บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)

414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับบุคคลภายนอก (Cyber Security Standard for Third Party)

กลุ่มเอไอเอส

เวอร์ชัน: 1.0

เจ้าของเอกสาร: Cyber Security

วันที่ปรับปรุงแก้ไข: 20 มิถุนายน 2567

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)

414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

รายละเอียดการจัดทำเอกสาร

ประวัติการปรับปรุงเอกสาร

เอกสารฉบับนี้มีการบันทึกการแก้ไขทั้งหมดตามตารางดังต่อไปนี้

เวอร์ชัน	วันที่	ผู้จัดทำ	รายละเอียด	ผู้สอบทาน	อนุมัติโดย
1.0	20 มิถุนายน 2567	Cyber Security	เอกสารตั้งต้น	H-DPO, H-PATH, H-CS	CIO

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)

414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

สารบัญ

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับบุคคลภายนอก

1. บทนำ

1.1 วัตถุประสงค์

1) เพื่อเป็นมาตรฐานทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้บุคคลภายนอกที่มีการเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของบริษัทได้ รวมถึงบุคคลภายนอกที่ให้บริการกับลูกค้าภายใต้ชื่อทางการค้าของบริษัท
2) เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท โดนบุกรุก ขโมย ทำลาย แทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่างๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัทเมื่อใช้บริการ การเชื่อมต่อหรือการเข้าถึงจากบุคคลภายนอก
3) เพื่อลดความเสี่ยงต่อความปลอดภัยของข้อมูลสารสนเทศของบริษัท เมื่อใช้บริการ การเชื่อมต่อหรือการเข้าถึงจากบุคคลภายนอก

1.2 ขอบเขต

มาตรฐานฉบับนี้ครอบคลุมถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ ความปลอดภัยของระบบสารสนเทศ และความปลอดภัยของข้อมูลสารสนเทศของบริษัท จากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของบริษัท

1.3 คำจำกัดความ

1) **“บริษัท (Company)”** หมายถึง บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) และบริษัทในสายธุรกิจ
2) **บุคคลภายนอก (Third Party)”** หมายถึง บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ รวมถึงบุคลากรหรือหน่วยงานภายนอกที่ได้รับสิทธิเข้าถึงข้อมูลส่วนบุคคลของลูกค้าของบริษัท เช่น
    - บริษัทคู่ค้า (Business Partner)
    - ผู้รับจ้างปฏิบัติงานให้กับบริษัทฯ (Outsource)
    - ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่างๆ (Supplier)
    - ผู้ให้บริการต่างๆ (Service Provider)
    - ที่ปรึกษา (Consultant)
    - ผู้ตรวจสอบอิสระ (External Auditor)
3) **“ข้อมูลสำคัญ”** หรือ **“ข้อมูลที่เป็นความลับ (Sensitive Information)”** หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือที่บริษัทมีพันธะผูกพันตามข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบธุรกิจ หรือสัญญาซึ่งบริษัทไม่อาจนำไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์อย่างอื่น นอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัท การรั่วไหลของข้อมูลสำคัญ หรือ

ข้อมูลที่เป็นความลับดังกล่าวอาจเป็นเหตุให้การดำเนินธุรกิจของบริษัท ต้องหยุดชะงัก ขาดประสิทธิภาพ หรือบริษัทเสื่อมเสียชื่อเสียง แบ่งเป็นประเภทข้อมูลตาม data domain ได้ 6 domain คือ ข้อมูลลูกค้า (Customer Data) ข้อมูลพนักงาน (Employee Data) ข้อมูลคู่ค้า (Partner Data) ข้อมูลด้านการเงิน (Financial Data) ข้อมูลเครือข่ายขององค์กร (Network Data) และข้อมูลเชิงกลยุทธ์ (Strategic Data)

4) **“สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Removable Media)”** หมายถึง อุปกรณ์ที่เคลื่อนย้ายได้ ซึ่งสามารถบันทึก และจัดเก็บข้อมูลได้ เช่น อุปกรณ์ Thumb drive, CD, Diskette, iPod, Electronic Organizer, PDA, Pocket PC เป็นต้น
5) **“ระบบซึ่งไวต่อการรบกวน”** หมายถึง ระบบงานที่ถือว่าไวต่อการรบกวนหรือระบบงานที่สำคัญยิ่งยวด และจำเป็นต้องได้รับการแยกสภาพแวดล้อม
6) **“การควบคุมการเปลี่ยนแปลง (Change Control)”** หมายถึง กระบวนการในการทบทวน ทดสอบและอนุมัติการเปลี่ยนแปลง รวมถึงผลกระทบก่อนการดำเนินงานในระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ
7) **“การเปลี่ยนแปลงที่สำคัญ (Major Change)”** หมายถึง การเปลี่ยนแปลงที่ส่งผลกระทบต่อการให้บริการหรืออาจส่งผลกระทบร้ายแรง ต่อทรัพย์สินและระบบงาน เช่น การหยุดชะงักของการให้บริการ เป็นระยะเวลานาน การสูญเสียทรัพย์สินหรือชีวิต การเกิดภัยพิบัติ เป็นต้น แต่เหตุการณ์อาจไม่เกิดขึ้นทันทีทันใด และไม่ต้องเร่งรีบแก้ไขแต่ต้องใช้เวลาในการพิจารณาผลกระทบ และดำเนินการแก้ไขอย่างระมัดระวัง
8) **“ข้อมูล Log file”** หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
9) **“ความปลอดภัยโดยการออกแบบ (Security by Design)”** หมายถึง แนวทางในการออกแบบระบบคอมพิวเตอร์หรือแอปพลิเคชันให้มีความปลอดภัยตั้งแต่เริ่มต้น เน้นการป้องกันความเสี่ยงจากภัยคุมคามทางไซเบอร์ตั้งแต่ขั้นตอนการเริ่มออกแบบระบบคอมพิวเตอร์ โดยคำนึงถึงหลักการด้านความปลอดภัยต่างๆ ได้แก่ ความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ตัวอย่างเช่น การเข้ารหัส (encryption) การใช้การพิสูจน์ตัวตนแบบหลายปัจจัย (multi-factor authentication)
10) **“ความปลอดภัยโดยค่าเริ่มต้น (Security by Default)”** หมายถึง แนวทางในการตั้งค่าให้ระบบคอมพิวเตอร์หรือแอปพลิเคชันให้มีความปลอดภัยตั้งแต่เริ่มต้น เน้นการป้องกันความเสี่ยงจากภัยคุมคามทางไซเบอร์โดยไม่ต้องให้ผู้ใช้งานปรับตั้งค่าความปลอดภัยเพิ่มเติม ตัวอย่างเช่น การปิดการใช้งานที่ไม่จำเป็น การตั้งค่ารหัสผ่านที่แข็งแกร่ง

1.4 ข้อยกเว้น

หากไม่สามารถดำเนินการตามมาตรฐานฉบับนี้ได้ บุคคลภายนอกต้องแจ้งพนักงานผู้ดูแลโครงการของบริษัททราบ เพื่อเข้าสู่กระบวนการพิจารณาจัดการความเสี่ยงของบริษัท

1.5 บทลงโทษ

กรณีบุคคลภายนอกละเมิดเอกสารมาตรฐานฉบับนี้ และรวมถึงนโยบาย มาตรฐาน แนวปฏิบัติ ระเบียบปฏิบัติของบริษัท ซึ่งอาจเป็นเหตุให้บริษัทได้รับความเสียหาย บริษัทสงวนสิทธิในการพิจารณาบทลงโทษตามสัญญาการใช้บริการ

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

2. หน้าที่และความรับผิดชอบ

2.1 พนักงานผู้ดูแลโครงการของบริษัท

ประสานงานกับบุคคลภายนอก และกำกับดูแลให้ปฏิบัติตามนโยบายของบริษัทและมาตรฐานฉบับนี้

2.2 บุคคลภายนอก

1) ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบาย มาตรฐาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติ แนวปฏิบัติ คำแนะนำ และกระบวนการต่างๆ ของบริษัทที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเคร่งครัด
2) ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท
3) แจ้งให้บริษัททราบทันที เมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม หรือพบเห็นการบุกรุก โจรกรรม ทำลาย แทรกแซงการทำงาน หรือจารกรรมที่อาจสร้างความเสียหายต่อบริษัท

3. มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

บุคคลภายนอกต้องยึดหลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย โดยมีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้

- **ความลับ (Confidentiality)** – การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของบริษัท
- **ความสมบูรณ์ (Integrity)** – การทำให้มั่นใจว่าข้อมูลของบริษัท ต้องไม่มีการแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต
- **ความพร้อมใช้งาน (Availability)** – การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและบริการได้อย่างรวดเร็วและเชื่อถือได้

3.1 การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Risk Management)

1) บุคคลภายนอกต้องจัดทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Risk Assessment) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
2) กรณีที่พบความเสี่ยงที่มีผลการประเมินสูงกว่าระดับที่ยอมรับได้ บุคคลภายนอกต้องจัดทำแผนจัดการความเสี่ยง (Risk Mitigation Plan / Risk Treatment Plan) และจัดส่งให้กับบริษัท
3) ต้องให้ความร่วมมือในการให้หน่วยงานที่รับผิดชอบของบริษัทเข้าตรวจสอบ (Audit) และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์ของบริษัท
4) สินค้าหรือบริการใดๆ ของบุคคลภายนอก ที่สามารถเข้าถึงข้อมูลส่วนบุคคลของลูกค้าของบริษัท บุคคลภายนอกต้องมีการตรวจสอบจากผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระ และมีการจัดทำรายงานการตรวจสอบ (Audit Report) อย่างน้อยปีละ 1 ครั้ง

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

3.2 การบริหารจัดการระบบ (System Management)

3.2.1 บัญชีทรัพย์สินและความเป็นเจ้าของ (Inventory and Ownership)

ต้องมีการจัดทำบัญชีทรัพย์สินของระบบ (System Inventory) ทั้งนี้บัญชีทรัพย์สินของระบบต้องมีรายละเอียดของการจำแนกชั้นความลับ ความเป็นเจ้าของทรัพย์สิน และมีการสอบทานบัญชีทรัพย์สินของระบบอย่างน้อยปีละ 1 ครั้ง หรือเมื่อบัญชีทรัพย์สินของระบบมีการเปลี่ยนแปลง

3.2.2 การบริหารจัดการซอฟต์แวร์ลิขสิทธิ์ (Software Licensing)

1) ใช้ซอฟต์แวร์ลิขสิทธิ์ที่ถูกกฎหมาย และเกี่ยวข้องกับการปฏิบัติงานกับบริษัทเท่านั้น
2) บริษัทไม่อนุญาตให้ใช้ซอฟต์แวร์ประเภท Hacking Tools หรือซอฟต์แวร์อื่นๆ ที่เกี่ยวข้องกับการตรวจสอบและรักษาความปลอดภัยข้อมูลและระบบ เช่น ซอฟต์แวร์ที่ใช้ในการทดสอบการตรวจสอบช่องโหว่ ซอฟต์แวร์ที่ใช้ในการเจาะระบบ ก่อนได้รับอนุญาต

3.3 การบริหารจัดการข้อมูลอย่างปลอดภัย (Data Security Management)

3.3.1 การจัดลำดับชั้นความลับและการควบคุมข้อมูล (Security Classification and Handling)

1) ต้องมีการจัดลำดับชั้นความลับและการควบคุมดูแลข้อมูลอย่างเหมาะสม สอดคล้องกับ *มาตรการจัดลำดับชั้นความลับและการควบคุมดูแลข้อมูล*ของบริษัท เพื่อความปลอดภัยของข้อมูล
2) ต้องมีการควบคุมดูแลข้อมูลตลอดวงจรชีวิต (Lifecycle) ไม่ว่าจะเป็นการสร้าง การใช้ การส่ง การจัดเก็บ การทำลายข้อมูล ให้เหมาะสมตามชั้นความลับและความสำคัญของข้อมูลนั้นๆ
3) การควบคุมดูแลข้อมูลของบริษัทในรูปแบบอิเล็กทรอนิกส์ (Electronic Format)
    a. การจัดส่งข้อมูลของบริษัทในชั้นความลับต้องจัดส่งผ่านทางอีเมลหรือช่องทางที่บริษัทกำหนดเท่านั้น และสำหรับข้อมูลในชั้นความลับ Highly Confidential เอกสารแนบต้องใส่ password protection ก่อนส่งออก แล้วจัดส่งรหัสผ่านในช่องทางอื่นแยกกับเอกสารที่จัดส่ง เช่น ส่งข้อมูลเอกสารผ่านทางอีเมล และส่งรหัสผ่านในช่องทาง SMS
    b. บริษัทไม่อนุญาตให้ถ่ายรูปข้อมูลของบริษัท โดยเฉพาะอย่างยิ่ง ข้อมูลส่วนบุคคลของลูกค้า
    c. บริษัทไม่อนุญาตให้โพสต์ข้อมูลของบริษัทลงในสื่อสังคมออนไลน์ (Social Media)
    d. ต้องทำการขออนุญาตจากบริษัทและต้องได้รับอนุญาตจากบริษัทเป็นลายลักษณ์อักษร ก่อนการลบทำลายข้อมูลสำคัญของบริษัท
4) การควบคุมดูแลข้อมูลของบริษัทในรูปแบบสิ่งพิมพ์ (Publishing Format)
    a. บริษัทไม่อนุญาตให้พิมพ์ข้อมูลที่เป็นความลับ ข้อมูลสำคัญของบริษัท ข้อมูลส่วนบุคคลของลูกค้า ออกมาในรูปแบบสิ่งพิมพ์ (Publishing Media) โดยไม่ได้รับอนุญาตจากบริษัท
    b. การลบทำลายข้อมูลความลับ ข้อมูลสำคัญของบริษัท ต้องได้รับการอนุญาตก่อนการลบทำลาย และต้องทำลายเอกสารโดยการย่อยเอกสารทิ้งแบบ cross-shred หรือ strip-shred หรือ ย่อยซ้ำหลายๆ ครั้ง จนไม่สามารถนำกลับมาประกอบเป็นข้อมูลเดิมได้ ตามมาตรฐานสากลทันที

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

5) กรณีที่บุคคลภายนอกมีการเข้าถึงข้อมูลส่วนบุคคล ต้องมีการจัดทำและปฏิบัติตามสัญญาการประมวลผลข้อมูล (Data Processing Agreement: DPA)

3.3.2 การเข้ารหัสข้อมูล (Data Encryption)

บริษัทกำหนดให้ข้อมูลที่ต้องทำการเข้ารหัส ได้แก่ ข้อมูลสำคัญ (Sensitive Information) ของบริษัท โดยเฉพาะอย่างยิ่ง ข้อมูลส่วนบุคคล ทั้งระหว่างการจัดเก็บ (Data at Rest) และการส่งข้อมูล (Data in Transit) ตามมาตรฐานของบริษัท

3.3.2.1 การจัดเก็บข้อมูล (Data at Rest) ต้องทำการเข้ารหัสข้อมูลด้วยมาตรฐานการเข้ารหัสดังต่อไปนี้

- สำหรับการเข้ารหัสแบบ Symmetric
  - AES-128 หรือสูงกว่า
- สำหรับการเข้ารหัสแบบ Asymmetric
  - RSA-1024 หรือสูงกว่า โดยเฉพาะอย่างยิ่งระบบที่ in-scope ของ PCI DSS และ Digital ID
  - ECC-224 หรือสูงกว่า
  - DSA-2048 หรือสูงกว่า
  - D-H-224 หรือสูงกว่า

ทั้งนี้ กรณีที่มีการใช้งานข้อมูลสำคัญที่ต้องได้รับการปกป้องเป็นพิเศษ 4 ประเภท ดังต่อไปนี้ จะต้องทำการเข้ารหัสโดยการใช้วิธีการ Field-level encryption

1) หมายเลขบัตรประชาชน หรือ หนังสือเดินทาง หมายรวมถึง เลขควบคุมหลังบัตรประจำตัวประชาชน (Laser ID) เลขชิปการ์ดของบัตรประชาชน (Chip ID) เลขคำขอมีบัตรจากกรมการปกครอง (bp1no)
2) MSISDN (เช่น หมายเลขโทรศัพท์ และ IoT Number) หรือ หมายเลข FBB-ID
3) หมายเลขบัญชีธนาคาร
4) หมายเลขบัตรเครดิต หรือบัตรเดบิต

3.3.2.2 การรับส่งข้อมูล (Data in Transit) การรับส่งข้อมูลในระบบเครือข่าย (Data Transmission) จะต้องทำการเข้ารหัสข้อมูลด้วยมาตรฐานการเข้ารหัสดังต่อไปนี้

1) กรณีใช้การเชื่อมต่อ VPN: การตรวจสอบเวอร์ชันของ TLS ใน VPN concentrator จะต้องถูกกำหนดค่าให้ใช้ TLS 1.2 (หรือสูงกว่า) และห้ามใช้การเชื่อมต่อที่มีเวอร์ชัน SSL 3.0 และต่ำกว่า
2) กรณีที่ใช้การเชื่อมต่อ HTTPS: TLS จะต้องถูกกำหนดค่าให้ใช้ TLS 1.2 (หรือสูงกว่า) และห้ามใช้การเชื่อมต่อที่มีเวอร์ชัน SSL 3.0 และต่ำกว่า
3) กรณีที่ใช้การเชื่อมต่อที่ปลอดภัยอื่นๆ: การเชื่อมต่ออื่นทำได้โดยใช้โปรโตคอลที่ปลอดภัย เช่น FTP ที่มีความปลอดภัยการเข้ารหัส (SFTP), SSH (ไม่อนุญาตให้เข้าสู่ระบบด้วยผู้ใช้งานที่เป็นสิทธิสูงสุดของระบบที่มีมาพร้อมระบบปฏิบัติการ (Root User)

3.3.3 การจัดการบัญชีทรัพย์สินข้อมูล (Data Asset Inventory Management)

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

1) บุคคลภายนอกต้องจัดทำบัญชีสินทรัพย์ข้อมูล (Data Asset Inventory) ซึ่งระบุรายชื่อเจ้าของข้อมูล ผู้ดูแล จุดประสงค์ของการจัดเก็บ สถานที่จัดเก็บข้อมูล รูปแบบ/ประเภทการจัดเก็บข้อมูล ระยะเวลาในการจัดเก็บข้อมูล lawful basis of processing เพื่อให้ง่ายต่อการจัดการที่เป็นระบบและมีมาตรฐานตามแนวทางการควบคุมดูแลข้อมูล
2) บุคคลภายนอกต้องสอบทานบัญชีทรัพย์สินข้อมูลอย่างน้อยปีละ 1 ครั้ง หรือเมื่อบัญชีทรัพย์สินของระบบมีการเปลี่ยนแปลง

3.3.4 ระยะเวลาการจัดเก็บข้อมูล (Data Retention and Archiving)

1) จัดเก็บข้อมูลสำคัญตามระยะเวลาที่กำหนด โดยหลังจากพ้นจากระยะเวลาที่กำหนดใน Retention Period ตามตารางดังต่อไปนี้ ให้มีการลบทำลายข้อมูลอย่างปลอดภัยตามมาตรฐานสากล เพื่อให้ตรงกับวัตถุประสงค์การจัดเก็บข้อมูลตามระยะเวลาที่กำหนด สอดคล้องกับมาตรฐานการจัดเก็บข้อมูลของบริษัท

No.	Category	Retention Period	Lawful Basis / การบริหารจัดการข้อมูลของบริษัท
1	ข้อมูลสำคัญทั้ง 6 Domain รวมถึงข้อมูลส่วนบุคคลของลูกค้า	เก็บตลอดระยะเวลาการใช้บริการตามสัญญา	ฐานสัญญาการให้บริการ
2	ข้อมูล Log file	90 วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์	มาตรา 26 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

2) หลังจากมีการยกเลิกหรือสิ้นสุดสัญญาการให้บริการ บุคคลภายนอกต้องทำการส่งมอบข้อมูลของบริษัท รวมถึงข้อมูลสำคัญในโครงการที่จัดทำร่วมกันให้กับบริษัท และทำการลบทำลายข้อมูลที่จัดเก็บไว้กับบุคคลภายนอกหลังจากการส่งมอบข้อมูลแล้วเสร็จไม่เกิน 7 วันทำการ เว้นแต่ในกรณีจำเป็นต้องเก็บรักษาข้อมูลส่วนบุคคลเพื่อการปฏิบัติตามกฎหมายที่ใช้บังคับเท่านั้น
3) การลบทำลายข้อมูลที่เป็นความลับ รวมถึงข้อมูลส่วนบุคคลของลูกค้าของบริษัท ต้องแจ้งแก่พนักงานผู้ดูแลโครงการของบริษัทและได้รับการอนุมัติจากบริษัทก่อน นอกจากนั้น ต้องจัดทำรายงานบันทึกการลบข้อมูล รวมถึงจัดเก็บหลักฐานการลบทำลายข้อมูลให้บริษัททุกครั้ง

3.4 การบริหารจัดการหน่วยงานและบุคลากร (Human Resource Management)

บุคคลภายนอกต้องมีการฝึกอบรมพนักงานของบุคคลภายนอกทุกคนที่เกี่ยวข้องกับโครงการของบริษัท ให้มีความรู้ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม รวมถึงมีการประเมินความรู้ความเข้าใจด้านความมั่นคงปลอดภัยไซเบอร์

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

3.5 การบริหารจัดการการรับเหมาช่วง (Sub-contract Management)

กรณีมีการรับเหมาช่วง (Sub-contract) ต้องปฏิบัติดังนี้

1) ผู้รับเหมาช่วง ต้องมีการลงนามข้อตกลงผูกพันเป็นรายบุคคลหรือนิติบุคคลในการห้ามเปิดเผยข้อมูล และยินยอมที่จะปฏิบัติตามมาตรฐานฉบับนี้
2) บุคคลภายนอก ต้องทำการตรวจประเมินการปฏิบัติตามมาตรฐานและความเสี่ยงทางด้านไซเบอร์และการคุ้มครองข้อมูลของผู้รับเหมาช่วงที่ใช้บริการ อย่างน้อยปีละ 1 ครั้ง
3) การพัฒนาซอฟต์แวร์จากผู้รับเหมาช่วง (Sub-contract) ต้องได้รับการดูแล ตรวจสอบ รวมถึงดำเนินการโดยใช้มาตรฐานความมั่นคงปลอดภัยที่ได้รับอนุญาต บุคคลภายนอกทั้งหมดที่พัฒนาซอฟต์แวร์ในนามของบริษัท ต้องผูกพันตามสัญญาที่ได้อนุมัติและลงนามแล้ว ซึ่งในสัญญาต้องประกอบด้วย คำจำกัดความของกรรมสิทธิ์ในทรัพย์สิน (Property Right) การจัดการสิทธิการใช้ (License Arrangement) มาตรการความมั่นคงปลอดภัย (Security Measure) สิทธิในการตรวจสอบ (Auditing Right) และกระบวนการทดสอบ (Testing Right)

3.6 การรักษาความมั่นคงปลอดภัยสถานที่และอุปกรณ์ (Physical and Equipment Security)

3.6.1 การควบคุมการผ่านเข้าออกสถานที่

1) บุคคลภายนอกต้องมีมาตรการควบคุมการเข้าถึงพื้นที่ โดยแบ่งพื้นที่ออกเป็นโซนตามระดับความเสี่ยงและมีการควบคุมสิทธิ์ในการเข้าถึงอย่างเหมาะสม
2) ต้องไม่เปิดเผยที่ตั้งสถานที่สำคัญของบริษัท เช่น สถานที่ประมวลผลข้อมูล ห้องผู้บริหาร ฯลฯ

3.6.2 การเข้าปฏิบัติงานกับระบบคอมพิวเตอร์

ต้องมีการจำกัดการเข้าปฏิบัติงานกับระบบคอมพิวเตอร์เฉพาะผู้มีหน้าที่เกี่ยวข้องและได้รับอนุญาตเท่านั้น

3.6.3 การป้องกันภัยคุกคามทางกายภาพและสภาพแวดล้อม

ระบบที่ใช้ในการประมวลผลข้อมูลสำคัญของบริษัทต้องดำเนินการดังต่อไปนี้

1) สถานที่ติดตั้งและเก็บรักษาระบบคอมพิวเตอร์ ต้องมีสภาพแวดล้อมที่ปลอดภัยจากสิ่งที่อาจก่อให้เกิดอันตราย มีความเหมาะสมต่อการทำงาน และสะดวกในการแก้ไขปัญหาของระบบคอมพิวเตอร์ เช่น มีการทำป้ายที่ชัดเจน มีระบบเตือนภัย มีระบบดับเพลิงอัตโนมัติ มีการรักษาอุณหภูมิและความชื้นให้อยู่ในระดับที่เหมาะสม มีระบบไฟฟ้าที่พร้อมสำหรับการใช้งานทั้งในภาวะปกติ และไม่ปกติอย่างเหมาะสม
2) สถานที่ตั้งที่มีข้อมูลหรือระบบที่มีความสำคัญของบริษัท ต้องติดตั้งระบบเฝ้าระวังเพื่อตรวจสอบทุกวันตลอด 24 ชั่วโมง (24x7)

3.6.4 การทำลายหรือการนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย

ต้องจัดให้มีการทำลายสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ให้สอดคล้องกับลำดับชั้นความลับของข้อมูล เพื่อทำให้มั่นใจว่าข้อมูลสำคัญและซอฟต์แวร์ ถูกลบหรือเขียนทับอย่างปลอดภัยตามมาตรฐานสากล

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

3.7 การบริหารจัดการการสื่อสารและการดำเนินงาน (Communications and Operation Management)

3.7.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedure and Responsibilities)

3.7.1.1 เอกสารขั้นตอนการปฏิบัติงาน (Operating Procedure Document)

ต้องจัดทำและทบทวนเอกสารขั้นตอนการปฏิบัติงาน ซึ่งเอกสารต้องประกอบไปด้วยขั้นตอนการประมวลผลและจัดการข้อมูล คำแนะนำสำหรับจัดการข้อผิดพลาด และหน่วยงานที่สนับสนุนปัญหาจากการดำเนินงานหรือปัญหาอื่น ๆ ที่คาดไม่ถึง

3.7.1.2 การบริหารจัดการการเปลี่ยนแปลง (Change Management)

1) ต้องมีกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Process) และควบคุมการเปลี่ยนแปลงใดๆ กับของซอฟต์แวร์ ฮาร์ดแวร์ เครือข่ายการสื่อสาร อย่างเหมาะสม โดยเฉพาะอย่างยิ่งระบบปฏิบัติการที่ใช้งานจริง (Production Operating System) ให้มีหัวข้อครอบคลุมอย่างน้อยดังนี้
   - การประเมินความเสี่ยงของการเปลี่ยนแปลง
   - การประเมินช่องโหว่ระบบ
   - ทดสอบการเจาะระบบ ในกรณีที่ ระบบเป็น Web Application, Application Program Interface
   - การจัดเตรียมขั้นตอนการ rollback ในกรณีที่เกิดข้อผิดพลาด
2) เมื่อมีการเปลี่ยนแปลงใดๆ กับระบบคอมพิวเตอร์ ต้องมีการบันทึกเป็นลายลักษณ์อักษร
3) กรณีบริษัทฯ เป็นผู้ดูแลระบบ ผู้ให้บริการจะต้องปฏิบัติตามกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Process) ของบริษัท

3.7.1.3 การแยกระบบสำหรับการพัฒนา การทดสอบ และการใช้งานจริงออกจากกัน (Separation of Development, Test and Production Systems)

1) ต้องมีการแยกระบบสำหรับการพัฒนา (Development System) การทดสอบ (Test System) และการใช้งานจริง (Production System) ออกจากกัน เพื่อจัดการกับข้อมูลสำคัญ โดยการแยกระบบต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) และ/หรือ การควบคุมการเข้าถึงทางตรรกะ (Logical Access Control)
2) ไม่อนุญาตให้ใช้ข้อมูลใน Production System ข้อมูลสำคัญ ข้อมูลส่วนบุคคล หรือข้อมูลที่เป็นความลับในการทดสอบระบบ

3.7.2 การบริหารจัดการปริมาณความจุของระบบ (Capacity Management)

1) ต้องมีกระบวนการวางแผนปริมาณความจุของระบบ เพื่อคาดการณ์ปริมาณความจุสูงสุดของทรัพยากรในระบบคอมพิวเตอร์ มีการติดตาม (Monitoring) และปรับแต่ง (Tuning) ประสิทธิภาพการใช้งานทรัพยากรของระบบคอมพิวเตอร์อย่างสม่ำเสมอ ให้รองรับกับปริมาณงานที่ได้คาดการณ์ไว้อย่างถูกต้อง
2) ควรจัดทำเอกสารขั้นตอนการปฏิบัติสำหรับการบริหารจัดการปริมาณความจุของระบบ โดยให้มีการประกาศใช้และปรับปรุงเอกสารอย่างสม่ำเสมอ

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

3.7.3 การป้องกันซอฟต์แวร์ไม่ประสงค์ดี (Protection Against Malicious Software)

1) ต้องมีการกำหนดมาตรการที่เหมาะสมในการป้องกัน ตรวจจับ และ/หรือ แก้ไขระบบคอมพิวเตอร์ทั้งหมดอย่างเหมาะสม เพื่อป้องกันไวรัส และซอฟต์แวร์ไม่ประสงค์ดีอื่น ๆ
2) ต้องมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสและซอฟต์แวร์ไม่ประสงค์ดี รวมถึง Endpoint Detection and Response ที่ได้รับอนุญาตจากบริษัท โดยต้องเปิดใช้งานและปรับปรุงตลอดเวลา รวมถึงต้องมีการตรวจหาซอฟต์แวร์ไม่ประสงค์ดี

3.7.4 การสำรองและการกู้คืนข้อมูล (Back Up and Restoration)

1) ต้องมีการสำรองข้อมูลอย่างสม่ำเสมอ และจัดให้มีมาตรการด้านความปลอดภัยของการเก็บข้อมูลสำรองเทียบเท่ากับการจัดเก็บข้อมูลต้นทาง รวมถึงอาจจัดให้มีการตัดการเชื่อมต่อกับระบบเครือข่ายเพื่อป้องกันการโจมตีจากแรนซัมแวร์
2) ควรมีการทดสอบการกู้คืนข้อมูลสำคัญ อย่างน้อยปีละ 1 ครั้งและบันทึกผลการทดสอบเป็นลายลักษณ์อักษร เพื่อเป็นการตรวจสอบให้มั่นใจว่าข้อมูลที่ทำการกู้คืน เป็นไปตามระยะเวลาที่ใช้ในการกู้คืนข้อมูล (Recovery Time Objective: RTO) และ จุดที่สามารถย้อนเวลากลับไปได้ (Recovery Point Objective: RPO) ที่กำหนดไว้ในข้อตกลงหรือสัญญาการใช้บริการ

3.7.5 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)

1) ต้องมีการจัดทำแผนผังรายละเอียดที่แสดงการเชื่อมต่อระบบและอุปกรณ์ต่างๆ โดยถือเป็นเอกสารสำคัญที่อนุญาตให้เฉพาะผู้มีหน้าที่รับผิดชอบเท่านั้นที่สามารถใช้เอกสารนี้ได้
2) ต้องมีการกำหนดมาตรการควบคุมความปลอดภัยเครือข่าย ปิดการใช้งานหรือตัดการเชื่อมต่อพอร์ต เมื่อไม่มีการใช้งานบนอุปกรณ์ รวมถึงป้องกันระบบและแอปพลิเคชันที่เกี่ยวข้อง พร้อมทั้งมีการแจ้งเตือนสถานะความปลอดภัยเมื่ออุปกรณ์เครือข่ายล้มเหลว
3) ต้องมีมาตรการควบคุมการใช้ซอฟต์แวร์หรือโปรแกรมเพื่อใช้ในการสอดส่องระบบเครือข่ายการสื่อสาร (Monitoring Tool) ที่อาจก่อให้เกิดการละเมิดการรักษาความปลอดภัย

3.7.6 การควบคุมสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Removable Media Handling)

1) จัดเก็บสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ที่มีข้อมูลสำคัญของบริษัทไว้ในสถานที่ที่ปลอดภัย และป้องกันการถูกเปิดเผยโดยไม่ได้รับอนุญาตไม่ว่าจะโดยเจตนาหรือไม่เจตนา
2) การจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ที่มีข้อมูลสำคัญของบริษัท ต้องทำโดยผู้ที่ได้รับอนุญาตเท่านั้น
3) การลบทำลายข้อมูลสำคัญของบริษัทในสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ต้องได้รับการอนุญาตการทำลายข้อมูลเป็นลายลักษณ์อักษรจากบริษัททุกครั้งก่อนการทำลาย ทั้งนี้การทำลายข้อมูลสำคัญต้องมีบันทึกไว้เป็นหลักฐานเพื่อใช้ในการตรวจสอบ

3.7.7 การจัดการข้อมูลแบบคลาวด์ (Cloud Storage)

1) กรณีมีการจัดเก็บข้อมูลแบบคลาวด์ต้องจัดเก็บข้อมูลเท่าที่จำเป็นและไม่ขัดต่อกฎหมายเท่านั้น
2) ต้องมีมาตรการควบคุมการเข้าถึงข้อมูล และเก็บบันทึกการเข้าถึง (Access Log) ที่จัดเก็บแบบคลาวด์ที่บริษัทกำหนดอย่างเหมาะสม

3.7.8 การรับส่งข้อมูล (Information Transfer)

3.7.8.1 นโยบายและข้อตกลงการรับส่งข้อมูล (Information Transfer Policies and Agreements)

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

ต้องมีการจัดทำข้อตกลงในการรับส่งข้อมูลระหว่างบริษัท รวมทั้งมีการควบคุมข้อมูลตามลำดับชั้นความลับอย่างเหมาะสม

3.7.8.2 การรับส่งสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายทางกายภาพ (Physical Removable Media in Transit)

ต้องมีการป้องกันการเข้าใช้งานสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายที่มีข้อมูลของบริษัทหรือนำไปใช้กับอุปกรณ์หรือเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต

3.7.8.3 การควบคุมการรับส่งข้อมูลในเครือข่าย

1) มีการเข้ารหัสข้อมูลที่ตามมาตรฐานที่บริษัทกำหนด ในการรับส่งที่มีความสำคัญผ่านระบบเครือข่าย โดยเฉพาะอย่างยิ่งข้อมูลที่ต้องติดต่อกับเครือข่ายภายนอก
2) ควรเปลี่ยนรหัสผ่านที่ใช้ในการป้องกันกุญแจของการเข้ารหัสทันทีที่ได้รับ และเปลี่ยนค่าใหม่ตามช่วงเวลาที่เหมาะสมเป็นประจำ
3) ควรมีการกำหนดหลักเกณฑ์ในการยืนยันความถูกต้องตรงกับข้อมูลต้นฉบับสำหรับข้อมูลที่เกี่ยวข้องทางด้านการอนุมัติทางการเงิน

3.7.8.4 การยืนยันความถูกต้องของข้อมูล

ระบบคอมพิวเตอร์ที่มีการรับส่งข้อมูล ต้องได้รับการตรวจสอบยืนยันความถูกต้องของข้อมูลที่รับส่งด้วยวิธีต่างๆ เช่น การตรวจสอบหมายเลขลำดับ หรือการตรวจสอบจำนวนข้อมูลที่รับส่ง เป็นต้น เพื่อให้มั่นใจว่าข้อมูลที่รับส่งมีความครบถ้วน รวมทั้งมีการเรียงลำดับอย่างถูกต้อง

3.7.9 การเฝ้าระวัง (Monitoring)

3.7.9.1 การจัดการการบันทึกข้อมูล Log (Managing Log Information)

1) ต้องมีการจัดเก็บ Activity Log ของผู้ดูแลระบบและผู้ปฏิบัติงานระบบ โดยต้องตรวจสอบ Log ที่บันทึกไว้อย่างสม่ำเสมอ โดยผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึง Log ดังกล่าวได้
2) ต้องมีการจัดเก็บ Audit Log ที่เก็บกิจกรรมของผู้ใช้งาน ข้อยกเว้นของการใช้งาน และเหตุการณ์ด้านความมั่นคงปลอดภัยข้อมูลของระบบที่สำคัญ ภายในระยะเวลาที่กฎหมายหรือข้อกำหนดการปฏิบัติงานกำหนด
3) ต้องมีการปกป้อง Log Facilities และข้อมูล Log จากการถูกปลอมแปลงและการเข้าถึงโดยไม่ได้รับอนุญาต
4) ต้องมีการจัดเก็บ Log ของอุปกรณ์หรือระบบที่สำคัญไว้ในสถานที่ที่ปลอดภัย

3.7.9.2 การเฝ้าระวังการใช้งานระบบ (Monitoring System Use)

1) ต้องมีการเก็บ Log และวิเคราะห์ความผิดพลาดของระบบที่มีสำคัญ รวมถึงต้องดำเนินการอย่างเหมาะสมเพื่อลดโอกาสที่จะเกิดเหตุการณ์ซ้ำ
2) การให้บริการและการบันทึกที่ได้จากระบบของบุคคลภายนอกต้องได้รับการตรวจสอบและทบทวนอย่างสม่ำเสมอ

3.7.9.3 การตั้งเทียบเวลาของระบบคอมพิวเตอร์และเครือข่าย

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

ต้องมีการตั้งเทียบเวลาของระบบคอมพิวเตอร์และเครือข่ายกับเวลามาตรฐาน โดยอ้างอิงจากแหล่งที่มาที่ได้มาตรฐาน ได้แก่ International Atomic Time (TAI) หรือ Coordinated Universal Time (UTC) เป็นต้น และกำหนดขั้นตอนในการตรวจสอบแก้ไขความคลาดเคลื่อนที่เกิดขึ้น

3.7.9.4 การตรวจจับผู้บุกรุกและการติดตามสืบค้น

1) ควรมีหลักเกณฑ์ที่ใช้พิจารณาทบทวนบันทึกของระบบคอมพิวเตอร์ต่างๆ เพื่อตรวจดูความพยายามหรือการละเมิดการรักษาความมั่นคงปลอดภัย โดยพิจารณาจากข้อมูลและข่าวสารที่เกี่ยวข้องกับช่องโหว่และการโจมตีทางด้านความมั่นคงปลอดภัยในระบบคอมพิวเตอร์และเครือข่าย ที่มาจากแหล่งต่างๆ เช่น เว็บไซต์ที่มีรายงานด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เผยแพร่โดยบริษัทผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์เจ้าของผลิตภัณฑ์กลุ่มแฮคเกอร์ (Hackers) องค์กรหรือหน่วยงานรัฐบาลที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อทำให้มั่นใจว่าความพยายามในการละเมิดหรือการละเมิดที่เกิดขึ้นแล้วนั้นได้รับการป้องกันและแก้ไขอย่างทันเวลา
2) บันทึกกิจกรรมของผู้ใช้ (user activity) ข้อผิดพลาด (exceptions) และเหตุการณ์ด้านความปลอดภัยสารสนเทศ (information security event) จะต้องถูกสร้างและเก็บรักษาไว้เป็นระยะเวลาน้อย 90 วัน

3.7.10 การบริหารจัดการแพทช์ (Patch Management)

1) ต้องมีการอัปเดตแพทช์ให้เป็นปัจจุบันเสมอ และต้องมีการตรวจสอบการนำซอฟต์แวร์แพทช์มาใช้ เพื่อลดการโจมตีช่องโหว่ที่อาจเกิดขึ้น โดยแหล่งที่มาของแพทช์ทั้งหมดต้องน่าเชื่อถือและถูกต้อง และแพทช์ต้องถูกต้องและสมบูรณ์ ทั้งนี้ก่อนการทำแพทช์ทั้งหมดต้องผ่านการทดสอบที่เหมาะสมก่อนที่จะประกาศใช้
2) มีการอัปเดทเฟิร์มแวร์ของเซิร์ฟเวอร์ อุปกรณ์ Network และ Appliance Box ที่เกี่ยวข้องกับความมั่นคงปลอดภัยเท่าที่ไม่ขัดกับการทำงานของระบบ ทั้งนี้ระบบใหม่ทั้งหมดต้องใช้แพทช์ปัจจุบัน หากมีข้อยกเว้นจะต้องมีการจัดทำแผนการดำเนินงานและแจ้งให้กับพนักงานผู้ดูแลโครงการของบริษัทรับทราบ พร้อมทั้งจัดทำมาตรการการควบคุมที่เหมาะสมเพื่อจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
3) อุปกรณ์ของบุคคลภายนอกที่ได้รับอนุญาต และมีความจำเป็นในการเชื่อมต่อกับบริษัท ต้องทำการอัปเดตแพทช์รวมถึงกำหนดค่า (Configuration) ก่อนการเชื่อมต่อ
4) ควรมีการสำรองข้อมูลก่อนการอัปเดตแพทช์ใดๆ เพื่อให้กู้คืนข้อมูลได้ในกรณีที่เกิดปัญหาขึ้น

3.8 การบริหารจัดการการควบคุมการเข้าถึง (Access Control Management)

3.8.1 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

3.8.1.1 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning)

1) กระบวนการการขอสิทธิการเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์
    - กรณีบุคคลภายนอกเป็นเจ้าของระบบคอมพิวเตอร์ บุคคลภายนอกต้องมีการกำหนดกระบวนการลงทะเบียนผู้ใช้งานและขอสิทธิการเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

- กรณีบุคคลภายนอกเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ของบริษัท ต้องปฏิบัติตามกระบวนการขออนุญาตและการลงทะเบียนผู้ใช้งานตามระเบียบการของบริษัท

2) กำหนดชื่อผู้ใช้งาน (User-ID) ของผู้ใช้งานและผู้ดูแลระบบ ด้วยหลักการ “หนึ่งคนต่อหนึ่งชื่อผู้ใช้งาน” เท่านั้น ห้ามกำหนดชื่อผู้ใช้งานในลักษณะที่เป็นชื่อเดียวกันหรือใช้ร่วมกันหลายคน
3) ต้องมีกระบวนการปรับปรุงสิทธิผู้ใช้งาน เมื่อผู้ใช้งานมีการเปลี่ยนแปลงบทบาทหน้าที่ในการปฏิบัติงาน
4) ต้องมีการกำหนดกระบวนการเพิกถอนหรือระงับสิทธิการเข้าถึงระบบและบริการของผู้ใช้งาน รวมทั้งดำเนินการตัดชื่อผู้ใช้ออกจากทะเบียนผู้ใช้งาน เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว ภายในระยะเวลาไม่เกิน 3 วันทำการหลังมีผลบังคับใช้

3.8.1.2 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Privilege Management)

1) การขอสิทธิใหม่และการเพิ่มเติมสิทธิการเข้าถึงระบบคอมพิวเตอร์และบริการ ต้องได้รับอนุญาตตามหน้าที่ความรับผิดชอบและเท่าที่จำเป็นต่อการปฏิบัติงาน (Least Privilege)
2) การขอใช้งานของชื่อผู้ใช้งาน (User-ID) ที่มีสิทธิพิเศษ เช่น ผู้ดูแลระบบ
   - กรณีบุคคลภายนอกเป็นเจ้าของระบบคอมพิวเตอร์ บุคคลภายนอกต้องมีการกำหนดวันหมดอายุ (Expired Date) ของสิทธิ และควรกำหนดชื่อผู้ใช้แยกสำหรับการตรวจสอบระบบประจำวัน (Monitoring) ที่ไม่จำเป็นต้องใช้สิทธิพิเศษ และกำหนดสิทธิเท่าที่จำเป็นต่อการตรวจสอบระบบประจำวันเท่านั้น
   - กรณีบุคคลภายนอกเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ของบริษัท บุคคลภายนอกจะได้รับอนุญาตให้ใช้เมื่อมีความจำเป็นจริง ๆ เท่านั้น ทั้งนี้บริษัทขอสงวนสิทธิการกำหนดวันหมดอายุครั้งละไม่เกิน 1 ปี ต้องผ่านการอบรมความรู้เรื่อง Centralized Remote System และผ่านการทดสอบก่อนสิทธิเข้าใช้งานในเกณฑ์ร้อยละ 90 ขึ้นไป
3) การเข้าใช้งานระบบที่มีข้อมูลสำคัญให้ใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication)

3.8.1.3 การระบุและการพิสูจน์ตัวตนผู้ใช้งาน (User Identification and Authentication)

1) มีการกำหนดบัญชีผู้ใช้งานให้กับบุคคลที่ได้รับอนุญาต เพื่อใช้งานระบบคอมพิวเตอร์ทั้งหมด โดยบัญชีผู้ใช้งานต้องไม่ซ้ำกัน (Unique-ID) และต้องสอดคล้องกับระดับความสำคัญของข้อมูลในระบบคอมพิวเตอร์ รวมทั้งระบบต้องมีความสามารถในการออกจากระบบโดยอัตโนมัติ เมื่อพ้นจากช่วงเวลาที่กำหนดไว้หลังจากสิ้นสุดการดำเนินการของผู้ใช้งาน
2) มีการป้องกันการเข้าถึงพื้นที่ที่จัดเก็บข้อมูลการพิสูจน์ตัวตนโดยไม่ได้รับอนุญาต และมีการบันทึก Log ของกระบวนการทั้งหมดที่เกิดขึ้นจากผู้ใช้งาน

3.8.1.4 การตั้งเวลาออกจากระบบอัตโนมัติ

ต้องมีการตั้งเวลาโดยบังคับให้ผู้ใช้งานออกจากระบบโดยอัตโนมัติ เมื่อถึงเวลาที่กำหนดหรือเมื่อผู้ใช้งานไม่ได้ใช้งานระบบภายในเวลาที่กำหนดไว้ โดยระบบที่เชื่อมต่อหรือ

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

ให้บริการข้อมูลสำคัญของบริษัทและข้อมูลส่วนบุคคลของลูกค้า มีระยะเวลาไม่เกิน 10 นาที สำหรับระบบอื่นใด มีระยะเวลาไม่เกิน 15 นาที

3.8.1.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

1) บุคคลภายนอกควรทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และระบบต้องแสดงให้เห็นถึงความซ้ำซ้อนหรือขัดแย้งของสิทธิการเข้าถึง โดยผู้ใช้งานที่ถูกยกเลิกสิทธิหรือไม่ได้ใช้งานต้องถูกลบจากระบบทันทีเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
2) ผู้มีหน้าที่รับผิดชอบต้องดูแลและตรวจสอบอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง เพื่อทำให้มั่นใจว่าไม่มีชื่อแสดงผู้ใช้งาน (User-ID) ที่ไม่ได้ใช้งานค้างอยู่ในระบบเป็นเวลานาน มีการให้ชื่อผู้ใช้งาน (User-ID) เก่ากับผู้ใช้งานรายใหม่ หรือโดยพิจารณาความเหมาะสม ตามจำเป็นและเพียงพอกับการใช้งานเท่านั้น รวมถึงปรับปรุงสิทธิผู้ใช้งานเมื่อผู้ใช้งานมีการเปลี่ยนแปลงบทบาทหน้าที่ในการปฏิบัติงานหรือได้รับสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
3) ผู้มีหน้าที่รับผิดชอบต้องทบทวนสิทธิของผู้ใช้งานอย่างสม่ำเสมอ และดำเนินการยกเลิกสิทธิการเข้าใช้งานของผู้ใช้งานทันที เมื่อผู้ใช้งานมีการเปลี่ยนแปลงบทบาทหน้าที่ในการปฏิบัติงานหรือลาออก

3.8.2 การบริหารจัดการรหัสผ่าน (Password Management)

3.8.2.1 การใช้งานรหัสผ่าน (Use of Password)

1) ต้องเปลี่ยนรหัสผ่านและรหัสอื่นใด เมื่อรหัสเก่าหมดอายุตามระยะเวลาที่กำหนดหรือเมื่อเห็นสมควรต้องทำการเปลี่ยนรหัสผ่าน
2) รหัสผ่านต้องไม่ถูกเก็บแบบข้อความที่ชัดเจน (Clear Text)
3) การแสดงผล (Display) และการพิมพ์รหัสผ่านจะต้องถูก mask หรือใช้วิธีการอื่นที่ปลอดภัย เพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตสังเกตเห็นรหัสผ่าน
4) รหัสผ่านต้องไม่ถูกกำหนดค่าตายตัว (Hard-Coded) ในระบบคอมพิวเตอร์ เว้นแต่จะมีการควบคุมทดแทนที่เหมาะสม (Mitigation Control)
5) การส่งรหัสผ่านต้องส่งในรูปแบบที่เข้ารหัส (Encrypted) และป้องกันการโจมตีจากผู้ไม่หวังดี
6) ห้ามใช้รหัสผ่านที่กำหนดขึ้นโดยระบบ (Default) ระบบต้องกำหนดให้ผู้ใช้เปลี่ยนรหัสผ่านทันที หลังจากที่เข้าใช้งานครั้งแรก หรือเมื่อมีการติดตั้งระบบใหม่ หรือปรับปรุงระบบคอมพิวเตอร์

3.8.2.2 การรักษาความปลอดภัยของรหัสผ่าน (Password) หรือชื่อผู้ใช้งาน (User-ID)

1) รหัสผ่าน (Password) และรหัสอื่นใดที่บริษัทกำหนดเป็นความลับส่วนตัว ซึ่งจะต้องเก็บรักษาไว้มิให้ผู้อื่นล่วงรู้ และห้ามใช้ร่วมกันกับบุคคลอื่น
2) การใช้งานรหัสผ่านต้องมีการกำหนดความยาวขั้นต่ำและอายุการใช้งานให้เป็นไปตามข้อกำหนดโดยแบ่งไปตามประเภทของกลุ่มผู้ใช้งาน ดังนี้
    - ระดับผู้ใช้งานกำหนดรหัสผ่านที่มีความยาวอย่างน้อย 12 ตัวอักษร และเปลี่ยนรหัสผ่านอย่างน้อยทุก 90 วัน

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

- ระดับผู้ดูแลระบบ (Privilege User) กำหนดรหัสผ่านที่มีความยาวอย่างน้อย 20 ตัวอักษร และเปลี่ยนรหัสผ่านอย่างน้อยทุก 90 วัน
- ระดับ User ที่ใช้ภายในระบบงานเพื่อให้บริการ (Service Account) กำหนดรหัสผ่านที่มีความยาวอย่างน้อย 30 ตัวอักษร และเปลี่ยนรหัสผ่านอย่างน้อยทุก 1 ปี

3) รหัสผ่านต้องมีลักษณะต่อไปนี้
   - ประกอบด้วยตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ เช่น @ หรือ #
   - ไม่มีลักษณะเป็นหมายเลขลำดับ (Running Number) เช่น 12345678
   - ไม่ใช้คำที่ง่ายต่อการคาดเดา หรือคำที่อยู่ในพจนานุกรม เช่น Password
   - ไม่ใช้รหัสผ่านซ้ำเดิมอย่างน้อย 5 ครั้ง
4) ระบบที่มีความสำคัญ ต้องได้รับการกำหนดให้ยอมรับความผิดพลาดของการป้อนรหัสผ่านไม่เกิน 5 ครั้ง หรือตามข้อกำหนดของกฎหมายต่างๆ ที่เกี่ยวข้อง ระเบียบปฏิบัติ และบริษัทประกาศให้ใช้ หากการป้อนรหัสผ่านไม่ถูกต้องในครั้งต่อไป ซึ่งเกินจากจำนวนครั้งที่กำหนด ระบบคอมพิวเตอร์ต้องระงับการใช้งานของผู้ใช้งานนั้นเป็นการชั่วคราวทันที
5) ระบบที่มีความสำคัญ ต้องสามารถตรวจสอบการกำหนดรหัสผ่านของผู้ใช้งานย้อนหลังได้ เพื่อป้องกันการนำรหัสผ่านเดิมกลับมาใช้ใหม่ โดยอย่างน้อยต้องสามารถตรวจสอบย้อนหลังได้ 5 ครั้ง หรือตามกำหนดของกฎหมายต่างๆที่เกี่ยวข้อง ระเบียบปฏิบัติ และบริษัทประกาศให้ใช้
6) ต้องมีมาตรการป้องกันมิให้มีการกำหนดรหัสผ่านที่ง่ายต่อการสุ่ม หรือคาดเดา เช่น การใช้รหัสผ่านด้วยชื่อสะกดของตนเอง การใช้รหัสผ่านเช่นเดียวกับชื่อแสดงผู้ใช้งาน หรือการปล่อยว่างไว้ เป็นต้น
7) ต้องมีการกำหนดวิธีที่ปลอดภัย ในการแจกจ่ายรหัสผ่านหรือชื่อผู้ใช้งาน (User-ID) ให้แก่ผู้ใช้งาน

3.8.3 การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

1) ต้องออกจากระบบ (Log-out, Log-off) ทุกระบบเมื่อไม่ได้ใช้งานเป็นเวลานาน และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นทันทีหลังเลิกงาน
2) มีการควบคุมทรัพย์สินสารสนเทศ เช่น กระดาษ สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้าย (Removable Storage Media) และการควบคุมหน้าจอการทำงานระบบ (Clear Screen Practice) เพื่อจัดการความเสี่ยงต่อข้อมูลสำคัญ
3) ต้องมีวิธีปฏิบัติในการทำลายสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้าย การทำลายข้อมูลอิเล็กทรอนิกส์ และแฟ้มข้อมูลในสื่ออิเล็กทรอนิกส์ที่เป็นมาตรฐานและไม่สามารถกู้กลับมาใช้ใหม่ได้

3.8.4 การควบคุมการเข้าถึง (Access Control)

3.8.4.1 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

1) ต้องมีการแบ่งแยกเครือข่าย (Network in Segregation) รวมทั้งมีมาตรการควบคุมความปลอดภัยที่เหมาะสม และกำหนดการใช้งานเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะระบบที่ได้รับอนุญาตเท่านั้น
2) การเข้าถึงเครือข่ายจากบุคคลภายนอกไปยังเครือข่ายอื่นๆ ของบริษัท ต้องถูกจำกัดเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น และต้องมีการยืนยันตัวบุคคลที่ปลอดภัยเพื่อป้องกันการปลอมแปลงแหล่งที่มา
3) ต้องมีการกำหนดรหัสผ่านที่ไม่ซ้ำกัน (Unique Password) หรือมีกลไกการควบคุมการเข้าถึงอื่นๆ ที่สอดคล้องกับมาตรฐานของบริษัท เพื่อควบคุมการเข้าถึงอุปกรณ์เครือข่ายภายในทั้งหมด รวมไปถึง เราเตอร์ (Routers) ไฟร์วอลล์ (Firewall) และเซิร์ฟเวอร์ (Server)
4) อุปกรณ์ที่เชื่อมต่อกับเครือข่ายต้องได้รับอนุญาตจากหน่วยงานผู้รับผิดชอบ โดยการเชื่อมต่อนั้นต้องได้รับการประเมินผลกระทบที่เกิดขึ้นและความเข้ากันได้ของเครือข่าย
5) บุคคลภายนอกที่เข้าถึงอุปกรณ์เครือข่ายต้องได้รับการพิสูจน์ตัวตนแบบหลายปัจจัยที่ปลอดภัย (Strong Multi-Factor Authentication)

3.8.4.2 Remote Access

1) การเข้าใช้งาน Remote Access ของบริษัท ต้องมีการพิสูจน์ตัวตนแบบหลายปัจจัยที่ปลอดภัย (Strong Multi-Factor Authentication) และมีการ log การเข้าใช้งานทั้งหมด
2) บุคคลภายนอกที่เข้าถึงต้องมีการจำกัดเฉพาะระบบ อุปกรณ์ และโปรโตคอลที่จำเป็นเพื่อสนับสนุนการทำงานให้ตรงตามสัญญาที่กำหนดไว้ กรณีที่มีการอนุญาตให้บุคคลภายนอก Remote Access ระบบต้องถูกเปิดให้ใช้งานเฉพาะช่วงเวลาที่ระบุไว้เท่านั้น
3) ผู้ที่ทำหน้าที่พัฒนาระบบ ได้รับอนุญาตให้เข้าใช้งานระบบที่ให้บริการจริง (Production System) ได้เท่าที่จำเป็นและเป็นครั้งคราวเท่านั้น ทั้งนี้การอนุญาตให้เข้าใช้งานระบบนั้นต้องระงับลงทันทีที่หมดความจำเป็น

3.8.4.3 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

1) การกำหนดสิทธิให้ผู้ที่สามารถใช้งานคำสั่ง ตั้งค่า เปลี่ยนแปลงข้อมูลโปรแกรม เครื่องมือ หรือกระทำการอื่นใดที่อาจมีความเสี่ยงต่อการใช้งานระบบคอมพิวเตอร์ โปรแกรม หรือข้อมูลได้นั้น ต้องพิจารณาอนุญาตตามความจำเป็นอย่างแท้จริงเท่านั้น โดยต้องให้สอดคล้องกับหน้าที่ในการปฏิบัติงานที่ได้รับมอบหมายด้วย
2) ต้องมีการกำหนดให้ยุติการใช้งานระบบ (Session Time-out) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง เพื่อป้องกันการเข้าถึงจากบุคคลภายนอกที่ไม่ได้รับอนุญาต
3) ควรจำกัดระยะเวลาการเชื่อมต่อระบบ (Restriction on Connection Time) เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบหรือแอปพลิเคชันที่มีความสำคัญ

3.8.4.4 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและข้อมูลสารสนเทศ (Application and Information Access Control)

1) มีการควบคุมการเข้าถึงข้อมูลสำคัญของบริษัท ซึ่งรวมถึง Program Source Code ทั้งหมดแบบเข้มงวด และข้อมูลต้องไม่ถูกเปิดเผย ดัดแปลง และลบอย่างไม่เหมาะสม

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

2) จำกัดกิจกรรมหรือข้อมูลส่วนตัวของผู้ใช้งานแต่ละบุคคลตามสิทธิ
3) มีการควบคุมทางกายภาพและสิ่งแวดล้อมที่เหมาะสมสำหรับระบบที่มีความสำคัญ

3.8.5 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกบริษัท (Mobile Computing and Teleworking)

3.8.5.1 การควบคุมอุปกรณ์คอมพิวเตอร์พกพาและการสื่อสาร

1) สำหรับอุปกรณ์คอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ส่วนตัว (Personal Computer and Mobile Device) ที่ใช้เพื่อวัตถุประสงค์ที่เกี่ยวข้องกับการทำงานและอุปกรณ์ที่ได้รับอนุญาตให้เชื่อมต่อโดยตรงหรือผ่านอุปกรณ์อื่นๆ ไปยังเครือข่ายของบริษัท ทั้งนี้อุปกรณ์ดังกล่าวต้องใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกกฎหมายและอัปเดตให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ และต้องได้รับการป้องกันโดยซอฟต์แวร์รักษาความปลอดภัย (Anti-Virus) ที่ได้รับอนุญาตจากบริษัท
2) ผู้ใช้งานทุกคนต้องตระหนักถึงการจัดเก็บข้อมูลของบริษัทในอุปกรณ์สื่อสารเคลื่อนที่ (Mobile Device) อย่างปลอดภัยอยู่เสมอ
3) ระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ รวมถึงให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกบริษัท (Mobile Computing and Teleworking)

3.8.5.2 การปฏิบัติงานจากภายนอกบริษัท (Teleworking)

ผู้ใช้งานที่ปฏิบัติงานจากภายนอกบริษัท (Telecommuters) ต้องปฏิบัติตามนโยบาย และขั้นตอนการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง รวมไปถึงการปฏิบัติตามข้อตกลงการใช้งานซอฟต์แวร์ (Software License Agreement) และการสำรองข้อมูล

3.9 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

3.9.1 ข้อกำหนดการรักษาความมั่นคงปลอดภัยสำหรับระบบ (Security Requirements for Systems)

1) การพัฒนาระบบคอมพิวเตอร์หรือแอปพลิเคชันต้องคำนึงถึงความปลอดภัยทางไซเบอร์ตั้งแต่ขั้นตอนการออกแบบและการตั้งค่า ตามหลักการของ Security by Design และ Security by Default
2) ผู้ดูแลโครงการทุกคนต้องทำให้มั่นใจว่าข้อกำหนดการรักษาความมั่นคงปลอดภัย รวมไปถึงการวิเคราะห์ด้านความมั่นคงปลอดภัย (Security Analysis) การประเมินความเสี่ยงด้านความมั่นคงปลอดภัย (Security Risk Assessment) การประเมินช่องโหว่ (Vulnerability Assessment) มีการรวบรวมไว้ใช้เป็นองค์ประกอบสำคัญสำหรับการจัดหา การพัฒนาหรือปรับปรุงระบบคอมพิวเตอร์ใหม่ ทั้งนี้การรักษาความมั่นคงปลอดภัยต้องนำมาใช้ตลอดทุกขั้นตอนของวงจรการพัฒนาระบบคอมพิวเตอร์
3) บุคคลภายนอกที่เกี่ยวข้องกับการพัฒนาซอฟต์แวร์ต้องผูกพันตามสัญญาที่ได้อนุมัติและลงนามแล้ว ทั้งนี้การพัฒนาซอฟต์แวร์จากบุคคลภายนอกทั้งหมดต้องปฏิบัติตาม*มาตรฐานการพัฒนา*

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

*ซอฟต์แวร์*ของบริษัท และข้อกำหนดการรักษาความมั่นคงปลอดภัยที่เทียบเท่ากับข้อกำหนดบริษัท

3.9.2 การประมวลผลบนแอปพลิเคชัน (Correct Processing in Applications)

1) ระบุข้อกำหนดสำหรับการรับรองความถูกต้องและความสมบูรณ์ของข้อมูลในแอปพลิเคชัน โดยข้อกำหนดต้องถูกควบคุมและดำเนินการอย่างเหมาะสม
2) ข้อมูลที่นำเข้า และส่งออก จากแอปพลิเคชันต้องมีการตรวจสอบเพื่อทำให้มั่นใจว่าข้อมูลเหล่านั้นมีความถูกต้องและเหมาะสม และต้องอยู่ภายใต้การดำเนินงานหรือกิจกรรมที่บริษัทกำหนดเท่านั้น

3.9.3 การควบคุมการเข้ารหัส (Cryptographic Controls)

1) ต้องมีการบริหารจัดการการเข้ารหัสคีย์ (Cryptographic Key Management) เพื่อให้สอดคล้องกับเทคนิคการเข้ารหัส อ้างอิงตาม*ข้อ 3.3.2 การเข้ารหัสข้อมูล (Data Encryption)*
2) ต้องมีการควบคุมการเข้ารหัส (Cryptographic Control) ระบบคอมพิวเตอร์ที่จัดอยู่ในชั้นความลับสูงสุดอย่างเหมาะสม อ้างอิงตาม*ข้อ 3.3.2 การเข้ารหัสข้อมูล (Data Encryption)*
3) ควรจำกัดการเข้าถึงคีย์ที่ใช้ในการเข้ารหัส (Encryption Key) อย่างเคร่งครัด ผู้ที่รับผิดชอบในการบริหารจัดการคีย์ที่สำคัญ ต้องผ่านกระบวนการตรวจสอบประวัติ การตรวจสอบความมั่นคงปลอดภัยการดำเนินงาน และการลงนามในข้อตกลงการไม่เปิดเผยข้อมูลข่าวสารแล้วเท่านั้น

3.9.4 การรักษาความมั่นคงปลอดภัย System File (Security of System Files)

1) บริษัทไม่อนุญาตให้ติดตั้งซอฟต์แวร์ที่ไม่เหมาะสมหรือไม่ได้รับอนุญาตบนระบบคอมพิวเตอร์โดยเด็ดขาด
2) ต้องมีการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยของ System File เช่น การเข้ารหัสข้อมูล (Data Encryption) การควบคุมการเข้าถึง (Access Control) เพื่อป้องกันและควบคุมการรั่วไหลของข้อมูลสำคัญ
3) การติดตั้งหรือการอัปเดตซอฟต์แวร์ และ Program Library ต้องดำเนินการโดยพนักงานที่ได้รับอนุญาต รวมถึงต้องดำเนินการผ่าน การบริหารจัดการการเปลี่ยนแปลง (Change Management)

3.9.5 การรักษาความมั่นคงปลอดภัยในการพัฒนา และกระบวนการสนับสนุน (Security in Development and Support Processes)

3.9.5.1 การตรวจสอบทางเทคนิคของแอปพลิเคชันหลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Application After Operating System Changes)

1) การเปลี่ยนแปลงระบบปฏิบัติการและแอปพลิเคชันที่สำคัญต้องมีการทดสอบอย่างเหมาะสม เพื่อทำให้มั่นใจว่าไม่มีผลกระทบต่อความมั่นคงปลอดภัยหรือการดำเนินงานของบริษัท
2) บุคคลภายนอกต้องทำการสื่อสารการเปลี่ยนแปลงทั้งหมดของระบบให้พนักงานผู้ดูแลโครงการของบริษัทรับทราบ

3.9.5.2 ข้อจำกัดเกี่ยวกับการเปลี่ยนแปลงแพ็คเกจซอฟต์แวร์ (Restriction on Change to Software Package)

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

มีการควบคุมและอนุมัติความเสี่ยงที่เกี่ยวข้องกับการเปลี่ยนแปลงแพ็คเกจซอฟต์แวร์อย่างเหมาะสม

3.9.6 การบริหารจัดการช่องโหว่ และการทดสอบเจาะระบบ (Vulnerability Management & penetration testing)

1) ต้องมีการตั้งค่าความปลอดภัยของระบบ (System Hardening) เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ให้ครอบคลุมระบบที่สำคัญทั้งหมด
2) ต้องมีการประเมินเพื่อหาช่องโหว่ระบบคอมพิวเตอร์ที่เชื่อมต่อกับเครือข่าย กรณีที่พบช่องโหว่ต้องได้รับการประเมินรวมถึงจัดทำมาตรการการควบคุมที่เหมาะสมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
3) ต้องแจ้งแผนการดำเนินการรวมถึงเครื่องมือที่ใช้ในการดำเนินการแก่พนักงานผู้ดูแลโครงการของบริษัทและได้รับอนุญาตเป็นลายลักษณ์อักษรจากบริษัท ทุกครั้งก่อนทำการตรวจสอบช่องโหว่และทดสอบเจาะระบบ
4) บริษัทขอสงวนสิทธิ์ในการประเมินช่องโหว่และทดสอบการเจาะระบบ รวมถึงกิจกรรมอื่นใดที่เกี่ยวข้องกับการจำลองการโจมตี อาทิ Red Team Exercise, Attack Surface monitoring ในระบบที่มีการให้บริการลูกค้า โดยมิต้องแจ้งล่วงหน้า
5) ต้องทำการตรวจสอบหาช่องโหว่และทดสอบเจาะระบบอย่างสม่ำเสมอตามเกณฑ์ หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ (Major Change) กับทุกระบบที่เชื่อมต่ออินเทอร์เน็ต เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและเพื่อประเมินความมั่นคงปลอดภัยโดยรวม โดยบริษัทมีการกำหนดความถี่ในการตรวจสอบหาช่องโหว่และทดสอบการเจาะระบบ ไว้ดังต่อไปนี้

ประเภทของระบบ	การตรวจสอบหาช่องโหว่	การทดสอบเจาะระบบ
ระบบที่มีระดับความสำคัญสูง/นัยสำคัญ	1 ครั้ง/ปี	1 ครั้ง/ปี
ระบบที่มีระดับความสำคัญระดับปานกลาง	1 ครั้ง/ 24 เดือน	1 ครั้ง/ 24 เดือน
ระบบที่มีระดับความสำคัญระดับต่ำ	1 ครั้ง/ 36 เดือน	1 ครั้ง/ 36 เดือน
ระบบที่เกี่ยวข้องกับ PCI DSS	4 ครั้ง/ปี (Quarterly)	1 ครั้ง/ปี
ระบบที่เกี่ยวข้องกับ CSA Star	1 ครั้ง/ปี	1 ครั้ง/ปี
ระบบที่เกี่ยวข้องกับ ISO	1 ครั้ง/ปี	1 ครั้ง/ปี
ระบบที่ถูกกำกับโดยธนาคารแห่งประเทศไทย (ธปท.)	1 ครั้ง/ปี	1 ครั้ง/ปี
ระบบที่เกี่ยวข้องกับ NDID และ Public IdP	1 ครั้ง/ปี	1 ครั้ง/ปี

6) หากพบช่องโหว่จากการตรวจสอบหาช่องโหว่และทดสอบเจาะระบบ ต้องดำเนินการแก้ไขตามมาตรฐานของบริษัท ดังนี้
   - กรณีเป็นระบบคอมพิวเตอร์/แอปพลิเคชัน/ฟีเจอร์ใหม่ จะสามารถขึ้น Production ได้ต้องดำเนินการดังต่อไปนี้

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

Critical / High severity	Medium Severity	Low Severity
ต้องแก้ไขให้แล้วเสร็จก่อน	1.ส่งแผนการแก้ไขช่องโหว่ให้พนักงานผู้ดูแลโครงการของบริษัท ภายใน 15 วัน นับตั้งแต่วันที่ได้รับผลตรวจสอบล่าสุด 2.แก้ไขช่องโหว่ให้แล้วเสร็จภายใน 60 วัน นับตั้งแต่วันที่ได้รับผลตรวจสอบล่าสุด กรณีเมื่อถึงเวลาตามแผน แต่ยังไม่สามารถแก้ไขช่องโหว่ที่เกิดขึ้นได้ ต้องแจ้งพนักงานผู้ดูแลโครงการของบริษัท เพื่อเข้าสู่กระบวนการยอมรับความเสี่ยงที่เกิดขึ้นในอนาคต (Risk Acceptance Form)	1. ส่งแผนการแก้ไขช่องโหว่ให้พนักงานผู้ดูแลโครงการของบริษัท ภายใน 15 วัน นับตั้งแต่วันที่ได้รับผลตรวจสอบล่าสุด 2. แก้ไขให้แล้วเสร็จภายใน 90 วัน นับตั้งแต่วันที่ได้รับผลตรวจสอบล่าสุด กรณีเมื่อถึงเวลาตามแผน แต่ยังไม่สามารถแก้ไขช่องโหว่ที่เกิดขึ้นได้ ต้องแจ้งพนักงานผู้ดูแลโครงการของบริษัท เพื่อเข้าสู่กระบวนการยอมรับความเสี่ยงที่เกิดขึ้นในอนาคต (Risk Acceptance Form)

- <u>กรณีพบช่องโหว่จากการตรวจสอบช่องโหว่และเจาะทดสอบระบบตามรอบที่บริษัทกำหนด</u> ต้องดำเนินการดังต่อไปนี้

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

Critical / High severity	Medium Severity	Low Severity
1. ส่งแผนการแก้ไขช่องโหว่ให้พนักงานผู้ดูแลโครงการของบริษัท ภายใน 15 วัน นับตั้งแต่วันที่ได้รับผลตรวจสอบล่าสุด 2.แก้ไขช่องโหว่ให้แล้วเสร็จภายใน 45 วัน นับตั้งแต่วันที่ได้รับผลตรวจสอบล่าสุด กรณีเมื่อถึงเวลาตามแผนแต่ยังไม่สามารถแก้ไขช่องโหว่ที่เกิดขึ้นได้ ต้องแจ้งพนักงานผู้ดูแลโครงการของบริษัท เพื่อเข้าสู่กระบวนการยอมรับความเสี่ยงที่เกิดขึ้นในอนาคต (Risk Acceptance Form)	1.ส่งแผนการแก้ไขช่องโหว่ให้พนักงานผู้ดูแลโครงการของบริษัท ภายใน 15 วัน นับตั้งแต่วันที่ได้รับผลตรวจสอบล่าสุด 2.แก้ไขช่องโหว่ให้แล้วเสร็จภายใน 60 วัน นับตั้งแต่วันที่ได้รับผลตรวจสอบล่าสุด กรณีเมื่อถึงเวลาตามแผน แต่ยังไม่สามารถแก้ไขช่องโหว่ที่เกิดขึ้นได้ ต้องแจ้งพนักงานผู้ดูแลโครงการของบริษัท เพื่อเข้าสู่กระบวนการยอมรับความเสี่ยงที่เกิดขึ้นในอนาคต (Risk Acceptance Form)	1.ส่งแผนการแก้ไขช่องโหว่ให้พนักงานผู้ดูแลโครงการของบริษัท ภายใน 15 วัน นับตั้งแต่วันที่ได้รับผลตรวจสอบล่าสุด 2.แก้ไขให้แล้วเสร็จภายใน 90 วัน นับตั้งแต่วันที่ได้รับผลตรวจสอบล่าสุด กรณีเมื่อถึงเวลาตามแผนแต่ยังไม่สามารถแก้ไขช่องโหว่ที่เกิดขึ้นได้ ต้องแจ้งพนักงานผู้ดูแลโครงการของบริษัท เพื่อเข้าสู่กระบวนการยอมรับความเสี่ยงที่เกิดขึ้นในอนาคต (Risk Acceptance Form)

3.10 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Incident Management)

1) ต้องกำหนดกระบวนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ รวมทั้งจัดทำเอกสารขั้นตอนการปฏิบัติ โดยครอบคลุมการจัดระดับความสำคัญ และโครงสร้างการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ไปยังหน่วยงานที่เกี่ยวข้อง และต้องสื่อสารกับพนักงานรวมถึงบุคคลภายนอกที่เกี่ยวข้อง
2) ต้องมีการจัดทำแผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับความเสี่ยงที่เกี่ยวข้อง และนำไปสื่อสาร ฝึกอบรม ให้กับผู้ที่เกี่ยวข้องอย่างเหมาะสม
3) ต้องมีเครื่องมือและเทคนิคที่ปลอดภัยในการตรวจสอบเหตุการณ์บนระบบคอมพิวเตอร์ การตรวจจับการโจมตี และการแสดงการใช้งานระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต
4) ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ
5) ต้องกำหนดเจ้าที่ผู้รับผิดชอบทางด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อย 1 ท่าน เพื่อเป็นผู้ประสานงานและแจ้งให้บริษัททราบในกรณีที่พบเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และ

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)
414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

ประสานงานกับพนักงานของบริษัทในกรณีที่บริษัทเป็นผู้พบเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่มีส่วนเกี่ยวข้องกับบุคคลภายนอก

6) กรณีพบเหตุละเมิดด้านความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบกับบริษัท บุคคลภายนอกต้องแจ้งเหตุการณ์ละเมิดฯ พร้อมทั้งรายละเอียดเท่าที่มีของเหตุการณ์นั้นให้บริษัทรับทราบโดยไม่ชักช้า ภายในระยะเวลาไม่เกิน 12 ชั่วโมง และเมื่อมีความคืบหน้าหรือมีข้อมูลเพิ่มเติม ให้แจ้งแก่บริษัทเป็นระยะ และรีบจัดทำรายละเอียดของหนังสือแจ้งเตือนที่สมบูรณ์ให้แก่บริษัทโดยเร็ว

3.11 การจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)

1) จัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Disaster Recovery Plan) ที่ครอบคลุมถึงการให้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก เพื่อให้มีแนวทางรองรับและสามารถให้บริการและดำเนินธุรกิจได้อย่างต่อเนื่อง
2) แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรคำนึงถึงความเสี่ยงที่อาจส่งผลต่อการหยุดชะงักของการให้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ผลกระทบที่มีต่อการให้บริการ และการติดต่อสื่อสารระหว่างบุคคลภายนอกกับบริษัท รวมถึงการรายงานเหตุการณ์ผิดปกติให้บริษัททราบอย่างทันการณ์
3) มีการทดสอบและปรับปรุงแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ที่ครอบคลุมถึงการให้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก อย่างน้อยปีละ 1 ครั้ง
4) บุคคลภายนอกต้องสนับสนุนหรือมีส่วนร่วมกับการทดสอบการซักซ้อมแผนการทำธุรกิจอย่างต่อเนื่อง (Business Continuity Plan Testing) ของบริษัท

3.12 กฎหมายและข้อบังคับที่เกี่ยวข้อง (Regulatory and Compliance)

1) บุคคลภายนอกต้องปฏิบัติตามข้อกำหนดทางกฎหมาย กฎระเบียบข้อบังคับที่เกี่ยวข้องกับการให้บริการบริษัท ทั้งด้านความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล กฎระเบียบข้อบังคับของหน่วยงานกำกับดูแลของบริษัท รวมถึงกฎหมายอื่น และสัญญาที่เกี่ยวข้อง
2) บุคคลภายนอกต้องเก็บรักษาข้อมูลทางธุรกิจ (Business Information) ไว้ตามที่กฎหมาย ข้อบังคับ รวมถึงสัญญาที่เกี่ยวข้องกำหนด เพื่อวัตถุประสงค์ทางธุรกิจก่อนที่จะทำลายข้อมูล
3) บุคคลภายนอกต้องรักษาความลับข้อมูลตามข้อตกลง (Non-Disclosure Agreement) เพื่อวัตถุประสงค์ทางธุรกิจที่จะไม่เปิดเผยความลับข้อมูลต่อผู้อื่นและสาธารณชน

วันที่มีผล: ตั้งแต่วันที่ 15 กรกฎาคม 2567 เป็นต้นไป