook.com/thaimedcouncil/videos/121521026489673

เรื่อง "กฎหมายคุ้มครองส่วนบุคคลในมุมมองของศาล" วันพฤหัสบดี 25 มีนาคม 2564 เวลา 9-12.00 น. วิทยากร "ดร.วรวงศ์ อัจฉราวงศ์ชัย" ผู้พิพากษาศาลชั้นต้น ประจำสำนักประธานศาลฎีกา และ ผู้อำนวยการบริหารสถาบันอนุญาโตตุลาการ

https://www.facebook.com/thaimedcouncil/videos/473142353732583

Principles of Information Security

HIPAA	REGULATES HEALTH CARE PROVIDERS' COLLECTION AND DISCLOSURE OF SENSITIVE HEALTH INFORMATION
COPPA	REGULATES ONLINE COLLECTION AND USE OF INFORMATION OF CHILDREN
GLBA	REGULATES FINANCIAL INSTITUTIONS' USE OF NONPUBLIC PERSONAL INFORMATION
FCRA	REGULATES THE COLLECTION AND USE OF DATA CONTAINED IN CONSUMER CREDIT REPORTS
FTC ACT	PROHIBITS "UNFAIR OR DECEPTIVE ACTS OR PRACTICES"

Management & Policy
Regulations & Laws

HTTPS://WWW.SECURITYMADESIMPLE.ORG/CYBERSECURITY-BLOG/WHAT-ARE-THE-3-PRINCIPLES-OF-INFORMATION-SECURITY

THANK YOU FOR YOUR ATTENTION

yudthaphon.com