Third Party IT Practical Guideline

Version 1.1

CP ALL Public Company Limited

313 CP Tower Building, fl. 24, Silom Rd., Silom, Bangrak, Bangkok 10500

Website: www.cpall.co.th

Table of Contents

Page

1. Objective

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นคู่มือสำหรับผู้ให้บริการภายนอก เพื่อให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศและระบบบริหารจัดการข้อมูลส่วนบุคคล (ISMS/PIMS) สามารถดำเนินการต้องปฏิบัติงานได้อย่างเหมาะสม

This document guides service providers to comply with Information Security Management System and Privacy Information Management Systems (ISMS/PIMS) that must operate appropriately.

2. Scope

คู่มือปฏิบัติงานฉบับนี้ครอบคลุมถึงการดำเนินการงานของผู้ให้บริการภายนอก

The operating manual covers external service providers operation.

3. Roles and Responsibilities

Role	Responsibility
ผู้ให้บริการภายนอก (Service provider)	● รับทราบและปฏิบัติงานตามคู่มือฉบับนี้ ● ร่วมทำการประเมินความเสี่ยงในการดำเนินงาน ● Acknowledge and operate following operating manual. ● Participate in operation risk assessments.
ผู้ประสานงานโครงการ (Project coordinator)	● ประสานงานกับผู้ให้บริการภายนอก ● แจ้งผู้ให้บริการภายนอกให้ทราบถึงคู่มือปฏิบัติงานฉบับนี้ ● Coordinate with external service providers. ● Notify external service providers about this operating manual.
เจ้าของข้อมูล/เจ้าของระบบ (Data Owner/System Owner)	● กำหนดสิทธิในการเข้าถึงข้อมูลหรือระบบสำหรับผู้ให้บริหารภายนอก ● ทำการประเมินความเสี่ยงในการดำเนินงานของผู้ให้บริการภายนอก ● ตรวจสอบดูแลการดำเนินงานของผู้ให้บริการภายนอก ● Define access rights to information and systems for external administrators. ● Perform operation risk assessments of outsourced service providers. ● Supervise the operations of external service providers.

4. References

-

5. Definition

Vocabulary	Meaning
หน่วยงานภายนอก/ ผู้ให้บริการภายนอก/ บุคคลภายนอก (Service provider/Third party)	บริษัทคู่ค้า ผู้รับจ้างปฏิบัติงานให้กับบริษัทฯ ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่าง ๆ ผู้ให้บริการต่าง ๆ และ ที่ปรึกษา ผู้ให้บริการภายนอก ที่ใช้งานระบบสารสนเทศของบริษัท ได้เป็นครั้งคราว หรือตามสัญญา Business Partner, Outsource, Supplier, Service Provider, Consultant, and External service providers who use the company's information system from time to time or according to contract.
บริษัทผู้รับบริการ (Service provider)	บริษัท ซีพี ออลล์ จำกัด (มหาชน) และ/หรือ บริษัทย่อยที่ดำเนินการว่าจ้างกับหน่วยงานภายนอก CP All Public Company Limited and/or subsidiaries that engage with external agencies.
Removable Media	อุปกรณ์ที่ใช้เก็บข้อมูลที่สามารถเคลื่อนย้ายได้ เช่น Tape, DVD, Thumb drive, Flash drive, Hard disk Portable storage devices such as Tape, DVD, Thumb drive, Flash drive, and Hard disk.
Mobile Device	อุปกรณ์ที่สามารถประมวลผลและสามารถเคลื่อนย้ายได้ เช่น Smartphone, Tablet, Devices that can be processed and can be moved such as Smartphone and Tablet.
Notebook	เครื่องคอมพิวเตอร์ที่สามารถพกพาได้ Portable computer

6. Guidelines

หน่วยงานภายนอกจะต้องปฏิบัติเพื่อให้สามารถรักษาความมั่นคงปลอดภัยสารสนเทศได้ทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability) รวมทั้งดูแลรักษาข้อมูลส่วนบุคคลให้เป็นตามที่กำหนด

Third party must comply to maintain information security in all 3 aspects, including Confidentiality, Integrity, Availability, and sustaining personal data as required.

6.1 Legal practice guidelines and company policy

- ให้ปฏิบัติตามกฎหมายที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและระบบบริหารจัดการข้อมูลส่วนบุคคลทุกข้อกำหนด
- ต้องยอมรับการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศและระบบบริหารจัดการข้อมูลส่วนบุคคลที่บริษัท ซีพี ออลล์ จำกัด (มหาชน) และบริษัทย่อยที่กำหนด

- Comply with all laws related to Information Security Management System and Privacy Information Management Systems.
- Accept the information security and privacy security control set by CP All Public Company Limited and its subsidiaries.

6.2 Teleworking policy

- ผู้ใช้งานจะต้องขออนุมัติจากผู้ประสานของโครงการก่อนเข้ามาใช้งาน Remote Access เข้าสู่ระบบสารสนเทศ ผู้ให้บริการภายนอกจะต้องระบุวัตถุประสงค์ วิธีการเข้าถึง และขอบข่ายของการเข้าถึงที่แน่ชัดต่อผู้ประสาน และจะต้องทำการอนุมัติให้เป็นรายครั้ง หรือเป็นช่วงระยะเวลาจำกัดแล้วแต่กรณีและความจำเป็น
- การเชื่อมต่อระบบจากภายนอกบริษัท จะต้องมีการดำเนินการขออนุมัติและเชื่อมต่อผ่านช่องทางที่บริษัทกำหนดให้เท่านั้น
- สิทธิในการใช้งาน Remote Access เพื่อปฏิบัติงานชั่วคราวเป็นสิทธิที่บริษัทจะให้เฉพาะผู้ให้บริการภายนอก เป็นการชั่วคราวเท่านั้น ไม่สามารถถ่ายโอนกันได้
- บริษัทมีสิทธิเรียกร้องค่าเสียหายจากผู้ให้บริการภายนอก หากระบบคอมพิวเตอร์ของบริษัทได้รับความเสียหาย จากการติดไวรัส หรือ Malware คอมพิวเตอร์ เนื่องจากการใช้งาน Remote Access ของผู้ให้บริการภายนอก
- Users must request approval from the project coordinator before using remote access to the information system. External service providers must specify how to access the coordinators and defined access, which should be approved on a case-by-case basis or for a limited time, depending on each case and necessity.
- System connection from outside the company, approvals must be processed and connected through the channels specified by the company only.
- The company grants the right to use remote access for temporary work only to external service providers, which cannot be transferable.
- The company has the right to claim damages from the external service provider. If the company's computer system is damaged from a computer virus or malware infection due to remote access from external service providers.

6.3 Computing device and mobile device usage supervision

- มีการเก็บสำรองข้อมูลที่เกี่ยวกับผู้รับบริการ
- มีการติดตั้งโปรแกรมป้องกันไวรัส (Anti-virus) ที่ทันสมัย
- มีการใช้ Software Licenses
- มีมาตรการในการป้องกันอุปกรณ์ที่มีข้อมูลของผู้รับบริการมิให้ถูกโจรกรรมได้ง่าย

- เครื่องคอมพิวเตอร์จะต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง โดยทำการตั้งเวลาพักหน้าจอ (Screen Saver) หากไม่ใช้งานเกินกว่า 15 นาที
- Backup of data related to service users is provided.
- Up-to-date anti-virus program is installed.
- Use of software licenses
- Measures are in place to protect devices containing customer data from being stolen.
- The computer screen must be locked every time and must verify identity before using by setting Screen Saver if the computer is not in use for more than 15 minutes.

6.4 Guidelines and responsibilities towards the assets used by the service recipient company

- การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of electronic mail) การส่งข้อมูลส่วนบุคคลต้องมีการเข้ารหัส
- เอกสารที่เกี่ยวข้องกับข้อมูลส่วนบุคคลให้ปฏิบัติตามผู้ประสานงานโครงการแจ้งไว้อย่างเคร่งครัด และต้องมีการใช้ Hardcopy น้อยที่สุดเท่าที่จำเป็น
- ห้ามมิให้เปิดเผยข้อมูลสำหรับการพิสูจน์ตัวตน หรือที่เรียกว่า รหัสผ่านของระบบบริษัท (รวมถึงสิ่งที่ใช้ในการพิสูจน์ตัวตนอื่น ๆ เช่น ฮาร์ดโทเคน, ซอฟต์โทเคน, รหัส OTP) ให้บุคคลอื่นโดยเด็ดขาด
- ผู้ปฏิบัติงานต้องป้องกันดูแลรักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลของบริษัทผู้รับบริการ
- Use of electronic mail for transmission of personal data must be encrypted.
- The project coordinator must strictly follow documents related to personal data with less hardcopy as necessary.
- Disclosing information for authentication purposes is strictly prohibited, also known as company system password (including any other authentication such as hard tokens, soft tokens, OTPs), to any other person.
- Operators must protect and maintain client company information confidentiality, accuracy, and availability.

6.5 Information classification policy

- ให้ปฏิบัติตามชั้นความลับที่ผู้ประสานงานโครงการกำหนด
- Follow the confidentiality specified by the project coordinator.

6.6 Media handling policy

- การจัดเก็บไฟล์ที่มีข้อมูลส่วนบุคคลและข้อมูลที่สำคัญบน Media ทุกชนิด ต้องมีการเข้ารหัสไฟล์
- การจัดเก็บ หรือส่งข้อมูลทาง Removable Media ควรใช้อุปกรณ์ที่สามารถปิดล็อคได้หรือเป็นอุปกรณ์มีการเข้ารหัสแบบ Full-disk Encryption (FDE)

- เมื่อต้องการทำลายข้อมูล ต้องมีการลบข้อมูลแบบไม่สามารถกู้คืนได้ (Secure delete)
- ต้องมีการบันทึกรับเข้าและส่งออกสื่อบันทึกข้อมูลเฉพาะที่มีข้อมูลส่วนบุคคลและข้อมูลที่สำคัญ รวมถึงประเภทสื่อบันทึกข้อมูล ผู้ส่ง/ผู้รับที่ได้รับอนุญาต วันที่ เวลา และจำนวนสื่อบันทึกข้อมูล
- Storing files containing personal and sensitive data on all media must be encrypted.
- Storage or transferring should perform removable media with a lockable device or Full-disk Encryption (FDE) device.
- Destroying data is needed data deletion that cannot be recovered (Secure delete).
- Incoming and outgoing media containing personal and sensitive data must be recorded, including the type of storage media, authorized sender/recipient, date, time, and the number of storage media.

6.7 Information system access control policy

- **กรณีที่ผู้ให้บริการภายนอกต้องการเข้าถึงทรัพย์สินสารสนเทศของบริษัทผู้รับบริการ**
  - ต้องขออนุมัติการเข้าถึงทรัพย์สินสารสนเทศ ผ่านทางผู้ประสานงานโครงการ เพื่อให้พิจารณาอนุมัติเป็นครั้ง ๆ ไป
  - กรณีที่มีการเปลี่ยนแปลงผู้เข้าถึงทรัพย์สินสารสนเทศจะต้องแจ้งขอเปลี่ยนแปลง หรือยกเลิกสิทธิทันที
  - ต้องมีการทบทวนสิทธิผู้เข้าถึงระบบอย่างสม่ำเสมอ
  - ห้ามใช้ User ID ร่วมกัน
- **กรณีที่ผู้ให้บริการภายนอกเป็นผู้ดูแลระบบให้กับผู้รับบริการ หรือมีการนำข้อมูลของบริษัทผู้รับบริการไปใช้**
  - มีการกำหนดกฎเกณฑ์ในการเข้าถึง ใช้ แก้ไข ข้อมูล ตามหน้าที่ของผู้ใช้งาน (Role Base Authorization)
  - มีกระบวนการลงทะเบียน และถอนสิทธิผู้เข้าถึงระบบงานตามหน้าที่ เพื่อให้สามารถตรวจสอบได้
  - มีการทบทวนสิทธิการเข้าถึงอย่างน้อยปีละ 1 ครั้ง (ส่งหลักฐานการทบทวน)
  - มีการป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงในเครือข่ายภายในขององค์กร
  - การบริหารจัดการรหัสผ่าน
    - มีการกำหนดกฎเกณฑ์ในการตั้งรหัสผ่านให้คาดเดาได้ยาก
    - รหัสผ่านต้องมีการเก็บรักษาเป็นความลับไม่ให้ผู้อื่นล่วงรู้
    - มีการกำหนดรอบระยะเวลาในการเปลี่ยนรหัสผ่าน
    - ห้ามใช้ User ID ร่วมกัน
- **In case the service provider wants to access information assets of the service recipient company.**
  - Must obtain approval for access to information assets through the project coordinator from time to time.

- In case there is any change, the person accessing the information asset must request a change or cancel the right immediately.
- System access rights must be regularly reviewed.
- Do not share User IDs.

- **In case the service provider is an administrator for the service recipient or the information of the service recipient company is used.**
  - There are rules for accessing, using, and editing information according to the user's duties (Role Base Authorization).
  - There is a registration process and withdrawal of the right of access to the system according to their verification duties.
  - Access rights are reviewed at least once a year (submit proof of review).
  - Unauthorized persons are prevented from accessing the internal network of the organization.
  - Password Management
    - Setting passwords with hard encryption.
    - The password must be kept confidential from others.
    - There is a period to change the password.
    - Do not share the User ID

6.8 Physical and environmental security

- **กรณีที่ต้องเข้าพื้นที่ของบริษัทผู้รับบริการ**
  - ต้องขออนุมัติการเข้าถึงทรัพย์สินสารสนเทศ ผ่านทางผู้ประสานงานโครงการ เพื่อให้พิจารณาอนุมัติเป็นครั้ง ๆ ไป
  - ปฏิบัติตามกฎระเบียบการเข้าออกพื้นที่อย่างเคร่งครัด

- **กรณีที่ผู้ให้บริการภายนอกเป็นผู้ดูแลระบบให้กับผู้รับบริการ หรือมีการนำข้อมูลของบริษัทผู้รับบริการไปใช้**
  - มีการป้องกันผู้ที่ไม่ได้รับอนุญาตเข้าออกพื้นที่ปฏิบัติงานที่มีข้อมูลของผู้รับบริการ

- **กรณีที่ให้บริการเช่าพื้นที่ Data center หรือให้เช่าพื้นที่วาง Server**
  - มีมาตรการควบคุมการเข้าออกพื้นที่สำคัญ (Server Room)
  - มีการขออนุญาตเข้าออกพื้นที่ทำงาน
  - มีการบันทึกและตรวจสอบ Log การเข้าถึงพื้นที่
  - มีการติดตั้ง CCTV
  - มีการตรวจการตั้งเวลามาตรฐานสากล (Clock Synchronization)

- มีการจัดตั้งและป้องกันอุปกรณ์ปฏิบัติงานอย่างปลอดภัย (Equipment siting and protection) (น้ำ ไฟ แอร์)
- มีมาตรการตรวจสอบและบำรุงรักษาอุปกรณ์สนับสนุน (เช่น ระบบไฟฟ้า แอร์ เน็ตเวิร์ค เป็นต้น)

- **In case of having to enter the area of the service recipient company**
  - Must obtain approval for access to information assets through the project coordinator for approval from time to time.
  - Strictly follow the rules for entering and exiting the area.
- **In case the service provider is an administrator for the service recipient, or the information of the service recipient company is used.**
  - There is protection for unauthorized persons entering the area that contains customer information.
- **In the case of Data center rental or Server space rental**
  - There are measures to control access to essential areas (Server Room).
  - Permissions are granted to enter and exit work areas.
  - Area access logs are recorded and examined.
  - CCTV is installed
  - There is an international standard time setting check (Clock Synchronization)
  - Equipment siting and protection (water, electricity, air conditioning) are set up and protected.
  - There are measures to inspect and maintain supporting equipment (e.g., electrical systems, air conditioners, and networks).

6.9 Development and Maintenance Policy

- ต้องแยก Environment ตาม Phase ได้แก่ development, testing, production และกำหนดสิทธิการเข้าถึงของแต่ละ Environment
- ต้องมีการบริหารจัดการ Version Control และสิทธิการเข้าถึงของ Source Code
- การออกแบบระบบต้องปฏิบัติดังนี้
  - มีการตรวจสอบตัวตนก่อนใช้งาน
  - มีการกำหนดสิทธิตาม บุคคล/กลุ่มคน รวมถึง Level ของสิทธิ (Read only, Update, Delete)
  - มีการบันทึกการเข้าถึง และเปลี่ยนแปลงของข้อมูล
  - มีการเข้าใช้ระบบต้องผ่าน Secure channel เท่านั้น (กรณีที่ระบบเชื่อมต่อกับเครือข่ายสาธารณะ)
  - มีการเก็บสำรองข้อมูล
  - มีการเก็บ Log การเข้าถึงและการเปลี่ยนแปลงข้อมูล (Activity Log, Access Log, Transaction Log และ Security Event Log) ให้สามารถตรวจสอบย้อนหลังได้
  - ต้องลบ Temp file ที่ประมวลผลข้อมูลเรียบร้อยแล้วหลังจากใช้งาน ต้องมีการกำหนดรอบการลบ Temp file โดยสามารถตรวจสอบได้ว่าปฏิบัติจริง

- กรณีใช้บริการคลาวด์ (Cloud) พัฒนาระบบ IT ต้องดำเนินการตามแนวทางการพัฒนาที่ปลอดภัยของผู้ให้บริการคลาวด์ (Cloud) นั้น ๆ
- มีการทำทดสอบเจาะระบบเพื่อหาจุดอ่อน (Penetration Test) ก่อนขึ้นระบบ
- หลีกเลี่ยงการใช้ข้อมูลจริง (โดยเฉพาะข้อมูลส่วนบุคคล) มาใช้ในการทดสอบ และต้องดำเนินการดังนี้
  - ต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง
  - หลังจากดำเนินการ Test เสร็จสิ้นต้องทำการลบข้อมูลทันที
  - ต้องมีหลักฐานให้สามารถตรวจสอบได้ (ชื่อผู้เป็นผู้อนุมัติ, แหล่งข้อมูล)
- Environments must be separated according to Phases: development, testing, production, and set access rights for each environment.
- Version control and source code access rights must be appropriately managed.
- System design must comply with the following requirements:
  - Identity verification before use.
  - Rights are assigned according to Person/Group, Including Permission Level (Read only, Update, Delete)
  - Access logs are maintained. and change of information
  - Access to the system must be via a secure channel only (in case the system is connected to a public network).
  - Backups are kept.
  - There is a log of access and data change (Activity Log, Access Log, Transaction Log, and Security Event Log) for retrospective review.
  - Temp file that has already processed data must be deleted after use. Temp File deletion cycles must be set, which can be checked to see if it works.
- In the case of using cloud services to develop an IT system, the cloud service provider's secure development guidelines should be applied.
- There is a penetration test to find weaknesses (Penetration Test) before entering the system.
- Avoid using accurate data (especially personal data) used in the test and must proceed as follows:
  - There must be control over the test data like the control over the data in the entire system.
  - After completing the test, the data must be deleted immediately.
  - There must be evidence that can be verified (name of the approver, data source).

6.10 Patch Management

- มีการ Update Patch อย่างสม่ำเสมอ
- มีการ Update Antivirus and Malware Protection อย่างสม่ำเสมอ

- มีการทำ VA Scan อย่างน้อยปีละ 1 ครั้ง
- มีการทำทดสอบเจาะระบบเพื่อหาจุดอ่อน (Penetration Test) ก่อนขึ้นระบบ และดำเนินการทุกปี
- มีการวิเคราะห์ Log เพื่อค้นหาเหตุการณ์ผิดปกติอย่างสม่ำเสมอ
- Update Patch regularly.
- Update Antivirus and Malware Protection regularly.
- Perform VA scans at least once a year.
- Penetration Test is conducted to find weaknesses before the system is installed and carried out every year.
- Log analysis is regularly performed to find abnormal events.

6.11 Backup Policy

- ต้องมีแผนในการสำรองข้อมูล และมีการทดสอบการ Restore ข้อมูล อย่างน้อยปีละ 1 ครั้ง และสามารถตรวจสอบได้
- การสำรองข้อมูลที่มีข้อมูลส่วนบุคคลต้องเข้ารหัส
- Must have a backup plan, and there is a test to restore data at least once a year that can be checked.
- Backups containing personal data must be encrypted.

6.12 Information Transfer Policy

- ห้ามส่งข้อมูลให้บุคคลอื่นโดยไม่ได้รับอนุญาต
- การรับส่งข้อมูลต้องมีวิธีการให้ตรวจสอบได้
- การส่ง Email ที่มีข้อมูลส่วนบุคคลต้องส่งเป็นไฟล์แนบ และเข้ารหัส โดยส่งรหัส แยกกับ Email เอกสาร
- มีการใช้ Secure Protocol หรือ เข้ารหัสไฟล์ในการส่งข้อมูล
- Do not send information to other people without their permission.
- Data transmission must have a method to be verifiable.
- Sending e-mails containing personal information must be sent as an attachment and encrypted by sending a separate code from the E-mail document.
- Secure Protocol or file encryption is used to transmit data.

6.13 Notification of incidents

การแจ้งเหตุการณ์เมื่อเกิดเหตุเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ การรั่วไหล หรือเหตุการณ์ละเมิดข้อมูลส่วนบุคคล จะต้องดำเนินการดังนี้

- การแจ้งเหตุการละเมิดหรือรั่วไหล ให้ดำเนินการแจ้งกับผู้ประสานงานโครงงาน หรือ ผู้ดูแลระบบนั้น ๆ ภายใน 30 นาที โดยรายละเอียดอย่างน้อยดังนี้
  - คำอธิบายลักษณะเหตุละเมิด
  - ประเภทข้อมูลที่ได้รับผลกระทบ
  - จำนวนข้อมูลและเจ้าของข้อมูลที่เกี่ยวข้อง
  - ระยะเวลาที่เกิดเหตุ
  - มาตรการในการรับมือ
- ในส่วนของเหตุการณ์ผิดปกติอื่น ๆ ให้ดำเนินการตาม SLA ที่กำหนดกับผู้ประสานงาน

Incident notification when there is an incident related to information security, data leakage, or a personal data breach must proceed as follows:

- Notification of violations or leakage. Notify the project coordinator or administrator within 30 minutes with at least the following details:
  - Description of the nature of the violation
  - Affected data types
  - Number of data and associated data owners
  - Incident duration
  - Countermeasures
- As for other unusual events, implement the SLA assigned to the coordinator.

6.14 Processing of personal data

- ไม่มีสิทธิส่งข้อมูลหรือเปิดเผยให้กับผู้อื่น ยกเว้นแต่ได้รับคำอนุญาตเป็นลายลักษณ์อักษรต่อผู้ประสานงานโครงการ
- กรณีที่ผู้ให้บริการภายนอกเห็นว่าการประมวลผลนั้นอาจจะละเมิดกฎหมายหรือละเมิดการคุ้มครองข้อมูลส่วนบุคคลให้ระงับการประมวลผลและแจ้งกลับผู้ประสานงาน
- ต้องไม่ประมวลผลข้อมูลส่วนบุคคลนอกเหนือไปจากคำสั่งของผู้รับบริการ
- ห้ามดำเนินการตอบสนองการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (ยกเว้นมีการระบุไว้ในสัญญาอย่างชัดเจน) และต้องแจ้งเจ้าของข้อมูลว่าไม่มีสิทธิดำเนินการ รวมทั้งส่งต่อคำร้องให้กับผู้ประสานงานโครงการต่อไป
- ต้อง ลบ ทำลาย หรือส่งคืน ผู้รับบริการเมื่อเสร็จสิ้นการประมวลผลตามที่กำหนดไว้
- ต้อง ลบ หรือทำลาย ข้อมูลส่วนบุคคลนับตั้งแต่วันที่สัญญาสิ้นสุดลง (ยกเว้นต้องเก็บตามข้อบังคับของกฎหมาย)
- ผู้ประมวลผลต้องดำเนินการเก็บหลักฐาน (เก็บ ใช้ ส่ง ลบ) เพื่อให้ผู้รับบริการสามารถตรวจสอบว่าได้ปฏิบัติตามวัตถุประสงค์

- ต้องมีการจัดทำบันทึกกิจกรรมของข้อมูลส่วนบุคคลที่ผู้ประมวลผลต้องปฏิบัติ (Record of Processing Activities)
- ต้องจัดทำบันทึก เมื่อมีการเปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลหรือหน่วยภายนอก หลังจากได้รับอนุญาตจากผู้รับบริการ
- กรณีที่ผู้ประมวลผลข้อมูลมีการจ้างหน่วยงานภายนอก (ผู้รับจ้างช่วง) ประมวลผลข้อมูลส่วนบุคคล จะต้องขออนุมัติจากผู้รับบริการก่อน
- เมื่อมีการเปลี่ยนแปลง ผู้รับจ้างช่วง ต้องได้รับอนุญาตจากผู้รับบริการก่อนดำเนินการ
- No right to send information or disclose it to others. Except with the written permission of the project coordinator.
- If the external service provider considers that the processing may violate the law or the protection of personal data, they shall suspend the processing and notify the coordinator.
- Shall not process personal data beyond the instructions of the client.
- Do not respond to the exercise of rights of personal data subjects (unless explicitly stated in the contract) and must notify the data subject that he has no right to process, including forwarding the request to the project coordinator.
- Must delete, destroy, or return the client upon completion of the intended processing.
- Must delete or destroy personal data from the date of contract termination, except must be kept according to the regulations of the law.
- The processor must collect evidence (store, use, send, delete) so that the service recipient can verify that the objectives have been complied with.
- Records of Processing Activities must be maintained.
- Records must be made. When personal information is disclosed to a third party or entity after obtaining permission from the service recipient.
- If the data processor employs an outside agency (subcontractors) processing personal data, the processor must request approval from the service recipient first.
- When there is a change, the subcontractor must obtain permission from the service recipient before proceeding.