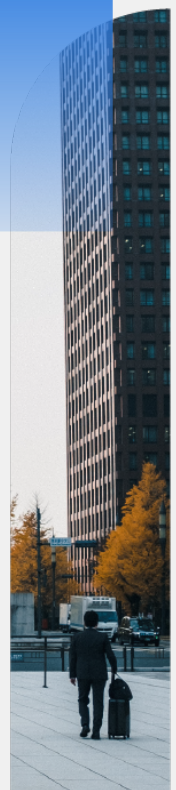
พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หรือ กฎหมาย PDPA สำหรับผู้บริหาร และข้อแนะนำในการปกป้องข้อมูล

Dr. Rattipong Putthacharoen, Com. Eng.
Senior Manager, Systems Engineering



Now : Fortinet
Previously : IBM, AT&T, Packeteer, BlueCoat, Symantec



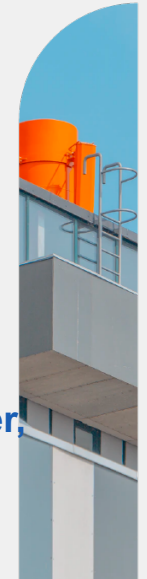


Table of Contents

1 ทบทวน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

2 กระบวนการที่สำคัญ

3 ข้อแนะนำสำหรับผู้บริหาร

4 การประเมินความเสี่ยงและการกำหนดมาตรการควบคุม

5 เครื่องมือสำหรับปกป้องข้อมูลที่เกี่ยวข้อง

© Fortinet Inc. All Rights Reserved.

ทบทวน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

วัตถุประสงค์

ใช้บังคับแก่การ เก็บรวบรวม ใช้ หรือเปิดเผย*

ข้อมูลส่วนบุคคลโดยผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ใน
ราชอาณาจักร ไม่ว่าการกระทำนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม





© Fortinet Inc. All Rights Reserved.

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล



1

อะไรคือข้อมูลส่วนบุคคล

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม

2

สิทธิเจ้าของข้อมูล



สิทธิเข้าถึงข้อมูลส่วนบุคคลของตนและขอให้เปิดเผยถึงการได้มา สิทธิขอให้ระงับการใช้ / ลบ หรือทำลาย สิทธิขอให้แก้ไขข้อมูลให้ถูกต้อง เป็นต้น



3

การละเมิดข้อมูลส่วนบุคคล

แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลทราบภายใน 72 ชั่วโมง เว้นแต่ไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

4

หน้าที่ผู้ควบคุมข้อมูล (Data Controller)

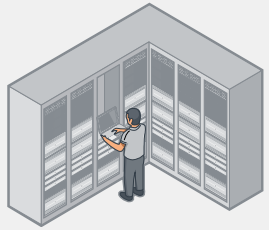
มีอำนาจตัดสินใจเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ต้องข้อความยินยอม แจ้งวัตถุประสงค์ชัดเจน หรือ ลบ หรือ ทำลายข้อมูลเมื่อพ้นระยะเวลา (‘Why’ and ‘How’, ‘Purposes’ and ‘means’)



5

หน้าที่ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ประมวลผลข้อมูลส่วนบุคคล ทั้งการเก็บรวบรวม ใช้ หรือเปิดเผย ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล



6

มาตรการความปลอดภัย

ให้ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

ที่มา ETDA

© Fortinet Inc. All Rights Reserved.

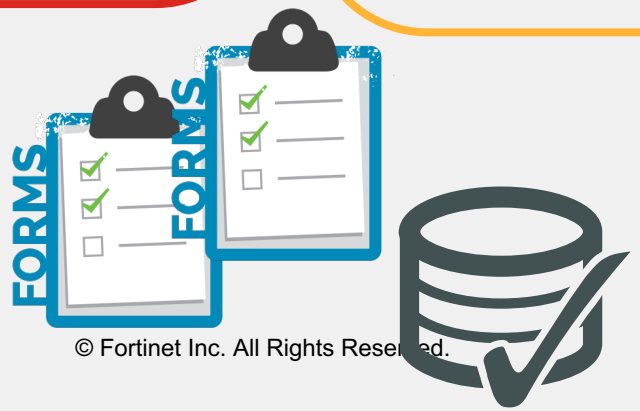
ข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล

ชื่อ นามสกุล, ที่อยู่, หมายเลขอีเมลล์, หมายเลขบัตรเครดิต, หมายเลข passport, หมายเลขใบขับขี่, หมายเลขประจำตัวอื่น ๆ ที่สามารถระบุตัวตนได้, หมายเลขไอพี, หมายเลขเครื่อง, หมายเลขโทรศัพท์, หมายเลขระบุตัวตนที่ใช้ออนไลน์ เช่น cookies, และ รูปถ่าย เป็นต้น

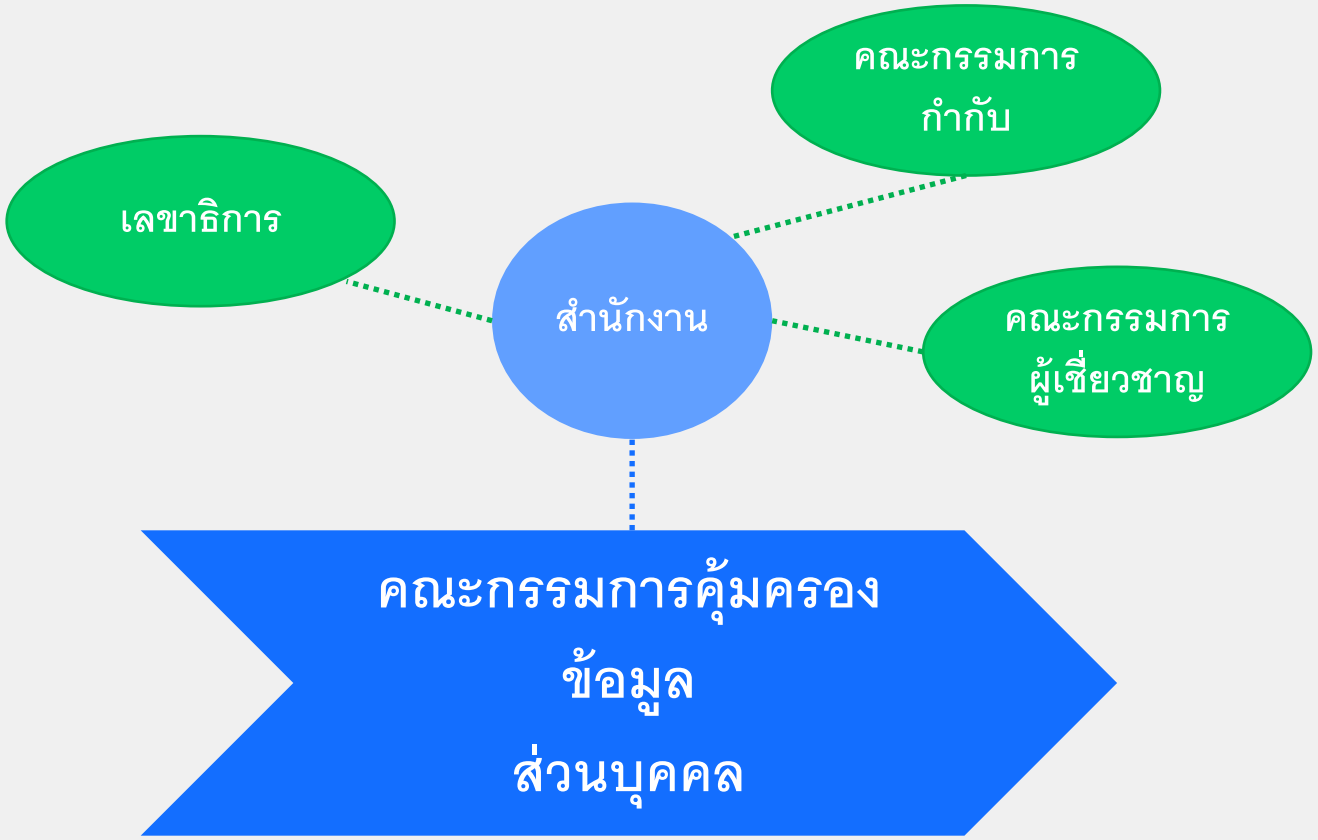
ข้อมูล Sensitive

เชื่อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคล



© Fortinet Inc. All Rights Reserved.

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล



จัดทำแผนแม่บท ส่งเสริมและสนับสนุน กำหนดมาตรการหรือแนวทางการดำเนินการ





เจ้าหน้าที่คุ้มครองข้อมูล
(DPO)

© Fortinet Inc. All Rights Reserved.

การคุ้มครองข้อมูลส่วนบุคคล

ตาม
วัตถุประสงค์

ได้รับความ
ยินยอม

เก็บรวบรวมได้
เท่าที่จำเป็น



ห้ามมิให้เก็บ
รวบรวมข้อมูล
จากแหล่งอื่น

ห้ามไม่ให้
เก็บข้อมูล
Sensitive*

* โดยไม่ได้ขอความ
ยินยอมโดยชัดแจ้ง

© Fortinet Inc. All Rights Reserved.

หน้าที่สำคัญของผู้ควบคุมข้อมูล



ผู้ควบคุมข้อมูล

...บันทึกรายการ...ให้สามารถตรวจสอบได้

...ป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูล...

...แต่งตั้งตัวแทน (ถ้าอยู่นอกราชอาณาจักร)...

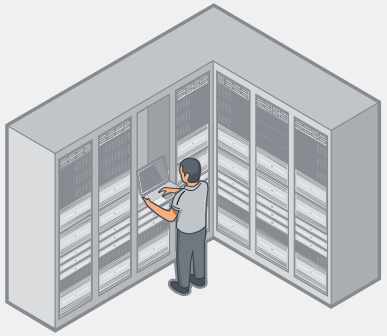
ในกรณีที่ต้องให้ข้อมูล... ต้องป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยโดยปราศจากอำนาจหรือโดยมิชอบ...

...แจ้งเหตุการละเมิดภายในเจ็ดสิบสองชั่วโมง เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบ...

...ดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล...

© Fortinet Inc. All Rights Reserved.

หน้าที่สำคัญของผู้ประมวลผลข้อมูล



ผู้ประมวลผลข้อมูล

- ดำเนิน...ตามคำสั่งที่ได้รับจากผู้ควบคุม...
- ...ป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล*...
- จัดทำและเก็บรักษาบันทึกรายการ...ตามหลักเกณฑ์และวิธีการที่...กำหนด**

*แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิด...

** คณะกรรมการกำหนด

ต้องจัดให้มี (DPO) ในกรณีดังต่อไปนี้



เจ้าหน้าที่คุ้มครองข้อมูล

(DPO)

...เป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด...

...ต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ...โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด

กิจกรรมหลัก...เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล **Sensitive**

บทกำหนดโทษ

ความรับผิดทางแพ่ง	ฝ่าฝืนหรือไม่ปฏิบัติตาม พ.ร.บ แล้วทำให้เกิดความเสียหาย ต้องชดใช้ค่าสินไหมทดแทน เพิ่มขึ้นได้ไม่เกินสองเท่า
โทษอาญา	เกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง (จำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท)
	แสวงหาประโยชน์ (จำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท)
โทษทางปกครอง	ปรับห้าแสน, 1ล้านบาท, 3 ล้านบาท,5 ล้านบาท - กระทำความผิดตาม พ.ร.บ. ในมาตราต่างๆ

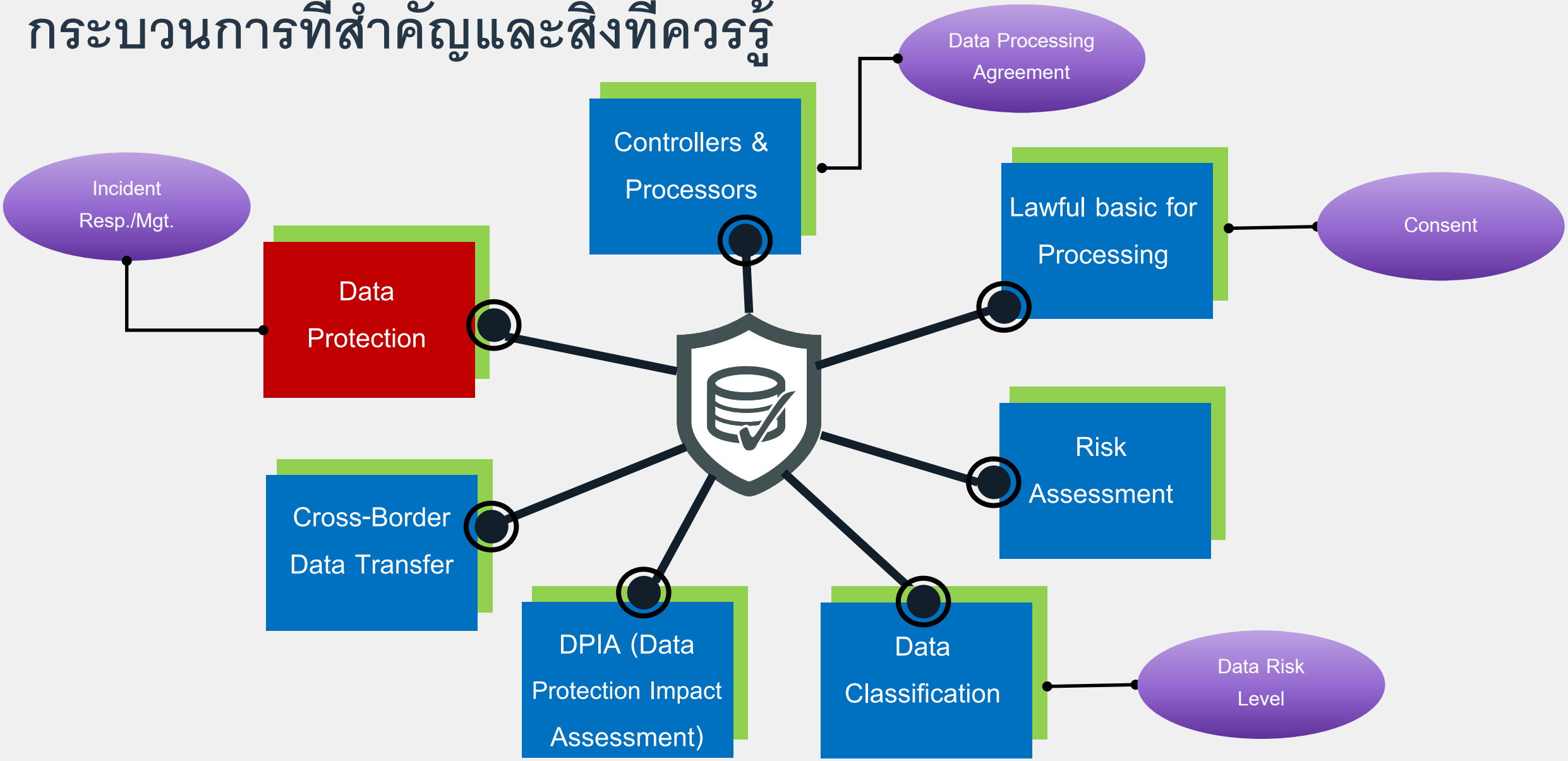
ใช้หรือเปิดเผยข้อมูล Sensitive โดยไม่ยินยอม, ผิดวัตถุประสงค์, หรือ ส่งข้อมูล Sensitive ไปยังประเทศที่มีความปลอดภัยไม่เพียงพอ

...เกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใด ซึ่งรับผิดชอบในการดำเนินงาน...สั่งการหรือกระทำการและละเว้นไม่สั่งการหรือกระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษ...ด้วย

© Fortinet Inc. All Rights Reserved.

กระบวนการที่สำคัญ

กระบวนการที่สำคัญและสิ่งที่ควรรู้



ที่มา Thailand Data Protection Guideline 3.1, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

© Fortinet Inc. All Rights Reserved.

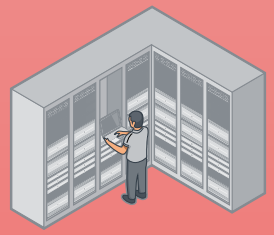
General Data Protection Regulation (GDPR), Information Commissioner's Office (ICO)

สิ่งที่ผู้ควบคุมข้อมูลต้องจัดเตรียม

Controllers

- Duties & Responsibility
- Data Processing Agreement
- User Requests
- Government Requests





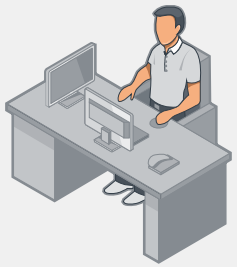
ที่มา Thailand Data Protection Guideline 3.1, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

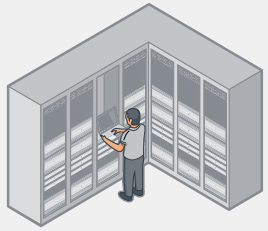
General Data Protection Regulation (GDPR), Information Commissioner's Office (ICO)

© Fortinet Inc. All Rights Reserved.

ข้อตกลงในการประมวลผลข้อมูล (Data Processing Agreement)







Web Users
(Data Subject)

Consent/
User Request

Company Websites
(Data Controller)

Data Processing Agreement

Behavior Analysis
(Data Processor)

Collect the personal data and track user behaviors

Apply for the membership and Accept the consent

Analyze the user behaviors, and automate profiling

ที่มา Thailand Data Protection Guideline 3.1, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

General Data Protection Regulation (GDPR), Information Commissioner's Office (ICO)

© Fortinet Inc. All Rights Reserved.

ฐานในการประมวลผลข้อมูล

Lawful Basic for Processing



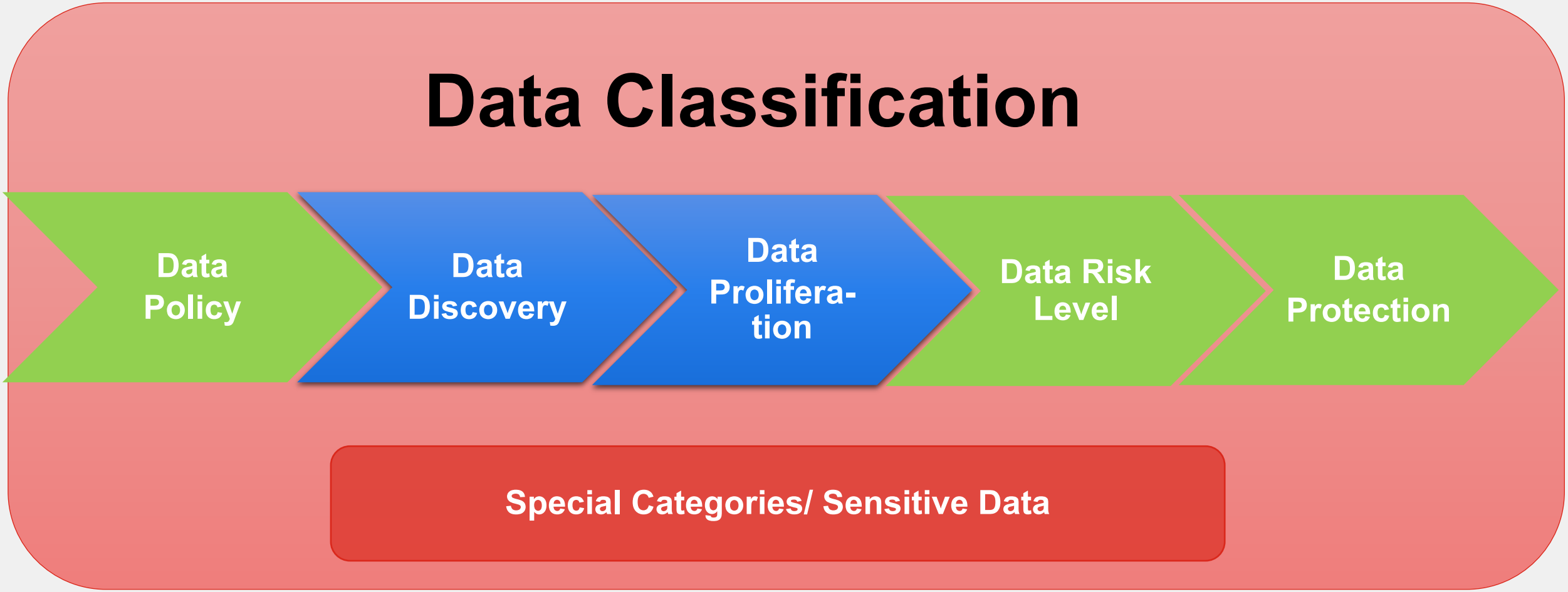


ที่มา Thailand Data Protection Guideline 3.1, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

General Data Protection Regulation (GDPR), Information Commissioner's Office (ICO)

© Fortinet Inc. All Rights Reserved.

การจัดทำ Data Classification



ที่มา Thailand Data Protection Guideline 3.1, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

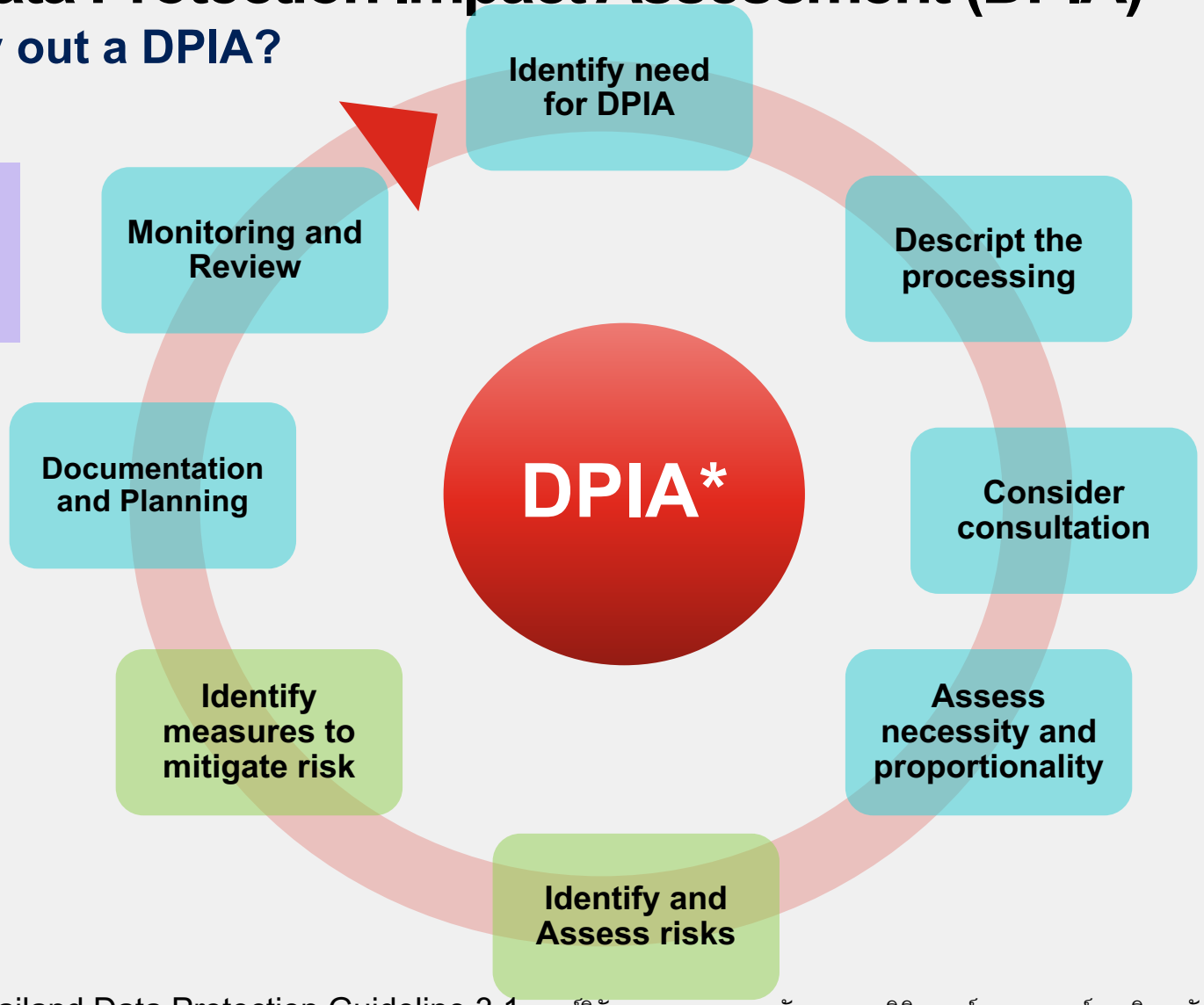
General Data Protection Regulation (GDPR), Information Commissioner's Office (ICO)

© Fortinet Inc. All Rights Reserved.

การจัดทำ Data Protection Impact Assessment (DPIA)

How do we carry out a DPIA?

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (ต่อสิทธิและเสรีภาพ)



***You may not have to carry out a DPIA if You are processing on the basis of legal obligation or public task**

ที่มา Thailand Data Protection Guideline 3.1, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

General Data Protection Regulation (GDPR), Information Commissioner's Office (ICO)

© Fortinet Inc. All Rights Reserved.

การตอบสนองต่อเหตุการณ์

Information Security Incident Management



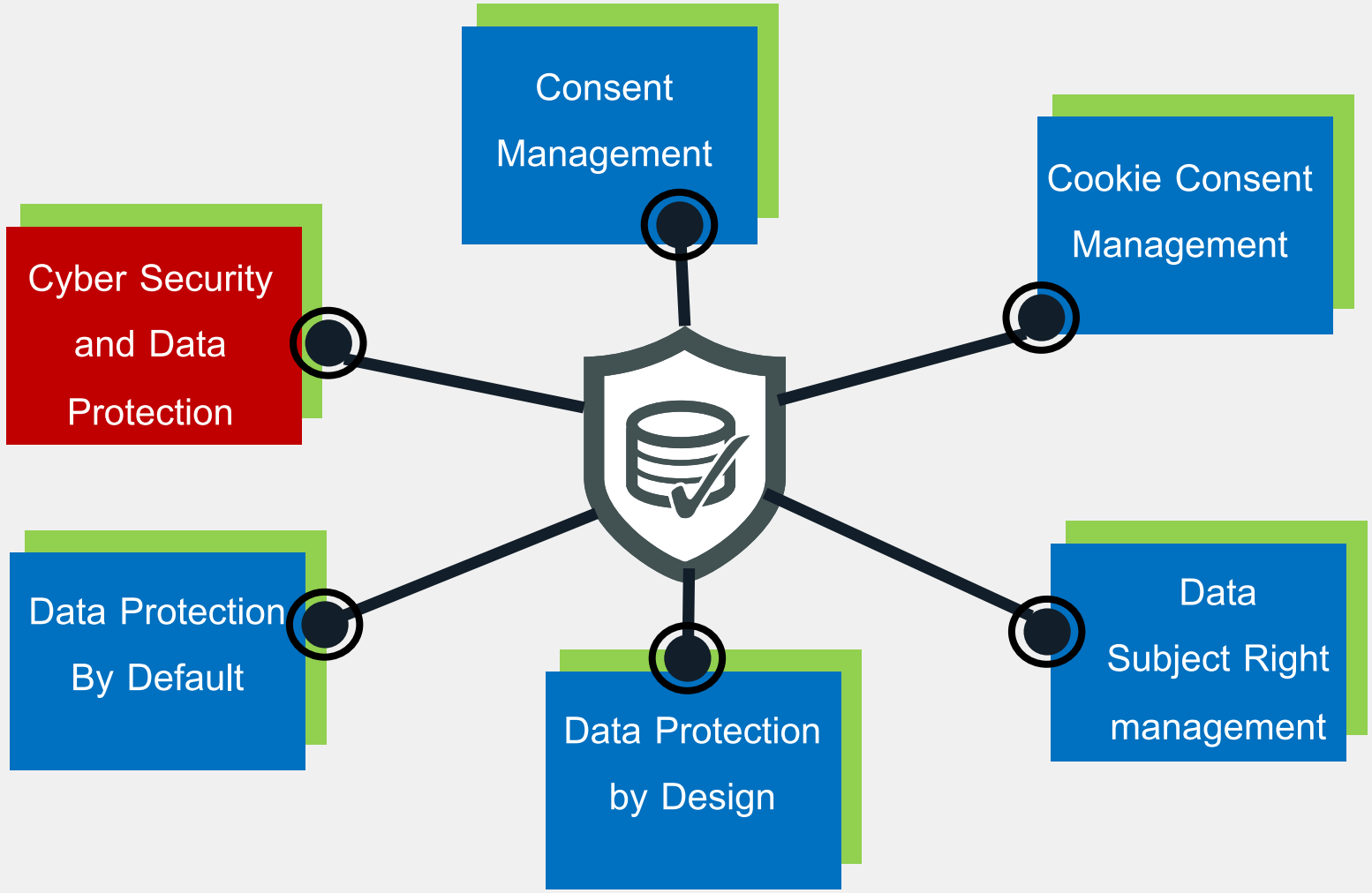


ที่มา Thailand Data Protection Guideline 3.1, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

General Data Protection Regulation (GDPR), Information Commissioner's Office (ICO)

© Fortinet Inc. All Rights Reserved.

เรื่องอื่น ๆ ที่สำคัญ



ที่มา Thailand Data Protection Guideline 3.1, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

General Data Protection Regulation (GDPR), Information Commissioner's Office (ICO)

© Fortinet Inc. All Rights Reserved.

ข้อแนะนำสำหรับผู้บริหาร

ข้อแนะนำสำหรับผู้บริหาร (Guideline for Executive)

1. รู้หน้าที่และความรับผิดชอบของตน
2. สนับสนุนให้มี DPO
3. พิจารณาอนุมัตินโยบายคุ้มครองข้อมูลส่วนบุคคล และนโยบายความเป็นส่วนตัว
4. พิจารณาอนุมัติแผนงานบริหารจัดการการคุ้มครองข้อมูลส่วนบุคคล
5. กำหนดให้องค์กรมีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วน (DPIA)
6. สนับสนุนและจัดให้มีการฝึกอบรม
7. วางกลยุทธ์ในการบริหารจัดการการคุ้มครองข้อมูลส่วนบุคคลทั้งระยะสั้นและยาว
8. กำหนดทิศทางการทำงานของ DPO



© Fortinet Inc. All Rights Reserved.

ข้อแนะนำสำหรับผู้บริหาร (ต่อ)

9. กำหนดทิศทางให้ **DPO** ในการทำการสื่อสารกับสำนักงาน

10. พิจารณาอนุมัติ และสื่อสารนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

11. จัดให้มีผู้รับผิดชอบในการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัย

12. จัดให้มีการตรวจสอบความเข้าใจ

13. จัดให้มีการสื่อสารกับลูกค้า

14. บริหารจัดการความเสี่ยงองค์กรอย่างมีประสิทธิภาพ



© Fortinet Inc. All Rights Reserved.

การประเมินความเสี่ยงและการกำหนดมาตรการควบคุม

กำหนดมาตรการควบคุมตามความเสี่ยง (Risk based Approach)

“การประเมินความเสี่ยงเป็นกิจกรรม
เพื่อให้องค์กรมีมาตรการในการรักษา
ความมั่นคงปลอดภัย”

© Fortinet Inc. All Rights Reserved.

การประเมินความเสี่ยงใน 3 ด้าน



Confidentiality

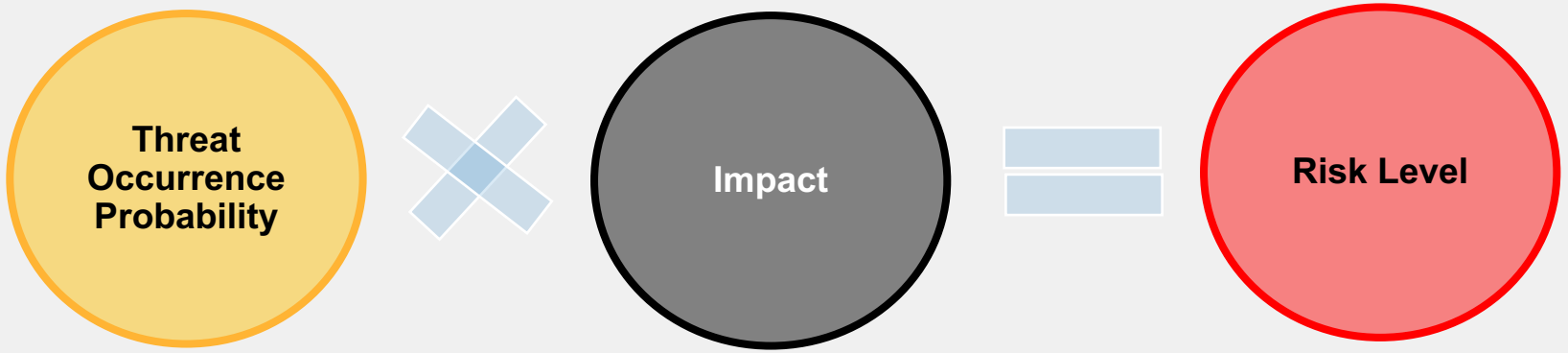
Access, distribution and Publicization

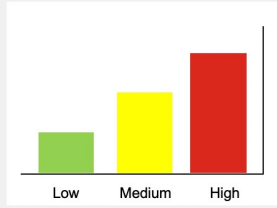
Integrity

Modification, Corruption and Tamping

High Availability

Unplanned loss, Destruction and Unavailability





© Fortinet Inc. All Rights Reserved.

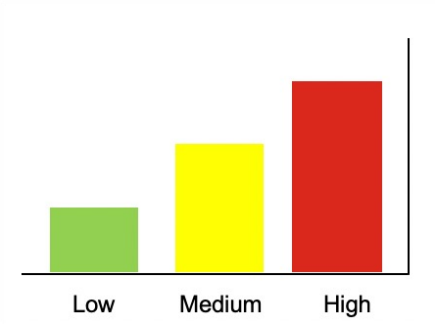
การกำหนดมาตรการควบคุม

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสำหรับข้อมูลส่วนบุคคล

กำหนดมาตรการควบคุมด้านความมั่นคงปลอดภัยที่เหมาะสม

Risk Assessment (Security)

ISO27005, NIST RMF, or ENISA (SME)



Risk level - Low, Medium, High

Risk level - Low, Medium, High

Organization Security Measures

มาตรการควบคุมด้านความมั่นคงปลอดภัยที่เกี่ยวกับการจัดการองค์กร

Measures for Low Risk, Medium Risk or High Risk

Technical Security Measures

มาตรการควบคุมด้านความมั่นคงปลอดภัยเชิงเทคนิค

Measures for Low Risk, Medium Risk or High Risk

© Fortinet Inc. All Rights Reserved.

มาตรการควบคุมด้านความมั่นคงปลอดภัยที่เกี่ยวกับการจัดการองค์กร

1 Security Management

- Policy and Procedure
- Role and Responsibility
- Access Control Policy
- Resource/Asset Management
- Change Management

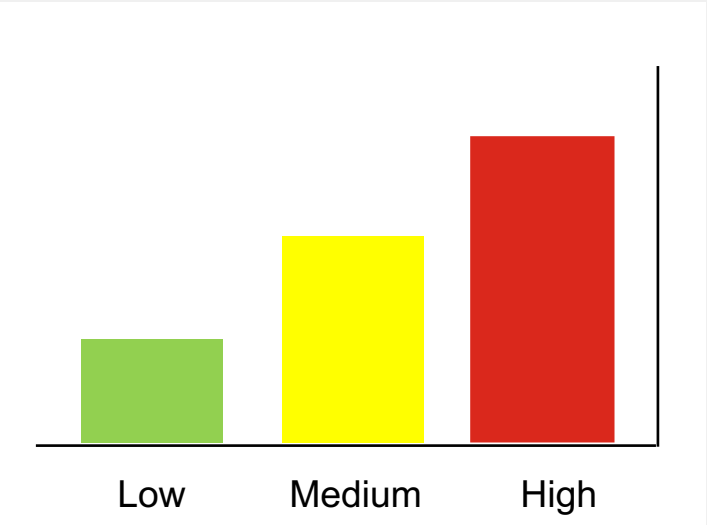
2 Incident Response and Business Continuity

- Incident Handling/ Personal Data Breach
- Bussines Continuity

3 Human Resources

- Confidentiality of personal
- Training

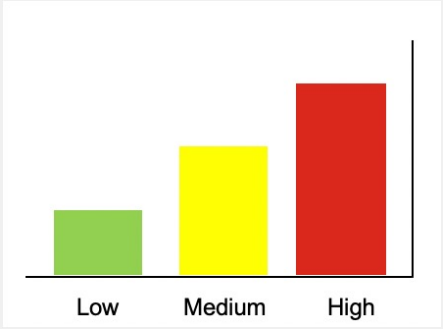
Organization Security Measures



© Fortinet Inc. All Rights Reserved.

มาตรการควบคุมด้านความมั่นคงปลอดภัยเชิงเทคนิค

1. Access Control and Authentication
2. Logging and Monitoring
3. Security of data at rest
   - Server/Database Security
   - Workstation Security
4. Network/Communication security
5. Back-ups
6. Mobile/Portable devices
7. Application Lifecycle Security
8. Data Deletion/Disposal
9. Physical Security



Technical Security Measures

© Fortinet Inc. All Rights Reserved.

ตัวอย่างการมาตรการควบคุมด้านความมั่นคงปลอดภัยเชิงเทคนิค

ตัวอย่างการกำหนดมาตรการควบคุมความปลอดภัยเชิงเทคนิค ในเรื่องการควบคุมการเข้าถึงและยืนยันตัวตน (Assess Control and Authentication)

K.1	ควรนำระบบควบคุมการเข้าถึงมาประยุกต์ใช้เพื่อควบคุมผู้ใช้ในการเข้าถึงระบบสารสนเทศ ระบบควรรองรับการสร้าง อนุมัติ ทบทวน และลบบัญชีผู้ใช้งาน	สีเขียว
K.2	ควรหลีกเลี่ยงการใช้งานบัญชีผู้ใช้ที่เป็นค่าตั้งต้นของระบบ หากมีความจำเป็นต้องใช้งาน ควรตรวจสอบให้มั่นใจว่าผู้ใช้งานที่ใช้บัญชีผู้ใช้ดังกล่าวมีหน้าที่และความรับผิดชอบที่เหมือนกัน	
K.3	ควรมีกลไกในการยืนยันตัวตนในการเข้าใช้ระบบสารสนเทศ (ซึ่งสอดคล้องกับนโยบายการควบคุมการเข้าถึง) โดยอย่างน้อยควรมีการใช้ ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยควรมีการกำหนดระดับของความซับซ้อนของรหัสผ่าน	
K.4	ระบบควบคุมการเข้าถึงควรตรวจสอบ และควบคุมไม่ให้ผู้ใช้ใช้รหัสผ่านที่ไม่สอดคล้องกับระดับของความซับซ้อนที่กำหนด	
K.5	ควรกำหนดนโยบายในการตั้งรหัสผ่าน และกำหนดไว้ในเอกสารอย่างชัดเจน รายละเอียดของนโยบายควรประกอบด้วย ความยาวของรหัสผ่าน ความซับซ้อนของรหัสผ่าน อายุของรหัสผ่านที่ใช้ และการกำหนดจำนวนครั้งของความพยายามในการเข้าสู่ระบบที่ไม่สำเร็จ (Unsuccessful login attempts)	สีเหลือง
K.6	ควรจัดเก็บรหัสผ่านของผู้ใช้งานโดยการแฮช (Hash) โดยใช้ Algorithm ที่ปลอดภัย	
K.7	ควรใช้การยืนยันตัวตนแบบ 2 ปัจจัย (Two-factor authentication) ในการเข้าถึงระบบสารสนเทศที่ประมวลผลข้อมูลส่วนบุคคล ปัจจัยที่ใช้ในการยืนยันตัวตน เช่น รหัสผ่าน โทเคน (Token) และข้อมูลชีวภาพ (Biometrics) เป็นต้น	สีแดง
K.8	ควรมีการยืนยันอุปกรณ์ที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล เพื่อยืนยันว่าการประมวลผลข้อมูลส่วนบุคคลเกิดขึ้นบนทรัพยากรที่กำหนด	
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.9 Access control		

© Fortinet Inc. All Rights Reserved.

ที่มา Thailand Data Protection Guideline 3.1, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

เครื่องมือสำหรับปกป้องข้อมูลที่เกี่ยวข้อง

ข้อแนะนำในการกำหนดเครื่องมือควบคุม

1

Cyber Security (Security)

CSA, NIST, ENISA, ISO27001

Data Protection (Privacy)

PDPA, GDPR, ISO27701

2

People

Technologies

Processes

3

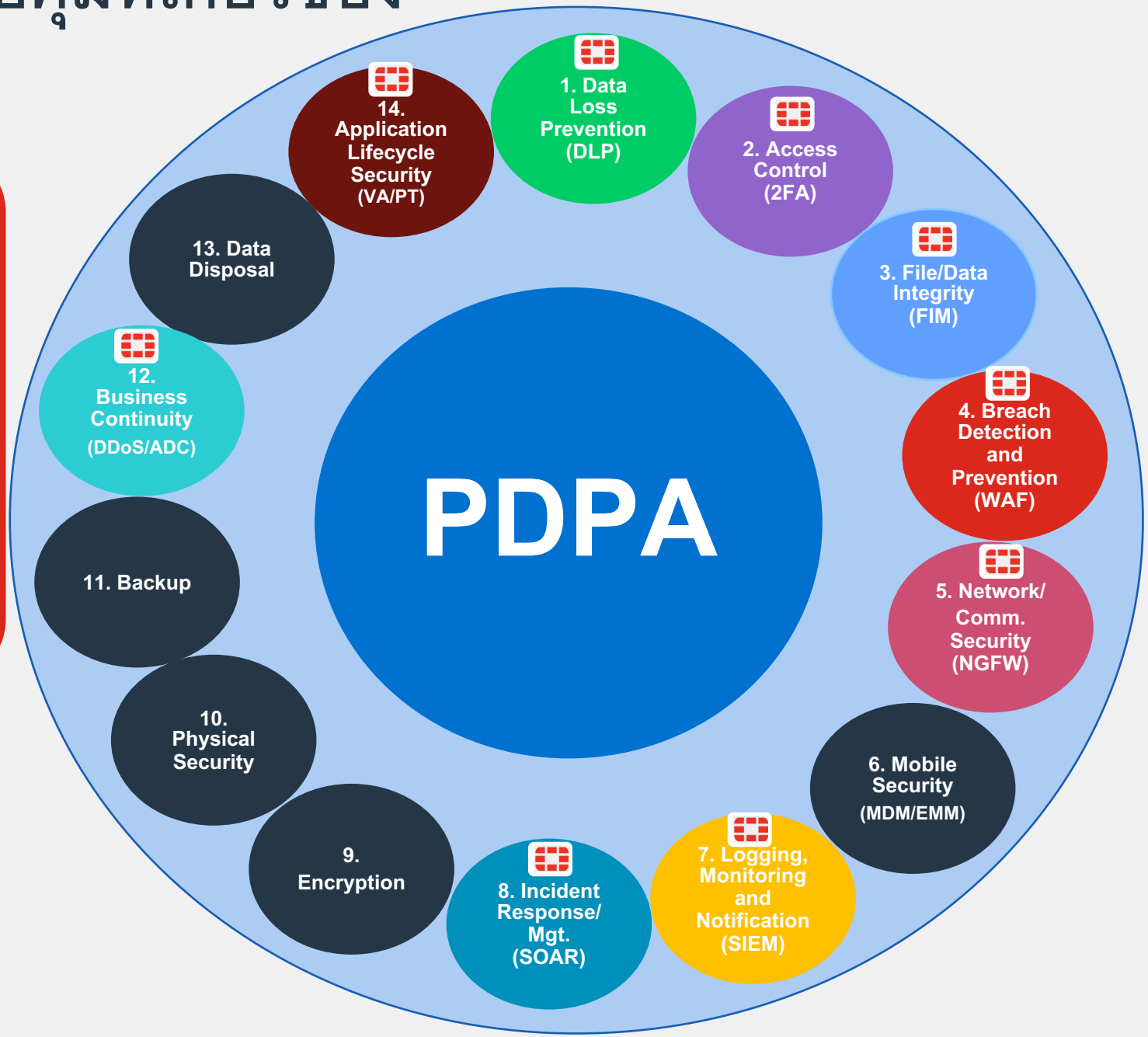
Data Classification

DPIA (Data Protection Impact Assessment)

© Fortinet Inc. All Rights Reserved.

เครื่องมือควบคุมที่เกี่ยวข้อง

...ป้องกันการ
สูญหาย เข้าถึง ใช้
เปลี่ยนแปลง
แก้ไข หรือ
เปิดเผยข้อมูล...



...แจ้งเหตุการ
ละเมิดภายในเจ็ด
สิบสองชั่วโมง
เว้นแต่การละเมิด
ดังกล่าวไม่มีความ
เสี่ยงที่จะมี
ผลกระทบ...



User Awareness and Training

สรุป

สรุป 10 สิ่งที่ควรจดจำ

1. การขอความยินยอม
2. สิทธิของเจ้าของข้อมูล
3. ผู้ควบคุม และ ผู้ประมวลผล
4. ข้อตกลงในการประมวลข้อมูล
5. การทำ **Data Classification**
6. ฐานในการประมวลผลข้อมูล
7. การจัดทำ **DPIA**
8. การส่งข้อมูลไปต่างประเทศ
9. การประเมินความเสี่ยง
10. มาตรการในการปกป้องข้อมูล

ที่มา Thailand Data Protection Guideline 3.1, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

General Data Protection Regulation (GDPR), Information Commissioner's Office (ICO)

© Fortinet Inc. All Rights Reserved.


FORTINET