คู่มือในการปฏิบัติงานเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอก

(Third Party IT Practical Guideline)

Version 1.0

บริษัท ซีพี ออลล์ จำกัด (มหาชน)
313 อาคาร ซี.พี. ทาวเวอร์ ชั้น 24 ถ.สีลม แขวงสีลม เขตบางรัก กรุงเทพฯ 10500
เว็บไซต์: www.cpall.co.th

สารบัญ

หน้า

1. วัตถุประสงค์

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นคู่มือสำหรับผู้ให้บริการภายนอก เพื่อให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศและระบบบริหารจัดการข้อมูลส่วนบุคคล (ISMS/PIMS) สามารถดำเนินการต้องปฏิบัติงานได้อย่างเหมาะสม

2. ขอบเขต

คู่มือปฏิบัติงานฉบับนี้ครอบคลุมถึงการดำเนินการงานของผู้ให้บริการภายนอก

3. หน้าที่และความรับผิดชอบ

บทบาท	ความรับผิดชอบ
ผู้ให้บริการภายนอก	● รับทราบและปฏิบัติงานตามคู่มือฉบับนี้ ● ร่วมทำการประเมินความเสี่ยงในการดำเนินงาน
ผู้ประสานงานโครงการ	● ประสานงานกับผู้ให้บริการภายนอก ● แจ้งผู้ให้บริการภายนอกให้ทราบถึงคู่มือปฏิบัติงานฉบับนี้
เจ้าของข้อมูล/เจ้าของระบบ	● กำหนดสิทธิในการเข้าถึงข้อมูลหรือระบบสำหรับผู้ให้บริหารภายนอก ● ทำการประเมินความเสี่ยงในการดำเนินงานของผู้ให้บริการภายนอก ● ตรวจสอบดูแลการดำเนินงานของผู้ให้บริการภายนอก

4. เอกสารอ้างอิง

-

5. คำจำกัดความ

คำศัพท์	ความหมาย
หน่วยงานภายนอก/ ผู้ให้บริการภายนอก/ บุคคลภายนอก	บริษัทคู่ค้า (Business Partner), ผู้รับจ้างปฏิบัติงานให้กับบริษัทฯ (Outsource), ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่างๆ (Supplier), ผู้ให้บริการต่างๆ (Service Provider) และ ที่ปรึกษา (Consultant) ผู้ให้บริการภายนอก ที่ใช้งานระบบสารสนเทศของบริษัท ได้เป็นครั้งคราว หรือตามสัญญา
บริษัทผู้รับบริการ	บริษัท ซีพี ออลล์ จำกัด (มหาชน) และ/หรือ บริษัทย่อยที่ดำเนินการว่าจ้างกับหน่วยงานภายนอก
Removable Media	อุปกรณ์ที่ใช้เก็บข้อมูลที่สามารถเคลื่อนย้ายได้ เช่น Tape, DVD, Thumb drive, Flash drive, Hard disk
Mobile Device	อุปกรณ์ที่สามารถประมวลผลและสามารถเคลื่อนย้ายได้ เช่น Smartphone, Tablet,
Notebook	เครื่องคอมพิวเตอร์ที่สามารถพกพาได้

6. แนวปฏิบัติ

หน่วยงานภายนอกจะต้องปฏิบัติเพื่อให้สามารถรักษาความมั่นคงปลอดภัยสารสนเทศได้ทั้ง 3 ด้านคือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability) รวมทั้งดูแลรักษาข้อมูลส่วนบุคคลให้เป็นตามที่กำหนด

6.1 แนวปฏิบัติตามกฎหมาย และนโยบายของบริษัท

- ให้ปฏิบัติตามกฎหมายที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและระบบบริหารจัดการข้อมูลส่วนบุคคลทุกข้อกำหนด

- ต้องยอมรับการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศและระบบบริหารจัดการข้อมูลส่วนบุคคลที่บริษัท ซีพี ออลล์ จำกัด (มหาชน) และบริษัทย่อยกำหนด

6.2 **แนวปฏิบัติงานจากระยะไกลหรือการทำงานนอกสำนักงาน** (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

6.3 **การดูแลการใช้งาน** Computing Device **และ** Mobile Device

- มีการเก็บสำรองข้อมูลที่เกี่ยวกับผู้รับบริการ
- มีการติดตั้งโปรแกรมป้องกันไวรัส (Anti-virus) ที่ทันสมัย
- มีการใช้ Software Licenses
- มีมาตรการในการป้องกันอุปกรณ์ที่มีข้อมูลของผู้รับบริการมิให้ถูกโจรกรรมได้ง่าย
- เครื่องคอมพิวเตอร์จะต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง โดยทำการตั้งเวลาพักหน้าจอ (Screen Saver) หากไม่ใช้งานเกินกว่า 15 นาที

6.4 **แนวปฏิบัติและหน้าที่ความรับผิดชอบต่อทรัพย์สินที่มีการใช้ข้อมูลของบริษัทผู้รับบริการ**

- การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of electronic mail) การส่งข้อมูลส่วนบุคคลต้องมีการเข้ารหัส
- เอกสารที่เกี่ยวข้องกับข้อมูลส่วนบุคคลให้ปฏิบัติตามผู้ประสานงานโครงการแจ้งไว้อย่างเคร่งครัด และต้องมีการใช้ Hardcopy น้อยที่สุดเท่าที่จำเป็น
- ห้ามมิให้เปิดเผยข้อมูลสำหรับการพิสูจน์ตัวตน หรือที่เรียกว่า รหัสผ่านของระบบบริษัท (รวมถึงสิ่งที่ใช้ในการพิสูจน์ตัวตนอื่นๆ เช่น ฮาร์ดโทเคน, ซอฟต์โทเคน, รหัส OTP) ให้บุคคลอื่นโดยเด็ดขาด
- ผู้ปฏิบัติงานต้องป้องกันดูแลรักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลของบริษัทผู้รับบริการ

6.5 **แนวปฏิบัติการดำเนินการตามชั้นความลับของสารสนเทศ** (Information Classification Policy)

- ให้ปฏิบัติตามชั้นความลับที่ผู้ประสานงานโครงการกำหนด

6.6 **แนวปฏิบัติการจัดการสื่อที่ใช้ในการบันทึกข้อมูล** (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

6.7 **แนวปฏิบัติการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ** (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

6.8 แนวปฏิบัติด้านความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (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)

6.9 แนวปฏิบัติในการพัฒนา และการบำรุงรักษาระบบสารสนเทศ (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

- มีการทำทดสอบเจาะระบบเพื่อหาจุดอ่อน (Penetration Test) ก่อนขึ้นระบบ
- หลีกเลี่ยงการใช้ข้อมูลจริง (โดยเฉพาะข้อมูลส่วนบุคคล) มาใช้ในการทดสอบ และต้องดำเนินการดังนี้
  - ต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง
  - หลังจากดำเนินการ Test เสร็จสิ้นต้องทำการลบข้อมูลทันที
  - ต้องมีหลักฐานให้สามารถตรวจสอบได้ (ชื่อผู้เป็นผู้อนุมัติ, แหล่งข้อมูล)

6.10 **แนวปฏิบัติในการควบคุมและจัดการช่องโหว่ในระบบงาน** (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

6.11 **แนวปฏิบัติในการสำรองข้อมูล** (Backup Policy)

- ต้องมีแผนในการสำรองข้อมูล และมีการทดสอบการ Restore ข้อมูล อย่างน้อยปีละ 1 ครั้ง และสามารถตรวจสอบได้
- การสำรองข้อมูลที่มีข้อมูลส่วนบุคคลต้องเข้ารหัส

6.12 **แนวปฏิบัติในการการถ่ายโอนข้อมูลสารสนเทศ** (Information Transfer Policy)

- ห้ามส่งข้อมูลให้บุคคลอื่นโดยไม่ได้รับอนุญาต
- การรับส่งข้อมูลต้องมีวิธีการให้ตรวจสอบได้
- การส่ง Email ที่มีข้อมูลส่วนบุคคลต้องส่งเป็นไฟล์แนบ และเข้ารหัส โดยส่งรหัส แยกกับ Email เอกสาร
- มีการใช้ Secure Protocol หรือ เข้ารหัสไฟล์ในการส่งข้อมูล

6.13 **การรับแจ้งเหตุการณ์ที่พบหรือปัญหาที่เกิดขึ้น** (Notification of incidents)

การแจ้งเหตุการณ์เมื่อเกิดเหตุเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ การรั่วไหล หรือเหตุการณ์ละเมิดข้อมูลส่วนบุคคล จะต้องดำเนินการดังนี้

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

6.14 **แนวปฏิบัติการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล** (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) ประมวลผลข้อมูลส่วนบุคคลจะต้องขออนุมัติจากผู้รับบริการก่อน
- เมื่อมีการเปลี่ยนแปลง ผู้รับจ้างช่วง ต้องได้รับอนุญาตจากผู้รับบริการก่อนดำเนินการ