บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)

414 เอไอเอส ทาวเวอร์ ถนนพหลโยธิน สามเสนใน พญาไท กทม. 10400

มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับบุคคลภายนอก (Cyber Security Standard for Third Party)

กลุ่มเอไอเอส

เวอร์ชัน: 2.0

เจ้าของเอกสาร: Cyber Security

วันที่มีผล: 25 สิงหาคม 2569

สารบัญ

1. บทนำ 4

1.1 วัตถุประสงค์ 4
1.2 ขอบเขต 4
1.3 คำจำกัดความ 4
1.4 ข้อยกเว้น 7
1.5 บทลงโทษ 7

2. หน้าที่และความรับผิดชอบ 8

2.1 พนักงานผู้ดูแลโครงการของบริษัท 8
2.2 บุคคลภายนอก 8

3. มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ 8

3.1 กฎหมายและข้อบังคับที่เกี่ยวข้อง (REGULATORY AND COMPLIANCE) 8
3.2 การบริหารจัดการทรัพยากรบุคคล (HUMAN RESOURCE MANAGEMENT) 9
3.3 การบริหารจัดการการรับเหมาช่วง (SUB-CONTRACT MANAGEMENT) 9
3.4 การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (CYBER SECURITY RISK MANAGEMENT) 10
3.5 การบริหารจัดการทรัพย์สิน (ASSET MANAGEMENT) 10
3.6 การบริหารจัดการช่องโหว่ทางเทคนิค (MANAGEMENT OF TECHNICAL VULNERABILITIES) 11
3.7 การรักษาความมั่นคงปลอดภัยทางกายภาพและอุปกรณ์ (PHYSICAL AND EQUIPMENT SECURITY) 13
3.8 การบริหารจัดการการควบคุมการเข้าถึง (ACCESS CONTROL MANAGEMENT) 14
3.8.1 การบริหารจัดการอัตลักษณ์และการเข้าถึง (Identity and Access Management) 14
3.8.2 การบริหารจัดการรหัสผ่าน (Password Management) 15
3.8.3 การปฏิบัติงานจากระยะไกล (Remote Access) 17
3.8.4 การควบคุมการเข้าถึงเครือข่าย (Network Access Control) 17
3.8.5 การเข้าถึงซอร์สโค้ด (Access to Source Code) 17
3.9 การบริหารจัดการอุปกรณ์ปลายทางอย่างปลอดภัย (ENDPOINT SECURITY MANAGEMENT) 18
3.9.1 การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen) 18
3.9.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection Against Malicious Software) 18
3.9.3 ซอฟต์แวร์ลิขสิทธิ์ (Software Licensing) 18
3.9.4 การควบคุมอุปกรณ์พกพาและการปฏิบัติงานจากภายนอกบริษัท (Mobile Computing and Teleworking) 19
3.10 การบริหารจัดการความเปลี่ยนแปลง (CHANGE MANAGEMENT) 19
3.11 การบริหารจัดการแอปพลิเคชันอย่างปลอดภัย (APPLICATION SECURITY MANAGEMENT) 20
3.11.1 ข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชัน (Application Security Requirements) 20
3.11.2 การเขียนชุดคำสั่งอย่างปลอดภัย (Secure Coding) 21
3.11.3 การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริงออกจากกัน (Separation of Development, Test and Production Environments) 21

3.11.4 การตั้งเวลาออกจากระบบโดยอัตโนมัติ 21
3.11.5 การจัดการ API และส่วนประกอบจากบุคคลภายนอก (API and Third Party Component Security) 21
3.12 การบริหารจัดการความปลอดภัยของข้อมูล (DATA SECURITY MANAGEMENT) 22
3.12.1 การจัดชั้นความลับและการควบคุมดูแลข้อมูล (Data Classification and Handling) 22
3.12.2 การเข้ารหัสข้อมูล (Data Encryption) 22
3.12.3 การเก็บรักษาข้อมูล (Data at Rest) 23
3.12.4 การโอนข้อมูล (Data in Transit) 23
3.12.5 การสำรองและกู้คืนข้อมูล (Data Backup and Restoration) 24
3.12.6 การลบทำลายข้อมูล (Information Disposal) 24
3.12.7 การใช้งานข้อมูลสำหรับการทดสอบระบบ (Test Information) 25
3.13 การบริหารจัดการความมั่นคงปลอดภัยโครงสร้างพื้นฐาน (INFRASTRUCTURE SECURITY MANAGEMENT) 25
3.13.1 การบริหารความมั่นคงปลอดภัยคลาวด์ (Cloud Security Management) 25
3.13.2 การบริหารความมั่นคงปลอดภัยเครือข่าย (Network Security Management) 26
3.13.3 การตรวจสอบและบันทึกเหตุการณ์ (Logging and Monitoring) 26
3.13.4 การบริหารจัดการระบบ (System Management) 28
3.14 การบริหารจัดการด้านความปลอดภัยการใช้งานปัญญาประดิษฐ์ (ARTIFICIAL INTELLIGENCE SECURITY MANAGEMENT) 29
3.15 การสร้างความตระหนักรู้และการอบรม (AWARENESS, EDUCATION AND TRAINING) 30
3.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (CYBER SECURITY INCIDENT MANAGEMENT) 30
3.17 การจัดการความต่อเนื่องทางธุรกิจ (BUSINESS CONTINUITY MANAGEMENT) 31

มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับบุคคลภายนอก

1. บทนำ

1.1 วัตถุประสงค์

1) เพื่อกำหนดมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับการควบคุมและกำกับดูแลบุคคลภายนอกที่มีการเชื่อมต่อ เข้าถึง ใช้บริการ หรือปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ ระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศของบริษัท รวมถึงผู้ให้บริการภายนอก คู่ค้า ผู้รับจ้าง ผู้รับจ้างช่วง หรือบุคคลใด ๆ ที่ปฏิบัติงานให้บริการ หรือดำเนินการในนามของบริษัท
2) เพื่อป้องกันระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศของบริษัทจากการบุกรุก โจมตี ขโมย ทำลาย แทรกแซงการทำงาน โปรแกรมไม่พึงประสงค์ ภัยคุกคามทางไซเบอร์ หรือการดำเนินงานของบุคคลภายนอกที่อาจก่อให้เกิดความเสียหายต่อการดำเนินธุรกิจของบริษัท
3) เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ความปลอดภัยของระบบสารสนเทศ และความปลอดภัยของข้อมูลสารสนเทศของบริษัท ที่อาจเกิดจากการเชื่อมต่อ การเข้าถึง การใช้บริการ หรือการปฏิบัติงานของบุคคลภายนอก
4) เพื่อให้การดำเนินงาน การให้บริการ หรือการปฏิบัติงานของบุคคลภายนอกที่เกี่ยวข้องกับบริษัทเป็นไปอย่างมั่นคงปลอดภัย สอดคล้องกับข้อกำหนดของบริษัท กฎหมาย กฎระเบียบ ข้อผูกพันตามสัญญา และมาตรฐานที่เกี่ยวข้อง

1.2 ขอบเขต

มาตรฐานฉบับนี้ครอบคลุมถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ ความปลอดภัยของระบบสารสนเทศ และความปลอดภัยของข้อมูลสารสนเทศของบริษัท จากการใช้บริการ การเชื่อมต่อ การเข้าถึงระบบหรือข้อมูลสารสนเทศ ตลอดจนการปฏิบัติงานหรือการให้บริการโดยบุคคลภายนอก ผู้ให้บริการ คู่ค้า ผู้รับจ้าง หรือผู้รับจ้างช่วงที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของบริษัท หรือดำเนินงานในนามของบริษัท

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) **“ข้อมูลสารสนเทศ (Information)”** หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่าง ๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือ หรืออุปกรณ์ใด ๆ
4) **“ข้อมูลสำคัญ (Sensitive Information)”** หมายถึง ข้อมูลสารสนเทศที่สำคัญที่อาจส่งผลกระทบต่อการดำเนินธุรกิจของบริษัท ข้อมูลที่อยู่ภายใต้ข้อกำหนดของกฎหมาย รวมถึงข้อมูลส่วนบุคคล ซึ่งต้องได้รับการปกป้องและไม่สามารถเปิดเผยต่อบุคคลอื่นหรือใช้ในวัตถุประสงค์อื่นที่ไม่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัท การรั่วไหลของข้อมูลเหล่านี้อาจส่งผลกระทบต่อประสิทธิภาพการดำเนินงาน ทำให้การดำเนินธุรกิจหยุดชะงัก หรือเป็นเหตุให้บริษัทเสื่อมเสียชื่อเสียง
5) “**อัตลักษณ์ทางดิจิทัล”** หรือ **“ดิจิทัลไอดี (Digital Identity)**” หมายถึง ชุดข้อมูลหรือคุณลักษณะในรูปแบบดิจิทัลที่ถูกสร้าง จัดเก็บ และบริหารจัดการโดยบริษัท หรือโดยบุคคลภายนอกตามที่เกี่ยวข้องกับการให้บริการแก่บริษัท เพื่อใช้ในการระบุและยืนยันตัวตนของบุคคล ผู้ใช้งาน ระบบ แอปพลิเคชัน หรืออุปกรณ์ ภายใต้สภาพแวดล้อมดิจิทัลของบริษัท โดยดิจิทัลไอดีเป็นองค์ประกอบพื้นฐานของกระบวนการพิสูจน์ตัวตน (Authentication) การกำหนดและควบคุมสิทธิการเข้าถึง (Authorization) และการบริหารจัดการตัวตนและการเข้าถึงระบบ (Identity and Access Management: IAM) รวมถึงรองรับการดำเนินธุรกรรมทางอิเล็กทรอนิกส์อย่างมั่นคงปลอดภัยและเชื่อถือได้
6) **"ประเภทของอัตลักษณ์ (Identity Type)"** หมายถึง การแบ่งแยกลักษณะของบุคคลหรือสิ่งใดสิ่งหนึ่งที่บันทึกในรูปแบบอิเล็กทรอนิกส์ ได้แก่ พนักงาน บุคคลภายนอก ระบบ แอปพลิเคชัน อุปกรณ์ หรือ RPA (Robotic Process Automation) ตามบริบทของการให้บริการแก่บริษัท
7) “**บัญชีผู้ใช้ (Account)**” หมายถึง ชื่อผู้ใช้งาน (User-ID) สำหรับเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท ไม่ว่าจะเป็นบัญชีผู้ใช้งานของพนักงาน บัญชีผู้ใช้งานภายนอก (Third Party Account) บัญชีผู้ใช้งานร่วม (Shared Account) บัญชีผู้ใช้งานกลาง (Central Account) รวมถึง Non-Human Account เช่น บัญชี RPA (Robotic Process Automation)
8) “**บัญชีผู้ใช้ร่วม (Shared Account)**” หมายถึง บัญชีผู้ใช้ที่ถูกใช้งานร่วมกันมากกว่าหนึ่งคน โดยใช้ข้อมูลการยืนยันตัวตนเดียวกัน เช่น ชื่อผู้ใช้และรหัสผ่านเดียวกัน
9) “**บัญชีผู้ใช้กลาง (Central Account)**” หมายถึง บัญชีผู้ใช้กลางที่บริษัทกำหนดขึ้นอย่างเป็นทางการ เพื่อใช้ในการบริหาร ควบคุม กำกับดูแล หรือใช้อ้างอิงเป็นตัวแทนของระบบ (System Identity) โดยมีวัตถุประสงค์และการใช้งานในลักษณะเฉพาะตามที่กำหนดไว้ และมีกระบวนการควบคุมสิทธิการเข้าถึงและการตรวจสอบอย่างเหมาะสม
10) “**บัญชีผู้ใช้สำหรับบริการระบบ (Service Account)**” หมายถึง บัญชีผู้ใช้ที่ถูกสร้างขึ้นเพื่อให้ระบบ แอปพลิเคชัน หรือบริการต่าง ๆ ที่เกี่ยวข้องกับการให้บริการแก่บริษัท ใช้สำหรับการยืนยันตัวตน (Authentication) และการกำหนดสิทธิการเข้าถึงทรัพยากรภายในระบบสารสนเทศของบริษัท โดยบัญชีดังกล่าวจะต้องไม่ถูกใช้งานโดยตรงโดยผู้ใช้งานที่เป็นบุคคล (Non-Interactive Account) แต่ถูกกำหนดขึ้นเพื่อรองรับการทำงานของกระบวนการอัตโนมัติหรือการสื่อสารระหว่างระบบเท่านั้น

11) “**ประเภทของผู้ใช้งาน (User Type)**” หมายถึง การแบ่งแยกผู้ใช้งานแบ่งตามระดับสิทธิการเข้าถึงระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท หรือระบบที่เกี่ยวข้องกับการให้บริการแก่บริษัท ได้แก่ ผู้ใช้งานทั่วไป (User Level) ผู้ใช้งานสิทธิการเข้าถึงระดับสูง (Privileged Level) และผู้ใช้งานระดับบัญชีบริการ (Service Account Level)
12) “**สิทธิการเข้าถึงขั้นพื้นฐาน (Birthright Access)”** หมายถึง สิทธิการเข้าถึงที่มอบให้พนักงานหรือบุคคลภายนอกตามหน้าที่และความรับผิดชอบเมื่อมีการสร้างดิจิทัลไอดีและบัญชีผู้ใช้ในระบบ เพื่อใช้สำหรับการปฏิบัติงานตามที่ได้รับอนุญาต
13) “**หลักความจำเป็นในการรู้ข้อมูล (Need to Know basis)”** หมายถึง หลักการเปิดเผยข้อมูลลับหรือข้อมูลสำคัญของบริษัท เฉพาะผู้ใช้งานข้อมูลที่มีหน้าที่ที่เกี่ยวข้อง หรือจำเป็นต้องรับรู้ข้อมูลเหล่านั้นเพื่อที่ปฏิบัติงานที่ได้รับอนุญาตเท่านั้น
14) “**การให้สิทธิเท่าที่จำเป็น (Least Privilege)”** หมายถึง การให้สิทธิการเข้าใช้งานระบบคอมพิวเตอร์และเข้าถึงข้อมูลสารสนเทศตามความจำเป็นต่อการปฏิบัติงานเท่านั้น
15) “**การยืนยันตัวตน (Authentication)”** หมายถึง กระบวนการยืนยันอัตลักษณ์ด้วยการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน
16) “**ระบบคอมพิวเตอร์ (Computer System)"** หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้งฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสายและไร้สาย วัสดุอุปกรณ์การเก็บรักษา และการถ่ายโอนข้อมูลชนิดต่าง ๆ ระบบอินเทอร์เน็ต (Internet) และระบบอินทราเน็ต (Intranet) รวมถึงอุปกรณ์ไฟฟ้า และสื่อสารโทรคมนาคมต่าง ๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือคล้ายคลึงกับคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของบริษัท ของบริษัทคู่ค้า และบริษัทอื่นที่อยู่ระหว่างการติดตั้ง และยังไม่ได้ส่งมอบ หรือของพนักงานที่นำเข้ามาติดตั้ง หรือใช้งานภายในสถานประกอบการของบริษัท
17) “**ระบบที่มีความสำคัญ (Critical System)”** หมายถึง ระบบสารสนเทศ แอปพลิเคชัน โครงสร้างพื้นฐานด้านเทคโนโลยี หรือระบบใดๆ ที่มีบทบาทสำคัญต่อการดำเนินธุรกิจ การให้บริการ การปฏิบัติตามกฎหมายและข้อกำหนด รวมถึงความมั่นคงปลอดภัยและชื่อเสียงขององค์กร หากระบบดังกล่าวหยุดชะงัก เสียหาย ถูกละเมิด หรือไม่สามารถใช้งานได้ อาจส่งผลกระทบอย่างมีนัยสำคัญต่อบริษัททั้งในด้านการดำเนินงาน การเงิน กฎหมาย และความเชื่อมั่นของผู้มีส่วนได้เสีย
18) “**สภาพแวดล้อมที่ให้บริการจริง (Production Environment)**” หมายถึง สภาพแวดล้อมที่ใช้ในการให้บริการจริงของบริษัท ซึ่งรองรับข้อมูลจริงขององค์กรและลูกค้า สภาพแวดล้อมนี้ต้องมีการควบคุมความมั่นคงปลอดภัยที่เข้มงวดที่สุด รวมถึงมาตรการด้านการเข้าถึง การบันทึกเหตุการณ์ การป้องกันข้อมูล และการบริหารจัดการการเปลี่ยนแปลง เพื่อรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลและบริการสำคัญขององค์กร
19) “**สภาพแวดล้อมที่ไม่ได้ให้บริการจริง (Non-Production Environment)**” หมายถึง สภาพแวดล้อมที่ใช้เพื่อการพัฒนา การทดสอบ การตรวจสอบคุณภาพ หรือการเตรียมความพร้อมของระบบก่อนนำไปใช้งานจริง สภาพแวดล้อมนี้อาจรวมถึง Development, Test, QA, UAT, Staging หรือ Sandbox Environment
20) “**สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Removable Media)”** หมายถึง อุปกรณ์หรือสื่อบันทึกข้อมูลที่สามารถถอดออกจากอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ได้ และสามารถใช้ในการ

จัดเก็บ โอนถ่าย หรือเคลื่อนย้ายข้อมูลระหว่างระบบต่าง ๆ ได้ เช่น USB Flash drive/Thumb drive, ฮาร์ดไดรฟ์ (HDD/SSD), Memory Card (SD Card, MicroSD Card, CF Card), แผ่น CD/DVD/Blu-ray Disc และอุปกรณ์จัดเก็บข้อมูลแบบพกพาอื่นที่มีลักษณะคล้ายคลึงกัน ทั้งนี้ไม่รวมถึงสื่อบันทึกข้อมูลประเภท Magnetic Tape/Tape Cartridge และการใช้งานฮาร์ดไดรฟ์สำหรับเซิร์ฟเวอร์

21) **"การแบ่งแยกเครือข่าย (Network Segmentation)"** หมายถึง กระบวนการในการออกแบบ บริหาร และควบคุมโครงสร้างเครือข่ายโดยแบ่งออกเป็นหลายส่วนหรือหลายโดเมน เพื่อจำกัดการสื่อสารระหว่างเครือข่ายตามระดับความเสี่ยงและความเชื่อถือ และลดผลกระทบจากการเข้าถึงโดยไม่ได้รับอนุญาตหรือการแพร่กระจายของภัยคุกคาม
22) **"การปฏิบัติงานจากระยะไกล (Remote Access)"** หมายถึง การเชื่อมต่อเพื่อเข้าถึงคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัท (ผ่านช่องทางการสื่อสารภายในบริษัท) หรือ จากภายนอกบริษัท (ผ่าน Internet)
23) **"ช่องโหว่ (Vulnerability)"** หมายถึง ข้อบกพร่อง หรือจุดอ่อนของระบบสารสนเทศ ทรัพย์สินสารสนเทศ กระบวนการ บุคลากร หรือมาตรการควบคุมด้านความมั่นคงปลอดภัย ซึ่งอาจถูกใช้ประโยชน์หรือถูกกระตุ้นโดยภัยคุกคาม และอาจนำไปสู่การละเมิดความลับ ความถูกต้องครบถ้วน หรือความพร้อมใช้งานของข้อมูล ระบบ หรือบริการขององค์กร
24) **"ความเสี่ยงที่เหลืออยู่ (Residual Risk)"** หมายถึง ระดับความเสี่ยงที่ยังคงมีอยู่ หลังจากที่มีการปฏิบัติตามมาตรการการควบคุมต่าง ๆ แล้ว
25) **"การทดสอบเจาะระบบ (Penetration Test)"** หมายถึง การทดสอบเชิงรุกด้านความมั่นคงปลอดภัย โดยใช้เทคนิค เครื่องมือ และวิธีการเช่นเดียวกับที่ผู้โจมตีอาจใช้ เพื่อประเมินประสิทธิภาพของมาตรการควบคุมด้านความปลอดภัย ระบุช่องโหว่ และให้ข้อเสนอแนะในการแก้ไข เพื่อช่วยลดความเสี่ยงและเพิ่มระดับความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร
26) **"Rollback"** หมายถึง การดำเนินการคืนค่าสภาพของระบบสารสนเทศ แอปพลิเคชัน หรือข้อมูล ให้กลับไปยังเวอร์ชันหรือสถานะก่อนการเปลี่ยนแปลง เช่น การอัปเดต การติดตั้ง หรือการปรับปรุงระบบ ในกรณีที่การเปลี่ยนแปลงดังกล่าวก่อให้เกิดความผิดพลาด ส่งผลกระทบต่อการให้บริการ หรือก่อให้เกิดความเสี่ยงต่อองค์กร
27) **"ปัญญาประดิษฐ์ (Artificial Intelligence: AI)"** หมายถึง เทคโนโลยีที่สร้างขึ้นเพื่อให้คอมพิวเตอร์สามารถเลียนแบบพฤติกรรมของมนุษย์ เช่น การเรียนรู้ การคิดวิเคราะห์ การตัดสินใจ การแก้ไขปัญหาต่าง ๆ โดยอาศัยข้อมูลจำนวนมากในการฝึกฝนตนเอง เพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพและแม่นยำมากขึ้น

1.4 ข้อยกเว้น

หากไม่สามารถดำเนินการตามมาตรฐานฉบับนี้ได้ บุคคลภายนอกต้องแจ้งพนักงานผู้ดูแลโครงการของบริษัททราบ เพื่อเข้าสู่กระบวนการพิจารณาจัดการความเสี่ยงของบริษัท

1.5 บทลงโทษ

กรณีบุคคลภายนอกละเมิดเอกสารมาตรฐานฉบับนี้ และรวมถึงนโยบาย มาตรฐาน แนวปฏิบัติ ระเบียบปฏิบัติของบริษัท ซึ่งอาจเป็นเหตุให้บริษัทได้รับความเสียหาย บริษัทสงวนสิทธิในการพิจารณาบทลงโทษตามสัญญาการใช้บริการ

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 กฎหมายและข้อบังคับที่เกี่ยวข้อง (Regulatory and Compliance)

<u>วัตถุประสงค์:</u> เพื่อกำหนดให้บุคคลภายนอกปฏิบัติตามกฎหมาย กฎเกณฑ์ ข้อบังคับ ข้อกำหนดของหน่วยงานกำกับดูแล และข้อผูกพันตามสัญญาที่เกี่ยวข้องกับการให้บริการ การเข้าถึงระบบสารสนเทศ หรือการประมวลผลข้อมูลของบริษัทอย่างครบถ้วนและเหมาะสม

1) บุคคลภายนอกต้องปฏิบัติตามข้อกำหนดทางกฎหมายกฎเกณฑ์ ข้อบังคับ ข้อกำหนดของหน่วยงานกำกับดูแล และข้อผูกพันตามสัญญาที่เกี่ยวข้องกับการให้บริการแก่บริษัท รวมถึงข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล ทรัพย์สินทางปัญญา และข้อกำหนดอื่นที่เกี่ยวข้องตามลักษณะของบริการนั้นๆ
2) ข้อมูลซอฟต์แวร์ เครื่องมือ หรือทรัพยากรดิจิทัลที่บุคคลภายนอกนำมาใช้ในการให้บริการแก่บริษัท ต้องเป็นสิ่งที่ได้มาโดยชอบด้วยกฎหมายและไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น

3) บุคคลภายนอกต้องรักษาความลับข้อมูลตามข้อตกลง (Non-Disclosure Agreement) และต้องไม่ใช้ เปิดเผย ทำซ้ำ ส่งต่อ หรือเผยแพร่ข้อมูลของบริษัทเกินกว่าวัตถุประสงค์ที่ได้รับอนุญาต หรือแก่บุคคลที่ไม่มีสิทธิรับทราบ
4) บุคคลภายนอกต้องแจ้งให้บริษัททราบโดยไม่ชักช้าหากพบว่ามีการไม่ปฏิบัติตามกฎหมาย ข้อกำหนดของหน่วยงานกำกับดูแล หรือข้อผูกพันตามสัญญาที่อาจส่งผลกระทบต่อการให้บริการ ข้อมูล หรือระบบของบริษัท

3.2 การบริหารจัดการทรัพยากรบุคคล (Human Resource Management)

<u>วัตถุประสงค์:</u> เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลที่อาจเกิดขึ้นจากบุคลากรของบุคคลภายนอกซึ่งเข้าปฏิบัติงาน เข้าถึงข้อมูล หรือเข้าถึงระบบสารสนเทศของบริษัท

1) บุคคลภายนอกต้องดูแลให้บุคลากรของตนที่เข้าปฏิบัติงานกับบริษัท หรือมีสิทธิเข้าถึงข้อมูลหรือระบบสารสนเทศของบริษัท ได้รับการสื่อสาร ฝึกอบรม หรือสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสมกับบทบาท หน้าที่ความรับผิดชอบ และระดับความเสี่ยงที่เกี่ยวข้อง
2) การสื่อสารหรือการฝึกอบรมตามข้อ 1) อย่างน้อยต้องครอบคลุมเรื่องการปกป้องข้อมูลของบริษัท การรักษาความลับของข้อมูล การใช้งานระบบและสิทธิการเข้าถึงอย่างเหมาะสม การรายงานเหตุการณ์หรือข้อผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ และข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการปฏิบัติงาน
3) ในกรณีที่ลักษณะงานมีความเสี่ยงสูง หรือเกี่ยวข้องกับข้อมูลสำคัญ ระบบสำคัญ หรือข้อมูลส่วนบุคคล บริษัทอาจกำหนดให้บุคลากรของบุคคลภายนอกต้องได้รับการอบรมเพิ่มเติม การรับทราบข้อกำหนดเฉพาะ หรือการประเมินความเข้าใจก่อนเริ่มปฏิบัติงาน ตามที่บริษัทเห็นสมควร
4) บุคคลภายนอกต้องดูแลให้บุคลากรของตนรับทราบและปฏิบัติตามนโยบาย มาตรฐาน ขั้นตอนการปฏิบัติงาน หรือข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลของบริษัทที่เกี่ยวข้องกับการปฏิบัติงาน

3.3 การบริหารจัดการการรับเหมาช่วง (Sub-Contract Management)

<u>วัตถุประสงค์:</u> เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และความมั่นคงปลอดภัยของข้อมูลที่อาจเกิดขึ้นจากการใช้ผู้รับเหมาช่วง โดยกำหนดให้บุคคลภายนอกที่ให้บริการแก่บริษัทต้องกำกับดูแลและรับผิดชอบต่อการปฏิบัติงานของผู้รับเหมาช่วงของตนอย่างเหมาะสมตามระดับความเสี่ยงที่เกี่ยวข้อง

1) บุคคลภายนอกต้องแจ้งให้บริษัททราบถึงการใช้ผู้รับเหมาช่วง ผู้รับจ้างช่วง หรือบุคคลภายนอกรายอื่นที่เกี่ยวข้องกับการให้บริการแก่บริษัท รวมถึงขอบเขตงานและลักษณะการเข้าถึงระบบหรือข้อมูลของบริษัทตามที่บริษัทกำหนด
2) บุคคลภายนอกต้องกำกับดูแลและควบคุมผู้รับเหมาช่วงให้ปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูล และข้อกำหนดอื่นที่เกี่ยวข้องของบริษัท ในระดับที่ไม่น้อยกว่าข้อกำหนดที่บุคคลภายนอกต้องปฏิบัติ

3) บุคคลภายนอกยังคงต้องรับผิดชอบต่อการปฏิบัติงาน ความเสี่ยง เหตุการณ์ด้านความมั่นคงปลอดภัย และความเสียหายที่เกิดจากผู้รับเหมาช่วง เสมือนเป็นการดำเนินงานของบุคคลภายนอกเอง
4) บุคคลภายนอกต้องไม่แต่งตั้งหรือเปลี่ยนแปลงผู้รับเหมาช่วงที่มีนัยสำคัญต่อการให้บริการแก่บริษัท โดยไม่แจ้งให้บริษัททราบหรือไม่ได้รับความเห็นชอบตามเงื่อนไขที่บริษัทกำหนด

3.4 การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Risk Management)

<u>วัตถุประสงค์:</u> เพื่อกำหนดให้บุคคลภายนอกสามารถระบุ ประเมิน ติดตาม และจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการให้บริการ การเข้าถึงระบบสารสนเทศ หรือการประมวลผลข้อมูลของบริษัทอย่างเหมาะสม และสอดคล้องกับระดับความเสี่ยงที่เกี่ยวข้อง

1) บุคคลภายนอกต้องมีกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับลักษณะของบริการ และต้องดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการให้บริการแก่บริษัทอย่างเหมาะสม
2) บุคคลภายนอกต้องผ่านการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลตามหลักเกณฑ์ที่บริษัทกำหนด ทั้งก่อนเริ่มให้บริการ ระหว่างการให้บริการ หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อการให้บริการแก่บริษัท
3) บุคคลภายนอกต้องให้ความร่วมมือในการให้ข้อมูล หลักฐาน หรือเข้ารับการตรวจประเมินตามที่บริษัทกำหนด เพื่อให้บริษัทสามารถประเมินระดับความเสี่ยงที่เกี่ยวข้องกับการให้บริการได้อย่างเหมาะสม
4) หากผลการประเมินพบความเสี่ยงหรือข้อบกพร่องที่ต้องได้รับการจัดการ บุคคลภายนอกต้องจัดทำแผนจัดการความเสี่ยงหรือแผนแก้ไขปรับปรุง พร้อมกำหนดระยะเวลาดำเนินการ และเสนอให้บริษัทพิจารณา
5) บุคคลภายนอกต้องดำเนินการตามแผนที่ได้รับความเห็นชอบจากบริษัท และรายงานความคืบหน้าหรือผลการดำเนินการตามระยะเวลาที่บริษัทกำหนด

3.5 การบริหารจัดการทรัพย์สิน (Asset Management)

<u>วัตถุประสงค์:</u> เพื่อให้มั่นใจว่าทรัพย์สินของบริษัทได้รับการระบุ จัดทำรายการ และควบคุมอย่างเหมาะสมตลอดวงจรชีวิต เพื่อป้องกันการสูญหาย การเข้าถึงโดยไม่ได้รับอนุญาต และลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับมาตรฐานสากล

1) บุคคลภายนอกต้องจัดทำ บันทึก และบำรุงรักษาทะเบียนทรัพย์สิน (Asset Inventory) สำหรับทรัพย์สิน ระบบ ข้อมูล เครือข่าย การเชื่อมต่อ และบริการที่ใช้ในการให้บริการแก่บริษัทหรือเกี่ยวข้องกับข้อมูลหรือระบบของบริษัท ซึ่งอย่างน้อยต้องครอบคลุมฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล เครือข่าย การเชื่อมต่อต่าง ๆ และบริการ เช่น คลาวด์หรือบริการจ้างทำ
2) ทะเบียนทรัพย์สินตามข้อ 1) ต้องมีรายละเอียดอย่างน้อยเกี่ยวกับการจัดหมวดหมู่ทรัพย์สิน การจำแนกชั้นความลับของข้อมูล และความเป็นเจ้าของหรือผู้รับผิดชอบทรัพย์สินที่เกี่ยวข้อง
3) บุคคลภายนอกต้องทบทวนและปรับปรุงทะเบียนทรัพย์สินให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้องกับทรัพย์สิน ระบบ ข้อมูล การเชื่อมต่อ หรือบริการที่ให้แก่บริษัท

4) บุคคลภายนอกต้องจัดส่งข้อมูลในทะเบียนทรัพย์สินหรือข้อมูลที่เกี่ยวข้องให้แก่บริษัทเมื่อบริษัทร้องขอภายใต้ขอบเขตที่จำเป็นต่อการบริหารจัดการความเสี่ยง การตรวจประเมิน หรือการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ของบริษัท

3.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

<u>วัตถุประสงค์:</u> เพื่อให้สามารถระบุจุดอ่อนและป้องกันระบบคอมพิวเตอร์และข้อมูลของบริษัทจากช่องโหว่ทางเทคนิค ซึ่งอาจเป็นสาเหตุให้เกิดการโจมตีทางไซเบอร์จากผู้ไม่ประสงค์ดี

1) ระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายที่เชื่อมต่อกับโครงข่ายของบริษัท ต้องได้รับการตั้งค่าความมั่นคงปลอดภัยของระบบ (System Hardening) ตามมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัย หรือ Security Baseline ที่บริษัทกำหนด
2) ต้องมีการประเมินช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Testing) สำหรับระบบคอมพิวเตอร์ ซอฟต์แวร์ ระบบเครือข่าย และอุปกรณ์หรือระบบอื่นใดที่เกี่ยวข้องกับการให้บริการแก่บริษัท ก่อนการติดตั้งหรือใช้งานบนสภาพแวดล้อมที่ให้บริการจริง (Production Environment) และต้องมีการดำเนินการเป็นระยะตามระดับความเสี่ยง รวมถึงเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ (Significant Change / Major Change) ทั้งนี้ ช่องโหว่ที่ตรวจพบต้องได้รับการแก้ไขตามกระบวนการและระยะเวลาที่บริษัทที่กำหนด
3) การประเมินช่องโหว่และทดสอบเจาะระบบโดยบุคคลภายนอกต้องแจ้งแผนการดำเนินการ รวมถึงเครื่องมือที่ใช้ในการดำเนินการแก่พนักงานผู้ดูแลโครงการของบริษัท และต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากบริษัทก่อนทำการตรวจสอบช่องโหว่และทดสอบเจาะระบบทุกครั้ง โดยผู้ดำเนินการทดสอบควรมีคุณสมบัติหรือใบรับรองที่เป็นที่ยอมรับในอุตสาหกรรมตามความเหมาะสม
4) ต้องดำเนินการอัปเดตแพตช์และเฟิร์มแวร์ที่ได้รับการอนุมัติสำหรับเซิร์ฟเวอร์ อุปกรณ์เครือข่าย และอุปกรณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยจากแหล่งที่เชื่อถือได้ ภายในระยะเวลาที่เหมาะสมตามระดับความเสี่ยง พร้อมบันทึกการติดตั้งทุกครั้งเพื่อการตรวจสอบย้อนหลัง ทั้งนี้ ระบบใหม่ต้องใช้แพตช์ปัจจุบัน และไม่ควรใช้งานซอฟต์แวร์ ระบบปฏิบัติการ หรืออุปกรณ์ที่สิ้นสุดการสนับสนุนจากผู้ผลิต (End-of-Support / End-of-Life) เว้นแต่ได้รับการประเมินความเสี่ยงและกำหนดมาตรการควบคุมเพิ่มเติมที่เหมาะสมและอยู่ในระบบความเสี่ยงที่ยอมรับได้
5) ก่อนดำเนินการอัปเดตแพตช์หรือเฟิร์มแวร์ ต้องมีการสำรองข้อมูลที่เกี่ยวข้องอย่างเหมาะสม เพื่อรองรับการกู้คืนในกรณีที่เกิดผลกระทบจากการอัปเดต
6) บริษัทขอสงวนสิทธิ์ในการประเมินช่องโหว่และทดสอบการเจาะระบบ รวมถึงกิจกรรมอื่นใดที่เกี่ยวข้องกับการจำลองการโจมตี อาทิ Red Team Exercise, Attack Surface monitoring ในระบบที่มีการให้บริการลูกค้า โดยมิต้องแจ้งล่วงหน้า
7) แอปพลิเคชันหรือระบบของบริษัทที่เชื่อมต่ออินเทอร์เน็ตต้องได้รับการตรวจหาช่องโหว่และทดสอบเจาะระบบตามความถี่ขั้นต่ำตามที่บริษัทกำหนด หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ (Major Change) เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและเพื่อประเมินความมั่นคงปลอดภัยโดยรวม ดังนี้

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

หากพบช่องโหว่จากการตรวจสอบหาช่องโหว่และทดสอบเจาะระบบ ต้องดำเนินการแก้ไขตามมาตรฐานของบริษัท ดังนี้

- กรณีเป็นระบบคอมพิวเตอร์/แอปพลิเคชัน/ฟีเจอร์ใหม่ จะสามารถขึ้น Production ได้ ต้องดำเนินการดังต่อไปนี้

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

Severity Level	Remediation Requirement
	ความเสี่ยงที่เกิดขึ้นในอนาคต (Risk Acceptance Form)

- <u>กรณีพบช่องโหว่จากการตรวจสอบช่องโหว่และเจาะทดสอบระบบตามรอบที่บริษัทกำหนด</u> ต้องดำเนินการดังต่อไปนี้

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

3.7 การรักษาความมั่นคงปลอดภัยทางกายภาพและอุปกรณ์ (Physical and Equipment Security)

<u>วัตถุประสงค์:</u> เพื่อป้องกันการเข้าถึงสถานที่และอุปกรณ์โดยไม่ได้รับอนุญาต ซึ่งอาจทำให้เกิดความเสียหายและการแทรกแซงการทำงานต่อระบบคอมพิวเตอร์ของบริษัท

3.7.1 การรักษาความมั่นคงปลอดภัยทางสถานที่ (Physical Security)

1) บุคคลบุคคลภายนอกที่เข้าปฏิบัติงานในสถานที่ของบริษัทต้องติดบัตรแสดงตนที่บริษัทออกให้อย่างถูกต้อง และเห็นได้เด่นชัดตลอดระยะเวลาการปฏิบัติงานในสถานที่ของบริษัท
2) บุคคลภายนอกต้องไม่เปิดเผยที่ตั้งสถานที่สำคัญ เช่น สถานที่ประมวลผลข้อมูล ห้องผู้บริหาร หรือพื้นที่สำคัญอื่นใดที่บริษัทกำหนด
3) พื้นที่ที่มีข้อมูลหรือระบบที่มีความสำคัญของบริษัทต้องมีมาตรการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมอย่างเหมาะสม โดยอย่างน้อยต้องครอบคลุมการเฝ้าระวังตลอด 24 ชั่วโมง (24x7) การตรวจจับอัคคีภัย การเตือนภัย การดับเพลิงอัตโนมัติ การควบคุมอุณหภูมิและความชื้น การเตรียมแผนฉุกเฉินสำหรับระบบไฟฟ้า และการมีสวิตช์ฉุกเฉินในบริเวณที่เหมาะสม
4) การนำอุปกรณ์เข้า-ออกจากพื้นที่สำคัญต้องได้รับอนุญาตจากผู้รับผิดชอบและต้องมีการบันทึกข้อมูลทุกครั้ง รวมถึงต้องมีการควบคุมการขนส่งอุปกรณ์หรือสื่อบันทึกข้อมูลเพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

3.7.2 การรักษาความมั่นคงปลอดภัยอุปกรณ์ (Equipment Security)

1) บุคคลภายนอกต้องดูแลให้มีการบำรุงรักษาอุปกรณ์และอุปกรณ์สนับสนุนที่ใช้ในการให้บริการแก่บริษัทอย่างสม่ำเสมอ เพื่อให้อุปกรณ์มีความพร้อมใช้งาน และต้องมีการบันทึกและทบทวนการบำรุงรักษาตามรอบเวลาที่เหมาะสม
2) บริษัทไม่อนุญาตให้ใช้งานสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Removable Media) ทุกประเภท เพื่อป้องกันความเสี่ยงด้านข้อมูลรั่วไหล การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการแพร่กระจายของมัลแวร์ เว้นแต่ได้รับอนุมัติเป็นกรณีพิเศษตามขั้นตอนที่บริษัทกำหนด
3) ก่อนการจำหน่าย หรือนำอุปกรณ์หรือสื่อบันทึกข้อมูลกลับมาใช้ซ้ำ ต้องมีการลบทำลายข้อมูลอย่างปลอดภัยตามข้อกำหนดของบริษัท และในกรณีที่ไม่สามารถกำจัดข้อมูลได้อย่างสมบูรณ์ ต้องดำเนินการทำลายทางกายภาพตามข้อกำหนดที่เกี่ยวข้อง

3.8 การบริหารจัดการการควบคุมการเข้าถึง (Access Control Management)

<u>วัตถุประสงค์:</u> เพื่อควบคุมการเข้าถึงข้อมูลและระบบคอมพิวเตอร์เฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต

3.8.1 การบริหารจัดการอัตลักษณ์และการเข้าถึง (Identity and Access Management)

a. บุคคลภายนอกต้องมีกระบวนการบริหารจัดการอัตลักษณ์ บัญชีผู้ใช้ และสิทธิการเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์อย่างเหมาะสม ครอบคลุมการลงทะเบียนผู้ใช้งาน การร้องขอ การอนุมัติ การเปลี่ยนแปลง การระงับ และการเพิกถอนสิทธิการเข้าถึง โดยกรณีที่บุคคลภายนอกเป็นเจ้าของระบบต้องกำหนดกระบวนการดังกล่าวเป็นลายลักษณ์อักษร และกรณีที่บุคคลภายนอกเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ของบริษัท ต้องปฏิบัติตามกระบวนการที่บริษัทกำหนด
b. บุคคลภายนอกต้องกำหนดและบริหารจัดการสิทธิการเข้าถึงตามหลักการให้สิทธิเท่าที่จำเป็น (Least Privilege Principle) และใช้รูปแบบการควบคุมการเข้าถึงที่เหมาะสม เช่น การควบคุมการเข้าถึงตามบทบาท (Role-based Access Control: RBAC) หรือการควบคุมการเข้าถึงตามแอตทริบิวต์

(Attribute-based Access Control: ABAC) โดยต้องมีทะเบียนสิทธิหรือทะเบียนบทบาทตามความเหมาะสม และทบทวนสิทธิอย่างน้อยปีละ 1 ครั้ง

c. ผู้ใช้งานและผู้ดูแลระบบต้องมีชื่อผู้ใช้งาน (User-ID) ที่สามารถระบุตัวตนและตรวจสอบย้อนกลับถึงเจ้าของบัญชีได้ โดยเป็นไปตามหลักการหนึ่งคนต่อหนึ่งชื่อผู้ใช้งาน เว้นแต่มีข้อจำกัดทางเทคนิคหรือเหตุจำเป็นที่ได้รับอนุมัติ และมีมาตรการควบคุมเพิ่มเติมที่เหมาะสม

d. ต้องมีการแยกหน้าที่ในการปฏิบัติงาน (Segregation of Duties: SoD) เพื่อลดความเสี่ยงจากการทุจริต ความผิดพลาด และการหลีกเลี่ยงการควบคุม โดยอย่างน้อยต้องแยกหน้าที่ระหว่างผู้ร้องขอ ผู้อนุมัติ ผู้ปฏิบัติงาน และผู้ตรวจสอบ หากไม่สามารถแยกหน้าที่ได้ ต้องกำหนดมาตรการควบคุมทดแทน

e. การให้หรือเปลี่ยนแปลงสิทธิการเข้าถึงต้องมีเหตุผลความจำเป็น ได้รับการอนุมัติจากผู้มีอำนาจ และต้องกำหนดสิทธิให้สอดคล้องกับหน้าที่ความรับผิดชอบ หลักการให้สิทธิเท่าที่จำเป็น และระยะเวลาที่จำเป็นต่อการปฏิบัติงาน ทั้งนี้ กรณีเป็นสิทธิการเข้าถึงของบุคคลภายนอก ต้องกำหนดวันที่สิ้นสุดหรือระยะเวลาการใช้งานทุกครั้ง

f. การใช้งานบัญชีผู้ใช้ร่วม บัญชีผู้ใช้กลาง หรือบัญชีสิทธิสูง ต้องจำกัดเฉพาะกรณีจำเป็นตามข้อจำกัดทางเทคนิคหรือการดำเนินงาน และต้องมีผู้รับผิดชอบบัญชีที่ชัดเจน มีทะเบียนเชื่อมโยงผู้ใช้งานกับบัญชี มีการควบคุมการใช้งาน และมีการติดตามหรือทบทวนการใช้งานตามที่กำหนด

g. ต้องมีการทบทวนและปรับปรุงสิทธิการเข้าถึงของผู้ใช้งานเมื่อมีการเปลี่ยนแปลงบทบาท หน้าที่ความรับผิดชอบ หรือเมื่อไม่มีความจำเป็นต้องเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์อีกต่อไป

h. ต้องมีการระงับหรือเพิกถอนสิทธิการเข้าถึงระบบและบริการของผู้ใช้งานอย่างเหมาะสม เมื่อสิ้นสุดระยะเวลาที่ได้รับอนุญาต สิ้นสุดการปฏิบัติงาน สิ้นสุดสัญญา หรือไม่มีความจำเป็นในการใช้งาน รวมถึงต้องปรับปรุงทะเบียนผู้ใช้งานให้เป็นปัจจุบันภายในระยะเวลาไม่เกิน 3 วันทำการนับจากวันที่การระงับหรือเพิกถอนสิทธิมีผล

3.8.2 การบริหารจัดการรหัสผ่าน (Password Management)

3.8.2.1 การกำหนดรหัสผ่าน

1) ห้ามตั้งรหัสผ่านที่ง่ายต่อการสุ่มหรือการคาดเดา เช่น การใช้ข้อมูลส่วนบุคคล การใช้รหัสผ่านเช่นเดียวกับชื่อผู้ใช้งาน หรือการปล่อยว่างไว้
2) ห้ามนำรหัสผ่านเดียวกันที่ใช้กับระบบอื่นนอกองค์กรมาใช้ในกับระบบของบริษัท
3) รูปแบบการตั้งรหัสผ่านต้องเป็นไปตามข้อกำหนดของบริษัท ดังนี้

	ระบบที่เข้าถึงข้อมูลสำคัญ ข้อมูลส่วนบุคคล หรือ อยู่ในเกณฑ์ความเสี่ยงสูง	ระบบอื่น ๆ
ความยาวและระยะเวลา	• ระดับผู้ใช้งานกำหนดรหัสผ่านที่มีความยาวอย่างน้อย 12 ตัวอักษร และเปลี่ยนรหัสผ่านอย่างน้อยทุก 90 วัน • ระดับผู้ดูแลระบบ (Privilege User) กำหนดรหัสผ่านที่มีความยาวอย่างน้อย 20 ตัวอักษร และเปลี่ยนรหัสผ่านอย่างน้อยทุก 90 วัน	อ้างอิงตามมาตรฐานสากล เช่น NIST SP 800-63B-4

	ระบบที่เข้าถึงข้อมูลสำคัญ ข้อมูลส่วนบุคคล หรือ อยู่ในเกณฑ์ความเสี่ยงสูง	ระบบอื่น ๆ
	• ระดับ User ที่ใช้ภายในระบบงานเพื่อให้บริการ (Service Account) กำหนดรหัสผ่านที่มีความยาวอย่างน้อย 30 ตัวอักษร และเปลี่ยนรหัสผ่านอย่างน้อยทุก 1 ปี	
ความซับซ้อน	รหัสผ่านต้องมีลักษณะดังนี้ • ประกอบด้วยตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ เช่น @ หรือ # • ไม่มีลักษณะเป็นหมายเลขลำดับ (Running Number) เช่น 12345678 • ไม่ใช้คำที่ง่ายต่อการคาดเดา หรือคำที่อยู่ในพจนานุกรม เช่น Password • ไม่ใช้รหัสผ่านซ้ำเดิมอย่างน้อย 5 ครั้ง	อ้างอิงตามมาตรฐานสากล เช่น NIST SP 800-63B-4
การยอมรับความผิดพลาด	ยอมรับความผิดพลาดของการป้อนรหัสผ่านไม่เกิน 5 ครั้ง หากการป้อนรหัสผ่านไม่ถูกต้องในครั้งต่อไป ซึ่งเกินจากจำนวนครั้งที่กำหนด ระบบคอมพิวเตอร์ต้องระงับการใช้งานของผู้ใช้งานนั้นเป็นการชั่วคราวทันที	อ้างอิงตามมาตรฐานสากล เช่น NIST SP 800-63B-4
การตรวจสอบย้อนหลัง	ต้องสามารถตรวจสอบการกำหนดรหัสผ่านของผู้ใช้งานย้อนหลังได้ เพื่อป้องกันการนำรหัสผ่านเดิมกลับมาใช้ใหม่ โดยอย่างน้อยต้องสามารถตรวจสอบย้อนหลังได้ 5 ครั้ง	อ้างอิงตามมาตรฐานสากล เช่น NIST SP 800-63B-4

3.8.2.2 การใช้งานรหัสผ่าน

1) บุคคลภายนอกต้องเก็บรักษารหัสผ่านไว้เป็นความลับส่วนตัว ห้ามเปิดเผย ส่งต่อ และห้ามใช้งานร่วมกับบุคคลอื่น
2) ห้ามใช้รหัสผ่านที่กำหนดขึ้นโดยระบบ (Default) ระบบต้องบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านทันที หลังจากที่เข้าใช้งานครั้งแรก หรือเมื่อมีการติดตั้งระบบใหม่ หรือปรับปรุงระบบคอมพิวเตอร์
3) รหัสผ่านต้องไม่ถูกกำหนดค่าตายตัว (Hard-Coded) ในระบบคอมพิวเตอร์
4) กรณีต้องมีการจัดเก็บรหัสผ่าน ต้องจัดเก็บในรูปแบบที่เข้ารหัส หรือใช้เครื่องมือบริหารจัดการรหัสผ่านที่ได้รับอนุญาตจากบริษัท โดยห้ามจัดเก็บรหัสผ่านในรูปแบบข้อความที่ชัดเจน (Clear Text)

5) ต้องมีการกำหนดวิธีที่ปลอดภัย ในการแจกจ่ายรหัสผ่านหรือชื่อผู้ใช้งาน (User-ID) ให้แก่ผู้ใช้งาน

3.8.3 การปฏิบัติงานจากระยะไกล (Remote Access)

1) บุคคลภายนอกต้องมีมาตรการในการควบคุมการปฏิบัติงานจากระยะไกลที่เหมาะสม และต้องกำหนดสิทธิการเข้าถึงตามหลักการ Least Privilege กำหนดระยะเวลาการใช้งาน และทบทวนสิทธิอย่างสม่ำเสมอ เพื่อป้องกันการเข้าถึงระบบคอมพิวเตอร์ เครือข่าย เซิร์ฟเวอร์โดยไม่ได้รับอนุญาต ทั้งนี้ การเข้าถึงระบบหรือเครือข่ายของบริษัทต้องเป็นไปตามข้อกำหนดของมาตรการของบริษัทด้วย
2) การเข้าใช้งาน Remote Access ของบริษัทต้องอยู่ภายใต้กระบวนการร้องขอสิทธิที่กำหนดไว้ โดยต้องกำหนดระยะเวลาการใช้งานหรือวันหมดอายุของสิทธิ ใช้การพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) และจัดเก็บ Log การเข้าใช้งานทั้งหมดเพื่อการตรวจสอบย้อนหลัง
3) การปฏิบัติงานจากระยะไกลเพื่อเข้าถึงสภาพแวดล้อมที่ให้บริการจริง (Production Environment) ต้องถูกควบคุมอย่างเข้มงวดและจำกัดเฉพาะเท่าที่จำเป็นตามวัตถุประสงค์การใช้งาน และต้องระงับสิทธิทันทีเมื่อหมดความจำเป็น

3.8.4 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

1) บุคคลภายนอกต้องมีการแบ่งแยกเครือข่าย (Network Segregation) และกำหนดมาตรการควบคุมความปลอดภัยที่เหมาะสม เพื่อป้องกันการโจมตีหรือเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต ทั้งนี้ เมื่อมีการเชื่อมต่อกับเครือข่ายของบริษัท ต้องปฏิบัติตามมาตรการของบริษัท
2) การเข้าถึงเครือข่ายจากบุคคลภายนอกไปยังเครือข่ายของบริษัท ต้องถูกจำกัดเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น และต้องมีการยืนยันตัวตนที่ปลอดภัยเพื่อป้องกันการปลอมแปลงแหล่งที่มา
3) อุปกรณ์ที่เชื่อมต่อกับเครือข่ายของบริษัทต้องได้รับอนุญาตตามกระบวนการที่กำหนด และอุปกรณ์ที่ไม่ใช่ของบริษัท รวมถึงอุปกรณ์ของบุคคลภายนอกที่ใช้ในการปฏิบัติงาน ต้องเชื่อมต่อผ่านเครือข่าย Wi-Fi ที่มีความปลอดภัยที่บริษัทจัดหาให้เท่านั้น
4) บุคคลภายนอกที่เข้าถึงเครือข่ายหรืออุปกรณ์เครือข่ายของบริษัท ต้องได้รับการพิสูจน์ตัวตนด้วยกลไกที่ปลอดภัย และในกรณีที่บริษัทกำหนดอาจต้องใช้การพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA)

3.8.5 การเข้าถึงซอร์สโค้ด (Access to Source Code)

1) ซอร์สโค้ดของบริษัทอนุญาตให้เข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายและมีความจำเป็นตามหน้าที่เท่านั้น โดยต้องกำหนดสิทธิตามหลัก Least Privilege และอยู่ภายใต้การกำกับดูแลของผู้รับผิดชอบที่ได้รับการแต่งตั้ง
2) ต้องมีการทบทวนสิทธิการเข้าถึงซอร์สโค้ดอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงบทบาทหน้าที่ของผู้ใช้งาน
3) การเข้าถึงหรือแก้ไขซอร์สโค้ดต้องดำเนินการผ่านช่องทาง เครื่องมือ และกระบวนการที่บริษัทอนุมัติ รวมถึงต้องมีการบันทึกกิจกรรมและประวัติการเปลี่ยนแปลงที่สามารถตรวจสอบย้อนหลังได้

4) ผู้ให้บริการต้องจัดให้มีมาตรการป้องกันการรั่วไหล สูญหาย ถูกแก้ไขโดยไม่ได้รับอนุญาต หรือถูกนำไปใช้นอกเหนือจากวัตถุประสงค์ที่กำหนด และต้องแจ้งบริษัททันทีเมื่อพบหรือสงสัยว่ามีเหตุผิดปกติเกี่ยวกับซอร์สโค้ด
5) เมื่อสิ้นสุดสัญญา สิ้นสุดการให้บริการ หรือเมื่อบริษัทแจ้งให้ดำเนินการ ผู้ให้บริการต้องยุติสิทธิการเข้าถึง และส่งคืนหรือลบซอร์สโค้ดและสำเนาทั้งหมดตามวิธีการที่บริษัทกำหนด พร้อมจัดส่งหลักฐานยืนยันการดำเนินการเมื่อได้รับการร้องขอ
6) กรณีมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงหรือรับซอร์สโค้ดของบริษัท ต้องได้รับอนุญาตจากบริษัทเป็นลายลักษณ์อักษร และต้องมีข้อตกลงด้านความมั่นคงปลอดภัยและ NDA ที่เหมาะสมก่อนทุกครั้ง

3.9 การบริหารจัดการอุปกรณ์ปลายทางอย่างปลอดภัย (Endpoint Security Management)

<u>วัตถุประสงค์:</u> เพื่อให้มั่นใจว่าอุปกรณ์ปลายทางที่เชื่อมต่อกับระบบสารสนเทศของบริษัทได้รับการปกป้อง ควบคุม และบริหารจัดการอย่างเหมาะสม ลดความเสี่ยงจากมัลแวร์ การเข้าถึงโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล และภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นจากอุปกรณ์ปลายทาง

3.9.1 การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen)

1) บุคคลภายนอกต้องไม่ปล่อย workstation, terminal หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานไว้โดยไม่มีการควบคุม และต้องล็อกหน้าจอหรือออกจากระบบเมื่อไม่ได้ใช้งาน
2) ต้องมีการตั้งค่า screen saver ที่มีการป้องกันด้วยรหัสผ่านหลังไม่มีการใช้งานเป็นระยะเวลาที่กำหนด เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
3) สื่อข้อมูลสำคัญทั้งในรูปแบบเอกสารและสื่ออิเล็กทรอนิกส์ต้องไม่ถูกปล่อยทิ้งไว้บนโต๊ะ ในห้องประชุม หรือในตู้ที่ไม่ได้ล็อกโดยไม่มีการควบคุม

3.9.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection Against Malicious Software)

1) บุคคลภายนอกต้องมีการกำหนดมาตรการที่เหมาะสมในการป้องกัน ตรวจจับ และ/หรือ แก้ไข ภัยคุกคามจากไวรัสและซอฟต์แวร์ไม่ประสงค์ดีในระบบคอมพิวเตอร์ที่ใช้ในการปฏิบัติงานให้แก่บริษัทอย่างเหมาะสม
2) อุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อกับระบบคอมพิวเตอร์และเครือข่ายของบริษัทต้องติดตั้งซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ที่ได้รับอนุญาตจากบริษัท เปิดใช้งานและปรับปรุงตลอดเวลา และต้องมีการกำหนดรอบเวลาในการตรวจหาซอฟต์แวร์ไม่ประสงค์ดีอย่างสม่ำเสมอ ทั้งนี้ ในกรณีที่บริษัทกำหนดอาจต้องใช้เครื่องมือด้านความมั่นคงปลอดภัยเพิ่มเติม เช่น Endpoint Detection and Response (EDR) ด้วย

3.9.3 ซอฟต์แวร์ลิขสิทธิ์ (Software Licensing)

1) บุคคลภายนอกต้องใช้งานเฉพาะซอฟต์แวร์ลิขสิทธิ์ที่ถูกกฎหมาย และเกี่ยวข้องกับการปฏิบัติงานกับบริษัทเท่านั้น
2) บุคคลภายนอกต้องไม่ติดตั้งหรือใช้งานซอฟต์แวร์ประเภท Hacking Tools หรือซอฟต์แวร์อื่นที่เกี่ยวข้องกับการตรวจสอบและรักษาความปลอดภัยของข้อมูลและระบบ เช่น ซอฟต์แวร์สำหรับการ

ตรวจสอบช่องโหว่หรือการทดสอบระบบ เว้นแต่ได้รับอนุญาตจากบริษัทเป็นลายลักษณ์อักษรก่อนทุกครั้ง

3.9.4 การควบคุมอุปกรณ์พกพาและการปฏิบัติงานจากภายนอกบริษัท (Mobile Computing and Teleworking)

1) บุคคลภายนอกต้องกำหนดมาตรการควบคุมอุปกรณ์คอมพิวเตอร์พกพา อุปกรณ์สื่อสารเคลื่อนที่ และอุปกรณ์ส่วนตัวที่ได้รับอนุญาตให้ใช้ปฏิบัติงาน หรือเชื่อมต่อกับระบบหรือเครือข่ายของบริษัท โดยอุปกรณ์ดังกล่าวต้องใช้ซอฟต์แวร์ที่ถูกกฎหมาย ได้รับการอัปเดตให้เป็นปัจจุบัน และได้รับการป้องกันด้วยซอฟต์แวร์รักษาความมั่นคงปลอดภัยที่เหมาะสม เช่น Anti-Malware หรือ Endpoint Protection
2) บุคคลภายนอกต้องมั่นใจว่าการจัดเก็บ ใช้งาน ส่งผ่าน หรือสำรองข้อมูลของบริษัทบนอุปกรณ์คอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อที่ เป็นไปตามข้อกำหนดด้านการจัดชั้นความลับ การควบคุมดูแลข้อมูล และการปกป้องข้อมูลของบริษัทอย่างเหมาะสม
3) อุปกรณ์ที่ใช้เชื่อมต่อกับระบบหรือเครือข่ายของบริษัทต้องได้รับการควบคุมการเข้าถึงอย่างเหมาะสม และต้องมีมาตรการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น การยืนยันตัวตน การตั้งค่าความมั่นคงปลอดภัย และการควบคุมการเชื่อมต่อเครือข่ายตามที่บริษัทกำหนด
4) ระบบที่มีความสำคัญสูงหรือมีผลกระทบสูงต่อบริษัท ต้องได้รับการแยกออกจากระบบอื่นอย่างเหมาะสม และมีมาตรการควบคุมด้านสภาพแวดล้อม การเข้าถึง และการเชื่อมต่อจากอุปกรณ์พกพาหรือการปฏิบัติงานจากภายนอกบริษัท เพื่อลดความเสี่ยงต่อความมั่นคงปลอดภัยของระบบและข้อมูลของบริษัท
5) การปฏิบัติงานจากภายนอกบริษัท (Teleworking) หรือการเข้าถึงระบบของบริษัทจากระยะไกล ต้องดำเนินการผ่านช่องทางที่บริษัทอนุญาต มีมาตรการเข้ารหัส และมีการควบคุมความมั่นคงปลอดภัยที่เหมาะสม
6) ผู้ปฏิบัติงานจากภายนอกบริษัทต้องปฏิบัติตามนโยบาย มาตรฐาน ขั้นตอนด้านความมั่นคงปลอดภัย ข้อตำลงการใช้งานซอฟต์แวร์ (Software License Agreement) และข้อกำหนดด้านการจัดเก็บหรือสำรองข้อมูลของบริษัทอย่างเคร่งครัด

3.10 การบริหารจัดการความเปลี่ยนแปลง (Change Management)

<u>วัตถุประสงค์:</u> เพื่อให้มั่นใจว่าการเปลี่ยนแปลงที่เกิดขึ้นกับระบบคอมพิวเตอร์ แอปพลิเคชัน ระบบเครือข่าย และระบบคลาวด์ ได้รับการควบคุมอย่างเหมาะสม เพื่อป้องกันผลกระทบต่อความมั่นคงปลอดภัยและความต่อเนื่องในการให้บริการขององค์กร

1) บุคคลภายนอกต้องมีกระบวนการบริหารจัดการความเปลี่ยนแปลงที่เกิดขึ้นต่อระบบคอมพิวเตอร์ แอปพลิเคชัน ระบบเครือข่าย และระบบคลาวด์อย่างเหมาะสม โดยเฉพาะอย่างยิ่งระบบปฏิบัติการที่ใช้งานจริง (Production Environment) ให้มีหัวข้อครอบคลุมอย่างน้อยดังนี้
    - การประเมินความเสี่ยงของการเปลี่ยนแปลง
    - การประเมินผลกระทบด้านความมั่นคงปลอดภัย
    - การประเมินช่องโหว่ของระบบ

- การทดสอบการเจาะระบบ สำหรับ Web Application, Application Program Interface (API) หรือระบบที่มีความเสี่ยงตามที่บริษัทกำหนด
- การอนุมัติการเปลี่ยนแปลงโดยผู้มีอำนาจก่อนดำเนินการ
- การจัดเตรียมขั้นตอนการย้อนกลับ (Rollback Plan) ในกรณีที่เกิดข้อผิดพลาด

2) การเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นต่อระบบที่ใช้งานจริง (Production Environment) ต้องได้รับการประเมินผลด้านความมั่นคงปลอดภัย และดำเนินการประเมินช่องโหว่ หรือการตรวจสอบเพิ่มเติมตามความเหมาะสม รวมถึงต้องมีการบันทึกผลการดำเนินการเป็นลายลักษณ์อักษร
3) บุคคลภายนอกต้องแจ้งล่วงหน้าเมื่อมีการเปลี่ยนแปลงใด ๆ ที่อาจส่งผลกระทบต่อระบบ การให้บริการหรือความมั่นคงปลอดภัยที่เกี่ยวข้องกับบริษัท
4) การเปลี่ยนแปลงที่สำคัญ (Major Changes) ต้องดำเนินการประเมินช่องโหว่ ทดสอบการเจาะระบบ ตามความเหมาะสมของประเภทระบบ และจัดทำแผนรองรับหรือแผนย้อนกลับ (Rollback Plan) ก่อนดำเนินการ
5) กรณีบริษัทเป็นผู้ดูแลระบบ ผู้ให้บริการจะต้องปฏิบัติตามกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Process) ของบริษัท

3.11 การบริหารจัดการแอปพลิเคชันอย่างปลอดภัย (Application Security Management)

<u>วัตถุประสงค์:</u> เพื่อให้มั่นใจว่าการพัฒนา การทดสอบ และการใช้งานแอปพลิเคชันเป็นไปตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ ลดความเสี่ยงจากช่องโหว่และการเข้าถึงโดยมิชอบ

3.11.1 ข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชัน (Application Security Requirements)

1) การออกแบบแอปพลิเคชันหรือระบบคอมพิวเตอร์ต้องพิจารณาปัจจัยด้านความมั่นคงปลอดภัยไซเบอร์เป็นพื้นฐาน รวมถึงการป้องกันช่องโหว่ที่ทราบและการใช้มาตรการควบคุมตามมาตรฐานสากล
2) ต้องมีการกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับแอปพลิเคชันทุกประเภท ครอบคลุมการยืนยันตัวตน การเข้ารหัสข้อมูล และการควบคุมการเข้าถึงตามบทบาท (Role-Based Access Control: RBAC)
3) ต้องมีการควบคุมการเข้าถึงซอร์สโค้ด เครื่องมือในการพัฒนา และซอฟต์แวร์ไลบรารีอย่างเหมาะสม เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้ตั้งใจหรือโดยมุ่งร้าย และเพื่อการรักษาทรัพย์สินทางปัญญาของบริษัท
4) ซอร์สโค้ดต้องจัดเก็บในระบบควบคุมเวอร์ชันที่บริษัทอนุมัติ หรือระบบที่ผ่านการประเมินด้านความมั่นคงปลอดภัยแล้วเท่านั้น ห้ามจัดเก็บในช่องทางที่บริษัทไม่ได้อนุญาต รวมถึง Public Repository, Public Cloud Storage หรือช่องทางใด ๆ ที่มีการตั้งค่าเป็นสาธารณะ (Public)
5) การติดตั้งหรืออัปเดตซอฟต์แวร์ ไลบรารีของโปรแกรม (Program Library) หรือส่วนประกอบที่เกี่ยวข้องกับแอปพลิเคชัน ต้องดำเนินการโดยผู้ที่ได้รับอนุญาต และอยู่ภายใต้กระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management) ตามที่บริษัทกำหนด

3.11.2 การเขียนชุดคำสั่งอย่างปลอดภัย (Secure Coding)

1) บุคคลภายนอกต้องมีมาตรฐานการพัฒนาแอปพลิเคชันและการเขียนชุดคำสั่งอย่างปลอดภัย (Secure Coding Standard) และต้องพัฒนาแอปพลิเคชันให้เป็นไปตามมาตรฐานด้านความมั่นคงปลอดภัยที่เหมาะสม
2) ผู้พัฒนาระบบต้องเข้ารหัสข้อมูลอย่างเหมาะสม และต้องมีการตรวจสอบโค้ด (Code Review) และการทดสอบช่องโหว่ด้านความมั่นคงปลอดภัยก่อนนำระบบหรือแอปพลิเคชันไปใช้งานจริง
3) บุคคลภายนอกที่พัฒนาแอปพลิเคชันให้แก่บริษัทต้องได้รับการฝึกอบรมหรือมีความรู้ความเข้าใจด้าน Secure Coding ที่เหมาะสม เพื่อให้มั่นใจว่ามีการพัฒนาซอฟต์แวร์อย่างปลอดภัยตามมาตรฐานที่เกี่ยวข้อง

3.11.3 การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริงออกจากกัน (Separation of Development, Test and Production Environments)

1) บุคคลภายนอกต้องจัดให้มีการแยกสภาพแวดล้อมสำหรับการพัฒนา (Development Environment) การทดสอบ (Test Environment) และการใช้งานจริง (Production Environment) ออกจากกันอย่างชัดเจน พร้อมมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) และ/หรือ การควบคุมการเข้าถึงทางตรรกะ (Logical Access Control) เพื่อลดโอกาสที่จะเกิดความเสี่ยงจากการเปลี่ยนแปลงโดยไม่ตั้งใจ หรือการเข้าถึงข้อมูลและแอปพลิเคชันโดยไม่ได้รับอนุญาต
2) ต้องมีการทดสอบการทำงานของแอปพลิเคชันในสภาพแวดล้อมการทดสอบ (Test Environment) ก่อนการติดตั้งในสภาพแวดล้อมที่ให้บริการจริง (Production Environment) เพื่อลดโอกาสที่จะเกิดความเสี่ยงจากการเปลี่ยนแปลงโดยไม่ตั้งใจ
3) ต้องมีการควบคุมการเข้าถึงข้อมูลสำคัญในสภาพแวดล้อมการพัฒนาและการทดสอบ เพื่อป้องกันการรั่วไหลของข้อมูล

3.11.4 การตั้งเวลาออกจากระบบโดยอัตโนมัติ

ต้องมีการตั้งเวลาโดยบังคับให้ผู้ใช้งานออกจากระบบโดยอัตโนมัติ เมื่อถึงเวลาที่กำหนดหรือเมื่อผู้ใช้งานไม่ได้ใช้งานระบบภายในเวลาที่กำหนดไว้ โดยระบบที่เชื่อมต่อหรือให้บริการข้อมูลสำคัญของบริษัทและข้อมูลส่วนบุคคลของลูกค้า มีระยะเวลาไม่เกิน 10 นาที สำหรับระบบอื่น ๆ มีระยะเวลาไม่เกิน 15 นาที

3.11.5 การจัดการ API และส่วนประกอบจากบุคคลภายนอก (API and Third Party Component Security)

1) ต้องมีการตรวจสอบความมั่นคงปลอดภัยของ API ไลบรารี และส่วนประกอบจากบุคคลภายนอก (Third Party Components) ที่ใช้งาน รวมถึงต้องมีการติดตามและอัปเดตเวอร์ชันอย่างเหมาะสมเพื่อป้องกันช่องโหว่ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบ
2) ต้องมีการควบคุมการเข้าถึง API อย่างเหมาะสม และต้องมีการเข้ารหัสข้อมูลที่รับส่งผ่าน API ตามมาตรฐานหรือแนวปฏิบัติด้านความมั่นคงปลอดภัยที่เป็นที่ยอมรับ

3.12 การบริหารจัดการความปลอดภัยของข้อมูล (Data Security Management)

<u>วัตถุประสงค์:</u> เพื่อปกป้องข้อมูลให้มีความปลอดภัย มีการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูล ลดความเสี่ยงจากการรั่วไหล การสูญหาย หรือการถูกเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อการดำเนินธุรกิจและชื่อเสียงของบริษัท

3.12.1 การจัดชั้นความลับและการควบคุมดูแลข้อมูล (Data Classification and Handling)

1) บุคคลภายนอกต้องมีการจำแนกชั้นความลับและการควบคุมดูแลข้อมูลตามระดับความสำคัญหรือความอ่อนไหวของข้อมูลอย่างเหมาะสมตลอดทั้งวงจรชีวิต (Data Lifecycle) ตั้งแต่การสร้าง การใช้งาน การส่งต่อ การจัดเก็บ จนถึงการทำลายข้อมูล
2) ต้องมีมาตรการควบคุมการเข้าถึง การใช้งาน และการเปิดเผยข้อมูลที่สามารถระบุตัวบุคคลได้ (Personal Identifiable Information: PII) อย่างเหมาะสมและสอดคล้องกับกฎหมายที่เกี่ยวข้อง เช่น การปิดบังข้อมูลบางส่วน (Data Masking) การจำกัดสิทธิการเข้าถึงตามความจำเป็นในการปฏิบัติงาน (Need-to-Know Basis) และการบันทึกเหตุการณ์การเข้าถึงหรือใช้งานข้อมูล (Logging)
3) การส่งต่อหรือเปิดเผยข้อมูลของบริษัทให้แก่บุคคลภายนอกหรือผู้รับจ้างช่วง ต้องได้รับอนุญาตจากบริษัท และต้องมีมาตรการปกป้องข้อมูลที่เหมาะสมตลอดกระบวนการส่งและจัดเก็บข้อมูล
4) การควบคุมดูแลข้อมูลของบริษัทในรูปแบบอิเล็กทรอนิกส์ (Electronic Format)
    a. การส่งหรือแลกเปลี่ยนข้อมูลของบริษัทต้องดำเนินการผ่านช่องทางที่บริษัทกำหนด และสำหรับข้อมูลชั้นความลับ Highly Confidential ต้องมีมาตรการป้องกันที่เหมาะสม เช่น เอกสารแนบต้องใส่ password protection ก่อนส่งออก แล้วจัดส่งรหัสผ่านในช่องทางอื่นแยกกับเอกสารที่จัดส่ง
    b. ห้ามถ่ายภาพ คัดลอก หรือบันทึกข้อมูลของบริษัทโดยไม่ได้รับอนุญาต โดยเฉพาะข้อมูลส่วนบุคคลของลูกค้า ข้อมูลสำคัญ และข้อมูลภายในของบริษัท
    c. ห้ามเผยแพร่หรือโพสต์ข้อมูลของบริษัทผ่านสื่อสังคมออนไลน์ (Social Media) หรือสื่อสาธารณะอื่นโดยไม่ได้รับอนุญาตจากบริษัท
    d. การลบหรือทำลายข้อมูลสำคัญของบริษัทต้องได้รับอนุญาตจากบริษัทก่อนดำเนินการ และต้องสามารถแสดงหลักฐานการลบหรือทำลายข้อมูลได้เมื่อบริษัทร้องขอ
5) การควบคุมดูแลข้อมูลของบริษัทในรูปแบบสิ่งพิมพ์ (Publishing Format)
    a. ห้ามพิมพ์ คัดลอก หรือจัดเก็บข้อมูลความลับ ข้อมูลสำคัญของบริษัท หรือข้อมูลส่วนบุคคลของลูกค้าในรูปแบบสิ่งพิมพ์ เว้นแต่ได้รับอนุญาตจากบริษัท
    b. การลบทำลายเอกสารที่มีข้อมูลความลับ ข้อมูลสำคัญของบริษัท หรือข้อมูลส่วนบุคคล ต้องได้รับการอนุญาตก่อนการลบทำลาย และต้องถูกทำลายด้วยวิธีการที่เหมาะสมตามมาตรฐานสากล เพื่อไม่ให้สามารถกู้คืน อ่าน หรือประกอบข้อมูลกลับคืนได้

3.12.2 การเข้ารหัสข้อมูล (Data Encryption)

1) บุคคลภายนอกต้องมีการบริหารจัดการกุญแจเข้ารหัส (Cryptographic Key Management) อย่างเหมาะสม ครอบคลุมตลอดวงจรชีวิตของกุญแจเข้ารหัส ตั้งแต่การสร้าง การจัดเก็บ การแจกจ่าย การหมุนเวียน การเพิกถอน และการทำลาย รวมถึงสอดคล้องกับมาตรฐานและแนวปฏิบัติสากลที่เกี่ยวข้อง

2) ต้องกำหนดและใช้งานมาตรฐานการเข้ารหัสข้อมูลที่มีกลไกการเข้ารหัสที่เหมาะสมและมั่นคงปลอดภัย เพื่อป้องกันข้อมูลในระหว่างการจัดเก็บข้อมูล (Data at Rest) และการถ่ายโอนข้อมูล (Data in Transit) จากการเข้าถึง การเปิดเผย การเปลี่ยนแปลง หรือการทำลายโดยไม่ได้รับอนุญาต
3) กุญแจเข้ารหัส (Cryptographic Keys) ต้องได้รับการป้องกันอย่างเหมาะสม และต้องมีการจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตตามความจำเป็นในการปฏิบัติงาน
4) ข้อมูลสำคัญ ข้อมูลส่วนบุคคลของลูกค้า และข้อมูลภายในของบริษัท ต้องได้รับการเข้ารหัสหรือได้รับการป้องกันด้วยมาตรการที่เหมาะสมเมื่อมีการจัดเก็บหรือรับส่งข้อมูลผ่านเครือข่ายสาธารณะ

3.12.3 การเก็บรักษาข้อมูล (Data at Rest)

1) บุคคลภายนอกต้องมีการกำหนดมาตรฐานการเข้ารหัสข้อมูลสำหรับข้อมูลที่จัดเก็บ (Data at Rest) ให้เหมาะสมกับระดับความสำคัญและความอ่อนไหวของข้อมูล
2) ต้องมีกระบวนการควบคุม ทบทวน และเพิกถอนสิทธิการเข้าถึงข้อมูลอย่างสม่ำเสมอ และเป็นไปตามหลัก Need-to-Know Basis และ Least Privilege
3) อุปกรณ์ ระบบ และสื่อบันทึกข้อมูลที่ใช้ในการจัดเก็บหรือประมวลผลข้อมูลของบริษัท ต้องได้รับการป้องกันทั้งทางกายภาพ (Physical) และทางตรรกะ (Logical) อย่างเหมาะสม มีการจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาต และจัดเก็บในสถานที่ที่มีความมั่นคงปลอดภัย
4) บริษัทกำหนดให้มีการเข้ารหัสข้อมูลสำคัญ (Sensitive Information) ของบริษัท โดยเฉพาะอย่างยิ่งข้อมูลส่วนบุคคล ตามมาตรฐานดังนี้
    a. สำหรับการเข้ารหัสแบบ Symmetric
        - AES-256 หรือสูงกว่า
    b. สำหรับการเข้ารหัสแบบ Asymmetric
        - RSA-2048 หรือสูงกว่า โดยเฉพาะอย่างยิ่งระบบที่ in-scope ของ PCI DSS และ Digital ID
        - ECC-256 หรือสูงกว่า
        - DSA-2048 หรือสูงกว่า
        - Diffie-Hellman 2048-bit หรือสูงกว่า

ทั้งนี้ กรณีที่มีการใช้งานข้อมูลสำคัญที่ต้องได้รับการปกป้องเป็นพิเศษ 2 ประเภทดังต่อไปนี้ จะต้องทำการเข้ารหัสโดยการใช้วิธีการ Field-level encryption

1) หมายเลขบัตรประชาชน หรือ หนังสือเดินทาง หมายรวมถึง เลขควบคุมหลังบัตรประจำตัวประชาชน (Laser ID) เลขชิปการ์ดของบัตรประชาชน (Chip ID) เลขคำขอมีบัตรจากกรมการปกครอง (bp1no)
2) หมายเลขบัตรเครดิต หรือบัตรเดบิต

3.12.4 การโอนข้อมูล (Data in Transit)

1) บุคคลภายนอกต้องมีมาตรการรักษาความปลอดภัยที่เหมาะสมสำหรับการถ่ายโอนข้อมูล เพื่อรักษาความลับ (Confidentiality) และความสมบูรณ์ (Integrity) ของข้อมูล
2) การรับส่งข้อมูลของบริษัทในระบบเครือข่าย (Data Transmission) จะต้องได้รับการเข้ารหัสตามข้อกำหนดดังต่อไปนี้

a. **กรณีใช้การเชื่อมต่อ VPN:**
การตรวจสอบเวอร์ชันของ TLS ใน VPN concentrator จะต้องถูกกำหนดค่าให้ใช้ TLS 1.2 (หรือสูงกว่า) และห้ามใช้การเชื่อมต่อที่มีเวอร์ชัน SSL 3.0 และต่ำกว่า

b. **กรณีที่ใช้การเชื่อมต่อ HTTPS:**
ต้องถูกกำหนดค่าให้ใช้ TLS 1.2 (หรือสูงกว่า) และห้ามใช้การเชื่อมต่อที่มีเวอร์ชัน SSL 3.0 และต่ำกว่า

c. **กรณีที่ใช้การเชื่อมต่อที่ปลอดภัยอื่น ๆ:**
ต้องใช้โปรโตคอลที่มีการเข้ารหัส เช่น SFTP, SSH หรือโปรโตคอลอื่นที่มีระดับความมั่นคงปลอดภัยเทียบเท่า

d. ไม่อนุญาตให้เข้าสู่ระบบผ่าน SSH โดยใช้บัญชีผู้ใช้งานสิทธิสูงสุดที่มีมาพร้อมระบบปฏิบัติการ (Root User)

3) การรับส่งข้อมูลสำคัญ (Sensitive Information) ข้อมูลความลับ หรือข้อมูลส่วนบุคคลผ่านเครือข่ายสาธารณะ (Public Network) ต้องได้รับการเข้ารหัสหรือได้รับการป้องกันด้วยมาตรการที่เหมาะสมตลอดกระบวนการรับส่งข้อมูล

3.12.5 การสำรองและกู้คืนข้อมูล (Data Backup and Restoration)

1) บุคคลภายนอกต้องมีการสำรองข้อมูลและระบบสำรองข้อมูลที่เหมาะสมกับความสำคัญของข้อมูลและบริการ รวมถึงมีมาตรการป้องกันทางกายภาพและทางตรรกะสำหรับระบบสำรองข้อมูลอย่างเหมาะสม
2) ระบบสำรองข้อมูลและสื่อบันทึกข้อมูลสำรองต้องจัดเก็บไว้ในสถานที่หรือสภาพแวดล้อมที่มีความมั่นคงปลอดภัย และได้รับการป้องกันจากการเข้าถึง การเปิดเผย การเปลี่ยนแปลง หรือการทำลายโดยไม่ได้รับอนุญาต เพื่อให้มั่นใจว่าสามารถเรียกคืนข้อมูลได้อย่างครบถ้วนเมื่อจำเป็น
3) บุคคลภายนอกต้องดำเนินการสำรองข้อมูลและทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอตามระดับความสำคัญของระบบและข้อมูล เพื่อให้มั่นใจว่าสามารถกู้คืนได้อย่างครบถ้วนสมบูรณ์
4) ต้องมีการสำรองข้อมูลอย่างสม่ำเสมอ และจัดให้มีมาตรการด้านความปลอดภัยของการเก็บข้อมูลสำรองเทียบเท่ากับการจัดเก็บข้อมูลต้นทาง รวมถึงต้องพิจารณามาตรการป้องกันการโจมตีจากแรนซัมแวร์ เช่น Immutable Backup, Offline Backup หรือการตัดการเชื่อมต่อจากระบบเครือข่ายตามความเหมาะสม
5) ต้องมีการทดสอบการกู้คืนข้อมูลสำคัญอย่างน้อยปีละ 1 ครั้ง และบันทึกผลการทดสอบเป็นลายลักษณ์อักษร เพื่อให้มั่นใจว่าสามารถกู้คืนข้อมูลได้ภายในระยะเวลาที่กำหนด (Recovery Time Objective: RTO) และ สามารถกู้คืนข้อมูลได้ตามจุดที่กำหนด (Recovery Point Objective: RPO) ตามข้อตกลงหรือสัญญาการใช้บริการ

3.12.6 การลบทำลายข้อมูล (Information Disposal)

1) บุคคลภายนอกต้องจัดเก็บข้อมูลบริษัทตามระยะเวลาที่กำหนด (Retention Period) และเมื่อครบระยะเวลาการจัดเก็บ ตามตารางดังต่อไปนี้ ต้องดำเนินการลบทำลายข้อมูลอย่างปลอดภัยตามมาตรฐานสากล เพื่อให้สอดคล้องกับวัตถุประสงค์การจัดเก็บข้อมูล ข้อกำหนดทางกฎหมาย และมาตรฐานการจัดเก็บข้อมูลของบริษัท

No.	Category	Retention Period	Lawful Basis / การบริหารจัดการข้อมูลของบริษัท
1	ข้อมูลสำคัญของบริษัท ข้อมูลที่ใช้ในโครงการ รวมถึงข้อมูลส่วนบุคคล	เก็บตลอดระยะเวลาการใช้บริการตามสัญญา	ฐานสัญญาการให้บริการ
2	ข้อมูล Log file	90 วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์	มาตรา 26 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

2) หลังจากมีการยกเลิกหรือสิ้นสุดสัญญาการให้บริการ บุคคลภายนอกต้องทำการส่งมอบข้อมูลของบริษัท รวมถึงข้อมูลสำคัญในโครงการที่จัดทำร่วมกันให้กับบริษัท และต้องลบทำลายข้อมูลทั้งหมด รวมถึงสำเนาข้อมูล (Copies) และข้อมูลสำรอง (Backup) ที่จัดเก็บไว้กับบุคคลภายนอกหลังจากการส่งมอบข้อมูลแล้วเสร็จไม่เกิน 7 วันทำการ เว้นแต่ในกรณีจำเป็นต้องเก็บรักษาข้อมูลส่วนบุคคลเพื่อการปฏิบัติตามกฎหมายที่ใช้บังคับเท่านั้น
3) การลบทำลายข้อมูลที่เป็นความลับ รวมถึงข้อมูลส่วนบุคคลของลูกค้าของบริษัท ต้องแจ้งแก่พนักงานผู้ดูแลโครงการของบริษัทและได้รับการอนุมัติจากบริษัทก่อน และต้องจัดทำรายงานบันทึกการลบข้อมูล (Deletion Record) หรือหนังสือรับรองการลบทำลายข้อมูล (Certificate of Destruction) พร้อมจัดเก็บหลักฐานการลบทำลายข้อมูลให้บริษัททุกครั้งเพื่อส่งมอบให้บริษัทเมื่อร้องขอ

3.12.7 การใช้งานข้อมูลสำหรับการทดสอบระบบ (Test Information)

ห้ามให้ใช้ข้อมูลสำคัญของบริษัท ข้อมูลส่วนบุคคล หรือข้อมูลความลับในการพัฒนาและทดสอบระบบโดยเด็ดขาด และต้องใช้ข้อมูลทดสอบ (Test Data) ที่ถูกสร้างขึ้นเพื่อวัตถุประสงค์ดังกล่าวเท่านั้น

3.13 การบริหารจัดการความมั่นคงปลอดภัยโครงสร้างพื้นฐาน (Infrastructure Security Management)

<u>วัตถุประสงค์:</u> เพื่อให้มั่นใจว่าโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศของบริษัท ได้แก่ ระบบคลาวด์ ระบบเครือข่าย และระบบตรวจสอบเหตุการณ์ มีการปกป้อง ควบคุม และบริหารจัดการอย่างเหมาะสม เพื่อลดความเสี่ยงจากภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ และสนับสนุนการดำเนินงานให้ปลอดภัย

3.13.1 การบริหารความมั่นคงปลอดภัยคลาวด์ (Cloud Security Management)

1) บุคคลภายนอกต้องมีนโยบาย มาตรฐาน หรือแนวปฏิบัติด้านความมั่นคงปลอดภัยที่สอดคล้องกับมาตรฐานสากล และครอบคลุมบริการคลาวด์ที่ใช้ในการให้บริการแก่บริษัท
2) ระบบที่ใช้งานคลาวด์ต้องได้รับการติดตาม ตรวจสอบ และทบทวนการตั้งค่าความปลอดภัยเสมอ เพื่อให้มั่นใจว่ายังคงสอดคล้องกับมาตรฐานด้านความปลอดภัย และระดับความเสี่ยงที่ยอมรับได้ของบริษัท

3) ต้องมีมาตรการป้องกันการกำหนดค่าที่ไม่เหมาะสม (Cloud Misconfiguration) และการปิดเผยข้อมูลหรือทรัพยากรบนคลาวด์สู่สาธารณะโดยไม่ได้รับอนุญาต
4) ต้องเปิดใช้งานการบันทึกเหตุการณ์ (Logging) และติดตามตรวจสอบ (Monitoring) สำหรับระบบคลาวด์ที่ใช้ในการให้บริการแก่บริษัท เพื่อให้สามารถตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยและสนับสนุนการสืบสวนย้อนหลังได้
5) ต้องมีการกำหนดบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยระหว่างผู้ให้บริการคลาวด์ (Cloud Service Provider) และบุคคลภายนอกอย่างชัดเจน โดยคำนึงถึงหลักการ Shared Responsibility Model

3.13.2 การบริหารความมั่นคงปลอดภัยเครือข่าย (Network Security Management)

1) บุคคลภายนอกต้องกำหนดและดำเนินมาตรการรักษาความมั่นคงปลอดภัยของเครือข่ายที่เหมาะสมสำหรับเครือข่ายที่เชื่อมต่อกับระบบกับเครือข่ายของบริษัท
2) ต้องมีการแบ่งแยกเครือข่าย (Network Segmentation) ตามระดับความสำคัญของระบบและข้อมูลเพื่อลดความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต หรือการแพร่กระจายของภัยคุกคามด้านความมั่นคงปลอดภัย
3) ต้องมีการควบคุมและกรองการรับส่งข้อมูลผ่านอุปกรณ์หรือเทคโนโลยีด้านความมั่นคงปลอดภัยที่เหมาะสม เช่น Firewall หรือเทคโนโลยีอื่นที่เทียบเท่า
4) ต้องมีการเฝ้าระวัง ติดตาม และบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัยของเครือข่ายอย่างเหมาะสม เพื่อรองรับการตรวจสอบย้อนหลังและการตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัย
5) ต้องมีการทบทวนการเชื่อมต่อเครือข่ายกับบริษัทอย่างสม่ำเสมอ และยกเลิกการเชื่อมต่อที่ไม่มีความจำเป็น
6) กรณีที่มีการใช้งานเครือข่ายไร้สาย (Wireless Network) ต้องใช้การพิสูจน์ตัวตนและการเข้ารหัสที่เหมาะสม และต้องไม่ใช้มาตรฐานหรือการตั้งค่าความปลอดภัยที่ล้าสมัยหรือมีความเสี่ยงด้านความมั่นคงปลอดภัย

3.13.3 การตรวจสอบและบันทึกเหตุการณ์ (Logging and Monitoring)

3.13.3.1 การจัดการบันทึกข้อมูล Log (Managing Log Information)

1) บุคคลภายนอกต้องมีการบันทึกเหตุการณ์สำคัญของระบบ (Audit Log / Activity Log) รวมถึงกิจกรรมของผู้ใช้งาน ผู้ดูแลระบบที่เกี่ยวข้องกับระบบหรือบริการที่ให้แก่บริษัท โดยต้องมีการกำหนดสิทธิการเข้าถึงข้อมูล Log อย่างชัดเจนและเหมาะสม
2) Log ที่จัดเก็บต้องครอบคลุมเหตุการณ์ที่จำเป็นต่อการตรวจสอบย้อนหลังและการสืบสวนเหตุการณ์ด้านความมั่นคงปลอดภัย เช่น การใช้งานสิทธิระดับสูง การเข้าถึงระบบหรือข้อมูล การพยายามเข้าสู่ระบบที่ไม่สำเร็จ การใช้งานกลไกยืนยันตัวตน การเปลี่ยนแปลงบัญชีผู้ใช้ และการเริ่มต้น หยุด หรือเปลี่ยนแปลงการบันทึก Log
3) ต้องกำหนดระยะเวลาการจัดเก็บ Log ให้เหมาะสมและเป็นไปตามกฎหมาย สัญญา หรือข้อกำหนดที่เกี่ยวข้อง โดย Log ที่จำเป็นต่อการติดตามสืบค้นหรือการพิสูจน์หลักฐานดิจิทัลต้องจัดเก็บไว้ไม่น้อยกว่า 90 วัน หรือเป็นไปตามที่บริษัทหรือกฎหมายกำหนด

4) ต้องมีมาตรการป้องกันข้อมูล Log และระบบจัดเก็บ Log จากการถูกแก้ไข ปลอมแปลง ลบ หรือเข้าถึงโดยไม่ได้รับอนุญาต และต้องจำกัดการเข้าถึง Log เฉพาะผู้ที่ได้รับอนุญาตตามความจำเป็นในการปฏิบัติงาน
5) Log ของระบบ อุปกรณ์ หรือบริการที่มีความสำคัญต้องจัดเก็บไว้ในพื้นที่หรือระบบที่มีมาตรการควบคุมความปลอดภัยอย่างเหมาะสม และต้องมั่นใจว่าข้อมูล Log มีความพร้อมใช้งานสำหรับการตรวจสอบย้อนหลังเมื่อจำเป็น
6) กรณีมีการส่งข้อมูล Log ผ่านเครือข่ายที่ไม่น่าเชื่อถือ ต้องมีการเข้ารหัสช่องทางการส่งข้อมูล Log หรือใช้โปรโตคอลที่ปลอดภัย เพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูล Log ระหว่างการรับส่ง
7) กรณีระบบหรือบริการอยู่ภายใต้ข้อกำหนดเฉพาะ เช่น PCI DSS หรือข้อกำหนดด้านกฎหมายอื่น บุคคลภายนอกต้องจัดเก็บและปกป้อง Log ให้เป็นไปตามข้อกำหนดดังกล่าวด้วย

3.13.3.2 การเฝ้าระวังการใช้งานระบบ (Monitoring System Use)

1) บุคคลภายนอกต้องกำหนดระบบ เหตุการณ์ หรือกิจกรรมที่ต้องเฝ้าระวังด้านความมั่นคงปลอดภัย โดยพิจารณาจากระดับความเสี่ยง ความสำคัญของระบบ และผลกระทบที่อาจเกิดขึ้นต่อข้อมูลหรือบริการของบริษัท
2) ต้องมีการเก็บ วิเคราะห์ และเฝ้าระวังข้อมูล Log จากระบบที่มีความสำคัญอย่างเหมาะสม เพื่อสนับสนุนการตรวจจับพฤติกรรม ความผิดพลาดของระบบ หรือเหตุการณ์ผิดปกติที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบหรือข้อมูลของบริษัท
3) เมื่อพบความผิดพลาดของระบบ พฤติกรรมผิดปกติ หรือเหตุการณ์ด้านความมั่นคงปลอดภัย ต้องมีการวิเคราะห์สาเหตุและดำเนินการแก้ไขหรือปรับปรุงมาตรการควบคุมอย่างเหมาะสม เพื่อลดโอกาสที่จะเกิดเหตุการณ์ซ้ำ
4) ต้องมีการกำหนดกลไกการแจ้งเตือนเมื่อพบพฤติกรรมหรือเหตุการณ์ผิดปกติ เช่น การเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานสิทธิระดับสูงที่ผิดปกติ การพยายามเข้าสู่ระบบที่ไม่สำเร็จซ้ำ ๆ หรือเหตุการณ์ที่อาจบ่งชี้ถึงภัยคุกคามด้านความมั่นคงปลอดภัย
5) การให้บริการและข้อมูล Log ที่เกี่ยวข้องกับระบบหรือบริการของบุคคลภายนอกที่ให้แก่บริษัท ต้องได้รับการตรวจสอบและทบทวนอย่างสม่ำเสมอ เพื่อให้มั่นใจว่ายังคงมีประสิทธิผลและเพียงพอต่อการตรวจจับ วิเคราะห์ และตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย
6) ต้องมีการเฝ้าระวังและประเมินความเพียงพอของความสามารถในการจัดเก็บข้อมูล Log และต้องมีการแจ้งเตือนเมื่อทรัพยากรหรือระบบที่เกี่ยวข้องกับการจัดเก็บ Log มีความเสี่ยงต่อความพร้อมใช้งาน
7) สำหรับระบบที่มีความสำคัญหรือเกี่ยวข้องกับการให้บริการแก่บริษัท บุคคลภายนอกต้องมีระบบหรือกระบวนการเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัย เช่น Security Information and Event Management (SIEM) หรือระบบเฝ้าระวังอื่นที่เหมาะสม เพื่อสนับสนุนการวิเคราะห์และตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัยแบบรวมศูนย์

3.13.3.3 การเทียบตั้งเวลาระบบ (System Time Synchronization)

1) บุคคลภายนอกต้องจัดให้ระบบคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบที่เกี่ยวข้องกับการให้บริการแก่บริษัท มีการเทียบตั้งเวลากับแหล่งเวลามาตรฐานเดียวกัน เช่น Coordinated Universal Time (UTC) หรือแหล่งเวลามาตรฐานอื่นที่เชื่อถือได้ เพื่อให้ข้อมูล Log มีความถูกต้อง น่าเชื่อถือ และสามารถใช้ในการตรวจสอบย้อนหลังได้
2) ต้องมีการตรวจสอบความคลาดเคลื่อนของเวลาระบบอย่างเหมาะสม และดำเนินการแก้ไขเมื่อพบความคลาดเคลื่อน เพื่อให้ข้อมูล Log สามารถใช้ในการอ้างอิง วิเคราะห์เหตุการณ์ และสนับสนุนการสืบสวนเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างถูกต้อง

3.13.3.4 การตรวจจับผู้บุกรุกและการติดตามสืบค้น (Intrusion Detection and Investigation)

1) บุคคลภายนอกต้องกำหนดหลักเกณฑ์ในการทบทวนและวิเคราะห์ข้อมูล Log เพื่อตรวจหาความพยายามหรือเหตุการณ์ที่อาจบ่งชี้ถึงการละเมิดด้านความมั่นคงปลอดภัยไซเบอร์ โดยพิจารณาจากข้อมูลภัยคุกคาม ช่องโหว่ และรูปแบบการโจมตีจากแหล่งข้อมูลที่น่าเชื่อถือ
2) เมื่อพบความพยายามในการบุกรุก เหตุการณ์ผิดปกติ หรือการละเมิดด้านความมั่นคงปลอดภัยไซเบอร์ ต้องดำเนินการป้องกัน แก้ไข หรือควบคุมผลกระทบอย่างเหมาะสมและทันท่วงที พร้อมแจ้งบริษัทตามกระบวนการที่กำหนด
3) ต้องจัดเก็บข้อมูล Log ที่จำเป็นต่อการติดตามสืบค้น การวิเคราะห์เหตุการณ์ และการพิสูจน์หลักฐานดิจิทัล (Digital Forensic Evidence) ไว้ไม่น้อยกว่า 90 วัน หรือเป็นไปตามข้อกำหนดของกฎหมาย สัญญา หรือบริษัทกำหน
4) ต้องมีการเฝ้าระวังและติดตามเหตุการณ์ที่มีความเสี่ยงสูง รวมถึงการวิเคราะห์ความเชื่อมโยงของเหตุการณ์จากหลายระบบ (Event Correlation) เพื่อเพิ่มประสิทธิภาพในการตรวจจับและตอบสนองต่อภัยคุกคาม

3.13.4 การบริหารจัดการระบบ (System Management)

1) บุคคลภายนอกต้องจัดทำและทบทวนเอกสารขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบหรือบริการที่ให้แก่บริษัทอย่างเหมาะสม โดยครอบคลุมขั้นตอนการประมวลผลและจัดการข้อมูล การจัดการข้อผิดพลาด และช่องทางหรือหน่วยงานที่รับผิดชอบในการสนับสนุนการดำเนินงานหรือแก้ไขปัญหาที่อาจเกิดขึ้น
2) บุคคลภายนอกต้องมีการติดตามและประเมินขีดความสามารถของระบบ ทรัพยากร และบริการที่เกี่ยวข้องกับการให้บริการแก่บริษัทอย่างเหมาะสม เพื่อให้มั่นใจว่าสามารถรองรับการใช้งานและการให้บริการได้อย่างต่อเนื่อง
3) ต้องมีการวางแผนรองรับการเพิ่มขึ้นของปริมาณงาน การใช้ทรัพยากร หรือการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อประสิทธิภาพ ความพร้อมใช้งาน หรือความต่อเนื่องของบริการ
4) เมื่อพบว่าทรัพยากรของระบบมีความเสี่ยงต่อความไม่เพียงพอหรืออาจส่งผลกระทบต่อการให้บริการแก่บริษัท ต้องดำเนินการแก้ไขหรือจัดทำแผนรองรับอย่างเหมาะสม
5) ระบบที่เกี่ยวข้องกับการให้บริการแก่บริษัทต้องมีการตั้งค่า Session Timeout หรือการออกจากระบบอัตโนมัติเมื่อไม่มีการใช้งานภายในระยะเวลาที่กำหนด โดยระบบที่เชื่อมต่อหรือ

ให้บริการข้อมูลสำคัญของบริษัทหรือข้อมูลส่วนบุคคลของลูกค้า ต้องกำหนดระยะเวลาไม่เกิน 10 นาที และระบบอื่นไม่เกิน 15 นาที หรือเป็นไปตามข้อกำหนดที่บริษัทกำหนด

3.14 การบริหารจัดการด้านความปลอดภัยการใช้งานปัญญาประดิษฐ์ (Artificial Intelligence Security Management)

<u>วัตถุประสงค์:</u> เพื่อให้การพัฒนา การให้บริการ และการใช้งานระบบปัญญาประดิษฐ์ (AI) ที่เกี่ยวข้องกับการให้บริการแก่บริษัท ได้รับการกำกับดูแลและควบคุมด้านความมั่นคงปลอดภัย ความเป็นส่วนตัว และการปฏิบัติตามกฎหมายและนโยบายที่เกี่ยวข้องอย่างเหมาะสม ครอบคลุมทั้งระบบที่ใช้งานภายในองค์กร (On-premise/Private) และบริการภายนอก (SaaS/PaaS/IaaS/Model-as-a-Service)

1) บุคคลภายนอกต้องจัดให้มีมาตรการควบคุมด้านความมั่นคงปลอดภัยและความเป็นส่วนตัวสำหรับระบบปัญญาประดิษฐ์อย่างเหมาะสม ครอบคลุมการควบคุมการเข้าถึง การตรวจจับพฤติกรรมผิดปกติ การทดสอบความทนทานของปัญญาประดิษฐ์ และการจัดเก็บข้อมูลที่จำเป็นเพื่อรองรับการตรวจสอบย้อนหลัง เช่น เวอร์ชันของโมเดล (Model Versioning) น้ำหนักโมเดล (Model Weights) ชุดข้อมูลฝึก (Training Datasets) และพารามิเตอร์ที่เกี่ยวข้อง
2) การนำข้อมูลของบริษัทไปใช้เพื่อฝึก ทดสอบ หรือใช้งานกับระบบปัญญาประดิษฐ์ ต้องเป็นไปตามข้อกำหนดด้านการจัดชั้นความลับและการควบคุมดูแลข้อมูล การเข้ารหัส การควบคุมการเข้าถึง และการปกป้องข้อมูลส่วนบุคคลที่บริษัทกำหนด
3) ห้ามนำข้อมูลสำคัญ ข้อมูลความลับ หรือข้อมูลส่วนบุคคลของบริษัทไปใช้กับปัญญาประดิษฐ์ภายนอก เว้นแต่ได้รับอนุญาตจากบริษัท และมีมาตรการปกป้องข้อมูลที่เหมาะสม เช่น การปกปิดข้อมูล (Data Masking) การทำให้ไม่สามารถระบุตัวบุคคลได้ (De-identification) หรือมาตรการอื่นที่เทียบเท่า
4) ต้องมีการอัปเดตแพตช์ ไลบรารี เฟรมเวิร์ก และส่วนประกอบที่เกี่ยวข้องกับปัญญาประดิษฐ์อย่างสม่ำเสมอ เพื่อป้องกันความเสี่ยงจากภัยคุกคาม เช่น การโจรกรรมโมเดลปัญญาประดิษฐ์ (Model Theft) การอนุมานข้อมูลย้อนกลับจากโมเดลปัญญาประดิษฐ์ (Model Inversion) การปลอมปนข้อมูลฝึก (Data Poisoning) และข้อมูลนำเข้าที่ถูกออกแบบเพื่อโจมตีโมเดล (Adversarial Input)
5) การใช้บริการปัญญาประดิษฐ์จากผู้ให้บริการภายนอกหรือเครื่องมือปัญญาประดิษฐ์ใด ๆ ที่เกี่ยวข้องกับข้อมูล ระบบ หรือบริการของบริษัท ต้องผ่านการประเมินและได้รับอนุญาตตามกระบวนการที่บริษัทกำหนด และไม่อนุญาตให้ใช้เครื่องมือหรือบริการปัญญาประดิษฐ์ที่ไม่ได้รับอนุมัติจากบริษัท (Shadow AI)
6) ผลลัพธ์ที่สร้างจากปัญญาประดิษฐ์ซึ่งอาจส่งผลกระทบต่อธุรกิจ ลูกค้า กฎหมาย หรือภาระผูกพันของบริษัท ต้องได้รับการตรวจสอบโดยมนุษย์ (Human Validation) ก่อนนำไปใช้งาน
7) ห้ามใช้ปัญญาประดิษฐ์เพื่อสร้างเนื้อหาที่ละเมิดกฎหมาย ทรัพย์สินทางปัญญา สิทธิของบุคคลอื่น หรือจริยธรรมของบริษัท
8) กรณีเกิดเหตุด้านความมั่นคงปลอดภัยไซเบอร์ เหตุการณ์เกี่ยวกับข้อมูลส่วนบุคคล หรือการละเมิดกฎหมายที่เกี่ยวข้องจากการใช้งานปัญญาประดิษฐ์ บุคคลภายนอกต้องรายงาน ตรวจสอบ และจัดการเหตุการณ์ตามกระบวนการที่กำหนด และแจ้งบริษัทโดยไม่ชักช้า

3.15 การสร้างความตระหนักรู้และการอบรม (Awareness, Education and Training)

<u>วัตถุประสงค์:</u> เพื่อยกระดับให้บุคลากรของบุคคลภายนอกที่เกี่ยวข้องกับการให้บริการแก่บริษัท มีความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ สามารถรู้เท่าทัน ป้องกัน และรับมือกับภัยคุกคามทางไซเบอร์ในยุคปัจจุบันได้อย่างเหมาะสมและทันท่วงที

1) บุคคลภายนอกต้องจัดให้มีการให้ความรู้และการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล รวมถึงนโยบาย มาตรฐาน และข้อกำหนดที่เกี่ยวข้องของบริษัทอย่างต่อเนื่อง โดยเนื้อหาต้องเหมาะสมกับหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับการให้บริการแก่บริษัท
2) บุคคลภายนอกต้องมีการอัปเดตเนื้อหาการอบรมหรือการสื่อสารข้อมูลที่เกี่ยวข้องกับภัยคุกคาม มาตรการป้องกัน และข้อกำหนดที่เกี่ยวข้องอย่างสม่ำเสมอ เพื่อให้บุคลากรสามารถรับมือกับความเสี่ยงใหม่ได้อย่างเหมาะสม
3) บุคคลภายนอกต้องมีการวัดผลหรือประเมินความเข้าใจหลังการอบรมตามความเหมาะสม และต้องจัดเก็บหลักฐานการอบรมหรือผลการประเมินไว้ เพื่อใช้เป็นหลักฐานในการตรวจสอบเมื่อบริษัทร้องขอ
4) บุคลากรของบุคคลภายนอกที่ได้รับได้รับสิทธิเข้าถึงข้อมูล ระบบ หรือทรัพย์สินสารสนเทศของบริษัทต้องได้รับการอบรมหรือรับทราบข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลก่อนหรือภายในระยะเวลาที่เหมาะสมของการเริ่มปฏิบัติงาน
5) บุคคลภายนอกต้องทบทวนและปรับปรุงแผนการอบรมหรือกิจกรรมสร้างความตระหนักรู้ให้สอดคล้องกับการเปลี่ยนแปลงของภัยคุกคาม เทคโนโลยี กฎหมาย และข้อกำหนดที่เกี่ยวข้อง

3.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Incident Management)

<u>วัตถุประสงค์:</u> เพื่อให้สามารถรับมือจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพสอดคล้องกับกฎหมายและมาตรฐานสากล

1) บุคคลภายนอกต้องกำหนดกระบวนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ รวมทั้งจัดทำเอกสารขั้นตอนการปฏิบัติ โดยครอบคลุมการจัดประเภทเหตุการณ์ การกำหนดระดับความรุนแรง และโครงสร้างการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ไปยังหน่วยงานที่เกี่ยวข้อง รวมถึงต้องสื่อสารให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องรับทราบ
2) บุคคลต้องจัดทำแผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับความเสี่ยงที่เกี่ยวข้อง และต้องมีการสื่อสาร ฝึกอบรม หรือซักซ้อมให้กับผู้ที่เกี่ยวข้องอย่างเหมาะสม
3) บุคคลภายนอกต้องมีเครื่องมือ เทคนิค หรือกระบวนการที่เหมาะสมและปลอดภัย เพื่อสนับสนุนการตรวจสอบเหตุการณ์บนระบบคอมพิวเตอร์ การตรวจจับการโจมตี และการตรวจพบการใช้งานระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต
4) บุคคลภายนอกต้องทบทวนแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง นับแต่วันที่แผนได้รับการอนุมัติ หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

5) บุคคลภายนอกต้องกำหนดเจ้าหน้าที่ผู้รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อย 1 คน เพื่อเป็นผู้ประสานงานและแจ้งให้บริษัททราบเมื่อพบเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงประสานงานกับพนักงานของบริษัทในกรณีที่บริษัทเป็นผู้พบเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบุคคลภายนอก
6) กรณีพบเหตุการณ์ละเมิดด้านความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบต่อบริษัท บุคคลภายนอกต้องแจ้งเหตุการณ์พร้อมรายละเอียดเท่าที่มีให้บริษัทรับทราบโดยไม่ชักช้า และภายในระยะเวลาไม่เกิน 12 ชั่วโมง นับตั้งแต่ทราบเหตุการณ์ ทั้งนี้ เมื่อมีความคืบหน้าหรือมีข้อมูลเพิ่มเติม ต้องแจ้งให้บริษัททราบเป็นระยะ และจัดทำรายงานเหตุการณ์ที่สมบูรณ์แบบให้แก่บริษัทโดยเร็ว
7) ภายหลังการจัดการเหตุการณ์ บุคคลภายนอกต้องวิเคราะห์สาเหตุของเหตุการณ์ จัดทำบทเรียนที่ได้รับ (Lesson Learned) และปรับปรุงมาตรการควบคุมหรือกระบวนการที่เกี่ยวข้อง เพื่อลดโอกาสเกิดเหตุการณ์ซ้ำ

3.17 การจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)

วัตถุประสงค์: เพื่อป้องกันและลดผลกระทบต่อกระบวนการทางธุรกิจที่สำคัญของบริษัทจากเหตุขัดข้องร้ายแรงของระบบสารสนเทศ เหตุฉุกเฉิน หรือภัยพิบัติ และเพื่อให้บริษัทสามารถดำเนินงานได้อย่างต่อเนื่องหรือฟื้นฟูการดำเนินงานได้ภายในระยะเวลาที่เหมาะสม

1) บุคคลภายนอกต้องจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Disaster Recovery Plan: DRP) ที่ครอบคลุมถึงการให้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก เพื่อให้มีแนวทางรองรับและสามารถให้บริการและดำเนินธุรกิจได้อย่างต่อเนื่อง
2) แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรคำนึงถึงความเสี่ยงที่อาจส่งผลต่อการหยุดชะงักของการให้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ผลกระทบที่มีต่อการให้บริการ ความพร้อมใช้ของข้อมูลและทรัพยากรที่จำเป็น การติดต่อสื่อสารระหว่างบุคคลภายนอกกับบริษัท รวมถึงการรายงานเหตุการณ์ผิดปกติให้บริษัททราบอย่างทันท่วงที
3) บุคคลภายนอกต้องมีการทดสอบ ทบทวน และปรับปรุงแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ที่ครอบคลุมถึงการให้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลที่เกี่ยวข้องกับบริษัท อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
4) บุคคลภายนอกต้องสนับสนุนหรือมีส่วนร่วมกับการทดสอบหรือการซักซ้อมแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan Testing) ของบริษัท ตามที่บริษัทกำหนด