“วิธีการและกระบวนการทำลายและการชำระล้างข้อมูลจากสื่ออิเล็กทรอนิกส์ ตามมาตรฐานสากล”

โดย อ.ไชยกร อภิวัฒโนกุล

CISSP, CSSLP, GCFA, (IRCA:ISMS), (ISC)2:ISLA

CEO S-Generation Co., Ltd.

อนุกรรมการความมั่นคงปลอดภัย ธอ.

กรรมการสมาคมความมั่นคงปลอดภัยยระบบสารสนเทศ (TISA)

17 กันยายน 2556

Name:	**Chaiyakorn Apiwathanokul** **ไชยกร อภิวัฒโนกุล**
Title:	**Chief Executive Officer**
Company:	**S-GENERATION Company Limited** **S-FORENSICS Company Limited**
Certificates:	*CISSP, CSSLP, IRCA:ISMS (ISO27001), SANS:GCFA*

- CSO ASEAN Award 2010 by International Data Group (IDG)
- 2010 Asia-Pacific Information Security Leadership Achievements (ISLA) by $(ISC)^2$
- Security Sub-commission under Thailand Electronic Transaction Commission (ET Act B.E. 2544)
- Contribute to Thailand Cyber Crime Act B.E.2550
- Workgroup for CA service standard development
- Committee of national standard adoption of ISO27001/ISO27002
- Committee of Thailand Information Security Association (TISA)
- Committee of Cybersecurity workforce development, Division of Skill Development, Ministry of Labour
- Advisor to Department of Special Investigation (DSI)
- Advisor to Cybersecurity Monitoring Center, Ministry of Defense (MOD)

Committee Member of Thailand Information Security Association

1997 1999 1999 2004 2006 2011

chaiyakorna@hotmail.com

อ้างอิง

หน้า ๑
เล่ม ๑๒๒ ตอนพิเศษ ๘๘ ง ราชกิจจานุเบกษา ๒๓ กันยายน ๒๕๔๘

ระเบียบสำนักนายกรัฐมนตรี

ว่าด้วยงานสารบรรณ

พ.ศ. ๒๕๒๖

โดยที่เป็นการสมควรปรับปรุงระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๐๖ เสียใหม่ให้เหมาะสมยิ่งขึ้น คณะรัฐมนตรีจึงวางระเบียบไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่วันที่ ๑ มิถุนายน ๒๕๒๖ เป็นต้นไป

ส่วนที่ ๓

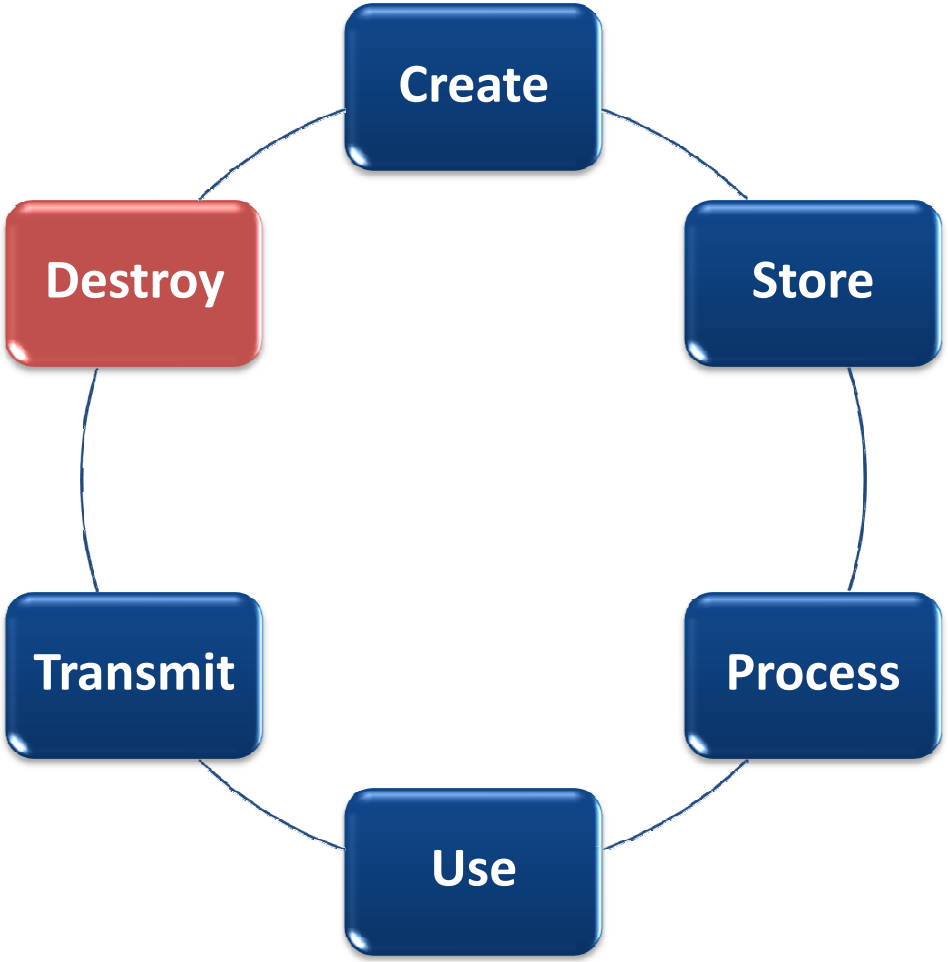
การทำลาย

๖๘.๕ ควบคุมการทำลายหนังสือซึ่งผู้มีอำนาจอนุมัติให้ทำลายได้แล้ว **โดยการเผา หรือวิธีอื่นใด**ที่จะไม่ให้หนังสือนั้นอ่านเป็นเรื่องได้ และเมื่อทำลายเรียบร้อยแล้วให้ทำบันทึกลงนามร่วมกันเสนอผู้มีอำนาจอนุมัติทราบ

การทำลายข้อมูลและสื่อบันทึกข้อมูลอิเล็กทรอนิกส์

- หากไม่ดำเนินการตามกรรมวิธีที่ถูกต้องเหมาะสม อาจทำให้ **ข้อมูลรั่วไหล**ได้
- ผลจากข้อมูลรั่วไหล
  - ข้อมูลสำคัญหรือความลับทางราชการถูกเปิดเผย
  - ข้อมูลส่วนบุคคลถูกเปิดเผยหรือนำไปใช้ประโยชน์
  - ข้อมูลผู้ป่วย ข้อมูลแฟ้มคดีลับ ฯลฯ
  - ทรัพย์สินทางปัญญาถูกขโมย
  - ประชาชนขาดความเชื่อมั่น
  - ธุรกิจเสียหาย
  - ภาพลักษณ์องค์กรและประเทศเสียหาย

ข้อมูล มีโอกาสรั่วไหลได้ ณ จุดต่างๆ ของวงจรชีพ หากขาดมาตรการที่เหมาะสม

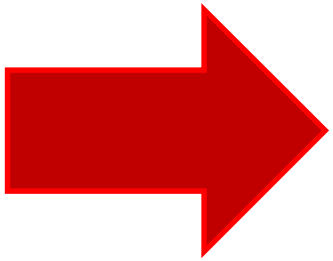


ตัวอย่างเหตุการณ์ความเสี่ยงข้อมูลรั่วไหล

- เครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลที่เลิกใช้ นำไปบริจาคหรือขายทอดตลาด
- โทรศัพท์มือถือขายเป็นเครื่องมือสอง
- โน๊ตบุ๊คหรืออุปกรณ์พกพาหายหรือถูกขโมย
- ข้อมูลชั่วคราว (cache) ในเครื่องถ่ายเอกสาร/multifunction

วิธีดำเนินการในปัจจุบัน

- Delete
- Format



100% Recoverable

- Non-conform to compliances & standards
  - ISO27002
  - PCIDSS
  - SOX, GLB
  - HIPAA/HITECH
  - ระเบียบสำนักนายกว่าด้วยงานสารบรรณ

เอกสารอิเล็กทรอนิกส์ ทำลายอย่างไร?

- **Media sanitization types**

  (อ้างอิงเอกสาร NIST SP800-88rev1 Guidelines for Media Sanitization)

  - Disposal: การทิ้ง
  - Clearing: secure overwriting (against desktop attack)
  - Purging: secure erase command (in ATA drive only)
    or degaussing (against laboratory attack)
  - Destroy: disintegration, shredding and melting

Magnetic-type Media (Hard Drive)

Tier 1
File Deletion

- Indexing removed, data remains

100% of Data Recoverable

Tier 2
Physical Alteration

- Drill Hole in Platters
- Crush Electronics (platters intact)

50-60% of Data Recoverable

Tier 3
Overwrite

- NIST SP 800-88 Single Pass
- DoD Directive 5220.22 (Triple Pass)

10% of Data Recoverable*

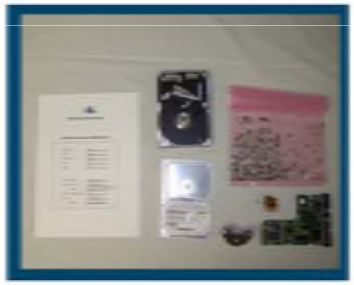
Tier 4
Secure Erase

- (Proposed for Classified Secret or Corporate Sensitive Information)
- Secure Erase
- Degauss Non-NSA Equipment (<5,000Oe)

3-5% of Data Recoverable*

Tier 5
Degauss & Disintegrate

- (Proposed for Classified Top Secret or Corporate Confidential Information)
- Degauss NSA Evaluated Equipment (5,000Oe)
- Disassemble and Recycle Components



0% of Data Recoverable

Tape Destruction

Tier 1
File Deletion

- Only removes file name. Data still 100% intact

100% of Data Recoverable

Tier 2
Physical Destruction

- Cut Tape - Large amount of data remains

95% of Data Recoverable

Tier 3
Chopping

- Chopping a tape
- Data is still recoverable

25-75% of Data Recoverable*

Tier 4
Degauss

- Degauss non-NSA Evaluated Equipment

25-50% of Data Recoverable**

Tier 5
Degauss & Disintegrate

- (Proposed for Top Secret or Corporate Sensitive Data)
- Degauss NSA Evaluated Equipment
- Disassemble and Recycle Components

0% of Data Recoverable

* Depends on particle size
** Depends on field strength of magnets

Optical Disk Destruction

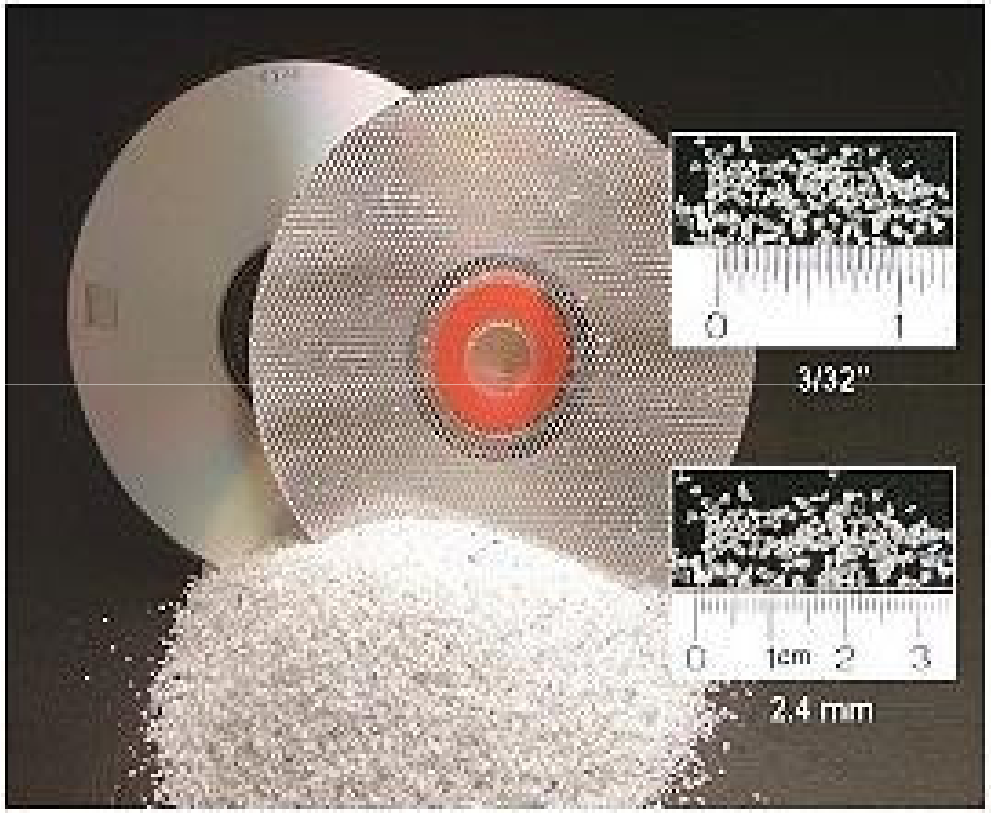
Tier 1
Dimpling
85-100% of
data remaining

Tier 2
Strip-cut Shredding
65-85% of
data remaining

Tier 3
Cross-cut Shredding
35-65% of
data remaining

Tier 4
Disintegration
15-40% of
data remaining

Tier 5
Grinding
0% of
data remaining


0
1
3/32"
0
1cm
2
3
2.4 mm

Legal Penalties for Failure to Sanitize Data

	Gramm-Leach-Bliley	Sarbanes-Oxley	FACTA	HIPAA
	Financial Services Modernization Act	Public Company Accounting Reform & Investor Protection Act	Fair and Accurate Credit Transaction Act	Health Insurance Portability & Accountability Act
Directors and Officers	$10,000	$1,000,000		$50,000 to $250,000
Institution	$100,000			
Years in Prison	5 to 12 years	20 years		1 to 10 years
FDIC Insurance	Terminated			
Impact on Operations	Cease and Desist			
Individual	$1,000,000		Civil Action	$25,000
Institution	1% of assets			

ความท้าทาย

- กระบวนการและกรรมวิธีที่ถูกต้องเหมาะสม
- ระยะเวลา บุคลากร และเครื่องมือที่เหมาะสม
- ป้องกันการรั่วไหลจากการเลิกใช้
- ความเป็นมิตรต่อสิ่งแวดล้อม
- ผู้รับผิดชอบของหน่วยงาน
- หน่วยงานที่รับผิดชอบ/ตรวจสอบ

https://www.facebook.com/chaiyakorna

http://www.s-generation.com

Thank You

ขอบคุณครับ