Infographic แนวปฏิบัติเมื่อตกเป็นเหยื่อถูกแอบอ้าง
รูปภาพบน Facebook ตัดต่อบิดเบือนข้อเท็จจริง

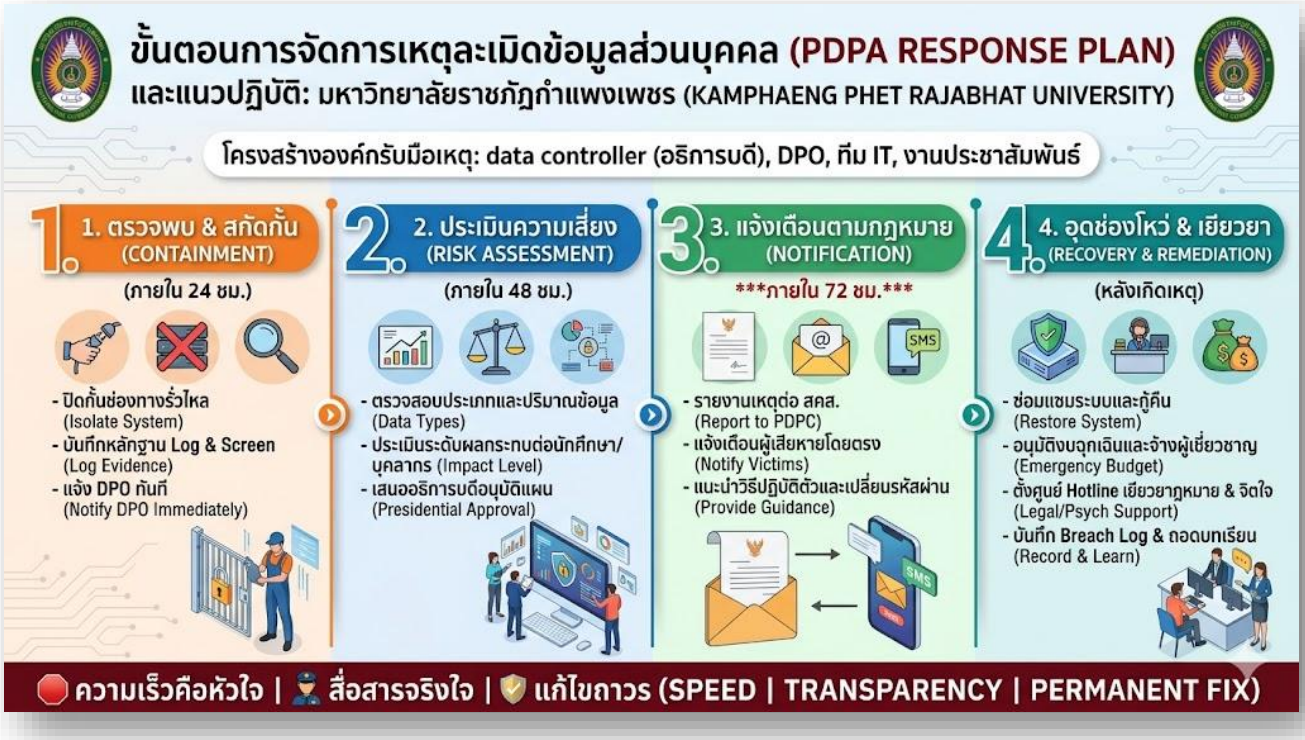
มาตรการแก้ไขปัญหาและแก้ไขสถานการณ์เบื้องต้นในการระงับเหตุการละเมิดข้อมูลส่วนบุคคล

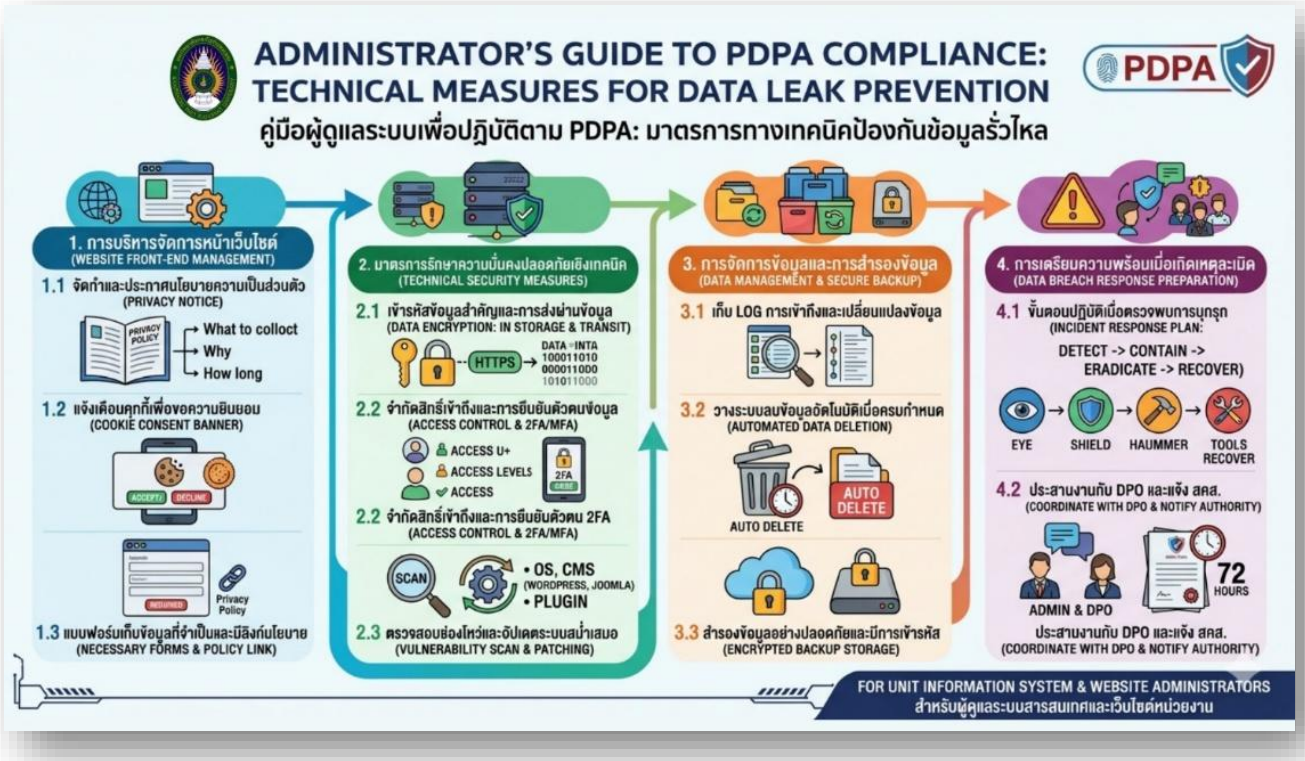

[ด่วนที่สุด]
แนวทางยกระดับความปลอดภัย
Facebook Page หน่วยงาน
เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล
สืบเนื่องจากกรณีการนำภาพบุคคลมาดัดแปลงและบิดเบือน
ข้อเท็จจริงในช่องทาง Comment ของเพจหน่วยงาน
เพื่อเป็นการป้องกันเชิงรุกและรักษามาตรฐานความ
ปลอดภัยสารสนเทศ ขอให้ Admin ทุกหน่วยงานดำเนินการ
ตั้งค่า Facebook Page ดังนี้
1
1. ปิดสิทธิ์โพสต์สาธารณะ
ไม่อนุญาตให้บุคคลภายนอกโพสต์
เนื้อหาบน Timeline ของเพจโดยตรง
2
2. เปิดระบบคัดกรองอัตโนมัติ
ใช้งาน Moderation Assist
เพื่อตั้งค่าซ่อนความเห็นที่มีคำไม่สุภาพ
หรือ Keywords ที่เข้าข่ายบิดเบือน
ข้อมูล/สร้างความเสียหาย
ทั้งนี้ เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลและป้องกันมิให้
พื้นที่ของมหาวิทยาลัยถูกใช้ในทางที่ผิดกฎหมาย


แนวทางยกระดับความมั่นคงปลอดภัยสารสนเทศ
และการสื่อสารผ่านสื่อสังคมออนไลน์ของหน่วยงาน
สืบเนื่องจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เมื่อวันที่ 15 มีนาคม 2569
โดยการบิดเบือนรูปภาพและเผยแพร่ผ่านความคิดเห็นในหน้าเพจ Facebook
1. จำกัดสิทธิ์การโพสต์
• ปิดการอนุญาตให้บุคคลภายนอก
โพสต์บนหน้าเพจโดยตรง
2. ยกระดับการคัดกรอง
• เปิดใช้งาน 'ตัวช่วยการควบคุม' (Moderation Assist)
• ตั้งค่าคัดกรองความคิดเห็น (Comment Filtering)
• ซ่อนข้อความที่มีคำไม่สุภาพหรือคำสำคัญบิดเบือนอัตโนมัติ
อ้างอิง: มติคณะกรรมการบริหารมหาวิทยาลัย ครั้งที่ 4/2569 วันที่ 2 เมษายน 2569


การปิดสิทธิ์โพสต์บนเพจ Facebook ของหน่วยงาน
เพื่อความปลอดภัยและภาพลักษณ์ที่เป็นทางการ
Username
Password
Log in
1. เข้าสู่ระบบ
ด้วยบัญชีผู้ดูแล (Admin)
2. สลับไปเพจหน่วยงาน
เลือกสลับการใช้งานไปยังเพจ
การตั้งค่าและความเป็นส่วนตัว
การตั้งค่า
3. ไปที่การตั้งค่า
คลิกรูปโปรไฟล์ > การตั้งค่าและความเป็นส่วนตัว > การตั้งค่า
ความเป็นส่วนตัว
เพจและการแท็ก
4. เลือกความเป็นส่วนตัว & เพจและการแท็ก
ในเมนูด้านซ้าย เลือก “ความเป็นส่วนตัว” > “เพจและการแท็ก”
ใครสามารถโพสต์บนเพจของคุณได้บ้าง
เฉพาะฉัน
เฉพาะฉัน
5. ตั้งค่าใครสามารถโพสต์ได้
เลือก “เฉพาะฉัน”
6. บันทึกอัตโนมัติ
ระบบจะบันทึกการตั้งค่าให้โดยอัตโนมัติ
จัดการเพจอย่างมืออาชีพ


การตั้งค่าตัวกรองคำหยาบและคำเฉพาะ
เพื่อการควบคุมเนื้อหาและภาพลักษณ์ที่ดี
Username
Password
Log in
1. สลับโปรไฟล์ไปที่หน้าเพจ
เลือกสลับบัญชีเป็นผู้ดูแลเพจ
2. ไปที่การตั้งค่า (Settings)
คลิกรูปโปรไฟล์ > การตั้งค่าและความเป็นส่วนตัว > ความเป็นส่วนตัว
3. เลือกโพสต์สาธารณะ (Public Posts)
ในเมนูด้านซ้าย เลือก “โพสต์สาธารณะ”
4. ตรวจสอบเนื้อหา (Content Moderation)
มองหาและคลิกหัวข้อ “การตรวจสอบเนื้อหา”
5. ซ่อนความคิดเห็น
ซ่อนความคิดเห็นที่มีคำบางคำ
มึ_มึ_ , กู_กู_ , คำไม่สุภาพ , คำด่า
6. บันทึก (Save)
กดปุ่ม “บันทึก” เพื่อสิ้นสุด
จัดการเพจอย่างมืออาชีพ


ขั้นตอนการจัดการเหตุละเมิดข้อมูลส่วนบุคคล (PDPA RESPONSE PLAN)
และแนวปฏิบัติ: มหาวิทยาลัยราชภัฏกำแพงเพชร (KAMPHAENG PHET RAJABHAT UNIVERSITY)
โครงสร้างองค์กรรับมือเหตุ: data controller (อธิการบดี), DPO, ทีม IT, งานประชาสัมพันธ์
1. ตรวจพบ & สกัดกั้น (CONTAINMENT)
(ภายใน 24 ชม.)
- ปิดกั้นช่องทางรั่วไหล (Isolate System)
- บันทึกหลักฐาน Log & Screen (Log Evidence)
- แจ้ง DPO ทันที (Notify DPO Immediately)
2. ประเมินความเสี่ยง (RISK ASSESSMENT)
(ภายใน 48 ชม.)
- ตรวจสอบประเภทและปริมาณข้อมูล (Data Types)
- ประเมินระดับผลกระทบต่อนักศึกษา/บุคลากร (Impact Level)
- เสนออธิการบดีอนุมัติแผน (Presidential Approval)
3. แจ้งเตือนตามกฎหมาย (NOTIFICATION)
ภายใน 72 ชม.
SMS
- รายงานเหตุต่อ สคส. (Report to PDPC)
- แจ้งเตือนผู้เสียหายโดยตรง (Notify Victims)
- แนะนำวิธีปฏิบัติตัวและเปลี่ยนรหัสผ่าน (Provide Guidance)
4. อุดช่องโหว่ & เยียวยา (RECOVERY & REMEDIATION)
(หลังเกิดเหตุ)
- ซ่อมแซมระบบและกู้คืน (Restore System)
- อนุมัติงบฉุกเฉินและจ้างผู้เชี่ยวชาญ (Emergency Budget)
- ตั้งศูนย์ Hotline เยียวยากฎหมาย & จิตใจ (Legal/Psych Support)
- บันทึก Breach Log & ถอดบทเรียน (Record & Learn)
ความเร็วคือหัวใจ | สื่อสารจริงใจ | แก้ไขถาวร (SPEED | TRANSPARENCY | PERMANENT FIX)


ADMINISTRATOR'S GUIDE TO PDPA COMPLIANCE:
TECHNICAL MEASURES FOR DATA LEAK PREVENTION
PDPA
คู่มือผู้ดูแลระบบเพื่อปฏิบัติตาม PDPA: มาตรการทางเทคนิคป้องกันข้อมูลรั่วไหล
1. การบริหารจัดการหน้าเว็บไซต์
(WEBSITE FRONT-END MANAGEMENT)
1.1 จัดทำและประกาศนโยบายความเป็นส่วนตัว
(PRIVACY NOTICE)
What to collect
Why
How long
1.2 แจ้งเตือนคุกกี้เพื่อขอความยินยอม
(COOKIE CONSENT BANNER)
ACCEPT
DECLINE
1.3 แบบฟอร์มเก็บข้อมูลที่จำเป็นและมีลิงก์นโยบาย
(NECESSARY FORMS & POLICY LINK)
REQUIRED
Privacy Policy
2. มาตรการรักษาความมั่นคงปลอดภัยเชิงเทคนิค
(TECHNICAL SECURITY MEASURES)
2.1 เข้ารหัสข้อมูลสำคัญและการส่งผ่านข้อมูล
(DATA ENCRYPTION: IN STORAGE & TRANSIT)
HTTPS
DATA→INTA
100011010
000011000
1010111000
2.2 จำกัดสิทธิ์เข้าถึงและการยืนยันตัวตนข้อมูล
(ACCESS CONTROL & 2FA/MFA)
ACCESS U+
ACCESS LEVELS
ACCESS
2FA
2.2 จำกัดสิทธิ์เข้าถึงและการยืนยันตัวตน 2FA
(ACCESS CONTROL & 2FA/MFA)
SCAN
• OS, CMS
(WORDPRESS, JOOMLA)
• PLUGIN
2.3 ตรวจสอบช่องโหว่และอัปเดตระบบสม่ำเสมอ
(VULNERABILITY SCAN & PATCHING)
3. การจัดการข้อมูลและการสำรองข้อมูล
(DATA MANAGEMENT & SECURE BACKUP)
3.1 เก็บ LOG การเข้าถึงและเปลี่ยนแปลงข้อมูล
3.2 วางระบบลบข้อมูลอัตโนมัติเมื่อครบกำหนด
(AUTOMATED DATA DELETION)
AUTO DELETE
AUTO DELETE
3.3 สำรองข้อมูลอย่างปลอดภัยและมีการเข้ารหัส
(ENCRYPTED BACKUP STORAGE)
4. การเตรียมความพร้อมเมื่อเกิดเหตุละเมิด
(DATA BREACH RESPONSE PREPARATION)
4.1 ขั้นตอนปฏิบัติเมื่อตรวจพบการบุกรุก
(INCIDENT RESPONSE PLAN:
DETECT -> CONTAIN ->
ERADICATE -> RECOVER)
EYE
SHIELD
HAUMMER
TOOLS
RECOVER
4.2 ประสานงานกับ DPO และแจ้ง สคส.
(COORDINATE WITH DPO & NOTIFY AUTHORITY)
ADMIN & DPO
72
HOURS
ประสานงานกับ DPO และแจ้ง สคส.
(COORDINATE WITH DPO & NOTIFY AUTHORITY)
FOR UNIT INFORMATION SYSTEM & WEBSITE ADMINISTRATORS
สำหรับผู้ดูแลระบบสารสนเทศและเว็บไซต์หน่วยงาน


"มาตรการด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (สำหรับผู้ปฏิบัติงาน)
อ้างอิงตามแผนดำเนินงานรอบ 6 เดือนของมหาวิทยาลัย
เพื่อยกระดับความคืบหน้าของการจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล
1. มาตรการด้านการบริหารจัดการ
(Administrative Measures)
CIO &
DPO
การลงนามรักษาความลับ
Confidentiality
ผู้ปฏิบัติงานที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลทุกคน ต้องลงนามในสัญญารักษาความลับ (Non-Disclosure Agreement: NDA) เพื่อป้องกันการนำข้อมูลไปใช้ผิดวัตถุประสงค์
การกำหนดหน้าที่และสิทธิเข้าถึง
Role-based Access
เจ้าถึงข้อมูลตามความจำเป็นของงานภาคหน้าที่ โดยมีโครงสร้างการทำงานดูแลห่านผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
การตรวจสอบสถานะความเสี่ยง
Risk Review/KM
มีการจัดประชุมเพื่อทบทวนแผนจัดการความรู้ (KM) และวิเคราะห์ความเสี่ยงที่มีโอกาสทำให้ข้อมูลรั่วไหลอย่างอย่างสม่ำเสมอ
2. มาตรการเชิงเทคนิคและระบบสารสนเทศ
(Technical Measures)
การแจ้งวัตถุประสงค์และขอความยินยอม
กระบบสารสนเทศต้องมีแบบฟอร์มการจัดเก็บข้อมูลที่ชัดเจน และต้องมีการกล่าววัตถุประสงค์ (Privacy Notice) รวมถึงการขอความยินยอม (Consent) ก่อนการเก็บ ใช้ หรือเปิดเผยข้อมูล
ความปลอดภัยของสื่อสังคมออนไลน์
สำหรับแอดมิน Facebook Page ของหน่วยงาน ต้องปฏิบัติตามมาตรการเชิงเทคนิคเพื่อป้องกันการถูกโจมตี หรือการโพสต์รูปภาพ/ข้อมูลที่อาจเป็นการเผยแพร่ข้อมูลส่วนบุคคล
การใช้เทคโนโลยีป้องกัน
Preventive Tech
สนับสนุนการใช้มาตรการเชิงเทคนิค (เช่น การคัดกรอง IP หรือระบบตรวจสอบสิทธิ์) เพื่อลดความเสี่ยงจากการคุกคามทางไซเบอร์ที่อาจส่งผลต่อข้อมูลของบุคลากรและนักศึกษา
PDPA
3. มาตรการด้านบุคลากรและการสร้างความตระหนัก
(Human Measures)
การเข้ารับการอบรม
ผู้ปฏิบัติงาน (ลายสนับสนุนและสายวิชาการ) ต้องเข้ารับการอบรมด้านความปลอดภัยข้อมูลส่วนบุคคลและ: 'วัคซีนไซเบอร์' ตามรอบที่มหาวิทยาลัยกำหนด
โดยมีเป้าหมายไม่ต่ำกว่า
ร้อยละ 60
ของบุคลากรทั้งหมด
การแลกเปลี่ยนเรียนรู้ (KM)
เข้าร่วมกิจกรรมแลกเปลี่ยนแนวทางการบริหารจัดการข้อมูลส่วนบุคคล (Case Study) เพื่อปรับปรุงกระบวนการทำงานให้ลอดคล้องกับ PDPA
4. มาตรการการตอบสนองและรายงานเหตุละเมิด
(Incident Response)
ช่องทางการร้องเรียน
ผู้ปฏิบัติงานต้องทราบช่องทางการแจ้งเหตุหรือช่องทางการร้องเรียน กรณีพบเห็นเหตุการณ์ที่อาจเป็นการละเมิดข้อมูลส่วนบุคคล
แนวปฏิบัติเมื่อเกิดเหตุ
หากพบเหตุละเมิด ต้องดำเนินการตาม 'หมวดปฏิบัติการรับมือเหตุละเมิด' และมาตรการแก้ไขสถานการณ์เบื้องต้นเพื่อระงับเหตุทันที


แนวปฏิบัติที่ดีที่สุดสำหรับการจัดการเหตุการณ์ด้านความปลอดภัยทางไซเบอร์
เพื่อสร้างความพร้อมและลดผลกระทบต่อองค์กร
NEWS
NEWS
Chain of Custody
POLICE
POLICE
1 ทำให้แผนรับมือเหตุการณ์ฉุกเฉิน (IRP) เป็นเอกสารที่มีการพัฒนาอย่างต่อเนื่อง
ทบทวนและปรับปรุงอย่างสม่ำเสมอ (อย่างน้อยปีละครั้ง)
หลังจากมีการเปลี่ยนแปลงที่สำคัญ
อิงจากบทเรียนการฝึกซ้อมและเหตุการณ์จริง
2 สื่อสารอย่างชัดเจน
ทันท่วงทีและชัดเจน
สื่อสารทั้งภายในและภายนอก (ผู้ได้รับผลกระทบ, หน่วยงาน, สาธารณชน)
กำหนดช่องทางและระเบียบปฏิบัติก่อนวิกฤต
3 ใช้ระบบอัตโนมัติในส่วนที่ทำได้
งานตรวจจับและการควบคุมที่ซ้ำซาก
เร่งความเร็วในการตอบสนอง
ใช้คู่มือและเครื่องมือการทำงานอัตโนมัติ (เช่น SOAR)
4 การมีส่วนร่วมของที่ปรึกษาด้านกฎหมาย
ปรึกษาตั้งแต่เนิ่นๆ ในการวางแผนและระหว่างเหตุการณ์
โดยเฉพาะเหตุการณ์รั่วไหลของข้อมูล
ดูแลเรื่องการควบคุม, การแจ้งเตือน, และการจัดการหลักฐาน
5 รักษาหลักฐาน
รักษาความสมบูรณ์ของหลักฐาน
เพื่อวิเคราะห์สาเหตุและทางกฎหมาย
ฝึกอบรมทีมงานในการเก็บรวบรวมที่ถูกต้อง
Chain of Custody


เทคนิคการจัดการ LOG FILES ให้สอดคล้องกับ PDPA
รักษาสมดุลระหว่าง “เก็บหลักฐาน” และ “คุ้มครองความเป็นส่วนตัว”
DATA MINIMIZATION
(เก็บเท่าที่จำเป็น)
ตัดข้อมูลที่ไม่เกี่ยวออก
(CUT IRRELEVANT DATA)
เล็กเก็บเฉพาะ METADATA
ใคร ทำอะไร เมื่อไหร่ ที่ไหน
(WHO, WHAT, WHEN, WHERE)
PSEUDONYMIZATION
(การใช้นามแฝง)
Name
Employee ID
IP address hashing
ใช้ ID แทนชื่อ
USE ID INSTEAD OF NAME)
HASHING IP ADDRESS
DATA MASKING
(การปกปิดข้อมูล)
081-XXX-XXXX
user_***@email.com
เซ็นเซอร์ข้อมูลอ่อนไหว
(SENSOR SENSITIVE DATA)
กรองรูปแบบ
Credit Card ออก
ACCESS CONTROL
(การจำกัดสิทธิ์)
Principle of
Least Privilege
ให้สิทธิ์เฉพาะผู้จำเป็น
(ONLY ESSENTIAL STAFF)
แยกคนมีสิทธิ์ดู Log
กับแก้ไขระบบ
(SEPARATE VIEWER &
SYSTEM ADMIN ROLES)
RETENTION POLICY
(กำหนดอายุการเก็บ)
90
days
Auto-
ตั้งระบบลบ Log ทันที
(AUTO-DELETION)
Log รอการลบต้องเข้ารหัส
(ENCRYPTION AT REST)
จุดที่มักพลาด
(COMMON PITFALLS)
GUG FILE LOGS
และ 'คุ้มครองความเป็นส่วนตัว'
DEBUG MODE
บันทึกข้อมูลทุกอย่าง
ERROR LOGS
เผลอพ่นข้อมูลลูกค้าออกมา


UNIVERSITY
DATA SECURITY
GUIDELINES
ข้อควรปฏิบัติและข้อห้าม (Do’s & Don’ts)
ในการจัดการข้อมูลส่วนบุคคลของมหาวิทยาลัย
UNIVERSITY DATA
SECURITY GUIDELINES
ข้อควรปฏิบัติ (DO’S)
1
ใช้ระบบขององค์กรเท่านั้นในการทีข้อมูล
USE UNIVERSITY SYSTEMS
ONLY FOR DATA
2
Checked
ตรวจสอบสิทธิ์ก่อนเปิดเผยข้อมูล
VERIFY PERMISSIONS
BEFORE DISCLOSING
3
SECURE
เก็บข้อมูลอย่างปลอดภัย
STORE DATA SECURELY
4
HELP DESK
รายงานเหตุผิดปกติทันที
REPORT INCIDENTS IMMEDIATELY
ข้อห้าม (DON’TS)
1
LINE
ใช้ LINE / Facebook
ส่วนตัวส่งข้อมูล
DO NOT USE PERSONAL
LINE / FACEBOOK
2
NO TALK
พูดถึงข้อมูลกับบุคคลภายนอก
DO NOT DISCUSS CONFIDENTIAL
INFO WITH OUTSIDERS
3
NOT SECURE
เก็บเอกสารสำคัญไว้นอกระบบ
DO NOT STORE IMPORTANT DOCS OUTSIDE SYSTEM
SECURITY IS EVERYONE’S RESPONSIBILITY
MARCORN UNIVERSITY