นโยบายความมั่นคงปลอดภัยสารสนเทศและเทคโนโลยี

(Information Security and Technology Policy)

บริษัท โปร อินไซด์ จำกัด (มหาชน)

ฉบับ: ISO/IEC 27001:2022

วันที่มีผลบังคับใช้: 26 มิถุนายน 2569

เจ้าของเอกสาร: แผนกเทคโนโลยีสารสนเทศ ส่วนงานความมั่นคงปลอดภัยสารสนเทศ

ระดับชั้นความลับ: ข้อมูลภายใน

รอบทบทวน: อย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงสาระสำคัญ

การควบคุมเอกสาร

ประวัติการแก้ไข: v1.0 — จัดทำตาม ISO/IEC 27001:2022

ขอบเขตการเผยแพร่: อนุญาตให้เข้าถึงเฉพาะพนักงาน/ผู้รับจ้างที่จำเป็นต่อหน้าที่ และต้องยอมรับเงื่อนไขการใช้งานข้อมูลของ บริษัท โปร อินไซด์ จำกัด (มหาชน)

สารบัญ

บทนำ (Introduction) 8
บทสรุปผู้บริหาร 8
1. วัตถุประสงค์และขอบเขต 9
2. มาตรฐาน กฎหมาย และพระราชบัญญัติที่เกี่ยวข้อง 10
3. คำนิยามศัพท์และคำจำกัดความ (Terminology and Abbreviation) 11
ส่วนประกอบของความปลอดภัยข้อมูลสารสนเทศ 15
โครงสร้างการจัดการเรื่องความปลอดภัยข้อมูล 15
4. บทบาทและความรับผิดชอบ (Role and Responsibility) 16
สิทธิหน้าที่และความรับผิดชอบ 18
การบริหารข้อยกเว้น (Exception Management) 25
นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) 26
5. มาตรการควบคุมด้านบริษัทฯ (Organization controls) Annex 5 26
5.1. นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศ (Policies for Information Security) 26
5.2. บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยี (Information Security Roles and Responsibilities) 26
5.3. การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties) 27
5.4. การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with Authorities) 27
5.5. การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with Special Interest Groups) 27
5.6. ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม (Threat intelligence) 27
5.7. ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information Security in Project Management) 28
5.8. บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ (Inventory of information and other associated assets) 28
5.8.1. ทะเบียนสินทรัพย์ (Inventory of Assets) 28
5.8.2. การใช้งานข้อมูลและทรัพย์สินสารสนเทศที่เกี่ยวข้องอื่น ๆ อย่างเหมาะสม (Acceptable Use for information and other associated Assets) 28
5.8.3. การจัดการสินทรัพย์ (Handling of Asset) 29
5.8.4. การคืนสินทรัพย์ (Return on Assets) 29
5.8.5. การจัดหมวดหมู่ข้อมูลและสินทรัพย์สารสนเทศ (Classification Information Control) 29
5.8.6. การจัดทำป้ายชื่อของข้อมูล (Labeling of Information Control) 30
5.8.7. การถ่ายโอนข้อมูล (Information Transfer) 30
5.9. การควบคุม การเข้าถึง (Access Control) 31
5.10. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) 32
5.10.1. การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User Registration and De-Registration) 32
5.10.2. การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning) 32

5.10.3. การบริหารจัดการสิทธิตามระดับสิทธิการเข้าถึง (Management of Privileged Access Right) 32
5.10.4. การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of User) 32
5.10.5. การทบทวนสิทธิในการเข้าถึงระบบของผู้ใช้งาน (Review of User Access Rights) 32
5.10.6. การถอนหรือการจัดการสิทธิการเข้าถึง (Removal or Adjustment of Access Rights) 32
5.11. การควบคุมการเข้าถึงระบบ (System and Application Access Control) 32
5.11.1. การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) 32
5.11.2. การใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs) 33
5.11.3. การควบคุมการเข้าถึงรหัสต้นฉบับสำหรับระบบ (Access Control to Program Source Code) 33
5.11.4. การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network and Network Services) 33
5.11.5. การบริหารจัดการ อัตลักษณ์ (Identify Management) 36
5.11.6. การพิสูจน์ตัวตน (Authentication Information) 36
5.11.7. การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information) 37
5.12. ความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Supplier Relationships) 37
5.12.1. นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships) 37
5.12.2. การควบคุมการเข้าใช้งานของผู้ให้บริการภายนอก (Third Party) 37
5.12.3. การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการผู้ให้บริการภายนอก (Assessing Security within Supplier Agreements) 38
5.12.4. ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศ และการสื่อสารโดยผู้ให้บริการภายนอก (Information and Communication Technology Supply Chain) 38
5.12.5. การบริหารจัดการ การให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management) 38
5.12.6. การบริหารการจัดด้านความปลอดภัยบริการคลาวด์ (Information Security for using Cloud Services) 39
5.13. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีและการปรับปรุง (Management of Information Security Incidents and Improvements) 39
5.13.1. การกระทำอื่น ๆ ที่ถือเป็นข้อห้ามของบริษัท 40
5.13.2. การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ (Reporting information security weaknesses) 40
5.13.3. การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events) 41
5.13.4. การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents) 41
5.13.5. การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents) 42
5.14. การเก็บรวบรวมหลักฐาน (Collection of Evidence) 42
5.15. ความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีระหว่างการหยุดชะงัก (Information security during disruption) 43

5.15.1. ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีของการบริหารจัดการ เพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management) 43
5.15.2. ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity) 43
5.15.3. การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing information security continuity) 44
5.16. การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies) 44
5.16.1. สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities) 44
5.16.2. ความพร้อม ICT เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity) 45
5.17. กฎหมาย ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับและข้อผูกพันตามสัญญา (Legal, statutory, regulatory and contractual requirements) 45
5.17.1. การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements) 45
5.18. สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights) 46
5.18.1. การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records) 47
5.18.2. ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information) 47
5.18.3. การป้องกันข้อมูลสำคัญของบริษัท (Protection of Organizational Records) 47
5.18.4. การควบคุมการเข้ารหัส (Regulation of cryptographic controls) 47
5.18.5. การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of Misuse of Information Processing Facilities) 47
5.18.6. การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยี (Independent Review of Information Security) 48
5.18.7. การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความปลอดภัยสารสนเทศ (Compliance with policies, rules and Security Standards for information security) 48
5.18.8. การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review) 48
5.18.9. เอกสารขั้นตอนการปฏิบัติงาน (Document Operating Procedures) 48
6. มาตรการควบคุมด้านเจ้าหน้าที่ (People Control) Annex 6 49
6.1. ก่อนการจ้างงาน (Prior to Employment) 49
6.1.1. การสรรหาเจ้าหน้าที่ (Screening) 49
6.1.2. ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and Conditions of Employment) 49
6.2. ระหว่างการจ้างงาน (During employment) 50
6.2.1. การสร้างความตระหนัก การให้ความรู้ บุคลากรฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training) 50
6.2.2. กระบวนการทางวินัย (Disciplinary process) 50

6.3. ความรับผิดชอบหลังการสิ้นสภาพหรือการเปลี่ยนแปลงการจ้างงาน (Responsibilities after Termination or Change of Employment) 51
6.3.1. การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or change of employment responsibilities) 51
6.3.2. การรักษาความลับ หรือข้อตกลงการไม่เปิดเผยข้อมูล (Confidentiality or Non-Disclosure Agreements) 51
6.3.3. การปฏิบัติงานจากระยะไกล (Teleworking) 51
6.3.4. การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Information Security Event Reporting) 52
7. มาตรการทางกายภาพ (Physical Controls) Annex 7 52
7.1 ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมของบริษัท (Physical and Environmental Security) 52
7.2. พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas) 53
7.2.1. การควบคุมการเข้าออกทางกายภาพ (Physical Entry Controls) 53
7.2.2. การรักษาความมั่นคงปลอดภัยบริษัท ห้องทำงาน และเครื่องมือต่าง ๆ (Securing Offices, Rooms and Facilities) 54
7.2.3. การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external and environmental threats) 54
7.2.4. การปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Working in secure areas) 54
7.2.5. พื้นที่สำหรับรับส่งสิ่งของ (Delivery and loading areas) 55
7.3. ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security) 55
7.3.1. การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection) 55
7.3.2. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) 55
7.3.3. ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security) 56
7.3.4. การบำรุงรักษาอุปกรณ์ (Equipment maintenance) 56
7.3.5. การนำทรัพย์สินของบริษัทออกนอกบริษัท (Removal of assets) 56
7.3.6. ความมั่นคงปลอดภัยของอุปกรณ์ และทรัพย์สินที่ใช้งานอยู่ภายนอกบริษัท (Security of equipment and assets off premises) 56
7.3.7. นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy) 56
8. มาตรการควบคุมทางด้านเทคโนโลยี (Technological Control) Annex 8 57
8.1. นโยบายสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile Device Policy) 57
8.1.1. การป้องกันอุปกรณ์ของผู้ใช้งานที่ไม่มีผู้ดูแล (Unattended User Equipment) 58
8.1.2. การบริหารจัดการสิทธิตามระดับสิทธิการเข้าถึง (Privileged Access Right) 58
8.1.3. การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) 58
8.1.4. การควบคุมการเข้าถึงรหัสต้นฉบับสำหรับระบบ (Access Control to Program Source Code) 58
8.1.5. ขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure authentication) 58
8.1.6. การบริหารจัดการขีดความสามารถของระบบ (Capacity management) 59

8.1.7. การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, testing and operational environments) 59
8.2. การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware) 59
8.2.1. มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware) 59
8.2.2. การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical Vulnerability) 60
8.2.3. การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review) 60
8.2.4. การจัดการการตั้งค่า (Configuration Management) 60
8.2.5. การลบข้อมูล (Information deletion control) 61
8.2.6. การซ่อนข้อมูล (Data Marking) 61
8.2.7. การป้องกันข้อมูลรั่วไหล (Data Leakage prevent control) 61
8.2.8. การสำรองข้อมูล (Information backup) 61
8.2.9. การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies) 62
8.3. การบันทึกข้อมูลการใช้งาน และการเฝ้าระวัง (Logging and Monitoring) 63
8.3.1. การบันทึกข้อมูลเหตุการณ์ (Event logging) 63
8.3.2. การป้องกันข้อมูลล็อก (Protection of log information) 63
8.3.3. ข้อมูล ล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs) .. 65
8.3.4. การเฝ้าติดตามกิจกรรม (Monitoring activities) 65
8.3.5. การตั้งเวลาให้ถูกต้อง (Clock Synchronization) 65
8.3.6. การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operation software) 66
8.3.7. การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation) 66
8.4. ความมั่นคงปลอดภัยระบบเครือข่าย (Network Security) 66
8.4.1. การควบคุมการเข้าถึงเครือข่าย (Network Control) 66
8.4.2. ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Service) 67
8.4.3. การจัดแบ่งเครือข่ายภายในสำนักงานฯ (Segregation in Network) 67
8.4.4. การกรองเว็บ (Web Filtering) 68
8.5. การกำหนดการควบคุมการเข้ารหัสข้อมูล (Use of Cryptography) 69
8.5.1. มาตรการการเข้ารหัสลับข้อมูล (Cryptographic Controls) 69
8.5.2. การบริหารจัดการกุญแจในการเข้ารหัสข้อมูล (Key Management) 69
8.6. ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes) 70
8.6.1. นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy) 70
8.6.2. ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System change control procedures) 70
8.6.3. การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes) 70
8.6.4. การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages) 70
8.6.5. หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles) 70

8.6.6. สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)..... 71
8.6.7. การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development)..... 71
8.7.8. การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing) 72
8.7.9. การทดสอบเพื่อรับรองระบบ (System acceptance testing) 72
8.8. ข้อมูลสำหรับการทดสอบ (Test data) 73
8.8.1. การป้องกันข้อมูลสำหรับการทดสอบ (Protection of test data) 73
8.9. การบริหารการเปลี่ยนแปลง (Change Management) 73
8.9.1. นโยบายการบริหารการเปลี่ยนแปลง (Change Management)..... 73
8.9.2. กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (System Change Control Procedures)..... 73
8.9.3. การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating Platform Changes)..... 74
8.9.4. การควบคุมการเปลี่ยนแปลงของซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)74
9. ข้อปฏิบัติและข้อบังคับตามกฎหมาย 75
การปฏิบัติตามนโยบายและระเบียบ 75
การปฏิบัติตามกฎหมายและข้อบังคับต่าง ๆ 75
10. ระเบียบและบทลงโทษ..... 75
บทสรุป..... 77

บทนำ (Introduction)

บทสรุปผู้บริหาร

ในยุคดิจิทัลปัจจุบัน ข้อมูลและเทคโนโลยีคือทรัพย์สินเชิงกลยุทธ์ที่ขับเคลื่อนความสำเร็จของ บริษัท โปร อินไซด์ จำกัด (มหาชน) ความมั่นคงปลอดภัยของสารสนเทศและเทคโนโลยีจึงเป็นรากฐานสำคัญในการสร้างความเชื่อมั่นให้แก่ลูกค้า พันธมิตร ผู้ถือหุ้น และสังคมโดยรวม นโยบายความมั่นคงปลอดภัยสารสนเทศและเทคโนโลยีฉบับนี้จัดทำขึ้นเพื่อกำหนดทิศทาง มาตรฐาน และแนวปฏิบัติที่ชัดเจน ครอบคลุมการคุ้มครองข้อมูล การบริหารความเสี่ยง ความต่อเนื่องทางธุรกิจ ความเป็นส่วนตัวของข้อมูลส่วนบุคคล ความมั่นคงปลอดภัยของระบบคลาวด์ เครือข่าย อุปกรณ์ปลายทาง และโปรแกรมประยุกต์ รวมถึงการบริหารผู้ให้บริการภายนอก

ผู้บริหารของ บริษัท โปร อินไซด์ จำกัด (มหาชน) ขอยืนยันความมุ่งมั่นดังต่อไปนี้

- ปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้องทั้งหมด รวมถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และแนวปฏิบัติสากลที่เหมาะสม (เช่น ISO/IEC 27001)
- บริหารจัดการความเสี่ยงด้านไซเบอร์อย่างเป็นระบบ โดยอิงหลักการบริหารความเสี่ยง ให้ความสำคัญกับผลกระทบทางธุรกิจและความต่อเนื่องในการให้บริการ
- ลงทุนและสนับสนุนทรัพยากร บุคลากร กระบวนการ และเทคโนโลยีที่จำเป็น เพื่อเสริมสร้างความพร้อมในการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากเหตุการณ์ด้านความมั่นคงปลอดภัย
- สร้างวัฒนธรรมความมั่นคงปลอดภัยในทุกระดับ ส่งเสริมการเรียนรู้และการอบรมสม่ำเสมอ เพื่อให้ทุกคนตระหนักและปฏิบัติตามได้อย่างมีประสิทธิภาพ
- ทบทวนและปรับปรุงนโยบาย มาตรการ และการควบคุมอย่างต่อเนื่อง ผ่านการประเมิน การทดสอบ และการตรวจประเมินอิสระตามระยะเวลา

ความมั่นคงปลอดภัยเป็นความรับผิดชอบร่วมกันของทุกคนในบริษัท จึงขอความร่วมมือพนักงานและผู้เกี่ยวข้องทุกท่าน

- ศึกษา ทำความเข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติของบริษัทอย่างเคร่งครัด
- ปกป้องข้อมูลตามระดับความอ่อนไหว ใช้การยืนยันตัวตนที่รัดกุม (เช่น MFA) และจัดการรหัสผ่านอย่างปลอดภัย
- ระมัดระวังภัยคุกคามทางสังคมออนไลน์และE-mail Phishing รายงานเหตุการณ์หรือข้อผิดปกติทันทีผ่านช่องทางที่กำหนด
- ปฏิบัติตามกระบวนการจัดซื้อและบริหารความเสี่ยงของผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าห่วงโซ่อุปทานมีความมั่นคงปลอดภัย
- สนับสนุนการทดสอบ แผนความต่อเนื่องทางธุรกิจ/ กู้คืนระบบ และการปรับปรุงอย่างต่อเนื่อง

นโยบายฉบับนี้มีผลบังคับใช้กับพนักงาน ลูกจ้างชั่วคราว ที่ปรึกษา ผู้รับจ้าง และคู่ค้าทุกฝ่ายที่เข้าถึงข้อมูลหรือระบบของ บริษัท โปร อินไซด์ จำกัด (มหาชน) และจะได้รับการทบทวนอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านความเสี่ยง เทคโนโลยี หรือข้อกำกับดูแลที่มีนัยสำคัญ

1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทได้ถูกใช้งานโดยผู้ใช้งาน เป็นไปอย่างเหมาะสม มีประสิทธิภาพ และมีความมั่นคงปลอดภัยและอีกทั้งยังสามารถดำเนินงานในการใช้งานระบบได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยคุกคามในหลากหลายรูปแบบที่มีผลต่อการดำเนินการทางธุรกิจอีกทั้งยังช่วยลดความเสี่ยงที่มีแนวโน้มว่าจะเกิดขึ้น โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

1.1. การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของบริษัท ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผลที่ดีที่สุด

1.2. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอ้างอิงตามมาตรฐานสากลและมีการปรับปรุงอย่างต่อเนื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อีกทั้งยังนำกรอบการประเมินความเสี่ยงของส่วนงานมาใช้ในการจัดการกับการทำงานด้านเทคโนโลยีสารสนเทศด้วยกรอบของ Information Security คือ ความลับ Confidentiality (C) ความถูกต้อง Integrity (I) ความพร้อมใช้ Availability (A)

1.3. นโยบายนี้จะต้องทำการเผยแพร่ให้กับพนักงานทุกระดับได้รับทราบ และพนักงานทุกคนจะต้องยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

1.4. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร พนักงาน ผู้ดูแลระบบ (System Administrators) และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

1.5. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้งต่อปี

1.6. นโยบายฉบับนี้ดำเนินการภายใต้กรอบกระบวนการคุ้มครองข้อมูลส่วนบุคคลประกาศใช้เมื่อ วันที่ 1 มิถุนายน ปีพุทธศักราช 2565

2. มาตรฐาน กฎหมาย และพระราชบัญญัติที่เกี่ยวข้อง

2.1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (พ.ศ. 2550) และฉบับแก้ไข (พ.ศ. 2560): กำหนดความผิดและบทลงโทษเกี่ยวกับการเข้าถึงข้อมูลโดยมิชอบ, การรบกวนระบบคอมพิวเตอร์, การเผยแพร่ข้อมูลอันเป็นเท็จ, การปลอมแปลงข้อมูล, และการก่อให้เกิดความเสียหายต่อระบบสาธารณูปโภค

2.2. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (พ.ศ. 2544) และฉบับแก้ไข: ให้การรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ ให้มีผลผูกพันเหมือนเอกสารและลายมือชื่อจริง เพื่อรองรับการทำธุรกรรมออนไลน์

2.3. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (พ.ศ. 2562 - PDPA): กำหนดหลักเกณฑ์การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อคุ้มครองสิทธิของเจ้าของข้อมูล

2.4. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2562): กำหนดมาตรการและกรอบการทำงานเพื่อรับมือกับภัยคุกคามทางไซเบอร์ และการรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

2.5. พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ (พ.ศ. 2563): รับรองการประชุมผ่านสื่ออิเล็กทรอนิกส์ ให้มีผลทางกฎหมายเช่นเดียวกับการประชุมปกติ

2.6. พระราชบัญญัติลิขสิทธิ์: คุ้มครองผู้สร้างสรรค์ทันทีที่สร้างผลงาน (ไม่ต้องจดทะเบียน) โดยให้สิทธิแต่เพียงผู้เดียวในการทำซ้ำ ดัดแปลง เผยแพร่ เช่น งานวรรณกรรม ศิลปกรรม ดนตรี ภาพยนตร์ โปรแกรมคอมพิวเตอร์ และอื่นๆ

2.7. ISO/IEC 27001: มาตรฐานระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ที่ได้รับการยอมรับทั่วโลก เน้นหลัก Confidentiality, Integrity, Availability (CIA Triad)

2.8. NIST Cybersecurity Framework (CSF): กรอบการทำงานของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา (NIST) ให้แนวทางปฏิบัติที่ดีที่สุดในการบริหารจัดการความเสี่ยงด้านไซเบอร์

2.9. PCI DSS: มาตรฐานความปลอดภัยข้อมูลสำหรับอุตสาหกรรมการชำระเงิน (Payment Card Industry Data Security Standard)

2.10. ISO/IEC 20000: (IT Service Management - ITSM) สำหรับการบริหารจัดการบริการด้าน IT ให้เป็นระบบและมีประสิทธิภาพ เช่น การจัดการเหตุการณ์ (Incident Management), การจัดการปัญหา (Problem Management) และการกำหนดระดับบริการ (Service Level Management).

2.11. ISO/IEC 27701: ส่วนขยายของ ISO 27001 สำหรับการบริหารจัดการข้อมูลส่วนบุคคล (Privacy Information Management)

2.12. ITIL (Information Technology Infrastructure Library): เป็นกรอบแนวปฏิบัติที่ดีที่สุด (Best Practice) ในการบริหารจัดการบริการ IT ซึ่งสามารถนำมาใช้ร่วมกับ ISO 20000 ได้

3. คำนิยามศัพท์และคำจำกัดความ (Terminology and Abbreviation)

- บริษัท หมายถึง บริษัท บริษัท โปร อินไซด์ จำกัด (มหาชน)

- พนักงาน, คนทำงาน, และ ผู้ใช้งาน หมายถึง พนักงานที่ถูกว่าจ้างทุกประเภท เพื่อทำงานให้กับ บริษัท โปร อินไซด์ จำกัด (มหาชน) เช่น พนักงานประจำ, พนักงานว่าจ้างตามสัญญา, พนักงานว่าจ้างชั่วคราว, และ พนักงานว่าจ้างเป็นช่วงเวลา รวมถึงผู้บริหารในระดับต่าง ๆ ที่อยู่ภายใต้การว่าจ้างของบริษัทฯ

- ระบบ หรือ ระบบคอมพิวเตอร์ หมายถึง เครื่องมือทุกชนิด, เซิร์ฟเวอร์ทุกประเภท และอุปกรณ์คอมพิวเตอร์ ทั้งในแบบมีสายและไร้สาย ทุกอย่างที่อยู่ในอุปกรณ์และสื่อบันทึกต่าง ๆ เพื่อใช้สำหรับส่งข้อมูลผ่านทางอินเทอร์เน็ต

(ออกภายนอกบริษัท) เอ็กซ์ทราเน็ต (ภายในเครือข่ายที่เชื่อถือได้ที่ต่อกับบริษัท) และอินทราเน็ต (ภายในบริษัท) รวมถึงอุปกรณ์อิเล็กทรอนิกส์ทุกอย่างและอุปกรณ์โทรคมนาคมที่ใช้งานคล้ายคลึง กับคอมพิวเตอร์ ทั้งนี้ยังรวมไปถึงสิ่งของต่าง ๆ ที่เป็นทรัพย์สินของ บริษัทและกลุ่มบริษัทในเครือสกาย ไอซีที และที่เป็นของผู้ร่วมทำงานหรือหุ้นส่วน และที่เป็นของผู้ขายที่มีการซื้อ ติดตั้ง และตั้งอยู่ในพื้นที่ของ บริษัทฯ ไม่ว่าสิ่งของหรืออุปกรณ์เหล่านั้นจะอยู่ในสภาวะแบบใด

- ข้อมูล หรือ ข้อมูลคอมพิวเตอร์ หมายถึง สัญญาณอิเล็กทรอนิกส์ ไฟฟ้า เสียง หรือรูปแบบอื่น ๆ ทุกชนิดที่สามารถถูกเปลี่ยนหรือแปลงให้มีความหมายเพื่อให้มนุษย์เข้าใจได้ เช่น ตัวอักษร รูปภาพนิ่งภาพเคลื่อนไหว เสียง หรือรูปแบบอื่น ๆ ที่สามารถใช้เพื่อการสื่อสารระหว่างคนด้วยกันได้โดยใช้อุปกรณ์อิเล็กทรอนิกส์ หรืออุปกรณ์คอมพิวเตอร์ในการส่งสารจากอีกที่หนึ่งไปยังอีกที่หนึ่ง หรือเก็บบันทึกไว้ในเครื่องมืออื่น ๆ และสามารถนำไปใช้ใหม่ ชั่วคราวหรือตลอดไปได้

- การเข้าถึง หมายถึง การเข้าสถานที่ การใช้งานทางอิเล็กทรอนิกส์หรือกายภาพ รวมถึงการรับรู้ซึ่งข้อมูล

- การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ การตรวจสอบ การอนุมัติและการกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ การเพิกถอนหรือการยกเลิกสิทธิการเข้าถึง

- การควบคุมการเข้าถึง หมายถึง การอนุญาต การกำหนดสิทธิการเปลี่ยนแปลง การเพิกถอนหรือการยกเลิกสิทธิการเข้าถึง

- การจัดการทรัพยากรระบบ (Capacity Management) หมายถึง การบริหารจัดการทรัพยากรและการกำหนดค่าขีดความสามารถของเจ้าหน้าที่แผนการดำเนินงาน และอื่น ๆ

- การบริหารจัดการเปลี่ยนแปลง (Change Management) หมายถึง กระบวนการควบคุมการเปลี่ยนแปลงระบบสารสนเทศหรือระบบงาน ซึ่ง การเปลี่ยนแปลงดังกล่าวจะมีผลกระทบต่อฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ ระบบ (System Software) ซอฟต์แวร์ประยุกต์ (Application Software) และระบบเครือข่าย (Network System) เป็นต้น

- การประเมินความเสี่ยง หมายถึง กระบวนการทั้งหมดในการวิเคราะห์และประเมินความเสี่ยง

- กลุ่มข้อมูลใช้ภายใน (Internal Use) หมายถึง ข้อมูลข่าวสารที่ใช้เฉพาะภายในบริษัทเท่านั้น สามารถเผยแพร่ภายในบริษัทได้แต่ห้ามเผยแพร่แก่บุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยผู้บริหารระดับผู้จัดการฝ่ายส่วนเจ้าของข้อมูลขึ้นไปและต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง

- กลุ่มข้อมูลลับ (Confidential) หมายถึง ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่บิรษัทฯ ซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยผู้จัดการฝ่ายเจ้าของข้อมูลขึ้นไปโดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอานาจที่กฎหมายให้การรับรอง

- กลุ่มข้อมูลลับมาก (Confidential) หมายถึง ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอก เว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยระดับผู้จัดการฝ่ายที่เป็นเจ้าของข้อมูลขึ้นไป โดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง

- กลุ่มข้อมูลลับที่สุด (Highly Confidential) หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ อย่างร้ายแรงที่สุดซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) ต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง

- กลุ่มข้อมูลสาธารณะ (Public) หมายถึง ข้อมูลข่าวสารที่เปิดเผยสามารถเผยแพร่แก่สาธารณะได้

- ข้อมูล (Data) หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของซีดี (CD) ดีวีดี (DVD) Hard Disk Thumb drive เอกสาร แฟ้มรายงาน หนังสือ แผนที่ แผนผัง ภาพวาด ภาพถ่าย การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

- ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

- ความต่อเนื่องในการดำเนินงานของบริษัท (Business Continuity Management: BCM) หมายถึง แนวทางในการบริหารจัดการธุรกิจได้อย่างต่อเนื่อง เมื่อบริษัทอยู่ภายใต้สภาวะวิกฤตและเหตุฉุกเฉินต่าง ๆ ทำให้มั่นใจได้ว่า ขั้นตอนการดำเนินงานและระบบสารสนเทศต่าง ๆ ของบริษัท ที่สำคัญได้รับการวางแผนความต่อเนื่องในการดำเนินงานของบริษัท (Business Continuity Plan หรือ BCP) และแผนสำรองฉุกเฉิน (Disaster Recovery Plan หรือ DRP) อย่างเหมาะสม

- เจ้าของข้อมูล (Information Owner) หมายถึง ผู้ซึ่งรับผิดชอบข้อมูลของบริษัทซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยเจ้าของข้อมูลเป็นผู้ที่รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรง หากข้อมูลเหล่านั้นเกิดสูญหาย

- เจ้าของระบบงาน (System Owner) หมายถึง ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ในบริษัท

- นิสิตและนักศึกษาฝึกงาน หมายถึง นิสิตและนักศึกษาที่บริษัทอนุญาตให้เข้ามาทดลองปฏิบัติงานโดยมีช่วงระยะเวลาที่กำหนดไว้

- โปรแกรมประยุกต์ หรือ แอปพลิเคชัน (Application) หมายถึง โปรแกรมประเภทหนึ่งที่ถูกสร้างขึ้นสำหรับใช้งานเฉพาะทาง

- พื้นที่ใช้งานระบบสารสนเทศ (Information System Workspaces) หมายถึง พื้นที่ที่บริษัทอนุญาตให้มีการใช้งานระบบสารสนเทศ โดยแบ่งเป็น

พื้นที่มั่นคงปลอดภัย (Secure Area) คือ พื้นที่ที่มีการควบคุมการเข้าถึง และมีระบบการป้องกันจากภัยคุกคามต่าง ๆ

พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator / Operator Area) คือ พื้นที่สำหรับพนักงานดูแลระบบใช้ในการปฏิบัติงานในการดูแลระบบสารสนเทศของบริษัท

ห้องปฏิบัติงานทั่วไป (Working Area) ห้องประชุม เช่น พื้นที่ปฏิบัติงานทั่วไปของพนักงานของบริษัท

พื้นที่ทั่วไป (General Area) คือ พื้นที่สำหรับใช้รับรองบุคคลที่มาติดต่อบริษัท

- ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือส่งข้อมูลระหว่าง ระบบคอมพิวเตอร์ได้แก่ ระบบ LAN (Local Area Network) ระบบ WLAN (Wireless LAN) ระบบ Intranet และระบบ เป็นต้น

- ระบบเครือข่ายไร้สาย (Wireless LAN: WLAN) หมายถึง ระบบเครือข่ายที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ รวมถึงการติดต่อสื่อสารระหว่างช่องทางการสื่อสารแทน

- ระบบสารสนเทศ (Information System) หมายถึง ระบบงานที่นำเทคโนโลยีมาช่วยในการสร้างสารสนเทศที่สามารถนามาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งประกอบด้วยเทคโนโลยีคอมพิวเตอร์และ เทคโนโลยีการสื่อสารโทรคมนาคม ได้แก่ ระบบคอมพิวเตอร์ (Computer System) ระบบเครือข่าย (Network System) ซอฟต์แวร์ (Software) ข้อมูล (Data) และสารสนเทศ (Information) เป็นต้น

- ระบบ Intranet หมายถึง ระบบเครือข่ายที่สามารถเข้าถึงได้โดยผู้ใช้งานภายในบริษัทเท่านั้น โดยมีจุดประสงค์เพื่อการติดต่อ สื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในบริษัท

- ระบบ Internet หมายถึง ระบบเครือข่ายที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ของบริษัทเข้ากับระบบคอมพิวเตอร์ทั่วโลก

- ระบบ LAN หมายถึง ระบบเครือข่ายแบบเชื่อมต่อคอมพิวเตอร์เข้าด้วยกันในระยะจำกัด เช่น ในอาคารเดียวกัน หรือบริเวณเดียวกันที่สามารถลากสายถึงกันได้โดยตรง

- สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายถึง สถานการณ์ซึ่งมีแนวโน้มทำให้ระบบของบริษัทถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

- สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผนการตัดสินใจ และอื่น ๆ

- สิทธิของผู้ใช้งาน สิทธิและหน้าที่ตามบทบาท (Role) ที่เกี่ยวข้องกับระบบสารสนเทศของบริษัท มีดังนี้

- สิทธิใช้งานทั่วไป หมายถึง คณะกรรมการ ผู้อำนวยการ รองผู้อำนวยการผู้จัดการฝ่าย พนักงาน ลูกจ้าง บุคคลที่ใช้งานระบบสารสนเทศพื้นฐานของบริษัท ผู้ใช้งานต้องขออนุญาตจากผู้จัดการฝ่ายส่วนขึ้นไป โดยให้ใช้แบบฟอร์มเพื่อขออนุมัติตามที่บริษัทกำหนด

- สิทธิพิเศษ หมายถึง สิทธิที่ได้รับมอบหมายเพิ่มเติมจากผู้บังคับบัญชาเป็นกรณีพิเศษ ผู้ใช้งานต้องได้รับมอบหมายจากผู้บังคับบัญชาเป็นครั้งคราว

- สื่อสังคมออนไลน์ (Social Media) หมายถึง สังคมออนไลน์ที่ผู้ใช้อินเทอร์เน็ตสามารถแลกเปลี่ยนประสบการณ์ซึ่งกันและกัน โดยใช้สื่อต่าง ๆ เป็นตัวแทนในการสนทนา โดยได้มีการจัดแบ่งประเภทของ Social Media ออกเป็นหลายประเภท ได้แก่

- ประเภทสื่อสิ่งพิมพ์ (Publish) หมายถึง เช่น Wikipedia, WordPress, Pantip ฯลฯ

- ประเภทสื่อสนทนาและส่งข้อความ (Discuss/SMS/Instant Messaging) เช่น Line, Skype, Facebook Messenger ฯลฯ

- ประเภทเครือข่ายสังคมออนไลน์ (Social Network) เช่น Facebook, LinkedIn, Instagram, Twitter ฯลฯ

- ประเภทบริการวิดีโอออนไลน์ (Online Video) เช่น YouTube, Netflix, TikTok ฯลฯ

- ประเภทบริการฝากรูปภาพ (Photo Sharing) เช่น Flickr, Photobucket ฯลฯ

- หน่วยงานภายนอก/ ผู้ให้บริการภายนอก/ บุคคลภายนอก หมายถึง ผู้ให้บริการภายนอก (Third Party) หรือบุคคลภายนอก ที่ใช้งานระบบสารสนเทศของบริษัท ได้เป็นครั้งคราวหรือตามสัญญา

- เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event) กรณีที่เกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

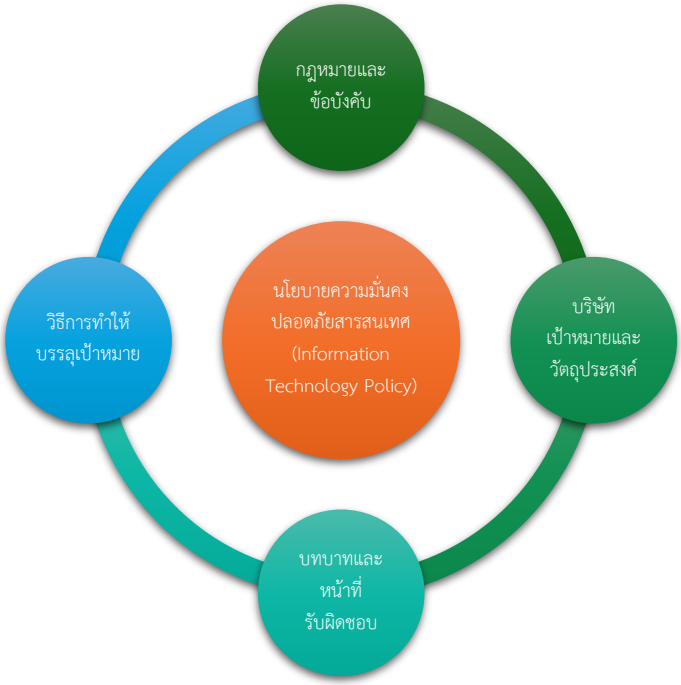
- อุปกรณ์เคลื่อนที่ (Mobile Device) อุปกรณ์ประมวลผลแบบพกพา ที่มีขนาดเล็กสามารถใช้เพียงมือเดียวในการใช้งานส่วนของการรับข้อมูลเป็นแบบสัมผัส โดยไม่ต้องใช้ Keyboard และสามารถเชื่อมต่อเครือข่ายแบบไร้สาย เครือข่ายโทรศัพท์ได้ เช่น Smartphone, Tablet เป็นต้น

- อุปกรณ์ประมวลผล (Computing Device) อุปกรณ์ที่มีหน่วยประมวลผล หน่วยความจำ ส่วนบันทึกข้อมูล ส่วนการเชื่อมต่อเครือข่าย ส่วนรับข้อมูล และส่วนแสดงผล ได้แก่

คอมพิวเตอร์แบบตั้งโต๊ะ เช่น Desktop Computer เป็นต้น

คอมพิวเตอร์แบบพกพา เช่น Notebook, Netbook เป็นต้น

ส่วนประกอบของความปลอดภัยข้อมูลสารสนเทศ



แผนผังด้านบนกล่าวถึงนโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลสารสนเทศนั้นเป็นเอกสารที่มีเนื้อหาอ้างถึงเป้าหมาย วัตถุประสงค์และคุณค่าของบริษัท ซึ่งมีผลต่อภาพลักษณ์ของบริษัทเป็นหลัก ดังนั้นการนำวิธีการต่าง ๆ มาประยุกต์ใช้เพื่อให้สอดคล้องกับนโยบายและทิศทางของธุรกิจจึงเป็นเรื่องที่จำเป็นต้องมีการปฏิบัติใช้จริง นอกจากนี้กฎเกณฑ์ข้อบังคับทางกฎหมายมีส่วนสำคัญในการร่างนโยบายความมั่นคงปลอดภัยสารสนเทศและข้อมูลฉบับนี้เช่น กฎหมายในเรื่องการป้องกันข้อมูล และเอกสารทางอิเล็กทรอนิกส์ที่มีผลบังคับใช้แล้วเป็นต้น และสุดท้ายการกำหนดบทบาทหน้าที่ความรับผิดชอบของพนักงานในแต่ละส่วนงานที่เกี่ยวข้องก็เป็นองค์ประกอบที่สำคัญในการที่จะทำให้พนักงานสามารถทำงานได้ตรงตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

โครงสร้างการจัดการเรื่องความปลอดภัยข้อมูล

นโยบายและระเบียบขั้นตอนทั้งหมดถูกจัดเก็บในรูปแบบเอกสารที่ได้รับการอนุมัติและยอมรับจากทางผู้บริหารอีกทั้งพนักงานของ บริษัท ได้รับทราบถึงการมีนโยบาย ในแง่มุมมองของนโยบายฯ นั้นมีความสำคัญกับทุกฝ่ายและทุกฝ่ายทั้งบริษัทดังนั้นข้อมูลของบริษัทที่มีให้กับพนักงานและข้อมูลที่อยู่ภายใต้ความรับผิดชอบและการกระทำของพนักงาน รักษาข้อมูล หรือระบบที่ใช้ในการประมวลผลข้อมูล หรือแม้แต่วิธีที่ใช้โอนถ่ายข้อมูล ก็จะต้องมีการตรวจสอบ

4. บทบาทและความรับผิดชอบ (Role and Responsibility)

เพื่อสนับสนุนวิสัยทัศน์ (VISION) และพันธกิจ (MISSION) ของกลุ่มบริษัทในการพัฒนาโซลูชันเทคโนโลยีอัจฉริยะให้ภาคเอกชนและภาครัฐ กลุ่มบริษัทกำหนดบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศและระบบเทคโนโลยีสารสนเทศ ดังต่อไปนี้

4.1. คณะกรรมการบริษัท / คณะกรรมการกำกับดูแลที่เกี่ยวข้อง (Board / Governance Committee)

- อนุมัติและกำกับทิศทางเชิงนโยบายด้านความมั่นคงปลอดภัยสารสนเทศของกลุ่มบริษัท
- กำกับให้มีการบริหารความเสี่ยงไซเบอร์ในระดับองค์กร และติดตามประเด็นความเสี่ยงที่มีนัยสำคัญ
- รับทราบรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ร้ายแรง (Major Incident) และผลการทบทวน/ปรับปรุงมาตรการสำคัญ

4.2. ประธานเจ้าหน้าที่บริหาร (CEO) และผู้บริหารสูงสุดของบริษัทในเครือ

- สนับสนุนทรัพยากร (คน/ งบประมาณ/ เครื่องมือ) ให้เพียงพอสำหรับการดำเนินงานด้านความมั่นคงปลอดภัย
- แต่งตั้งผู้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ และกำหนดอำนาจหน้าที่
- อนุมัติการยอมรับความเสี่ยง (Risk Acceptance/ Exception) ในระดับที่กำหนดตามระเบียบของกลุ่มบริษัท

4.3. คณะทำงาน/ คณะกรรมการความมั่นคงปลอดภัยสารสนเทศของกลุ่มบริษัท (Information Security Committee)

- กำหนดเป้าหมาย แผนงาน และตัวชี้วัด (KPI/KRI) ด้านความมั่นคงปลอดภัยของกลุ่มบริษัท
- พิจารณาและจัดลำดับความสำคัญของประเด็นความเสี่ยง/โครงการด้านความปลอดภัย
- ทบทวนเหตุการณ์สำคัญ ช่องโหว่สำคัญ และติดตามการปิดประเด็นคงค้าง
- ตามประกาศหนังสือเลขที่ 2568/06-1 แต่งตั้งคณะกรรมการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยี (Information Security and Technology Services Management System : ISTS) ลงวันที่ “1 มิถุนายน 2568”

4.4. ส่วนงานด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Officer)

- จัดทำ บำรุงรักษา และทบทวนนโยบาย/ มาตรฐาน/ ขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยให้เป็นปัจจุบัน
- ให้คำแนะนำด้านการบริหารความเสี่ยง การจัดชั้นข้อมูล และการกำหนดมาตรการควบคุม (controls)
- กำกับกระบวนการสำคัญ เช่น Vulnerability Management, Incident Response, Security Awareness, Access Control (ในเชิงนโยบาย/การกำกับ)
- รายงานสถานะความเสี่ยง เหตุการณ์สำคัญ และการปฏิบัติตามนโยบายต่อผู้บริหาร/คณะกรรมการที่เกี่ยวข้อง
- ประสานงานกับหน่วยงานภายนอก (เช่น ลูกค้า หน่วยงานรัฐ ผู้ให้บริการ) เมื่อเกี่ยวข้องกับเหตุความมั่นคงปลอดภัย

4.5. ฝ่ายเทคโนโลยีสารสนเทศ/ผู้ดูแลระบบ (IT / System & Network Administrators)

- ดำเนินการควบคุมทางเทคนิคตามนโยบาย เช่น การตั้งค่าความปลอดภัย (hardening), การจัดการแพตช์, การสำรองข้อมูล, การบันทึกเหตุการณ์ (logging), การแยกเครือข่าย, การบริหารสิทธิ
- ปฏิบัติตามกระบวนการ Change Management/ CAB และจัดทำหลักฐานการเปลี่ยนแปลงที่มีผลต่อความมั่นคงปลอดภัย
- สนับสนุนการตรวจสอบ/ ตรวจซ้ำ (retest) ช่องโหว่ และการเก็บหลักฐานเมื่อเกิดเหตุการณ์ผิดปกติ

4.6. เจ้าของทรัพย์สินสารสนเทศ/ เจ้าของระบบ (Information Asset Owner / System Owner)

- รับผิดชอบการกำหนดความสำคัญของระบบ/ ข้อมูล (criticality) และการอนุมัติสิทธิเข้าถึงตามหลักความจำเป็น (need-to-know/ least privilege) ตามแต่บริษัทกำหนด
- รับผิดชอบให้ระบบในความดูแลปฏิบัติตามนโยบาย รวมถึงการแก้ไขช่องโหว่ภายใน SLA ที่กำหนด
- อนุมัติ/ ร่วมพิจารณาแผนแก้ไข ความเสี่ยงคงเหลือ และการยกเว้น (Exception) พร้อมมาตรการชดเชยตามที่กำหนด

4.7. ทีมพัฒนา/ ผู้ดูแลโปรแกรมประยุกต์ (Application Owner / Development Team)

- พัฒนาและบำรุงรักษาซอฟต์แวร์ตามแนวทาง Secure SDLC (เช่น การจัดการช่องโหว่ในโค้ด/ ไลบรารี/ คอนฟิก)
- แก้ไขช่องโหว่ของแอป/ส่วนประกอบ (dependency) และส่งมอบแพตช์/ เวอร์ชันแก้ไขตาม SLA
- บันทึกและทบทวนการเปลี่ยนแปลงผ่านกระบวนการ Change Management ตามที่กำหนด

4.8. ทีมเฝ้าระวังและตอบสนองเหตุการณ์ (Incident Response Team)

- เฝ้าระวัง ตรวจจับ วิเคราะห์ และประสานการตอบสนองเหตุการณ์ความมั่นคงปลอดภัย
- ดำเนินการคุมสถานการณ์ (containment) ร่วมกับ IT/ เจ้าของระบบ และจัดทำรายงานเหตุการณ์ (incident report)/ lessons learned
- ประสานการสื่อสารเหตุการณ์ตามสายการบังคับบัญชาและแผนการสื่อสารขององค์กร

4.9. ฝ่ายกำกับดูแล/ บริหารความเสี่ยง/ กฎหมาย/ คุ้มครองข้อมูลส่วนบุคคล (Compliance/ Risk/ Legal/ DPO)

- กำกับให้การดำเนินงานสอดคล้องข้อกำหนดกฎหมาย/ สัญญา/ มาตรฐานที่เกี่ยวข้อง
- สนับสนุนการประเมินผลกระทบและการจัดการเหตุการณ์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลตามขั้นตอนองค์กร
- ให้คำแนะนำด้านข้อกำหนดการเก็บรักษาหลักฐาน การแจ้งหน่วยงาน/ คู่สัญญา (ตามเงื่อนไขที่เกี่ยวข้อง)

4.10. ฝ่ายบริหารและพัฒนาทรัพยากรบุคคล (PD)

- นำแนวนโยบายมาปรับปรุงและกำหนดแนวทางตามเงื่อนไขและวิธีการ และเพื่อการกำหนดด้านความมั่นคงปลอดภัยในกระบวนการบุคลากร (เช่น Onboarding/ Offboarding, การยอมรับนโยบาย, มาตรการทางวินัย)
- สนับสนุนการสื่อสารและการอบรมความตระหนักรู้ด้านความมั่นคงปลอดภัยให้พนักงาน/ ผู้รับจ้าง

4.11. จัดซื้อ (Procurement)

- กำหนดข้อกำหนดความมั่นคงปลอดภัยในสัญญา/ การจัดซื้อ (เช่น SLA, การรักษาความลับ, การแจ้งเหตุ, สิทธิ์การตรวจประเมิน)
- ติดตามการประเมินความเสี่ยงและการปฏิบัติตามข้อกำหนดของผู้ให้บริการ/ คู่ค้า

4.12. ผู้ใช้งานทุกคน (Employees/ Contractors/ Third Parties)

- ปฏิบัติตามนโยบายและมาตรการที่เกี่ยวข้อง (เช่น การใช้งานรหัสผ่าน, MFA, การจัดการข้อมูล, การใช้อีเมล/ อินเทอร์เน็ต, การรายงานอีเมล phishing)
- รายงานเหตุการณ์/ สิ่งผิดปกติด้านความมั่นคงปลอดภัยต่อช่องทางที่บริษัทกำหนดโดยทันที
- รักษาความลับของข้อมูลและทรัพย์สินของกลุ่มบริษัท และไม่ดำเนินการใด ๆ ที่ฝ่าฝืนนโยบายหรือกฎหมาย

4.13. บริษัทในเครือ (Subsidiaries/Affiliates) และผู้ประสานงานด้านความมั่นคงปลอดภัยของแต่ละหน่วยงานนำไปปฏิบัติตามนโยบายนี้และเอกสารลูก (standards/ procedures) ของกลุ่มบริษัท

- แต่งตั้งผู้ประสานงานด้านความมั่นคงปลอดภัย (Security Focal Point) เพื่อประสานกับส่วนงาน Cybersecurity ของกลุ่มบริษัท
- รายงานสถานะความเสี่ยง เหตุการณ์ และผลการดำเนินการตาม SLA/ ข้อกำหนดของกลุ่มบริษัทตามรอบที่กำหนด

สิทธิหน้าที่และความรับผิดชอบ

“ผู้บริหารระดับสูงสุด” หน้าที่ และความรับผิดชอบ

- ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูงที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศของ ต้องเป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหายหรืออันตรายที่เกิดขึ้น โดยมีอำนาจจัดตั้งคณะกรรมการเพื่อสอบสวนข้อเท็จจริงที่เกิดขึ้น

สิทธิ

- สามารถกำหนดชั้นความลับทุกชั้นความลับ สำหรับข้อมูล และสารสนเทศที่กำหนดชั้นความลับของ บริษัทที่อยู่ภายใต้สายงานการบังคับบัญชา
- สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับทุกชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา
- สามารถสั่งการอนุญาต เพิกถอน และระงับสิทธิของผู้ใช้งานในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับทุกชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา
- สามารถมอบอำนาจอย่างเป็นลายลักษณ์อักษรให้ผู้ใต้บังคับบัญชามีสิทธิในการสั่งการอนุญาต เพิกถอน และระงับสิทธิของผู้ใช้งานในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนด ชั้นความลับทุกชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา
- สามารถแต่งตั้งให้ “เจ้าหน้าที่” ทำหน้าที่เป็นผู้ดูแลระบบสำหรับงานระบบสารสนเทศที่อยู่ภายใต้สายงานการบังคับบัญชา
- สามารถอนุญาตให้หน่วยงานภายนอกเข้ามาปฏิบัติงานกับระบบสารสนเทศของบริษัท
- สามารถกำหนดและจำแนกพื้นที่ใช้งานระบบสารสนเทศของ ที่อยู่ภายใต้สายงานการบังคับบัญชา
- สามารถกำหนดสิทธิของผู้ใช้งานในการผ่านเข้าออกพื้นที่ใช้งานระบบสารสนเทศที่อยู่ภายใต้สายงานการบังคับบัญชา และต้องกำกับดูแลให้ผู้ที่มีสิทธิผ่านเข้าออกดังกล่าว ปฏิบัติตามนโยบาย กฎระเบียบ ข้อบังคับ อันเกี่ยวข้องกับระบบสารสนเทศของบริษัทที่กำหนดไว้อย่างเคร่งครัด

“ผู้บริหารระดับสูง” หน้าที่ และความรับผิดชอบ

- ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่ บริษัทหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูงที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศของ บริษัทต้องเป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหายหรืออันตรายที่เกิดขึ้น โดยมีอำนาจจัดตั้งคณะกรรมการเพื่อสอบสวนข้อเท็จจริงที่เกิดขึ้น

- มีหน้าที่แจ้งต่อหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ เพื่อให้รับทราบและรวบรวมข้อมูลอันเกี่ยวกับ

- การกำหนดหรือเปลี่ยนแปลงสิทธิของผู้ใช้งานที่อยู่ภายใต้สายงานการบังคับบัญชา

- การกำหนดหรือเปลี่ยนแปลงพื้นที่ใช้งานระบบสารสนเทศที่อยู่ภายใต้สายงานการบังคับบัญชา

- การกำหนดหรือเปลี่ยนแปลงชั้นความลับของข้อมูลที่อยู่ภายใต้สายงานการบังคับบัญชา

สิทธิ

- สามารถกำหนดชั้นความลับทุกชั้นความลับ สำหรับข้อมูลและสารสนเทศที่กำหนดชั้นความลับของ บริษัทที่อยู่ภายใต้สายงานการบังคับบัญชา

- สามารถเสนอต่อผู้บริหารระดับสูง เพื่อพิจารณาสั่งการให้ข้อมูลหรือสารสนเทศอันเป็นผลลัพธ์ ซึ่งเกิดจากการประมวลผลข้อมูลหรือสารสนเทศที่มาจากสายงานการบังคับบัญชา ได้แก่ ผลลัพธ์จากการประมวลผลข้อมูลหรือสารสนเทศที่มาจากหลายหน่วยงาน หรือมีการกำหนดชั้นความลับไว้ต่างกัน ได้รับการกำหนดชั้นความลับตามความเหมาะสม

- สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับทุกชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา

- สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับอื่น ๆ ของบริษัทเท่าที่ ได้รับอนุญาตจากผู้บริหารระดับสูง

- สามารถสั่งการ อนุญาต เพิกถอน และระงับสิทธิของผู้ใช้งานในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา

- สามารถเสนอต่อผู้บริหารระดับสูงเพื่อขออนุญาตให้หน่วยงานภายนอกเข้าปฏิบัติงานกับระบบสารสนเทศของ บริษัทที่อยู่ภายใต้สายงานการบังคับบัญชา

- สามารถกำหนดและจำแนกพื้นที่ใช้งานระบบสารสนเทศของบริษัท ที่อยู่ภายใต้สายงานการบังคับบัญชา

- สามารถกำหนดสิทธิของผู้ใช้งานในการผ่านเข้าออกพื้นที่ใช้งานระบบสารสนเทศของบริษัทที่อยู่ภายใต้สายงานการบังคับบัญชา และมีหน้าที่ต้องกำกับดูแลให้ผู้ที่มีสิทธิผ่านเข้า - ออกดังกล่าว ปฏิบัติตามนโยบาย กฎระเบียบ ข้อบังคับ อันเกี่ยวข้องกับระบบสารสนเทศของบริษัทอย่างเคร่งครัด

“ผู้บริหาร” หน้าที่ และความรับผิดชอบ

- ควบคุมดูแลให้ผู้ใต้บังคับบัญชาปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด และเป็นผู้อนุมัติและสนับสนุนทรัพยากร

- ควบคุม ดูแล รับผิดชอบอุปกรณ์ด้านเทคโนโลยีสารสนเทศของหน่วยงาน

สิทธิ

- สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับเฉพาะ “ชั้นลับ” ที่อยู่ภายใต้สายงานการบังคับบัญชา

- สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับเฉพาะ “ชั้นลับมาก” เท่าที่ได้รับอนุญาตจาก “ผู้บริหารระดับสูง” โดยต้องผ่านความเห็นชอบของ “ผู้บริหารระดับกลาง” ที่เป็นเจ้าของงานระบบสารสนเทศ

- สามารถอนุญาตให้บุคคลหรือผู้ใช้งานยืมอุปกรณ์ด้านเทคโนโลยีสารสนเทศในความรับผิดชอบ

“ผู้ดูแลระบบ (System Administrator)” หน้าที่ และความรับผิดชอบ

- ไม่มีสิทธิเปิดอ่านจดหมายอิเล็กทรอนิกส์หรือการสื่อสารระหว่างกันที่เป็นส่วนตัว (ได้แก่ Gmail, Outlook, line) ของ “ผู้ใช้งาน” ยกเว้นในกรณีที่ใช้ในการสืบสวนเกี่ยวกับการใช้งาน ระบบอย่างไม่ถูกต้อง หรือละเมิดสิทธิผู้อื่น หรือมีการร้องขอจากหน่วยงานภายนอกตามคำสั่ง ศาลหรือตามกฎหมาย

- ไม่มีสิทธิเปิดอ่าน หรือใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับ ยกเว้นในกรณีที่ได้รับอนุญาตสิทธิเป็นลายลักษณ์อักษรจากผู้บริหาร ที่สามารถอนุญาตสิทธิในการเข้าถึง หรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับนั้น

- แจ้งให้ผู้ใช้งานทราบล่วงหน้าถึงวันเวลาที่ต้องปิดระบบเพื่อบำรุงรักษาปรับปรุง หรือเปลี่ยนแปลงระบบ ซึ่งส่งผลให้ต้องหยุดบริการในช่วงเวลาหนึ่ง ยกเว้นในกรณีฉุกเฉิน ผู้ดูแล ระบบมีสิทธิปิดระบบทันที และจะต้องพยายามให้ผู้ใช้งานสามารถเก็บบันทึกข้อมูลได้อย่างสมบูรณ์ก่อนที่จะดำเนินการปิดระบบ และทำรายงานให้ผู้บังคับบัญชาทราบ

- ต้องดูแลรักษา ตรวจสอบแก้ไข และเสนอ ให้ปรับปรุงระบบสารสนเทศและระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อให้ระบบสามารถใช้งานได้ดี มีเสถียรภาพ มีความมั่นคงปลอดภัย และมีประสิทธิภาพอยู่เสมอ

- ติดตาม กำชับผู้ใช้งาน และปรับปรุงฐานข้อมูลของผู้ใช้งาน ให้มีความถูกต้องเป็นปัจจุบันอยู่เสมอ รวมทั้งต้องลบบัญชีผู้ใช้งานของผู้ที่หมดสิทธิในการใช้งานระบบออกจากฐานข้อมูล

- ต้องติดตามข่าวสาร ภาวะภัยคุกคาม ช่องโหว่ของระบบสารสนเทศ และต้องปรับปรุงดูแลระบบเพื่อลดความเสี่ยงของการถูกบุกรุกอย่างสม่ำเสมอ

- ต้องขออนุญาตผู้บังคับบัญชาในกรณีที่มีการร่วมมือกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศ ในการประเมิน ตรวจสอบ ทดสอบ หาจุดอ่อนช่องโหว่ อันเกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศ และทำการแก้ไขอย่างรวดเร็ว

- ต้องแจ้งต่อหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศทันทีและทำรายงานแจ้งผู้บังคับบัญชาตามลำดับชั้น ในกรณีที่ตรวจพบหรือได้รับรายงานจาก ผู้ใช้งานหรือสงสัยว่าระบบสารสนเทศที่รับผิดชอบโดยตรงหรือระบบที่เกี่ยวข้องอื่นใดของบริษัท ถูกละเมิดทางด้านความมั่นคงปลอดภัย

สิทธิ

- สามารถยุติการทำงานของระบบสารสนเทศ ซึ่งพบว่าเป็นภัยต่อความมั่นคงปลอดภัยหรือ สร้างภาระให้ระบบสารสนเทศของ บริษัทโดยไม่จำเป็นต้องมีการแจ้งล่วงหน้าในกรณี ฉุกเฉิน เท่านั้น และติดตามสอบสวนหาสาเหตุที่มาของภัยหรือภาระนั้น และทำรายงานให้ผู้บังคับบัญชาที่รับผิดชอบระบบทราบ

- สามารถยุติการทำงานของระบบสารสนเทศที่เปิดใช้โดยไม่ได้รับอนุญาตจาก บริษัท โดยไม่ต้องมีการแจ้งล่วงหน้าและติดตามสอบสวนหาสาเหตุที่มาของระบบงานนั้น และทำรายงาน ให้ผู้บังคับบัญชาทราบ

- สามารถจำกัดหรือระงับสิทธิของผู้ใช้งานระบบอย่างไม่เหมาะสม และแจ้งให้ผู้บริหารของบริษัท ตั้งคณะกรรมการพิจารณาสอบสวนหรือลงโทษตามความเหมาะสม

“เจ้าของข้อมูล (Information Owner)” หน้าที่ และความรับผิดชอบ

- กำหนดชั้นความลับและสิทธิ์เข้าถึง
- ตรวจทานระดับชั้นความปลอดภัยของข้อมูลเพื่อให้มั่นใจว่ายังเป็นไปตามความต้องการของการปฏิบัติงานและมีความเหมาะสมและสอดคล้องกับระดับความปลอดภัยนั้น ๆ
- ตรวจสอบให้แน่ใจว่าข้อมูลที่ได้มีการระบุหรือแสดงระดับความปลอดภัยตามที่ได้จัดระดับไว้อย่างถูกต้องและเหมาะสม ไม่ว่าจะอยู่ในรูปแบบหรือสื่อประเภทใดก็ตาม
- จัดทำข้อกำหนดในการสำรองข้อมูล และดำเนินการให้มีการจัดการในเรื่องของการละเมิดความปลอดภัยอย่างเหมาะสม

สิทธิ

- อนุมัติและตรวจทานเพื่อให้แน่ใจว่าสิทธิของผู้ใช้งานถูกต้องเหมาะสม
- กำหนดระดับชั้นความปลอดภัยให้กับข้อมูล
- กำหนดพื้นฐานการรักษาความปลอดภัยในการเข้าถึงข้อมูลของหน่วยงาน

“เจ้าของระบบงาน (Application Owner)” หน้าที่ และความรับผิดชอบ

- ตรวจสอบให้แน่ใจว่าระบบงานสามารถทำงานได้ถูกต้องตามความต้องการได้อย่างสม่ำเสมอ
- ควบคุมดูแลความปลอดภัยในการเข้าใช้งานระบบงาน และความปลอดภัยของข้อมูล
- อนุมัติ ตรวจทาน และรับรองสิทธิการเข้าใช้ระบบที่เหมาะกับระดับความสำคัญของข้อมูล
- จัดทำข้อกำหนดในการสำรองข้อมูลและ Source Code ของระบบงาน
- ดำเนินการหรือมีการจัดการในเรื่องของการละเมิดความปลอดภัยอย่างเหมาะสม

สิทธิ

- สามารถมอบหมายหน้าที่และความรับผิดชอบดังกล่าวข้างต้นให้แก่บุคคลอื่นที่เหมาะสมแต่เจ้าของระบบงานยังคงมีหน้าที่และความรับผิดชอบต่อระบบงานดังกล่าวโดยสมบูรณ์

“ผู้ใช้ (Users)” หน้าที่ และความรับผิดชอบ

- อุปกรณ์ระบบคอมพิวเตอร์และระบบเครือข่าย ของบริษัทมีไว้เพื่อใช้ในกิจการของ บริษัท เท่านั้น ยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากผู้บริหารแล้วเท่านั้น
- ต้องช่วยกันรักษาอุปกรณ์ต่าง ๆ ไม่ให้เกิดความเสียหาย หากมีความเสียหายจากอุบัติเหตุหรือ ภัยต่าง ๆ ผู้ใช้งานต้องรายงานผู้ดูแลระบบ และผู้บังคับบัญชาให้รับทราบทันที
- การขอใช้งานอุปกรณ์และระบบต่าง ๆ ผู้ใช้งานต้องสามารถแสดงบัตรประจำตัวที่ถูกต้องได้หากผู้ดูแลระบบร้องขอ
- พึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ ได้แก่ ไม่ Download ไฟล์ขนาดใหญ่โดยไม่จำเป็น ไม่ส่งหรือกระจายส่งต่อจดหมายอิเล็กทรอนิกส์ในลักษณะจดหมายลูกโซ่ ฯลฯ
- เพื่อให้การบริหารระบบเป็นไปอย่างถูกต้อง ผู้ใช้งานต้องให้ข้อมูลประจำตัวที่ถูกต้องสำหรับการเปิดบัญชีผู้ใช้งาน (User ID หรือ Login Account)
- ต้องรับผิดชอบในการกำหนดรหัสผ่าน (Password) ที่ปลอดภัยตามนโยบายการบริหาร จัดการรหัสผ่าน (Password Management Policy)

- ต้องไม่อนุญาตให้ผู้อื่นใช้งานระบบคอมพิวเตอร์ผ่านบัญชีผู้ใช้งานของตนโดยเด็ดขาดมิฉะนั้น ผู้ใช้งานอาจมีความผิดทางวินัยและต้องรับผิดชอบต่อปัญหาที่เกิดขึ้น ได้แก่ การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย ฯลฯ

- ต้องรายงานต่อผู้ดูแลระบบและผู้บังคับบัญชาโดยทันที ในกรณีตรวจพบหรือสงสัยว่ามีการนำบัญชีผู้ใช้งานของตนหรือของผู้อื่นไปใช้งานโดยไม่ได้รับอนุญาต หรือใช้งานในทางมิชอบและพบเห็นพฤติกรรมการล่วงละเมิดความมั่นคงปลอดภัยทุกอย่างในระบบ

- ต้องป้องกันข้อมูลและสารสนเทศที่กำหนดชั้นความลับมิให้ถูกเปิดเผยไปสู่ผู้อื่น

- ไม่ล่วงล้ำเข้าในบริเวณพื้นที่ใช้งานระบบสารสนเทศที่ไม่ได้รับอนุญาต

- ต้องใช้ระบบในลักษณะที่ถูกต้องตามกฎหมาย ไม่ละเมิดสิทธิและไม่ก่อความเดือดร้อนหรือความเสียหายแก่บุคคลหรือบริษัทอื่น

- ไม่ติดตั้งหรือเปิดให้บริการระบบเครือข่ายบนเครื่องของ บริษัท เพื่อทำภารกิจส่วนตัว

- ต้องคืนสินทรัพย์ ของบริษัทอันเกี่ยวกับการปฏิบัติหน้าที่ในทันทีที่พ้นหน้าที่ ได้แก่ อุปกรณ์ ระบบสารสนเทศ ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ

- ต้องทำรายงานแจ้งให้ผู้ดูแลระบบและผู้บังคับบัญชาทราบทันที ในกรณีที่มีการเคลื่อนย้ายถอดถอนอุปกรณ์ระบบสารสนเทศ

- ต้องปฏิบัติตามมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และวิธีการปฏิบัติ (Procedure) อันเกี่ยวเนื่องกับความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

- ห้ามผู้ใช้งานติดตั้งโปรแกรมหรืออุปกรณ์ในเครื่องของ บริษัทก่อนได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ เพื่อป้องกันปัญหาด้านลิขสิทธิ์และ ปัญหาอื่น ๆ ที่จะเกิดขึ้นภายหลังการติดตั้ง ได้แก่การติดตั้ง Access Point ด้วยตนเองแล้วเกิดการเจาะระบบเข้ามาในระบบเครือข่ายหรือทำให้เกิดการแพร่กระจายของ ไวรัสและภัยคุกคามอื่น ๆ เป็นต้นควบคุมดูแลความปลอดภัยในการเข้าใช้งานระบบงานและความปลอดภัยของข้อมูล

- หากพบว่าระบบรักษาความปลอดภัยมีข้อบกพร่อง หรือสงสัยว่า มีผู้ใดกระทำการที่น่าสงสัยให้แจ้งต่อผู้ดูแลระบบโดยทันที

- ต้องให้ความร่วมมือกับเจ้าหน้าที่ที่ได้รับมอบหมายให้ทำการสืบสวนสอบสวนเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยของ สทอภ.

สิทธิ

- สามารถเข้าถึงข้อมูลข่าวสาร ที่มิใช่ข้อมูลและสารสนเทศที่กำหนดชั้นความลับของ บริษัทยกเว้นในกรณีที่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บริหารที่สามารถอนุญาตสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับนั้น

- การฝ่าฝืนอาจมีมาตรการทางวินัยตามระเบียบบริษัท กำหนดและผู้ใช้งานทุกคนต้องรับผิดตามระเบียบโดยไม่มีเงื่อนไข

“หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศ” หน้าที่ และความรับผิดชอบ

- พิจารณารายละเอียดการฝ่าฝืนหรือการละเมิดข้อบังคับและนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ ถ้าเป็นการฝ่าฝืนระเบียบขั้นรุนแรงหรือกรณีที่ฝ่าฝืนแล้วก่อให้เกิดความเสียหายแก่ บริษัทหรือต่อบุคคลก็จะจัดทำบันทึกรายงานเกี่ยวกับการฝ่าฝืนนโยบายดังกล่าวไปยังผู้บริหาร

- ในกรณีการละเมิดหรือฝ่าฝืนมีเจตนาไม่ชัดเจน ผู้ละเมิดหรือฝ่าฝืนจะถูกตักเตือนและชี้แจงให้เข้าใจถึงข้อปฏิบัติที่ถูกต้องหากมีการกระทำการฝ่าฝืนนั้นอีก ให้แต่งตั้งคณะกรรมการพิจารณา และต้องรายงานการกระทำดังกล่าว ไปยังผู้บริหารระดับสูง และผู้บังคับบัญชาที่เกี่ยวข้องทันที โดยให้มีการสอบสวน และดำเนินการทางวินัยตามความรุนแรงของผลกระทบจากการละเมิดหรือฝ่าฝืนข้อบังคับนั้น ๆ

- ป้องกันและแก้ไขปัญหาที่เกิดขึ้นทันที เพื่อให้แน่ใจว่าการละเมิดหรือฝ่าฝืนเหล่านั้นจะไม่ลุกลามเป็นปัญหาใหญ่

- จัดอบรมส่งเสริมให้ผู้ใช้งานตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศ

- ให้คำแนะนำด้านเทคนิคที่เกี่ยวกับการรักษาความปลอดภัยของระบบสารสนเทศ

- วางแผนควบคุมระบบความมั่นคงปลอดภัยด้านสารสนเทศและการเตือนภัยรวมถึงวิเคราะห์หาวิธีการแก้ไขจุดอ่อนของระบบสารสนเทศ

- สืบสวนเหตุการณ์ต่าง ๆ ที่ไม่เป็นไปตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

- ติดต่อและประสานงานเพื่อสร้างความร่วมมือทางด้านความมั่นคงปลอดภัยระหว่างบริษัท

- รวบรวมรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น ๆ ได้แก่ สำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ ศูนย์ประสานงานความมั่นคงปลอดภัยด้านสารสนเทศคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น

สิทธิ

- กำหนดกระบวนการในการอนุมัติการใช้งานระบบสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการนี้

- การดำเนินการทางกฎหมายใด ๆ ต้องได้รับความช่วยเหลือจากหน่วยงานดูแลรับผิดชอบด้านกฎหมายและตัวแทนของบริษัทและในการดำเนินคดีใด ๆ ที่เกี่ยวข้องกับบริษัทต้องเป็นหน้าที่ของเจ้าหน้าที่ระดับผู้บริหารที่ได้รับมอบหมายเท่านั้น

“หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ” หน้าที่ และความรับผิดชอบ

- พัฒนา ติดตั้ง ตรวจสอบ ปรับปรุง ซ่อมแซมและบำรุงรักษาอุปกรณ์ บริหารจัดการระบบเกี่ยวกับอุปกรณ์ IT Infrastructure ให้แก่หน่วยงานทั้งหมด

- บริหารจัดการระบบเครือข่ายเชื่อมโยงคอมพิวเตอร์ (Network Administration) ที่ใช้งานภายในบริษัท ทุกระบบและควบคุมการเชื่อมต่อเครือข่ายอินเทอร์เน็ตโดยตรงผ่านช่องทางอื่น ได้แก่ Dial up Modem รวมทั้งควบคุมการเชื่อมต่อเครือข่ายจากภายนอกได้แก่ การ Remote เครื่องคอมพิวเตอร์ การใช้งาน VPN เป็นต้น

- รับผิดชอบในการจัดหาและควบคุมการใช้งาน Corporate Antivirus จัดเตรียมคู่มือและข้อมูลต่าง ๆ ที่เกี่ยวกับ Corporate Antivirus จัดทำสถิติ กราฟ และผลการใช้งาน รวมไป ถึงการอนุญาตหรือจำกัดการใช้งานของผู้ใช้งาน

- รับผิดชอบในการบำรุงรักษา ปิดช่องโหว่ในระบบ Corporate Antivirus ปรับปรุง Virus Signature ระบบ Corporate Antivirus ให้ทันสมัย เสนองบประมาณผ่านหน่วยงานดูแล

- รับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศ ปรับเพิ่มลดจำนวนลิขสิทธิ์ของ Corporate Antivirus อนุญาตหรือจำกัดการใช้งานของผู้ใช้งาน และเนินการในส่วนที่เกี่ยวข้อง

- รับผิดชอบการจัดทำและปรับปรุงเนื้อหาของเว็บไซต์ของบริษัท

- ควบคุมการติดตั้งโปรแกรมหรืออุปกรณ์ในเครื่องคอมพิวเตอร์ ๆ

- รับผิดชอบร่วมกับผู้ดูแลระบบในการตรวจสอบซอฟต์แวร์ เพื่อป้องกันการละเมิดข้อตกลงและหาทางป้องกันซอฟต์แวร์ที่ใช้ในการตรวจประเมินระบบ มิให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิดหรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้น ๆ

- จัดทำข้อมูลสินทรัพย์ระบบสารสนเทศของบริษัท รวมถึงค่า Configuration ของอุปกรณ์เครือข่าย เพื่อประสิทธิภาพในบริหารจัดการระบบสารสนเทศของบริษัท

- ให้คำแนะนำและเป็นที่ปรึกษาในการพิจารณารายละเอียดการฝ่าฝืนหรือการละเมิดข้อบังคับและนโยบายความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทและแก้ไขปัญหาที่เกิดขึ้นดังกล่าว

- ควบคุมระบบความมั่นคงปลอดภัยด้านสารสนเทศและการเตือนภัย รวมถึงวิเคราะห์หา วิธีการแก้ไขจุดอ่อนของระบบสารสนเทศ

- กำหนดและควบคุมการสำรองและกู้คืน (Backup & Recovery) ระบบสารสนเทศของบริษัท

- ควบคุมการพิสูจน์ตัวตน (Authentication) ก่อนเข้าถึงระบบสารสนเทศของบริษัท

“หน่วยงานดูแลรับผิดชอบด้านตรวจสอบภายใน” หน้าที่ และความรับผิดชอบ

- ตรวจสอบการปฏิบัติงานของผู้ใช้งานให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทที่ดำเนินไปภายใต้มาตรฐานและแนวทางการปฏิบัติที่ได้กำหนดไว้ในนโยบาย และร่วมมือกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ เพื่อป้องกันสินทรัพย์และข้อมูลต่าง ๆ

- ให้ความช่วยเหลือแก่หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ในการชี้ถึงความเสี่ยงต่าง ๆ รวมถึงภัยคุกคามอันอาจก่อให้เกิดอันตรายต่อความมั่นคงปลอดภัย

“หน่วยงานดูแลรับผิดชอบด้านบริหารความเสี่ยง”

มีหน้าที่และความรับผิดชอบในการวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศ เพื่อปรับปรุงให้บริษัทมีคุณภาพ ประสิทธิภาพและลดโอกาสความเสียหายที่อาจจะเกิดขึ้นได้

“หน่วยงานดูแลรับผิดชอบด้านกฎหมาย”

มีหน้าที่และความรับผิดชอบในการให้ความเห็นหรือให้คำปรึกษาเกี่ยวกับระเบียบ ข้อกำหนด กฎเกณฑ์ ข้อบังคับกฎหมาย พระราชบัญญัติพระราชกฤษฎีกา การฟ้องร้องดำเนินคดี รวมถึงข้อละเมิดสินทรัพย์ทางปัญญา ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

“หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคล” หน้าที่ และความรับผิดชอบ

- ตรวจสอบคุณสมบัติของผู้สมัครเกี่ยวกับการละเมิดด้านความมั่นคงปลอดภัยระบบสารสนเทศ

- การให้“เจ้าหน้าที่” ลงนามมิให้เปิดเผยความลับของบริษัท

- รายงานข้อมูลการว่าจ้างงาน การเปลี่ยนแปลงสภาพการว่าจ้างงาน การลาออกจากงานการถึงแก่กรรม การโยกย้ายและการพักงานหรือการลงโทษทางวินัย ให้แก่ หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อบริหารจัดการทรัพยากรระบบสารสนเทศ และ สิทธิในการเข้าถึงระบบงานต่าง ๆ

“หน่วยงานดูแลรับผิดชอบด้านพัฒนาบุคลากรและวัฒนธรรมบริษัท”

มีหน้าที่และความรับผิดชอบในการให้ความเห็นหรือให้คำปรึกษาเกี่ยวกับระเบียบ ข้อกำหนด กฎเกณฑ์ ข้อบังคับ กฎหมายพระราชบัญญัติ พระราชกฤษฎีกา การฟ้องร้องดำเนินคดี รวมถึงข้อละเมิดสินทรัพย์ทางปัญญา ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

“หน่วยงานดูแลรับผิดชอบด้านอาคารและสถานที่”

มีหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ควบคุมการเข้า-ออกอาคาร และสำนักงานจัดเตรียมการป้องกันต่อภัยคุกคามต่าง ๆ ทั้งจากมนุษย์และธรรมชาติ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว ความไม่สงบของบ้านเมือง เป็นต้น

การบริหารข้อยกเว้น (Exception Management)

กรณีไม่สามารถปฏิบัติตามข้อกำหนดได้ ต้องยื่นคำขอข้อยกเว้น (Exception) พร้อมเหตุผล ความเสี่ยง มาตรการชดเชย (compensating controls) ระยะเวลา และผู้อนุมัติ”

ข้อยกเว้นมีอายุไม่เกิน 12 เดือน และต้องทบทวนก่อนหมดอายุทุกครั้ง

นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

5. มาตรการควบคุมด้านบริษัทฯ (Organization controls) Annex 5

วัตถุประสงค์

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) และแนวปฏิบัติที่เกี่ยวข้องฉบับนี้ถูกจัดทำขึ้น เพื่อกำหนดทิศทาง หลักการและกรอบของข้อกำหนดในการป้องกันทรัพย์สินที่เกี่ยวข้องกับสารสนเทศให้ปลอดภัยจากภัยคุกคามที่อาจก่อให้เกิดความเสียหายต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลและระบบงานสารสนเทศ เพื่อผลักดันให้มีการควบคุมภายในด้านสารสนเทศที่รัดกุมตามแนวความเสี่ยง (Risk Based Approach) ที่สอดคล้องกับมาตรฐานสากล และเพื่อสนับสนุนให้ผู้ใช้งานตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศรวมถึงความสำคัญในการบริหารจัดการความเสี่ยงด้านสารสนเทศ

5.1. นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศ (Policies for Information Security)

จัดทำนโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษรเพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ โดยนโยบายความมั่นคงปลอดภัยสารสนเทศ ดังกล่าวจะต้องได้รับการอนุมัติจากผู้บริหารของบริษัท และจัดให้มีการเผยแพร่เอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศให้กับ พนักงานและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบเป็นลายลักษณ์อักษรเพื่อลงนามรับทราบ

การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Review of the Policies for Information Security) นโยบายความมั่นคงปลอดภัยต้องมีการทบทวนตามรอบระยะเวลากำหนดไว้อย่างน้อย 1 ครั้งต่อปี และกรณีที่มีการเปลี่ยนแปลงที่มีนัยสำคัญให้ดำเนินการปรับปรุงนโยบายภายใน 6 เดือน

เพื่อให้มั่นใจว่าพนักงานในบริษัทฯ รับทราบเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการทำงาน

5.2. บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยี (Information Security Roles and Responsibilities)

เพื่อให้บริษัทมีการกำหนดขอบเขตการบริหารจัดการบริษัท มีการควบคุมการปฏิบัติงาน และมีการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศในบริษัท รวมทั้งการรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกล และของการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัทที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

5.2.1. ต้องกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการดำเนินงานทางด้านความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีไว้อย่างชัดเจน

5.2.2. ผู้บริหารฯต้องแต่งตั้งคณะหรือกลุ่มผู้ทำงานหลักตลอดจนทรัพยากรที่จำเป็นเพื่อบริหารและจัดการความมั่นคงปลอดภัยสารสนเทศ

5.3. การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties)

หน้าที่และส่วนงานที่รับผิดชอบที่จะทำให้เกิดการขัดต่อการปฏิบัติงานโดยการทำให้มีการเปลี่ยนแปลงทรัพย์สินของบริษัท หรือมีการใช้ทรัพย์สินผิดวัตถุประสงค์โดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนาก็ตาม ต้องมีการแยกหน้าที่ดังกล่าวออกจากกัน เพื่อลดโอกาสเกิดขึ้นของเหตุการณ์ความเสี่ยงนั้น ๆ

5.3.1. ต้องกำหนดให้พนักงานและผู้ที่ทำสัญญาจ้างทั้งหมด รักษาความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยี โดยปฏิบัติให้สอดคล้องกับนโยบาย และแนวปฏิบัติของบริษัทที่ได้กำหนดไว้ รวมทั้ง

5.3.2. ต้องสั่งการและสนับสนุนเจ้าหน้าที่เพื่อนำสู่ความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยี

5.3.3. กำหนดทิศทางการปฏิบัติของนโยบายเพื่อสร้างความมั่นคงปลอดภัยให้กระบวนการทางสารสนเทศทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยี

5.3.4. ต้องจัดหาทรัพยากรที่จำเป็นสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีเพื่อใช้ในการดำเนินการ

5.3.5. ต้องสื่อสารความสำคัญของระบบความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีที่สัมฤทธิ์ผลและดำเนินการตามความต้องการ ของระบบความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีที่กำหนดไว้

5.4. การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with Authorities)

ต้องกำหนดรายชื่อและข้อมูลสำหรับติดต่อกับผู้ที่เกี่ยวข้องภายในบริษัทฯ เมื่อเกิดเหตุการณ์ฉุกเฉินหรือหยุดชะงักทำให้บริษัทไม่สามารถปฏิบัติงานได้ตามปกติ

5.5. การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with Special Interest Groups)

การติดต่อกับกลุ่มที่มีความสนใจเรื่องเดียวกัน กลุ่มที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และสมาคมอาชีพ ต้องมีการรักษาไว้ซึ่งการติดต่อนั้นเพื่อให้สามารถติดต่อได้อย่างต่อเนื่อง

5.5.1. ต้องกำหนดรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่าง ๆ ที่มีความสนใจเป็นพิเศษในเรื่องเดียวกันกับกลุ่มที่มีความสนใจ ด้านความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีและข้อมูลสำหรับการติดต่อ ต้องได้รับการปรับปรุงให้ทันสมัยอย่างสม่ำเสมอ

5.5.2. ต้องกำหนดรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่น ๆ เช่น สำนักงานตำรวจแห่งชาติผู้ให้บริการอินเทอร์เน็ตศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (Thai CERT) เป็นต้นเพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยเมื่อเกิดเหตุการณ์หรือ กรณีที่มีความจำเป็นต้องติดต่อและข้อมูลสำหรับการติดต่อต้องได้รับการปรับปรุงให้ทันสมัยอย่างสม่ำเสมอ

5.6. ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม (Threat intelligence)

5.6.1. บริษัทฯ มีการจัดการข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งจะถูกรวบรวมและวิเคราะห์เพื่อสร้างข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม การควบคุมนี้กำหนดให้ผู้รับผิดชอบต้องรวบรวมข้อมูลเกี่ยวกับภัยคุกคามและวิเคราะห์เพื่อดำเนินการลดผลกระทบที่เหมาะสม ข้อมูลนี้อาจเกี่ยวกับการโจมตีเฉพาะวิธีการและเทคโนโลยีที่ผู้โจมตีใช้ และแนวโน้มการโจมตี ผู้รับผิดชอบรวบรวมข้อมูลนี้เป็นการภายใน รวมทั้งจากแหล่งข้อมูลภายนอก

5.6.2. บริษัทฯ มีการกำหนดกระบวนการในการรวบรวมข้อมูลภัยคุกคามเพื่อประเมินความเสี่ยงและลดความเสี่ยงในเหตุการณ์ที่จะเกิดขึ้นและบริษัทฯ มีการทบทวนข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีที่ได้รวบรวมไว้เป็นประจำทุก 3 เดือน เพื่อให้ทันต่อสถานการณ์ภัยคุกคามที่เปลี่ยนแปลง ตลอดเวลา

5.7. ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information Security in Project Management)

การบริหารโครงการไม่ว่าจะเป็นประเภทใดของโครงการก็ตาม ต้องมีการกำหนดระเบียบข้อบังคับกฎเกณฑ์ต่าง ๆ เกี่ยวกับการดำเนินงานและการเข้าถึงข้อมูลเพื่อให้งานโครงการมีความมั่นคงปลอดภัย เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน เป็นต้นกรณีโครงการที่จ้างบริษัทภายนอกโครงการที่หน่วยงานภายนอกดำเนินการให้และโครงการที่จัดทำเองต้องปฏิบัติตามวิธีปฏิบัติงานเรื่องการจัดทำโครงการด้านเทคโนโลยีสารสนเทศเพื่อให้การบริหารจัดการโครงการเกิดความมั่นคงปลอดภัยและลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น เช่น จ้างงาน Outsource มาพัฒนาโปรแกรม เป็นต้น

5.8. บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ (Inventory of information and other associated assets)

บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ เป็นเอกสารที่สำคัญในการบริหารจัดการความปลอดภัยสารสนเทศของบริษัท วัตถุประสงค์ของนโยบายนี้คือเพื่อให้แน่ใจว่าทรัพย์สินและข้อมูลของบริษัทได้รับการบันทึกและจัดเก็บอย่างถูกต้องและปลอดภัย

5.8.1. ทะเบียนสินทรัพย์ (Inventory of Assets)

- ต้องจัดทำบัญชีรายการทรัพย์สินที่อยู่ในความรับผิดชอบและตรวจสอบดูแลปรับปรุงบัญชีรายการทรัพย์สินดังกล่าวอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น
- บัญชีรายการทรัพย์สินต้องครอบคลุมถึงทรัพย์สินสารสนเทศ 6 ประเภท ได้แก่
  1) ฮาร์ดแวร์ (Hardware)
  2) ซอฟต์แวร์ (Software)
  3) ข้อมูลและสารสนเทศ (Data and Information)
  4) เครือข่าย (Network)
  5) พนักงาน (Personnel)
  6) อาคารสถานที่ (Facility)

5.8.2. การใช้งานข้อมูลและทรัพย์สินสารสนเทศที่เกี่ยวข้องอื่น ๆ อย่างเหมาะสม (Acceptable Use for information and other associated Assets)

- ต้องกำหนดขั้นตอนการปฏิบัติงานในการจัดการและจัดเก็บทรัพย์สินสารสนเทศเพื่อมิให้ข้อมูล สารสนเทศรั่วไหล หรือถูกนำไปใช้ผิดประเภท
- ผู้ใช้งานต้องไม่ทิ้งหรือปล่อยให้ทรัพย์สินสารสนเทศที่มีความสำคัญ เช่น เอกสารสื่อบันทึกข้อมูล ให้อยู่ในสถานที่ที่ไม่มีความปลอดภัย สถานที่สาธารณะ หรือพบเห็นได้ง่าย เป็นต้น

5.8.3. การจัดการสินทรัพย์ (Handling of Asset)

- ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น
- พนักงานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยเฉพาะอย่างยิ่งเครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไปข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัสหรือวิธีการอื่นใดของระบบปฏิบัติการหรือระบบ เทคโนโลยีสารสนเทศอย่างเหมาะสม
- พนักงานควรเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับในตู้ที่สามารถปิดล็อกได้ เมื่อไม่ได้ใช้งานโดยเฉพาะอย่างยิ่งเมื่ออยู่นอกช่วงเวลาการทำการหรือเมื่อต้องทิ้งเอกสาร หรือสื่อนั้นไว้โดยไม่อยู่ที่โต๊ะทำงาน
- ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร ฯลฯ โดยทันที
- พนักงานต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอกยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล
- สื่อบันทึกข้อมูลและอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ เช่น USB-Drive เป็นต้น ที่มีข้อมูลลับอยู่ ต้องได้รับการดูแลรักษา และใช้งานอย่างระมัดระวัง

5.8.4. การคืนสินทรัพย์ (Return on Assets)

พนักงาน บริษัทฯ ซึ่งพ้นสภาพจากการจ้างงานต้องคืนสินทรัพย์ทั้งหมด ซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ บัตรประจำตัวเจ้าหน้าที่ บัตรผ่านเข้า-ออก กุญแจ คอมพิวเตอร์ อุปกรณ์ต่อพ่วง คู่มือ และเอกสารที่เกี่ยวข้องต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน

5.8.5. การจัดหมวดหมู่ข้อมูลและสินทรัพย์สารสนเทศ (Classification Information Control)

การกำหนดชั้นความลับของสารสนเทศ (Classification of Information) ต้องมีการจำแนก หมวดหมู่ชั้นความลับ (Sensitivity) ระบุความสำคัญ (Criticality) และข้อกำหนดทางกฎหมาย (Legal Requirement) ของข้อมูลทั้งที่อยู่ในรูปแบบสำเนาถาวร (Hardcopy) และสำเนาอิเล็กทรอนิกส์ (Softcopy) ที่อยู่ในความรับผิดชอบ เพื่อป้องกันสารสนเทศให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม

ต้องกำหนดประเภทของข้อมูล ระดับความสำคัญ ลำดับชั้นความลับของข้อมูล รวมทั้ง ระดับชั้นการเข้าถึง และช่องทางการเข้าถึง เป็นลายลักษณ์อักษรและมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ โดยบริษัทกำหนดชั้นความลับ ดังนี้

ชั้นความลับ	รายละเอียด
ข้อมูลทั่วไป (External Data)	ข้อมูลที่สามารถเผยแพร่หรือเปิดเผยต่อสาธารณชนได้โดยไม่มีข้อจำกัด และไม่ส่งผลกระทบต่อความปลอดภัย การดำเนินงาน หรือชื่อเสียงของบริษัท เช่น ข้อมูลประวัติและวิสัยทัศน์บริษัท ข้อมูลประชาสัมพันธ์ เป็นต้น
ข้อมูลภายใน (Internal use)	ข้อมูลที่ถูกจำกัดการเข้าถึงและการใช้งานเฉพาะ ภายในบริษัทเท่านั้น ไม่สามารถเปิดเผยหรือเผยแพร่ให้บุคคลภายนอกทราบได้ เว้นแต่ได้รับการอนุมัติอย่างเป็นทางการจากผู้มีอำนาจ เช่น นโยบายและระเบียบการปฏิบัติ หรือ ระเบียบวาระการประชุม เป็นต้น
ข้อมูลลับ (Confidential)	ข้อมูลที่มีการประเมินแล้วว่าสามารถเปิดเผยได้เฉพาะบุคลากรที่อยู่ภายในบริษัทที่มีหน้าที่รับผิดชอบ และบุคคลภายนอกที่มีความเกี่ยวข้องโดยตรง ซึ่งได้รับสิทธิเท่านั้น ถ้าหากเปิดเผย

ชั้นความลับ	รายละเอียด
	ทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อบริษัทเช่น ข้อมูลทางบัญชีและการเงิน ข้อมูลลูกค้าและข้อมูลการบริหารธุรกิจ ข้อมูลโครงการ ข้อมูลจัดซื้อจัดจ้างและ NDA
ข้อมูลลับเฉพาะบุคคล (Sensitive Personal Confidential)	ข้อมูลที่สามารถระบุตัวบุคคลได้และมีความอ่อนไหวต่อความเป็นส่วนตัวหากถูกเปิดเผย อาจส่งผลกระทบต่อเจ้าของข้อมูล ทั้งในด้านความปลอดภัย ความเป็นส่วนตัว หรือทางกฎหมาย เช่น ข้อมูลส่วนบุคคล ข้อมูลสุขภาพ ข้อมูลรายได้พนักงาน ต้องได้รับการจัดการตามกฎหมายและข้อบังคับด้านการคุ้มครองข้อมูลส่วนบุคคล (เช่น PDPA, GDPR) รวมถึงมาตรการควบคุมความปลอดภัยที่เข้มงวดตาม ISO/IEC27001
ข้อมูลลับมาก (Highly Confidential)	ข้อมูลที่มีความสำคัญสูงสุดต่อการดำเนินธุรกิจหรือความก้าวหน้าของบริษัทซึ่งต้องได้รับการปกป้องอย่างเข้มงวดและจำกัดการเข้าถึงเฉพาะบุคคลที่ได้รับอนุญาตในระดับสูงสุดเท่านั้น เช่น “ข้อมูลผลประกอบการ แผนกลยุทธ์ระยะยาว ข้อมูลการควบรวมกิจการ” รวมถึงสัญญาต่าง ๆ

5.8.6. การจัดทำป้ายชื่อของข้อมูล (Labeling of Information Control)

- ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับปิดฉลากเอกสารข้อมูลและอุปกรณ์ทรัพย์สินสารสนเทศที่เกี่ยวข้องกับการบริหารด้านเทคโนโลยีสารสนเทศและการสื่อสาร

- ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้เจ้าหน้าที่ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย

5.8.7. การถ่ายโอนข้อมูล (Information Transfer)

5.8.7.1. นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures)

1. กำหนดนโยบาย ขั้นตอนการปฏิบัติงาน และมาตรการรองรับ โดยผ่านช่องทางการสื่อสารทุกชนิด
2. ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer)
3. กำหนดให้ผู้เข้ามาใช้งานขอรหัสผ่านเพื่อเข้าใช้งานระบบจากผู้ดูแลระบบจากผู้ดูแลระบบ ซึ่งรหัสผ่านสามารถใช้ได้ในช่วงเวลาที่กำหนดไว้เท่านั้น
4. กำหนดข้อตกลง แนวทาง วิธีปฏิบัติ ระยะเวลา ของการถ่ายโอนสารสนเทศ
5. มีการบันทึก วันเวลาที่มีการถ่ายโอนสารสนเทศในระหว่างบริษัท
6. จำกัดการเข้าถึงสารสนเทศเมื่อมีการโอนย้ายเสร็จสิ้นแล้ว

5.8.7.2. การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic massaging)

กำหนดวิธีการป้องกันการเข้าถึงข้อมูลอิเล็กทรอนิกส์รวมถึงการจัดส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเครือข่ายข้อตกลงการรักษาความลับหรือไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)

1. ต้องมีการจัดทำข้อตกลง หรือสัญญาการรักษาความลับ หรือข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement: NDA) ซึ่งเป็นไปตามความต้องการด้านการป้องกันข้อมูลของบริษัทและมีการทบทวนอย่างสม่ำเสมอ

2. พนักงาน บุคคล หรือผู้ติดต่อจากหน่วยงานอื่น ที่มีส่วนต้องเข้าถึงสารสนเทศของบริษัท ต้องจัดให้มีการลงนามในสัญญาระหว่าง “เจ้าหน้าที่” และ “ผู้ติดต่อ” ว่าจะไม่เปิดเผยความลับของหน่วยงาน (Non-Disclosure Agreement: NDA)

5.9. การควบคุม การเข้าถึง (Access Control)

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของบริษัทฯ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ ได้อย่างถูกต้อง

เพื่อให้มั่นใจว่ามีการจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต มีการกำหนดสิทธิในการเข้าถึงระดับของข้อมูลหรือสารสนเทศเพื่อป้องกันการเข้าถึงข้อมูลที่เป็นความลับทั้งหมด

นโยบาย

5.9.1. มีการกำหนดให้มีการควบคุมการใช้งานข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึง ให้เข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

5.9.2. ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ โดยปฏิบัติตามระเบียบปฏิบัติ ทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บังคับบัญชาตามความจำเป็นในการใช้งาน

5.9.3. ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศได้

5.9.4. ต้องมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทและเฝ้าระวังการละเมิดความปลอดภัย ที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

5.9.5. ต้องบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

5.9.6. ต้องกำหนดกฎเกณฑ์ข้อห้ามและบทลงโทษการเข้าถึงข้อมูลและระบบสารสนเทศสำหรับผู้ที่ละเมิดกฎเกณฑ์

5.9.7. การเข้าถึงข้อมูลและระบบสารสนเทศของบริษัทจะกระทำได้ก็ต่อเมื่อได้รับการอนุมัติโดยผู้บังคับบัญชาของบุคคลนั้นและสามารถเข้าใช้ข้อมูล และระบบเฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น ๆ เท่านั้น ความปลอดภัยของข้อมูลและกระบวนการรักษาความลับของข้อมูลถือว่าเป็นส่วนหนึ่งในการกำหนดนโยบาย และขั้นตอนการทำงานของระบบสารสนเทศ กระบวนการเหล่านี้หมายรวมถึงการให้สิทธิและการบริหารจัดการรหัสในการเข้าใช้งาน การกำหนดขอบเขตในการเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์และอุปกรณ์ที่เก็บข้อมูลประเภทอื่น ๆ การสำรองข้อมูลและการกู้ข้อมูลที่เสียหายกลับคืนมา

5.10. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

5.10.1. การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User Registration and De-Registration)

การลงทะเบียนผู้ใช้งานใหม่ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนผู้ใช้งานใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งระเบียบปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่นเมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายใน เป็นต้น โดยปฏิบัติตามระเบียบปฏิบัติ โดยผู้ใช้งานต้องได้รับการทบทวน และพิจารณาอนุมัติตามขั้นตอนอย่างเคร่งครัด

5.10.2. การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning)

การจัดการสิทธิการเข้าถึงของผู้ใช้งาน ต้องกำหนดให้มีวิธีการในการบริหารจัดการสิทธิการเข้าถึง ทั้งการให้สิทธิและการถอดถอนสิทธิต้องมีระเบียบวิธีการกำหนดไว้สำหรับผู้ใช้งานทุกประเภท

5.10.3. การบริหารจัดการสิทธิตามระดับสิทธิการเข้าถึง (Management of Privileged Access Right)

5.10.3.1. ต้องกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบด้วย

5.10.3.2. ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อมีการ Log-on เข้าสู่ระบบสารสนเทศ

5.10.4. การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of User)

5.10.4.1. ต้องมีกระบวนการจัดการที่ช่วยป้องกันข้อมูลในการส่งมอบให้แก่ผู้ใช้งานเพื่อพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นความลับ และการเก็บรักษาข้อมูลความลับของตัวเอง การส่งมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นข้อมูลลับ

5.10.4.2. พนักงานบริษัทฯ ต้องปฏิบัติตามระเบียบปฏิบัติเรื่อง การลงทะเบียนใช้งานระบบสารสนเทศ

5.10.5. การทบทวนสิทธิในการเข้าถึงระบบของผู้ใช้งาน (Review of User Access Rights)

ต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

5.10.6. การถอนหรือการจัดการสิทธิการเข้าถึง (Removal or Adjustment of Access Rights)

5.10.6.1. สิทธิการเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง และต้องได้รับการปรับปรุงให้ถูกต้องอย่างสม่ำเสมอ

5.10.6.2. ต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ตามระเบียบปฏิบัติ

5.11. การควบคุมการเข้าถึงระบบ (System and Application Access Control)

5.11.1. การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

5.11.1.1. ต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่กำหนดสิทธิในการใช้งาน เช่น เขียน อ่าน ลบ เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

5.11.1.2. บัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

บุคคลภายนอกต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy) ของบริษัทฯ อย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศ

5.11.1.3. การเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure log-on Procedure) โดยกำหนดให้ระบบมีการหน่วงเวลาการให้บริการเป็นเวลา 5 นาทีหากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน 3 ครั้ง และต้องวิเคราะห์ทบทวนว่าเป็นการโจมตีหรือไม่อย่างน้อยเดือนละ 1 ครั้ง

5.11.1.4. ระบบบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานระบบเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

5.11.1.5. ต้องกำหนดให้มีการใช้งานระบบการยืนยันตัวบุคคล Multifactor Authentications (MFA)

5.11.1.6. ระบบสารสนเทศที่ใช้งานมีความสามารถในการใช้งานอุปกรณ์ที่เป็นรหัสผ่าน (Passkey) จำเป็นให้มีการบังคับใช้แทนการใช้งานรหัสผ่านแบบเดิมได้

5.11.2. การใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

กำหนดข้อบังคับและกระบวนการควบคุมการใช้งาน “โปรแกรมอรรถประโยชน์ที่มีสิทธิพิเศษ (Privileged Utility Programs)” เพื่อป้องกันการเข้าถึง/ แก้ไขระบบและข้อมูลโดยมิชอบ ลดความเสี่ยงจากการยกระดับสิทธิ การเปลี่ยนแปลงที่ไม่ผ่านการอนุมัติ และสนับสนุนการตรวจสอบย้อนหลัง (audit trail)

- กำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่
- ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
- ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้เช่น ผู้ใช้งานระบบ เป็นต้น

5.11.3. การควบคุมการเข้าถึงรหัสต้นฉบับสำหรับระบบ (Access Control to Program Source Code)

ผู้พัฒนาระบบสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริงหรือให้บริการเช่น

- ไม่ควรเก็บ Source Code ไว้ในเครื่องที่ใช้งานจริงและต้องเก็บ Source Code ไว้ในที่ที่ปลอดภัย
- ต้องไม่เก็บ Source Code ที่อยู่ในระหว่างทำการทดสอบรวมไว้กับ Source Code ที่ใช้งานได้จริงแล้ว

5.11.4. การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network and Network Services)

ผู้ใช้งาน

- ผู้ใช้งานต้องได้รับสิทธิการเข้าถึงเฉพาะเครือข่ายและบริการของเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น
- ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ระบบเครือข่ายของหน่วยงานต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด โดยผู้ใช้งานต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย”

- การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงาน และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่น ๆ

- ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ผู้ดูแลระบบ

ต้องควบคุมการเข้าถึงระบบเครือข่ายเพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพดังต่อไปนี้

- ต้องจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

- ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

- ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

- ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

- ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/ Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

- การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

- ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

- ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

- การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

- อุปกรณ์ที่นำมาเชื่อมต่อจะได้รับหมายเลข IP Address ตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย

- ผู้ดูแลระบบต้องจากัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

- กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

- ผู้ขอใช้บริการต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย” ผ่าน Inception หรือ ติดต่อฝ่ายเทคโนโลยีสารสนเทศของบริษัท

- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

กำหนดระยะเวลาผู้ใช้งานที่อยู่ในระบบเครือข่ายให้ออกจากระบบเครือข่ายเมื่อ

- เว้นว่างจากการใช้งานไม่เกินกว่า 15 นาที

ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

กำหนดให้มีการจัดเก็บรหัสต้นฉบับ ชุดโค้ดสำเร็จรูป และเอกสารสำหรับซอฟต์แวร์ของระบบงาน ไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ คอมพิวเตอร์พุทธศักราช 2550

กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติดังต่อไปนี้

- บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากหัวหน้าหน่วยงาน
- มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม
- วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้าหน่วยงาน
- การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ
- การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง
- ต้องควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะเพื่อรักษาความมั่นคง ปลอดภัยแก่ข้อมูลและระบบเทคโนโลยีสารสนเทศ อาทิ การใช้งานโปรโตคอลที่มั่นคงปลอดภัยในการบริหารจัดการระบบเครือข่าย เช่น Secure Socket Layer (SSL) Simple Network Management Protocol (SNMP) และ Web Certificate
- การจำกัดการใช้งานเครือข่ายที่ส่งผลกระทบต่อ Bandwidth เช่น การรับ-ส่งไฟล์ขนาดใหญ่ ฟังเพลงออนไลน์ ดูทีวี Online หรือเล่นเกมส์ Online ในช่วง เวลาทำงานปกติ
- ระบบเครือข่ายต้องได้รับการออกแบบและตั้งค่าอย่างเหมาะสมเพื่อรักษาความมั่นคง ปลอดภัยให้แก่ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ อาทิอุปกรณ์ที่เชื่อมต่อกับกับระบบเครือข่ายทั้งหมดจำเป็นต้องได้รับการตั้งค่าให้มีความปลอดภัยและมีการตรวจสอบกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับระบบเครือข่าย ระบบสายสัญญาณต้องได้รับมาตรฐานอุตสาหกรรม และได้รับการติดตั้ง โดย ผู้ที่มีความชำนาญที่ผ่านการพิจารณาอนุมัติแล้ว อุปกรณ์เครือข่ายอาทิ
- Router Firewall Switch Wireless Access Point ต้องได้รับ การตั้งค่าตามความจำเป็นด้านความมั่นคงปลอดภัยของอุปกรณ์นั้น ๆ หรือ ตามคำแนะนำของผู้ผลิต อาทิ SANS Institute หรือสำนักงานความมั่นคงแห่งชาติ (NSA: National Security Agency)

กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ 1 ครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคล ที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติโดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

5.11.5. การบริหารจัดการ อัตลักษณ์ (Identify Management)

เพื่อให้สามารถระบุตัวตนที่เป็นลักษณะเฉพาะของแต่ละบุคคลและระบบต่าง ๆ ที่เข้าถึงสารสนเทศและทรัพย์สินที่เกี่ยวข้องอื่น ๆ ของบริษัทและเพื่อให้สามารถมอบหมายสิทธิการเข้าถึงได้อย่างเหมาะสม

บริษัทควรมีกระบวนการสนับสนุนในการจัดการการเปลี่ยนแปลงข้อมูลที่เกี่ยวข้องกับข้อมูล อัตลักษณ์ของผู้ใช้ กระบวนการเหล่านี้อาจรวมถึงการทวนสอบเอกสารที่เชื่อถือได้ที่เกี่ยวข้องกับบุคคล

เมื่อใช้ อัตลักษณ์ที่บุคคลภายนอกให้หรือออกให้ (เช่น ข้อมูลประจำตัวบนสื่อสังคมออนไลน์ เป็นต้น) บริษัทควรตรวจสอบให้แน่ใจว่าข้อมูล อัตลักษณ์จากบุคคลภายนอกระดับความน่าเชื่อถือที่เหมาะสม และความเสี่ยงที่เกี่ยวข้องใด ๆ เป็นที่ทราบและได้รับการปฏิบัติอย่างเพียงพอ ซึ่งอาจรวมถึงการควบคุมต่าง ที่เกี่ยวข้องกับบุคคลภายนอกรวมทั้งการควบคุมต่าง ๆ ที่เกี่ยวข้องกับข้อมูลการยืนยันตัวตน

5.11.6. การพิสูจน์ตัวตน (Authentication Information)

5.11.6.1. การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of User)

5.11.6.2. ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งานต้องเก็บรักษารหัสผ่านของผู้ใช้งานให้เป็นความลับดูแลบริหารจัดการบัญชีผู้ใช้งานต้องกำหนดรูปแบบรหัสผ่านให้มีความยาวอย่างน้อย 8 ตัวอักษร หรือมากกว่านั้น โดยต้องมีการผสมกันระหว่างอักษรตัวพิมพ์เล็กตัวพิมพ์ใหญ่ ตัวเลข อักขระ พิเศษต่าง ๆ เช่น ! @ # $ % ^ & * เข้าด้วยกันเพื่อให้ยากต่อการคาดเดา ห้ามใช้คำศัพท์ที่อยู่ในพจนานุกรมภาษาอังกฤษ (Dictionary) ห้ามใช้ข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ เช่น หมายเลขโทรศัพท์, วันเดือนปีเกิด, เลขบัตรประชาชน และห้ามใช้ลำดับตัวอักษรหรือลำดับตัวเลขที่ต่อเนื่องกัน เช่น abcd, 1234, abcd1234 เป็นต้น

5.11.6.3. การกำหนดรหัสผ่านให้กับผู้ใช้งานครั้งแรกให้ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งานกำหนด รหัสผ่านชั่วคราวจากการสุ่ม

5.11.6.4. กำหนดให้แจ้งรหัสผ่านกับผู้ใช้งานโดยตรงในวันแรกที่เข้ามาปฏิบัติงาน หรือในกรณีที่มีการร้องขอการรีเซ็ตรหัสผ่านผ่านระบบบริหารจัดการรหัสผ่าน

5.11.6.5. กำชับให้ผู้ใช้เปลี่ยนรหัสผ่านทันทีที่เข้าใช้งานครั้งแรก

5.11.6.6. ระบบที่รองรับต้องเปิดใช้ MFA โดยเฉพาะ Email, VPN, Admin console, ระบบข้อมูลสำคัญ

5.11.6.7. การล๊อกบัญชี/ จำกัดการเดารหัสผ่าน: ล้มเหลวเกิน 5 ครั้ง ให้ล๊อกชั่วคราว 5 - 15 นาที ตามรอบของการผิดพลาด

5.11.7. การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information)

การใช้งานและเก็บรักษาข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานต้องดำเนินการตามนโยบายหรือวิธีปฏิบัติของบริษัท สำหรับการใช้งานข้อมูลพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ เช่น

- การเก็บรักษาข้อมูล Username และ Password ต้องเป็นความลับห้ามเปิดเผย ให้บุคคลอื่นทราบ
- หลีกเลี่ยงการเก็บบันทึกข้อมูลเว้นแต่สามารถเก็บไว้อย่างปลอดภัยได้
- เมื่อได้รับข้อมูล Username และ Password ซึ่งเป็นข้อมูล Default ควรมีการแก้ไข ทันทีเมื่อเข้าใช้งานระบบครั้งแรก

5.12. ความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Supplier Relationships)

5.12.1. นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships)

การใช้บริการจากผู้ให้บริการภายนอก อาจก่อให้เกิดความเสี่ยงได้ ได้แก่ ความเสี่ยงต่อการเข้าถึงข้อมูลความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้นจึงจำเป็นต้องมีการควบคุมผู้ให้บริการภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางการคัดเลือก ควบคุมการปฏิบัติงานของผู้ให้บริการภายนอก

ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศเพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินของบริษัทโดยผู้ให้บริการภายนอก ต้องมีการกำหนดตกลงกับผู้ให้บริการภายใน และจัดทำเป็นลายลักษณ์อักษร

- บริษัทต้องกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับผู้ให้บริการภายนอก โดยผู้ที่เกี่ยวข้องต้องพิจารณา หรือประเมินความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนที่จะอนุญาตให้ผู้ให้บริการภายนอก หรือบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของบริษัท
- ผู้ดูแลระบบและฝ่ายต่าง ๆ ที่รับผิดชอบในการประสานงานกับผู้ให้บริการภายนอก ต้องกำกับให้มีการดูแลให้บุคคลหรือผู้ให้บริการภายนอกแก่หน่วยงานตามที่ว่าจ้างปฏิบัติตามสัญญา หรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

5.12.2. การควบคุมการเข้าใช้งานของผู้ให้บริการภายนอก (Third Party)

5.12.2.1. ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารต้องประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศหรืออุปกรณ์ที่ใช้ในการประมวลผล และมีมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบได้

5.12.2.2. ผู้ให้บริการภายนอก (Third Party) ที่ต้องการสิทธิในการเข้าถึงแหล่งข้อมูลของบริษัทจะต้องทำเรื่องขออนุมัติจากผู้จัดการฝ่ายและสำนักเจ้าของข้อมูล ซึ่งเป็นผู้รับผิดชอบต่อการกระทำทั้งหมดของบุคคลดังกล่าวเป็นลายลักษณ์อักษร ซึ่งต้องมีรายละเอียดอย่างน้อยดังนี้

- เหตุผลในการขอใช้
- ระยะเวลาในการใช้
- การตรวจสอบความปลอดภัยของอุปกรณ์เชื่อมต่อเครือข่าย
- การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

5.12.2.3. ผู้ให้บริการภายนอก (Third Party) ไม่ว่าจะปฏิบัติงานอยู่ภายในบริษัทหรือนอกบริษัทต้องลงนามในสัญญาการรักษาข้อมูลที่เป็นความลับของบริษัท

5.12.2.4. เจ้าของระบบมีหน้าที่กำหนดและทบทวนสิทธิของการเข้าใช้งานระบบสารสนเทศเฉพาะบุคคลที่จำเป็นเท่านั้น และมีการทบทวนสิทธิให้เป็นปัจจุบัน

5.12.2.5. บริษัทต้องพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของผู้ให้บริการภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศ

5.12.2.6. บริษัทมีสิทธิในการตรวจสอบตามสัญญาจ้างเพื่อให้มั่นใจได้ว่าบริษัทสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

5.12.2.7. ในกรณีที่มีการเปลี่ยนแปลงการดำเนินงาน ผู้ให้บริการจากภายนอกต้องแจ้งให้บริษัทรับทราบและอนุมัติการเปลี่ยนแปลงนั้น ก่อนการดำเนินงาน เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

5.12.2.8. เมื่อสิ้นสุดระยะเวลาการใช้งาน บริษัทต้องดำเนินการยกเลิกสิทธิในการเข้าถึงแหล่งข้อมูล และแจ้งผู้จัดการฝ่ายและเจ้าของข้อมูล

5.12.2.9. หากพบเหตุละเมิดด้านความมั่นคงปลอดภัยสารสนเทศให้แจ้งไปยังเจ้าของระบบ

5.12.2.10. ต้องดำเนินการตามนโยบายความมั่นคงปลอดภัยสารสนเทศที่บริษัทประกาศไว้อย่างเคร่งครัด

5.12.3. การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการผู้ให้บริการภายนอก (Assessing Security within Supplier Agreements)

ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการกำหนด และตกลงกับผู้ให้บริการภายนอกในเรื่องที่เกี่ยวข้องกับการเข้าถึง การประมวลผล การจัดเก็บ การสื่อสาร และการให้บริการ โครงสร้างพื้นฐานของระบบสำหรับสารสนเทศของบริษัท โดยผู้ให้บริการภายนอก

- บริษัทต้องแสดงนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้แก่ผู้ให้บริการภายนอกที่เกี่ยวกับการเข้าถึง การประมวลผล การจัดเก็บ การสื่อสาร และการให้บริการสารสนเทศของบริษัท
- ผู้ให้บริการภายนอกต้องยอมรับนโยบาย กฎหมายที่เกี่ยวข้องและการควบคุมด้านความมั่นคงปลอดภัยของบริษัท
- บริษัทมีสิทธิที่จะตรวจสอบสภาพแวดล้อมการทำงานรวมทั้งการตรวจสอบการทำงานของผู้ให้บริการภายนอก

5.12.4. ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศ และการสื่อสารโดยผู้ให้บริการภายนอก (Information and Communication Technology Supply Chain)

- ข้อตกลงกับผู้ให้บริการภายนอก ต้องรวมถึงความต้องการเรื่องการระบุความเสี่ยงอันเกิดจากห่วงโซ่ของการให้บริการเทคโนโลยีสารสนเทศและการสื่อสาร
- ต้องมีการประเมินความเสี่ยงจากการเข้าถึง ข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ที่ ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการควบคุมที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงข้อมูล และระบบสารสนเทศหรืออุปกรณ์ดังกล่าวได้

5.12.5. การบริหารจัดการ การให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)

เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระบบการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of Supplier Services)

- บริษัท ต้องจัดทำข้อตกลง กำหนดสิทธิสำหรับบริษัท ที่จะตรวจสอบสภาพแวดล้อมการทำงาน รวมทั้งการตรวจสอบการทำงานของหน่วยงานภายนอก โดยพิจารณาจากสัญญาจัดซื้อจัดจ้างของหน่วยงานภายนอก

- ต้องมีการทบทวนติดตามและตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

การบริหารจัดการ การเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing Changes to Supplier Services)

- การเปลี่ยนแปลงรายละเอียดการให้บริการของหน่วยงานภายนอก ที่เกี่ยวข้องกับบริการด้านสารสนเทศของบริษัท ทุกครั้ง ต้องเป็นไปตามเอกสาร

- การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอกรวมทั้งการปรับปรุงนโยบาย ขั้นตอนการปฏิบัติและมาตรการที่ใช้อยู่ในปัจจุบันต้องมีการบริหารจัดการ โดยต้องนำระดับความสำคัญของสารสนเทศ และกระบวนการทางธุรกิจที่เกี่ยวข้องมาพิจารณาด้วย และต้องมีการทบทวนการประเมินความเสี่ยงใหม่

5.12.6. การบริหารการจัดด้านความปลอดภัยบริการคลาวด์ (Information Security for using Cloud Services)

บริษัทฯ มีการควบคุมข้อกำหนดด้านความปลอดภัยสำหรับบริการระบบคลาวด์ เพื่อให้มีการปกป้อง ข้อมูลของ บริษัทฯ ในระบบคลาวด์ได้ดียิ่งขึ้นซึ่งรวมถึงการซื้อใช้งาน จัดการและยุติการใช้บริการคลาวด์ บริษัทฯ จัดทำมาตรการด้านความปลอดภัยสำหรับบริการระบบคลาวด์ และกำหนดเกณฑ์สำหรับการเลือก ผู้ให้บริการระบบคลาวด์ นอกจากนี้ บริษัทฯ มีการกำหนดกระบวนการพิจารณาการใช้งาน ระบบคลาวด์ที่ยอมรับได้ และกำหนดความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีเมื่อยกเลิกการใช้บริการระบบคลาวด์ โดยมีข้อกำหนด ดังนี้

- บริษัทอนุญาตให้ใช้บริการคลาวด์เฉพาะที่ผ่านการประเมินความเสี่ยงและได้รับอนุมัติตามกระบวนการ Cloud Service Onboarding และต้องเป็นบริการที่อยู่ในรายการ Approved Cloud Services

- บริการคลาวด์ที่เก็บ/ประมวลผลข้อมูลระดับ Confidential ขึ้นไป ต้องบังคับใช้ MFA, logging, encryption at rest/in transit และต้องมีการทบทวนสิทธิอย่างน้อยรายไตรมาส

- ก่อนยุติการใช้บริการคลาวด์ ต้องจัดทำ Exit Plan เพื่อย้าย/คืนข้อมูล ถอนสิทธิ์ และดำเนินการลบข้อมูลอย่างปลอดภัย พร้อมบันทึกหลักฐานการดำเนินการ

5.13. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีและการปรับปรุง (Management of Information Security Incidents and Improvements)

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของบริษัทได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และมีวิธีการที่สอดคล้องและได้ผลสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของบริษัท

- บริษัทต้องมีการกำหนดหน้าที่ความรับผิดชอบ และกำหนดขั้นตอนปฏิบัติเพื่อรับมือกับเหตุละเมิดด้านความมั่นคงปลอดภัยอย่างทันท่วงที

- บริษัทต้องกำหนดให้มีการจำแนกสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดออกจากเหตุการณ์ด้านการปฏิบัติงานทั่วไปเพื่อกำหนดแนวทางการแก้ไขที่ถูกต้องเหมาะสม

- บริษัทต้องกำหนดช่องทาง และเกณฑ์ในการรายงานเหตุการณ์ หรือจุดอ่อนหรือเหตุการณ์ความมั่นคงสารสนเทศหรือสื่อสารให้บุคลากรในองค์กร และหน่วยงานภายนอกรับทราบ

5.13.1. การกระทำอื่น ๆ ที่ถือเป็นข้อห้ามของบริษัท

- การกระทำใด ๆ ที่กฎหมายบัญญัติว่าเป็นความผิด ตลอดจนการกระทำในลักษณะอื่น ๆ ที่กล่าวถึงด้านล่างนี้ถือเป็นข้อห้ามของบริษัท ไม่ยินยอมให้พนักงานดำเนินการโดยเด็ดขาดทั้งนี้บริษัท มิได้เขียนระบุถึงข้อห้ามทั้งหมดที่ห้ามกระทำไว้ แต่เขียนเพื่อเป็นแนวทางให้แก่ผู้ใช้งานได้รับทราบเท่านั้น

หมายเหตุ: พนักงานบางส่วนอาจได้รับยกเว้นจากข้อห้ามบางข้อที่กล่าวไว้ด้านล่างนี้ (ตราบเท่าที่ไม่ขัดต่อกฎหมาย) หากเป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย เช่น ผู้ดูแลระบบสามารถระงับการเข้าถึงระบบเครือข่ายของอุปกรณ์ใด ๆ หากการเข้าถึงนั้นรบกวนการทำงานของระบบเทคโนโลยีสารสนเทศ

- การใช้งานทรัพยากรของบริษัท เพื่อการจัดหาหรือส่งต่อ วัสดุ เอกสาร หรือรูปภาพลามกอนาจาร หรือที่ขัดต่อกฎหมาย

- การฉ้อโกงโดยใช้ User ID และรหัสผ่านที่บริษัทกำหนดให้ เพื่อเสนอขายสินค้าหรือบริการใด ๆ

- การพยายามล่วงละเมิดความมั่นคงปลอดภัย หรือรบกวนการทำงานของระบบเครือข่ายตัวอย่างของการล่วงละเมิดความมั่นคงปลอดภัย ได้แก่ การเข้าถึงข้อมูลหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ตนไม่ได้รับอนุญาต เป็นต้น ส่วนตัวอย่างของการรบกวนการทำงานของระบบเครือข่าย ได้แก่ Sniffing, Pinged Floods, Pack Spoofing, Denial of Service และ Forged Routing Information ด้วยเจตนามุ่งร้าย เป็นต้น

- การใช้งาน Bandwidth จำนวนมากโดยเฉพาะอย่างยิ่งการใช้งานโปรแกรมประเภท P2P File Sharing

- การทำ Port Scanning และ Security Scanning เว้นแต่เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย

- การดักฟังหรือดักจับข้อมูลที่พนักงานไม่ได้รับอนุญาตให้รับรู้ด้วยวิธีการใด ๆ เว้นแต่เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย

- การค้นหาจุดบกพร่องของระบบ เพื่อทำการเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต

- การหลบเลี่ยงการพิสูจน์ตัวตนผู้ใช้งานหรือมาตรการด้านความมั่นคงปลอดภัยของคอมพิวเตอร์ระบบเครือข่ายใด ๆ

- การใช้โปรแกรม/ สคริปต์/ คำสั่ง หรือการส่งข้อความใด ๆ โดยมีเจตนารบกวน ลดประสิทธิภาพการให้บริการ หรือระงับการใช้งานของผู้ใช้งาน ทั้งโดยผ่านระบบภายใน หรือผ่านระบบเครือข่ายต่าง ๆ

- การให้ข้อมูลลับเกี่ยวกับรายชื่อพนักงาน รายชื่อลูกค้า ความลับของบริษัท และข้อมูลลับอื่น ๆ แก่บุคคลภายนอก

- การข่มขู่คุกคามทุกรูปแบบผ่านอีเมล์ โทรศัพท์ หรือระบบส่งข้อความ ไม่ว่าจะด้วยภาษา ความถี่ หรือขนาดของข้อความการแสดงความคิดเห็น หรือส่งข้อความใด ๆ ที่ไม่เกี่ยวข้องกับการทำงานไปหาบุคคลจำนวนมาก (Newsgroup Spam)

- การละเมิดสิทธิส่วนบุคคล ลิขสิทธิ์ของบริษัท ความลับของบริษัท สิทธิบัตร ทรัพย์สินทางปัญญา หรือกฎหมายอื่นใด

5.13.2. การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ (Reporting information security weaknesses)

พนักงานและผู้ที่ทำสัญญาจ้าง ซึ่งใช้ระบบและบริการสารสนเทศของบริษัท ต้องสังเกตและรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศในระบบหรือบริการที่สังเกตพบหรือที่สงสัย แบ่งเป็นระดับเหตุการณ์ได้ดังนี้

- เกณฑ์เหตุการณ์อยู่ในระดับต่ำ

ผู้ดูแลระบบสารสนเทศของฝ่ายสามารถแก้ไขเหตุการณ์ที่เกิดขึ้นเองได้ เช่นการติดไวรัส เป็นต้น และทำการรายงานเหตุการณ์ที่เกิดขึ้น ทุก ๆ 1 เดือน

- เกณฑ์เหตุการณ์อยู่ในระดับกลาง

ผู้ดูแลระบบสารสนเทศฝ่ายแจ้งให้ผู้บังคับบัญชา ทราบถึงเหตุการณ์ที่เกิดขึ้น หากเหตุการณ์ที่เกิดขึ้นฝ่าย ประเมินความเสี่ยงแล้ว ให้ฝ่ายแจ้งเป็นลายลักษณ์อักษร แจ้งไปยังฝ่ายเทคโนโลยีสารนสนเทศของบริษัท เพื่อเข้ามาแก้ไขเหตุการณ์ที่เกิดขึ้น

- เกณฑ์เหตุการณ์อยู่ในระดับสูง

ผู้ดูแลระบบสารสนเทศของฝ่ายต้องทำการแจ้งฝ่ายเทคโนโลยีสารนสนเทศของบริษัทอย่างเร่งด่วนหากเหตุการณ์ที่เกิดขึ้นเป็นเหตุการณ์ร้ายแรง และเร่งด่วน เพื่อหาแนวทางในการแก้ไขปัญหา จากนั้นทำการสรุปปัญหาที่เกิดขึ้นกับระบบสารสนเทศฝ่ายให้ผู้บริหารระดับสูงทราบ

5.13.3. การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)

สถานการณ์ความมั่นคงปลอดภัยสารสนเทศ ต้องมีการประเมินและต้องมีการตัดสินใจว่า สถานการณ์นั้นเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่ จากกระบวนการดังนี้

ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ: ต้องกำหนดนโยบายให้กับบุคลากรและผู้ดูแลระบบในหน่วยงาน นั้น ๆ ปฏิบัติตามนโยบายที่วางไว้

- ผู้ดูแลระบบต้องกำหนดให้มีการเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ เหตุการณ์ผิดปกติและการแจ้งเตือนต่าง ๆ ที่อุปกรณ์ตรวจพบ จะถูกทำการวิเคราะห์ และหาสาเหตุของการบุกรุก ในระบบสารสนเทศของบริษัท เพื่อเป็นเครื่องมือสืบสวน หาบุคคลที่โจมตี บุกรุก หรือใช้ระบบในทางที่ผิด

ผู้ดูแลระบบ: ต้องกำหนดให้มีการเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ เหตุการณ์ผิดปกติและการแจ้งเตือนต่าง ๆ ที่อุปกรณ์ตรวจพบ

- ผู้ดูแลระบบต้องเก็บสถิติเกี่ยวกับความพยายามที่จะบุกรุกหรือโจมตีกรม เป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันภัยของระบบรักษาความปลอดภัยอื่น เช่น ไฟวอล์เป็นต้น และเพื่อเป็นการป้องกันเครือข่ายคอมพิวเตอร์ภายในจากอันตราย ที่มาจากเครือข่ายคอมพิวเตอร์ภายนอก เช่น ผู้บุกรุก หรือ hacker รวมทั้ง ไวรัสประเภทต่าง ๆ

ผู้ดูแลระบบ: ผู้ดูแลระบบต้องมีการบริหารจัดการ การบุกรุกระบบ โดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับบริษัท

- ผู้ดูแลระบบต้องมีการบริหารจัดการ การบุกรุกระบบ โดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับบริษัท และจัดทำวิธีปฏิบัติที่ถูกต้อง ให้กับบริษัทเพื่อป้องกันเหตุการณ์ที่เกิดขึ้นซ้ำ

5.13.4. การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

- มีการกำหนดขั้นตอนไว้รองรับกรณีเกิดเหตุการณ์ที่ประเมินแล้วว่าก่อให้เกิดความไม่มั่นคงปลอดภัย
- เมื่อเกิดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร โดยได้จัดทำแยกประเภทตามระบบต่าง ๆ ดังนี้
- ระบบป้องกันผู้บุกรุก ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมีดังต่อไปนี้

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลขไอพีของเครือข่ายที่ผู้ไม่ประสงค์ดีใช้โจมตี

- ระบบ Firewall ดำเนินการตรวจสอบระบบป้องกันการบุกรุก อย่างน้อยเดือนละ 1 ครั้ง ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอล์สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

- Packet ที่ไฟร์วอล์ได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพีของเครือข่ายใดถูก Block เป็นจำนวนมาก

หมายเหตุ กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้าหน่วยงานเพื่อตัดสินใจดำเนินการแก้ไขปัญหา

- ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์ ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่ง มัลแวร์จากเครือข่ายภายในบริษัทไปยังภายนอกหรือไม่
- ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์โดยเฉพาะประเภทที่ตรวจพบว่ากระจาย อยู่ในเครือข่ายของบริษัท
- ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่ง มัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

5.13.5. การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)

ความรู้ที่ได้รับจากการวิเคราะห์และแก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ต้องถูกนำมาใช้เพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ความมั่นคงปลอดภัยที่จะเกิดขึ้นในอนาคต

- ผู้ดูแลระบบต้องบันทึกเหตุละเมิดด้านความมั่นคงปลอดภัย จุดอ่อน ช่องโหว่ ภัยคุกคามหรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไขจากเหตุการณ์ที่เกิดขึ้นเพื่อเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

- หน่วยงานที่รับผิดชอบ ต้องจัดทำสรุปรายงานการแจ้งเหตุละเมิดความมั่นคงปลอดภัยให้ผู้บังคับบัญชาอย่างน้อยเดือนละ 1 ครั้ง

- ต้องมีการทบทวนเหตุละเมิดความมั่นคงปลอดภัย เพื่อป้องกันการเกิดปัญหาเดิมซ้ำ

- ต้องมีการวิเคราะห์ความเสี่ยง และประเมินสถานการณ์การบุกรุก/ละเมิด/ระบาดที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

5.14. การเก็บรวบรวมหลักฐาน (Collection of Evidence)

บริษัทต้องกำหนดและประยุกต์ขั้นตอนปฏิบัติสำหรับการระบุ การรวบรวม การจัดหา และจัดเก็บสารสนเทศซึ่งสามารถใช้เป็นหลักฐานได้

หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ต้องดำเนินการให้หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญให้มีการรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในการวิเคราะห์

สืบสวนหรือเป็นหลักฐานในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่า ได้ปฏิบัติตามข้อกำหนดทางด้านกฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูลระเบียบของ บริษัทฯ และกฎหมาย (เช่น 90 วัน เป็นต้น)

หัวหน้าหน่วยงานดูแลรับผิดชอบด้านกฎหมายและหน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องศึกษากฎเกณฑ์ที่เกี่ยวข้อง เช่น ถ่อยแถลงในกฎหมายแพ่งหรืออาญา ซึ่งระบุถึงลักษณะของหลักฐานที่ต้องเก็บรวบรวมมา เพื่อใช้ในการดำเนินการทางกฎหมายกับผู้กระทำผิด เป็นต้น

หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องศึกษาถึงลักษณะของหลักฐานที่มีความสมบูรณ์และมีคุณภาพ เพื่อสามารถนำไปใช้ในกระบวนการของศาลได้

5.15. ความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีระหว่างการหยุดชะงัก (Information security during disruption)

5.15.1. ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีของการบริหารจัดการ เพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)

เพื่อเป็นแนวทางในการบริหารจัดการความต่อเนื่องในการดำเนินงานของบริษัท เมื่ออยู่ภายใต้สภาวะวิกฤตและเหตุฉุกเฉินต่าง ๆ ทำให้มั่นใจได้ว่า ขั้นตอนการดำเนินงานและระบบสารสนเทศต่าง ๆ ของบริษัทที่สำคัญ มีการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan หรือ BCP) และแผนกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Plan หรือ DRP) อย่างเหมาะสม เพื่อให้การดำเนินงานของบริษัท เป็นไปอย่างต่อเนื่อง

5.15.2. ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)

- บริษัทต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสถานการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดวิกฤตหรือภัยพิบัติ

- ต้องจัดทำแนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉิน ของระบบเทคโนโลยีสารสนเทศควรพิจารณาดังนี้

การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการดำเนินงานของบริษัทและการให้บริการด้านเทคโนโลยีสารสนเทศบริษัท

การตอบสนองต่อสถานการณ์ฉุกเฉินเพื่อควบคุมและจำกัดขอบเขตของความเสียหาย เช่น กำหนดแนวทางการควบคุมการแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น

การดำเนินการเพื่อให้บริษัทสามารถดำเนินงานเป็นไปได้อย่างต่อเนื่อง เช่น การสำรองข้อมูลและอุปกรณ์สำคัญการกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น

การกลับคืนสู่การทำงานปกติเพื่อให้การดำเนินงานของบริษัทกลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น

5.15.3. การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing information security continuity)

บริษัทต้องกำหนด จัดทำเป็นลายลักษณ์อักษร ปฏิบัติ และปรับปรุง กระบวนการขั้นตอนปฏิบัติ และมาตรการ เพื่อให้ได้ระดับความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ เมื่อมีสถานการณ์ความเสียหายหนึ่งเกิดขึ้น

- ต้องจัดตั้ง ISS (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ของระบบเทคโนโลยีสารสนเทศซึ่งประกอบไปด้วยตัวแทนจากหน่วยงาน เจ้าของข้อมูล เจ้าของระบบงาน หน่วยงานที่ดูแลข้อมูล เป็นต้น

- ISS (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ ที่เป็นลายลักษณ์อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอรวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละ 1 ครั้ง

- การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)

บริษัทต้องมีการตรวจสอบมาตรการสร้างความต่อเนื่องที่ได้เตรียมไว้ตามรอบระยะเวลาที่กำหนดไว้ เพื่อให้มั่นใจว่ามาตรการเหล่านั้นยังถูกต้อง และได้ผลเมื่อมีสถานการณ์ความเสียหายเกิดขึ้น

- ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่าง ๆ ไว้นอกสถานที่

- ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย

- ควรติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรองเพื่อให้สามารถค้นหาได้โดยเร็ว, เพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

- มีการขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจและควรจัดทำทะเบียนควบคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง

- ต้องกำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่ง รวมถึงข้อมูลสำคัญต่าง ๆ ในฮาร์ดดิสก์

5.16. การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies)

5.16.1. สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)

- มีการจัดลำดับความสำคัญของระบบงาน/ กระบวนงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้คืนแต่ละระบบงานด้วยการประเมินความเสี่ยง (Risk Assessment) และ/หรือ การประเมินผลกระทบของกระบวนงานหลัก
- มีการกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา
- มีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์
- มีการกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ
- มีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน
- หน่วยงานที่เป็นหน่วยสำรองข้อมูลหรือจัดเก็บข้อมูลก็ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน

- มีการทบทวนหรือปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ (ทุก 6 เดือน) และเก็บแผนฉุกเฉินไว้ในสถานที่มั่นคงปลอดภัย
- ทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 2 ครั้ง โดยต้องเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง
- ต้องสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องทุกระดับได้รับทราบเฉพาะเท่าที่จำเป็นและควรป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้รับทราบ
- กรณีที่เกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหาไว้ด้วย

5.16.2. ความพร้อม ICT เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)

ควรวางแผนด้านความพร้อมของ ICT ไปปฏิบัติดูแลรักษาและทดสอบโดยอิงตาม วัตถุประสงค์ ความต่อเนื่องทางธุรกิจและข้อกำหนดความต่อเนื่องของ ICT และควบคุมข้อกำหนดให้เทคโนโลยีสารสนเทศ และการสื่อสารของบริษัทฯพร้อมสำหรับการหยุดชะงักที่อาจเกิดขึ้นเพื่อให้ข้อมูลและสินทรัพย์ที่จำเป็นพร้อม ใช้งานเมื่อจำเป็นซึ่งรวมถึงการวางแผนความพร้อม การนำไปใช้งาน การบำรุงรักษา และการทดสอบ

บริษัทฯ มีการกำหนดกระบวนการ ขั้นตอนการวางแผนซึ่งคำนึงถึงความเสี่ยงและความต้องการ ทางธุรกิจในการกู้คืน บริษัทฯ มีการกำหนดการบำรุงรักษาสำหรับเทคโนโลยีสารสนเทศ และขั้นตอน การทดสอบสำหรับการกู้คืนจาก ความเสียหายและแผนความต่อเนื่องทางธุรกิจ โดยแผนดังกล่าวได้รับ การอนุมัติจากกรรมการผู้ช่วยประธานเจ้าหน้าที่บริหาร

บริษัทฯ มีการจัดทำเอกสารผ่านการวิเคราะห์ผลกระทบทางธุรกิจ กลยุทธ์ความต่อเนื่องทางธุรกิจ และแผนความต่อเนื่องทางธุรกิจ พร้อมกับการจัดทำรายงานการทดสอบความต่อเนื่องทางธุรกิจ โดยมี การทบทวนและทดสอบความต่อเนื่องทางธุรกิจอย่างน้อยปีละ 1 ครั้ง

5.17. กฎหมาย ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับและข้อผูกพันตามสัญญา (Legal, statutory, regulatory and contractual requirements)

เพื่อป้องกันการละเมิดที่เกี่ยวข้องกับการปฏิบัติงาน ระเบียบ ข้อบังคับ เงื่อนไขในสัญญา และข้อกำหนดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นแนวทางในการปฏิบัติงานของบริษัท ที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

5.17.1. การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

บริษัท ต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

พนักงาน ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด และมีรายการดังต่อไปนี้เป็นอย่างน้อย

- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- พระราชบัญญัติลิขสิทธิ์
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
- พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์
- นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ บริษัทฯ
- การควบคุมการเข้ารหัส (Regulation of cryptographic controls)
- ต้องมีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง

ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัท ถือเป็นสินทรัพย์ของบริษัท (ยกเว้นข้อมูลที่เป็นสินทรัพย์ของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้บริษัทสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท และขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่าง ๆ ของบริษัท กำหนดไว้

บริษัทฯ ขอสงวนสิทธิในการเข้าถึง ทบทวน และตรวจสอบอีเมลของผู้ใช้งาน โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า อย่างไรก็ตามบริษัท จะดำเนินการตรวจสอบ ดังกล่าวต่อเมื่อมีความจำเป็นเท่านั้นและจะไม่เปิดเผย ข้อมูลใด ๆ ของผู้ใช้งาน เว้น แต่เป็น การเปิดเผยตามคำสั่งศาลตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น

ห้ามพนักงานในบริษัท ใช้งานสินทรัพย์และระบบเทคโนโลยีสารสนเทศของบริษัท กระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม

การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใด ๆ ออกนอกประเทศ ไม่ขัดต่อข้อกฎหมายใด ๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ผู้ใช้งานต้องปรึกษาผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

5.18. สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights)

สิทธิในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ที่มีกรรมสิทธิต้องทำตามขั้นตอนกฎหมาย ข้อบังคับ และสัญญาจ้างเอกชน

บริษัทต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานสินทรัพย์ทางปัญญาที่หน่วยงานจัดหามาใช้งาน และต้องระมัดระวังที่จะไม่ละเมิดลิขสิทธิ์เหล่านั้นโดยเด็ดขาด

บริษัทต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ ที่ติดตั้งมีลิขสิทธิ์ถูกต้อง

ห้ามผู้ใช้งานดำเนินการทำซ้ำหรือเผยแพร่รูปภาพ บทเพลง บทความ หนังสือหรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัท โดยเด็ดขาด

เพื่อที่จะให้เกิดความแน่ใจว่าพนักงานในบริษัท มิได้ละเมิด ลิขสิทธิ์โดยไม่ได้ตั้งใจ หรือ พลั้งเผลอจึงไม่ควรจะทำสำเนาซอฟต์แวร์ใด ๆ ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของบริษัทเพื่อจุดประสงค์ใด ๆ ก็ตามโดยที่ไม่ได้รับอนุญาตและใน

ขณะเดียวกันพนักงานในบริษัทไม่ควรจะติดตั้งโปรแกรมใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัท โดยไม่ได้รับการอนุญาต ทั้งนี้เพื่อที่จะให้แน่ใจว่ามีใบอนุญาตที่ครอบคลุมการติดตั้งดังกล่าว

บริษัท กำหนดให้มีการตรวจ สอบเครื่องคอมพิวเตอร์อย่างน้อยปีละ 1 ครั้งเพื่อตรวจดูรายการของซอฟต์แวร์ในเครื่องคอมพิวเตอร์ และเพื่อให้แน่ใจว่าบริษัทมีใบอนุญาตการใช้งานสำหรับผลิตภัณฑ์ซอฟต์แวร์แต่ละตัวในเครื่องคอมพิวเตอร์ถ้าพบว่ามีซอฟต์แวร์ที่ไม่ได้รับอนุญาต ซอฟต์แวร์ เหล่านั้นจะถูกลบทิ้ง และถ้าหากมีความจำเป็นบริษัทอาจจะมีการพิจารณาให้นำซอฟต์แวร์ที่มีใบอนุญาตอย่างถูกต้องอื่นมาใช้แทนซอฟต์แวร์ดังกล่าวได้

5.18.1. การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records)

บริษัทต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎระเบียบ หรือข้อบังคับที่ได้กำหนดไว้โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูลระเบียบหน่วยงานว่าด้วยงานสารบรรณและกฎหมาย

5.18.2. ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information)

บริษัทต้องมีการการป้องกันข้อมูลและความเป็นส่วนตัวตามกฎหมาย ระเบียบ สัญญาที่เกี่ยวกับบริษัท

5.18.3. การป้องกันข้อมูลสำคัญของบริษัท (Protection of Organizational Records)

ข้อมูลสำคัญของบริษัท ต้องได้รับการป้องกันจากการสูญหาย การถูกทำลายการปลอมแปลง การเข้าถึง และการเผยแพร่โดยไม่ได้รับอนุญาต

ผู้ใช้งานจากข้อมูลสำคัญของบริษัทต้องดำเนินการให้สอดคล้องกับกฎหมาย นโยบายระเบียบ ข้อบังคับ ของบริษัท

5.18.4. การควบคุมการเข้ารหัส (Regulation of cryptographic controls)

บริษัทต้องมีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง

5.18.5. การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of Misuse of Information Processing Facilities)

อุปกรณ์ประมวลผลสารสนเทศของบริษัทมีไว้เพื่อใช้ในกิจการของบริษัทเท่านั้นยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากผู้บังคับบัญชาที่มีอำนาจ

ต้องกำหนดให้มีผู้รับผิดชอบ รวมถึงการจัดทำบัญชีรายการของอุปกรณ์ประมวลผลสารสนเทศที่ซื้อหรือเช่ามาใช้งาน

ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่าง ๆ เมื่อมีการเปลี่ยนแปลง เพื่อใช้เป็นข้อมูลในการควบคุมสินทรัพย์ของบริษัท

การดำเนินการใด ๆ ที่เป็นการติดตั้งซอฟต์แวร์หรืออุปกรณ์เพิ่มเติมต้องได้รับการอนุมัติจากผู้บังคับบัญชาที่มีอำนาจเป็นลายลักษณ์อักษร เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

อุปกรณ์ประมวลผลสารสนเทศจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนเป็นอย่างน้อย ก่อนการเข้าใช้งานด้วยวิธีการใส่รหัสผ่านตามนโยบายการบริหารจัดการรหัสผ่าน

5.18.6. การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยี (Independent Review of Information Security)

ต้องมีการทบทวนวิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยี และการปฏิบัติของ บริษัทฯ เช่น ทบทวนวัตถุประสงค์ มาตรการ นโยบาย วิธีปฏิบัติงานต่าง ๆ ให้ถูกต้องและเป็นปัจจุบันตามรอบระยะเวลาที่กำหนดอย่างน้อยปีละ 1 ครั้ง

5.18.7. การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความปลอดภัยสารสนเทศ (Compliance with policies, rules and Security Standards for information security)

การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน (Compliance with Security Policy and Standards)

- ต้องจัดให้มีการตรวจสอบระบบทั้งหมดของหน่วยงานตามนโยบายการรักษาความมั่นคงปลอดภัย สารสนเทศและระยะเวลาที่กำหนดไว้
- ต้องมีการตรวจสอบ และทบทวนเอกสารนโยบาย มาตรการ วิธีการปฏิบัติงานรวมถึง แบบฟอร์มที่เกี่ยวเนื่องกันตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลง

5.18.8. การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

ต้องจัดให้มีการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งานหรือให้บริการอยู่แล้วตามระยะ เวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดู ว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งาน เป็นไปอย่างปลอดภัย หรือไม่รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่อง ของระบบด้วย

5.18.9. เอกสารขั้นตอนการปฏิบัติงาน (Document Operating Procedures)

ต้องจัดทำเอกสารแนวปฏิบัติที่เหมาะสมสำหรับแต่ละระบบเทคโนโลยีสารสนเทศที่อยู่ในความรับผิดชอบของตนและประกาศให้ผู้ปฏิบัติงานทราบ

คู่มือและแนวปฏิบัติงานต้องได้รับการปรับปรุงเมื่อมีการปรับเปลี่ยนขั้นตอนและผู้รับผิดชอบการปฏิบัติงานนั้น ๆ โดยแนวปฏิบัติงานและเอกสารเกี่ยวข้องทุกฉบับต้องได้รับการทบทวน อย่างน้อยปีละ 1 ครั้ง รวมถึงมีการป้องกันมิให้ข้อมูลหรือเอกสารเกี่ยวกับระบบเทคโนโลยีสารสนเทศ ถูกเข้าถึงโดยมิได้รับอนุญาต

6. มาตรการควบคุมด้านเจ้าหน้าที่ (People Control) Annex 6

วัตถุประสงค์

เพื่อให้มั่นใจว่าพนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทของตนเองที่ได้รับการพิจารณา มีความตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเองเพื่อลดความเสี่ยงจากความผิดพลาด และการนำไปใช้งานในทางที่ไม่เหมาะสมของพนักงาน และเพื่อให้มั่นใจในกระบวนการเปลี่ยนแปลงหรือสิ้นสุดการจ้างงานไม่กระทบกับความปลอดภัยสารสนเทศ

6.1. ก่อนการจ้างงาน (Prior to Employment)

6.1.1. การสรรหาเจ้าหน้าที่ (Screening)

การคัดเลือก (Screening) การตรวจสอบภูมิหลังของผู้สมัครงาน ต้องมีการดำเนินการ โดยมีความสอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และต้องดำเนินการในระดับที่เหมาะสมกับความต้องการทางธุรกิจ ชั้นความลับของข้อมูลที่จะถูกเข้าถึง และความเสี่ยงที่เกี่ยวข้อง

บริษัทต้องกำหนดหน้าที่ความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศในคุณสมบัติของบุคลากรตามหน้าที่งานที่ได้รับมอบหมาย

ฝ่ายบริหารและพัฒนาทรัพยากรบุคคล ต้องตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นบุคลากรของบริษัท จะต้องมีการตรวจสอบประวัติอาชญากรรม หรืออื่น ๆ ตามเงื่อนไขที่เกี่ยวข้อง

ฝ่ายบริหารและพัฒนาทรัพยากรบุคคล ต้องจัดให้มีการลงนามในสัญญาระหว่าง "พนักงาน" และบริษัท ว่าจะไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement : NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างพนักงานนั้น ๆ ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องตามนโยบายการเก็บรักษาและระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล (SKY ICT Data Retention Policy) ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

6.1.2. ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)

ข้อตกลงและเงื่อนไขในสัญญาจ้างกับพนักงาน และผู้ที่ทำสัญญาต้องกล่าวถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของพนักงาน ของผู้ที่ทำสัญญาจ้าง และของบริษัทฝ่ายบริหารและพัฒนาทรัพยากรบุคคล ต้องกำหนดเงื่อนไขการจ้างงาน ที่รวมถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท

ฝ่ายบริหารและพัฒนาทรัพยากรบุคคล ต้องเตรียมข้อมูลที่เกี่ยวข้องกับ นโยบายความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท เพื่อให้พนักงานและผู้ใช้งานที่เข้ามาใหม่ได้ศึกษาและลงนามรับทราบ รวมถึงยอมรับสัญญาในการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับตำแหน่งหน้าที่ความรับผิดชอบตามนโยบายเหล่านั้นอย่างเคร่งครัด

เพื่อให้การบริหารจัดการ User ID เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุดฝ่ายบริหารและพัฒนาทรัพยากรบุคคลต้องแจ้งให้หน่วยงานที่รับผิดชอบทราบทันทีเมื่อมีการดำเนินการดังต่อไปนี้

- การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร พนักงานและลูกจ้าง หรือการถึงแก่กรรม
- การโยกย้ายหน่วยงาน

- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

คณะกรรมการ ผู้อำนวยการ รองผู้อำนวยการ ผู้จัดการฝ่าย พนักงาน และลูกจ้างใหม่ทุกคน ที่เข้ามาปฏิบัติงานในบริษัท ต้องลงนามรับทราบและยินยอมปฏิบัติตามสัญญาการรักษาข้อมูลที่เป็นความลับของบริษัท และเอกสารอื่น ๆ ที่เกี่ยวข้อง ก่อนอนุญาตให้เริ่มงานหรือเข้าถึงและใช้งานข้อมูลสารสนเทศของบริษัท

6.2. ระหว่างการจ้างงาน (During employment)

หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities) ผู้บริหารต้องกำหนดให้พนักงานและผู้ที่ทำสัญญาว่าจ้างทั้งหมดรักษาความมั่นคงปลอดภัยสารสนเทศโดยปฏิบัติให้สอดคล้องกับนโยบายและขั้นตอนปฏิบัติตามที่บริษัทกำหนดไว้อย่างเคร่งครัด

6.2.1. การสร้างความตระหนัก การให้ความรู้ บุคลากรฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training)

พนักงานของบริษัททั้งหมดและผู้ที่ทำสัญญาต่าง ๆ ที่เกี่ยวข้อง ต้องได้รับการสร้างความตระหนัก ให้ความรู้ และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ และต้องมีการเรียนรู้ และทบทวนเพิ่มเติมในนโยบายและขั้นตอนปฏิบัติของบริษัทที่เกี่ยวข้องกับงานที่ตนเองปฏิบัติ

พนักงานของบริษัททุกคนต้องได้รับการอบรมให้ความรู้โดยเนื้อหาที่แต่ละบุคคลจะได้รับการฝึกอบรมต้องเหมาะสมกับบทบาทหน้าที่ในการปฏิบัติงานของแต่ละบุคคล เพื่อเป็นการสร้างความตระหนัก และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ

ต้องจัดอบรมให้ความรู้แก่พนักงาน เกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยและการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศและการสื่อสาร

พนักงานใหม่ทุกคน ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและระเบียบปฏิบัติที่เกี่ยวข้องกับหน่วยงานก่อนหรืออย่างน้อยภายใน 90 วันนับจากเข้าทำงานในหน่วยงาน โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากรด้วย

ฝ่ายบริหารและพัฒนาทรัพยากรบุคคล มีหน้าที่ในการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารให้แก่บุคลากรด้วย

6.2.2. กระบวนการทางวินัย (Disciplinary process)

กระบวนการทางวินัยต้องกำหนดอย่างเป็นทางการ และมีการสื่อสารให้พนักงานได้รับทราบและพนักงานต้องยินยอมทำตามเงื่อนไขที่กำหนด เพื่อดำเนินการต่อพนักงานที่ละเมิดความมั่นคงปลอดภัยสารสนเทศของบริษัท

บริษัทจัดให้มีมาตรการดำเนินการกับผู้ฝ่าฝืนหรือละเมิดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทที่เป็นความผิดทางวินัยภายใต้ระเบียบ ข้อบังคับของบริษัทกรณีดำเนินกิจกรรมที่เกี่ยวกับการทดสอบระบบสารสนเทศ เพื่อตรวจสอบหรือส่งเสริมความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่าย ได้แก่ การสแกนหาช่องโหว่ในระบบ (Vulnerability Scan) การทดสอบการเจาะระบบ (Penetration Test) การทดลอง Crack Password การทดลองถอดรหัส การตรวจสอบ Network Traffic เป็นต้น แต่หากปฏิบัติโดยได้รับอนุญาตหรือเป็นหน้าที่ต้องดูแลในส่วนนี้ของบริษัท ถือเป็นข้อยกเว้น

6.3. ความรับผิดชอบหลังการสิ้นสภาพหรือการเปลี่ยนแปลงการจ้างงาน (Responsibilities after Termination or Change of Employment)

6.3.1. การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or change of employment responsibilities)

เมื่อมีการสิ้นสุดหรือการเปลี่ยนแปลงต้องแจ้งถึงส่วนที่เกี่ยวข้องทั้งหมด ว่าด้วยเรื่องของพนักงานมีการเปลี่ยนแปลงหรือ ออกจากหน้าที่

ต้องมีการถอดถอนสิทธิในการเข้าถึงข้อมูล และระบบสารสนเทศทันทีที่ถึงกำหนดในการคงไว้ซึ่งข้อมูลและหน้าที่ความรับผิดชอบ

- Account บนระบบ Portal ระบบ ERP เครื่องสแกนลายนิ้วมือจะถูกดำเนินการยกเลิก สิทธิพนักงาน ที่พ้นสภาพในเวลาเที่ยงคืนของวันสุดท้ายที่พนักงานยังคงมีสภาพ เป็นพนักงานของบริษัทฯ
- กรณียกเลิกสิทธิเร่งด่วนจะดำเนินการทันทีที่ได้รับแจ้ง

ด้านความมั่นคงปลอดภัยสารสนเทศที่ยังต้องคงไว้หลังการสิ้นสุดหรือเปลี่ยนการจ้างงาน ต้องมีการกำหนดและสื่อสารให้ได้รับทราบต่อพนักงานหรือผู้ที่ทำสัญญาจ้าง รวมทั้งควบคุมให้ปฏิบัติตามอย่างสอดคล้อง

พนักงานต้องทำการคืนอุปกรณ์ของบริษัท ที่อยู่ในความดูแลของพนักงาน ให้กับทางบริษัทในสภาพที่สมบูรณ์ ถ้าตรวจสอบแล้วพบว่ามีสภาพที่ไม่สมบูรณ์จะถือว่าพนักงานต้องรับผิดชอบในส่วนที่ไม่สบบูรณ์ โดยให้เป็นไปตามกรอบการปฏิเสธการรับผิดในส่วนนั้น ๆ

พนักงานที่สิ้นสุดหรือเปลี่ยนแปลงหน้าที่จะต้องไม่นำข้อมูลที่เป็นความลับของ บริษัทฯ ไปเปิดเผยโดยมิชอบหลังจากที่สิ้นสุดการเป็นพนักงาน ถ้าพบว่ามีการละเมิดข้อบังคับดังกล่าว ต้องมีการ ใช้บทลงโทษตามที่บริษัทกำหนดไว้ และจะดำเนินการให้ถึงที่สุด

6.3.2. การรักษาความลับ หรือข้อตกลงการไม่เปิดเผยข้อมูล (Confidentiality or Non-Disclosure Agreements)

ต้องมีการจัดทำข้อตกลง หรือสัญญาการรักษาความลับ หรือข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement: NDA) อย่างเป็นลายลักษณ์อักษรกับพนักงานภายในบริษัทและผู้ให้บริการภายนอก เพื่อป้องกันความปลอดภัยของข้อมูลมีการทบทวนอย่างเหมาะสมและจัดทำเป็นลายลักษณ์อักษร

6.3.3. การปฏิบัติงานจากระยะไกล (Teleworking)

การควบคุมการเข้าถึงการปฏิบัติงานภายนอกบริษัท ในกรณีที่ผู้ให้บริการภายนอก (Third Party) มีการ Remote Access เพื่อ ปฏิบัติงานชั่วคราว ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Third Party Relationship Policy) โดยควบคุมและตรวจสอบการใช้งาน หรือการเข้าถึงระบบตามสิทธิที่ได้รับอย่างเคร่งครัด

การเชื่อมต่อจากภายนอกบริษัท จะต้องมีการดำเนินการที่ได้รับการอนุมัติและเชื่อมต่อผ่านระบบ Virtual Private Network (VPN) ที่บริษัทอนุญาตและจัดหาให้เท่านั้น ห้ามมิให้ผู้ใช้งานเปลี่ยนแปลงโปรแกรมที่ใช้ในการเชื่อมต่อเป็นอันขาด

สิทธิในการใช้งาน Remote Access เพื่อปฏิบัติงานชั่วคราวเป็นสิทธิที่บริษัทจะให้เฉพาะผู้ใช้งาน ผู้ให้บริการภายนอกเป็นการชั่วคราวเท่านั้น ไม่สามารถถ่ายโอนกันได้

ผู้ใช้งานระบบ Remote Access จะต้องทำการขออนุมัติจากผู้บังคับบัญชาก่อนเข้ามาใช้งาน Remote Access การเข้าสู่ระบบสารสนเทศ ผู้ใช้งานจะต้องระบุวัตถุประสงค์ วิธีการเข้าถึง และ ขอบข่ายของการเข้าถึงที่แน่ชัด และจะต้องทำการอนุมัติให้เป็นรายครั้ง หรือเป็นช่วงระยะเวลาจำกัดแล้วแต่กรณีและความจำเป็น

บริษัทมีสิทธิเรียกร้องค่าเสียหายจากผู้ใช้งาน หรือผู้ให้บริการภายนอก หากระบบคอมพิวเตอร์ของบริษัทได้รับความเสียหาย โดยการติดไวรัสคอมพิวเตอร์จากการใช้งาน Remote Access ในการปฏิบัติงานชั่วคราว

6.3.4. การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Information Security Event Reporting)

สถานการณ์ความมั่นคงปลอดภัยสารสนเทศ ต้องมีการรายงานผ่านทางช่องทางการบริหารจัดการที่เหมาะสม และรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้

- ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท โดยผ่านช่องทางรายงานที่กำหนดไว้ จะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้ โดยปฏิบัติตามเอกสารวิธีปฏิบัติงานเรื่องการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

- ผู้ใช้งานและบุคคลภายนอกทุกคนมีหน้าที่รายงานเหตุละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใด ๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในบริษัท ต่อผู้บังคับบัญชาหรือหน่วยงานจัดการความปลอดภัย (Security Management) ทันทีที่พบเหตุ เพื่อให้สามารถดำเนินการแก้ไขปัญหาได้อย่างทันท่วงที

- ผู้ใช้งานที่พบหรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ ต้องรายงานต่อ IT-Security officer ทันที

- ผู้ใช้งานที่พบว่าฮาร์ดแวร์หรืออุปกรณ์ใด ๆ เกิดความเสียหาย หรือทำงานผิดปกติ ต้องรายงานต่อหน่วยงานที่เกี่ยวข้องทันที

- ผู้ใช้งานและบุคคลภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใด ๆ ในบริษัทต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้น ผู้บังคับบัญชา หน่วยงานจัดการความปลอดภัย IT-Security officer และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง

7. มาตรการทางกายภาพ (Physical Controls) Annex 7

7.1 ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมของบริษัท (Physical and Environmental Security)

วัตถุประสงค์

เพื่อให้มั่นใจว่ามีการป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีผลต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัท มีการป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่อทรัพย์สิน และป้องกันการหยุดชะงักต่อการดำเนินงานของบริษัท

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน และเป็นมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับกับผู้ใช้งานและผู้ให้บริการภายนอก

7.2. พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)

ข้อกำหนดทั่วไป

- ต้องมีการจำแนกและกำหนดบริเวณพื้นที่ใช้งานระบบสารสนเทศตามที่ได้นิยามไว้ รวมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศ เพื่อการเฝ้าระวัง ควบคุมและรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ และประกาศให้รับทราบทั่วกัน

- ต้องดำเนินการติดตั้งอุปกรณ์ในการรักษาความปลอดภัย ประกอบด้วยกล้องวงจรปิด ระบบ Access Control หรืออุปกรณ์ที่สามารถป้องกัน ภัยคุกคามจากผู้บุกรุก เป็นต้นในพื้นที่ใช้งานระบบสารสนเทศของบริษัทได้แก่ ห้อง Server/ Data Center เพื่อให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัย หน่วยงานต้องกำหนดการติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศใน “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” ให้สอดคล้องกับหมวดหมู่และความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ

- ต้องดูแลรักษาสภาพแวดล้อมในการทำงานเสมือนดูแลบ้านของตน

7.2.1. การควบคุมการเข้าออกทางกายภาพ (Physical Entry Controls)

หน่วยงานที่เกี่ยวข้องกับการบริหารจัดการอาคารและสถานที่ต้องจัดให้มีการควบคุมการเข้าออกในบริเวณ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” โดยให้ผ่านเข้าออกได้เฉพาะ “พนักงานบริษัทฯ” ที่มีสิทธิเท่านั้นและมีแนวทางปฏิบัติดังนี้

ต้องกำหนด “พนักงานบริษัทฯ” ที่มีสิทธิผ่านเข้าออก และช่วงเวลาที่มีสิทธิในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” อย่างชัดเจน

“พนักงานบริษัทฯ” จะได้รับสิทธิให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

หากมีบุคคลอื่นใดที่ไม่ใช่ “พนักงานบริษัทฯ” ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานต้องตรวจสอบเหตุผลและความจำเป็น ก่อนที่จะอนุญาต หรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้บุคคลจะต้องแสดงบัตรประจำตัวประชาชน หรือบัตรประจำตัวอื่นที่ราชการออกให้โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการขอเข้าออกไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาต และไม่อนุญาตให้เข้าพื้นที่) และต้องมีการบันทึกข้อมูลการเข้าออกศูนย์ปฏิบัติการ ของบุคคลภายนอกทุกครั้ง พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 1 ปี

บุคคลภายนอกต้องทำการแลกบัตรประจำตัวของตนที่ออกให้โดยหน่วยงานของรัฐ ตัวอย่างเช่น บัตรประชาชน ใบขับขี่ พาสปอร์ต ฯลฯ กับบัตรผู้มาติดต่อของหน่วยงาน ก่อนได้รับอนุญาตให้เข้าถึงพื้นที่

พนักงานบริษัทฯ และบุคคลภายนอก ต้องติดบัตรเจ้าหน้าที่ หรือบัตรผู้มาติดต่อตลอดเวลาที่อยู่ในพื้นที่บริษัท ทั้งนี้บัตรประจำตัวและบัตรผู้มาติดต่อ ไม่อนุญาตให้โอนกรรมสิทธิหรือหยิบยืมกันใช้งาน

พนักงานบริษัทฯ ต้องไม่เปิดประตูบริษัททิ้งไว้หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่โดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัวหรือบัตรผู้มาติดต่อได้เพื่อเป็นการป้องกันการเข้าถึงพื้นที่บริษัท และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

ผู้ใช้งานต้องแจ้งเจ้าหน้าที่รักษาความปลอดภัยทันทีเมื่อพบเห็นบุคคลแปลกหน้าหรือบุคคลที่ไม่แขวนบัตรเจ้าหน้าที่หรือบัตรผู้มาติดต่อในพื้นที่

พนักงานบริษัทฯ ควรติดตาม ควบคุมดูแล และให้คำแนะนำผู้ที่มาติดต่อกับตนตลอดเวลาที่ผู้มาติดต่อนั้นอยู่ในพื้นที่

7.2.2. การรักษาความมั่นคงปลอดภัยบริษัท ห้องทำงาน และเครื่องมือต่าง ๆ (Securing Offices, Rooms and Facilities)

ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่น ๆ ให้กับบริษัท ห้องทำงานและเครื่องมือต่าง ๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูง ต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก บริษัทหรือห้องจะต้อง ไม่มีป้าย หรือ สัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าวประตูหน้าต่างของบริษัท หรือห้องต้องใส่กุญแจเสมอ เมื่อไม่มีคนอยู่ต้องตั้งเครื่องโทรสารหรือเครื่องถ่ายเอกสารแยก ออกมาจากบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เป็นต้น

เจ้าหน้าที่ควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่าง ๆ ได้รับการปิดล็อค อย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

ข้อมูล สื่อบันทึก วัสดุและอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุมหรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด

ข้อมูล สื่อบันทึก วัสดุและอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม วิธีการทำลายข้อมูล สื่อบันทึก วัสดุและอุปกรณ์เหล่านี้โดยปฏิบัติตามเอกสารระเบียบปฏิบัติเรื่องการทำลาย

พนักงานต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการ และเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

7.2.3. การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external and environmental threats)

การป้องกันทางกายภาพต่อภัยพิบัติทางธรรมชาติ การโจมตีหรือการบุกรุก หรืออุบัติเหตุ ต้องมีการออกแบบและดำเนินการ ดังนี้

- มีระบบเตือนภัยฉุกเฉิน กรณีไฟไหม้ น้ำท่วม
- มีอุปกรณ์ดับเพลิงตามมาตรฐาน
- มีระบบปรับอากาศและความคุมความชื้น
- แผน คู่มือ การซักซ้อม และการสรุปผล การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม
- มีแผนการใช้งานด้าน Disaster Recovery Site หรือระบบคอมพิวเตอร์สำรองเมื่อมีเหตุการณ์ด้านภัยพิบัติของสภาพแวดล้อมขึ้น
- ในกรณีทีได้รับการแจ้งเตือนจากหน่วยงานของรัฐ ระบบที่ส่งข้อความฉุกเฉินไปยังมือถือทุกเครื่องในพื้นที่เป้าหมาย Cell Broadcast (CBS) ให้ปฏิบัติตามอย่างเคร่งครัด และประสานงานกับคณะบริหารความต่อเนื่องของบริษัท

7.2.4. การปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Working in secure areas)

7.2.4.1. ขั้นตอนปฏิบัติสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย

- ต้องรายงานการปฏิบัติงานและการตรวจสอบการปฏิบัติงาน เพื่อให้มั่นใจได้ว่าการปฏิบัติงานถูกต้อง ครบถ้วน เป็นไปตามนโยบายและขั้นตอนการปฏิบัติงาน และอยู่ในกรอบอำนาจหน้าที่และความรับผิดชอบตามที่กำหนดไว้ นอกจากนี้ในกรณีที่ได้ใช้บริการงานสนับสนุนด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอกบริษัท ต้องมีระบบการตรวจสอบการปฏิบัติงานของบุคคลภายนอกอย่างรอบคอบและรัดกุมเพียงพอ เช่น มีการตรวจสอบบันทึกการทำงาน (log files) ของบุคคลภายนอก และกำหนดให้บุคคลภายนอกรายงานการปฏิบัติงาน เป็นต้น

- แต่ละหน่วยงาน ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวีดีโอในบริเวณนั้น เป็นต้น

- หน่วยงานต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวีดีโอ” “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

7.2.5. พื้นที่สำหรับรับส่งสิ่งของ (Delivery and loading areas)

หน่วยงานต้องมีการจำกัดพื้นที่การเข้าถึงของบุคคลภายนอกที่อาจเข้ามาในพื้นที่ได้ หากเป็นไปได้ควรแบ่งแยกพื้นที่ที่เกี่ยวข้องกับการทำงานออกจากพื้นที่ที่บุคคลภายนอกเข้ามาได้ เช่น บริเวณเก็บและจัดส่งสินค้าจะต้องไม่อยู่ในพื้นที่ ๆ บุคคลภายนอกเข้าถึงได้

เจ้าหน้าที่และเจ้าหน้าที่ของหน่วยงานภายนอก (Third Party) ต้องติดบัตรประจำตัวตลอดเวลาขณะปฏิบัติหน้าที่ในบริเวณ และหากผู้ใดพบเห็นผู้ที่ไม่ติดบัตรประจำตัวถือเป็นหน้าที่ที่จะต้องแจ้งเจ้าหน้าที่รักษาความปลอดภัยโดยทันที

7.3. ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

เพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อให้มั่นใจได้ว่าอุปกรณ์คอมพิวเตอร์ได้มีการป้องกันอย่างเพียงพอจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่น ๆ

7.3.1. การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection)

กำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิตปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำจัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลังจัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

จัดสรรพื้นที่ในการติดตั้งอุปกรณ์ที่มีความสำคัญให้เข้าถึงยาก

การติดตั้งอุปกรณ์ต้องติดตั้งในตู้เก็บอุปกรณ์ให้มิดชิด

7.3.2. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

อุปกรณ์ต้องได้รับการป้องกันจากการล้มเหลวของกระแสไฟฟ้าและการหยุดชะงักอื่น ๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่าง ๆ กำหนดให้มีการดูแลรักษาอุปกรณ์ Utilities ที่เกี่ยวข้อง เช่น Uninterruptible Power Supply (UPS) อุปกรณ์ตรวจจับความชื้น อุปกรณ์ตรวจจับควัน เป็นต้น มีการตรวจสอบการให้บริการของอุปกรณ์อย่างน้อยปีละ 2 ครั้ง ยกตัวอย่างการแบ่งระดับความเสี่ยง ดังนี้

- ความเสี่ยงสูง ต้องมีระบบสำรองไฟฟ้าทั้ง UPS และ เครื่องกำเนิดไฟฟ้า
- ความเสี่ยงปานกลาง ต้องมีระบบสำรองไฟฟ้า UPS
- ความเสี่ยงต่ำมีระบบสำรองไฟฟ้าหรือไม่ก็ได้

7.3.3. ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)

มีการป้องกันการเดินสายไฟฟ้า หรือสายเคเบิ้ลเข้ามาภายในอาคารบริษัท บริเวณที่มีการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารบริษัท และมีการติดตั้งตู้พักสาย ต้องล็อคไว้ตลอดเวลาและจำกัดการเข้าใช้งานได้เฉพาะพนักงานที่หรือบุคคลที่มีสิทธิเท่านั้น

- ความเสี่ยงสูง การเดินสายต้องใช้สายป้องกันการรบกวนสัญญาณและการเข้าถึงสายสัญญาณ
- ความเสี่ยงปานกลาง การเดินสายต้องป้องกันการเข้าถึงสายสัญญาณ
- ความเสี่ยงต่ำใช้สายสัญญาณธรรมดา
- ต้องมีแผนการตรวจสอบระบบการเดินสายไฟ สายเคเบิ้ล สายสื่อสาร

7.3.4. การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้อง เพื่อให้มีสภาพความพร้อมใช้งานและการทำงานที่ถูกต้องอย่างต่อเนื่อง โดยจะแบ่งเป็นระดับของความเสี่ยง ดังนี้

- ระบบที่มีความเสี่ยงสูงต้องบำรุงรักษาทุก 1 เดือน
- ระบบที่มีความเสี่ยงปานกลางต้องบำรุงรักษาทุก 3 เดือน
- ระบบที่มีความเสี่ยงต่ำต้องบำรุงรักษาทุก 12 เดือน

7.3.5. การนำทรัพย์สินของบริษัทออกนอกบริษัท (Removal of assets)

อุปกรณ์สารสนเทศหรือซอฟต์แวร์ต้องไม่มีการนำออกนอกบริษัท โดยไม่ได้รับอนุญาต หากมีความประสงค์จะนำออกจากพื้นที่ต้องแจ้งต่อผู้บังคับบัญชาหรือผู้มีอำนาจในการอนุญาต โดยต้องปฏิบัติตามระเบียบปฏิบัติ

7.3.6. ความมั่นคงปลอดภัยของอุปกรณ์ และทรัพย์สินที่ใช้งานอยู่ภายนอกบริษัท (Security of equipment and assets off premises)

ทรัพย์สินที่ใช้งานอยู่ภายนอกบริษัทต้องมีการรักษาความมั่นคงปลอดภัย โดยพิจารณาจากความเสี่ยงของการปฏิบัติงานอยู่ภายนอกบริษัท

ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or reuse of equipment) อุปกรณ์ที่มีสื่อบันทึกข้อมูล ต้องมีการตรวจสอบเพื่อให้มั่นใจว่า ข้อมูลสำคัญของซอฟต์แวร์ที่มีใบอนุญาต มีการลบทิ้งหรือเขียนทับอย่างมั่นคงปลอดภัย ก่อนการกำจัดอุปกรณ์หรือก่อนการนำอุปกรณ์ไปใช้งานอย่างอื่น

อุปกรณ์ของผู้ใช้งานที่ ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended user equipment) ผู้ใช้งานต้องมีการป้องกันอุปกรณ์อย่างเหมาะสม ซึ่งเป็นอุปกรณ์ที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแล

7.3.7. นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)

เอกสารกระดาษและสื่อบันทึกข้อมูลที่ถอดแยกได้ และป้องกันสารสนเทศในอุปกรณ์ประมวลผลสารสนเทศ เมื่อมีการนำมาใช้งาน ต้องทำเรื่องขออนุญาตการนำไปใช้งานงานและกำหนดระยะเวลาเริ่มใช้งาน ระบุระยะเวลาในการนำส่งคืน ระบุถึงการจัดเก็บในระยะเวลาการใช้งาน

8. มาตรการควบคุมทางด้านเทคโนโลยี (Technological Control) Annex 8

วัตถุประสงค์

บริษัทกำหนดและบังคับใช้มาตรการควบคุมทางด้านเทคโนโลยีเพื่อให้การปกป้องระบบสารสนเทศ เครือข่าย อุปกรณ์และข้อมูลของบริษัทเป็นไปอย่างมีประสิทธิผลและสามารถตรวจสอบได้ โดยมุ่งลดความเสี่ยงจากการเข้าถึง การใช้งาน การเปิดเผย การแก้ไข หรือการทำลายข้อมูลโดยไม่ได้รับอนุญาต รวมถึงลดโอกาสการหยุดชะงักของระบบ ทั้งนี้เพื่อคงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลและบริการสารสนเทศ ตลอดจนสนับสนุนการปฏิบัติตามนโยบายของบริษัท กฎหมายและข้อกำหนดที่เกี่ยวข้อง และรองรับการเฝ้าระวัง ตรวจจับ และตรวจสอบย้อนหลังสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม

8.1. นโยบายสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile Device Policy)

- ผู้ปฏิบัติงานในบริษัทฯ ควรมีความตระหนักถึงการ ป้องกันดูแลรักษาอุปกรณ์สื่อสารประเภทพกพาทั้งทางกายภาพและข้อมูลสำคัญที่อยู่ ภายในอุปกรณ์โดยทางกายภาพให้ทำการล็อกอุปกรณ์ไว้กับโต๊ะหรือนำไปเก็บไว้ในตู้ ที่สามารถล็อกได้ ส่วนข้อมูลสำคัญที่อยู่ภายในอุปกรณ์ให้มีการป้องกันการเข้าถึงโดยบุคคลที่ไม่ได้รับ อนุญาตซึ่งทำได้โดยการเข้ารหัสข้อมูลเพื่อเข้าถึงข้อมูลสำคัญ ที่อยู่ภายในอุปกรณ์และรวมไปถึงให้มีการสำรองข้อมูลสำคัญที่อยู่ภายในอุปกรณ์ไว้อย่างสม่ำเสมอด้วย

- ผู้ปฏิบัติงานในบริษัทฯ ต้องทำการขออนุญาตก่อน ที่จะนำอุปกรณ์สื่อสารประเภทพกพาของตนเอง เช่น เครื่องคอมพิวเตอร์แบบพกพา/ Notebook/ Tablet / Smartphone อุปกรณ์สื่อสารเคลื่อนที่อื่น ๆ ที่เชื่อมต่อเข้ากับ เครือข่ายของบริษัทฯ รวมทั้งควรมีความตระหนักเพื่อให้มีความระมัดระวัง หากอุปกรณ์ สื่อสารประเภทพกพาของบริษัทฯ ออกไปเชื่อมต่อกับเครือข่ายภายนอก โดย บริษัทกำหนดแนวทางการใช้งานคอมพิวเตอร์ไว้ดังนี้

อุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ของบริษัทถือเป็นสินทรัพย์ของบริษัทโดยใช้เพื่อการดำเนินงานของบริษัทเท่านั้น

การคืน หรือส่งซ่อมอุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ของบริษัท ให้ทำการสำรองข้อมูลหรือลบข้อมูลอย่างปลอดภัยตามระดับความลับของข้อมูลที่อยู่ในอุปกรณ์นั้นไปไว้ในที่เตรียมไว้

ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไข Configuration หรือส่วนประกอบของอุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ของบริษัทโดยไม่ได้รับอนุญาต

ไม่ใช้อุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ของบริษัทผิดวัตถุประสงค์และหลีกเลี่ยงการใช้อุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ในสภาวะแวดล้อมที่มีผลกระทบต่ออุปกรณ์

หากมีความจำเป็นต้องใช้งานอุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ส่วนตัวมาใช้เชื่อมต่อเครือข่ายภายในของบริษัท รวมทั้งเข้าถึงระบบงานภายในต้องได้รับการอนุญาตจากผู้บังคับบัญชา และทำการชี้แจงเหตุผลต่อผู้บังคับบัญชาให้ทราบถึงสาเหตุที่ต้องนำอุปกรณ์ส่วนตัวนำมาใช้งานด้วยเหตุผลใด และนำอุปกรณ์ดังกล่าวไปขึ้นทะเบียนกับบริษัท เพื่อทำการตรวจสอบและติดตั้งในส่วนของโปรแกรมที่จำเป็นต่อการใช้งานรวมถึงโปรแกรมป้องกันไวรัสที่บริษัทได้ทำการซื้อและใช้งานภายในและต้องปฏิบัติตามขั้นตอนการใช้งานที่บริษัทกำหนด

ใช้อุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ส่วนตัว ในการเข้าถึงระบบงานทั่วไปของบริษัทเท่านั้น

ไม่ใช้อุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ส่วนตัว ในการเข้าถึงระบบบริหารจัดการบริการของบริษัท

8.1.1. การป้องกันอุปกรณ์ของผู้ใช้งานที่ไม่มีผู้ดูแล (Unattended User Equipment)

- ผู้ใช้งานต้องป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์ระบบเทคโนโลยีสารสนเทศเครื่องคอมพิวเตอร์และระบบเครือข่ายที่ไม่มีผู้ดูแล

- ผู้ใช้งานต้องออกจากระบบสารสนเทศและปิดเครื่องคอมพิวเตอร์ทันทีหลังเสร็จสิ้นภารกิจประจำวัน

- ผู้ดูแลระบบคอมพิวเตอร์กำหนดให้เครื่องคอมพิวเตอร์พักหน้าจอ (Screen Saver) แบบที่มีรหัสป้องกันทุก 15 นาที หรือ ล็อกหน้าจอเมื่อไม่มีการใช้งาน

8.1.2. การบริหารจัดการสิทธิตามระดับสิทธิการเข้าถึง (Privileged Access Right)

บัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงระบบสารสนเทศในระดับสูง เช่น Root หรือ Administrator หรือเทียบเท่า ต้องได้รับการพิจารณามอบหมายแก่ผู้ปฏิบัติงานตามความจำเป็นและมีการ กำหนดระยะเวลาในการเข้าถึง อย่างเหมาะสมกับการทำงาน เท่านั้น

กรณีมีความจำเป็นต้องให้สิทธิในระดับสูงแก่ผู้ปฏิบัติการหรือบุคคลภายนอกต้องมีการพิจารณา การควบคุม อย่างรัดกุม โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

- ต้องได้รับความเห็นชอบและอนุมัติจากเจ้าของระบบสารสนเทศนั้น ๆ
- ต้องควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะ กรณีจำเป็นเท่านั้น
- ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- ต้องมีการเปลี่ยนรหัสผ่านหลังเสร็จสิ้นการใช้งาน

8.1.3. การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

ต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่กำหนดสิทธิในการใช้งาน เช่น เขียน อ่าน ลบ เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

บัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงาน เท่านั้น

บุคคลภายนอกต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (IT Security Policy) ของบริษัทฯ อย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศ

8.1.4. การควบคุมการเข้าถึงรหัสต้นฉบับสำหรับระบบ (Access Control to Program Source Code)

ผู้พัฒนาระบบสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริงหรือให้บริการเช่น

- ไม่ควรเก็บ Source Code ไว้ในเครื่องที่ใช้งานจริงและต้องเก็บ Source Code ไว้ในที่ที่ปลอดภัย
- ต้องไม่เก็บ Source Code ที่อยู่ในระหว่างทำการทดสอบรวมไว้กับ Source Code ที่ใช้งานได้จริงแล้ว

8.1.5. ขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure authentication)

ควรกำหนดคุณสมบัติ หรือวิธีการล็อกอินเข้าใช้ระบบให้มีความปลอดภัย (Secure Log-on) เมื่อมีระบบใหม่ที่ได้รับการอนุมัติให้จัดหา และติดตั้งพิจารณากำหนดคุณสมบัติ เช่น

- การไม่แสดงชื่อหรือรายละเอียดของระบบจนกว่าจะล็อกอินสำเร็จ

- การไม่มี หรือ การไม่แสดงตัวเลือกให้การช่วยเหลือ (Help Menu) ในระหว่างที่ทำการล็อกอิน
- การบันทึกข้อมูลความสำเร็จ หรือการล้มเหลวในการล็อกอินแต่ละครั้งของผู้ใช้งาน (เพื่อใช้ในการตรวจสอบในภายหลัง)
- การไม่แสดงข้อมูลรหัสผ่านให้เห็นบนหน้าจอในขณะที่ผู้ใช้งานใส่ข้อมูลรหัสผ่านของตน

8.1.6. การบริหารจัดการขีดความสามารถของระบบ (Capacity management)

เพื่อเป็นแนวทางในการบริหารจัดการทรัพยากรระบบของบริการให้เพียงพอตามข้อตกลงระดับการให้บริการ และต่อการให้บริการผู้มาติดต่อบริษัท หรือผู้ใช้งานทั้งในปัจจุบันและในอนาคต

มีการกำหนดหน้าที่ความรับผิดชอบของผู้ดูแลข้อมูล

มีการวางแผนการตรวจสอบประเมินขีดความสามารถของระบบและกำหนดค่าสูงสุดที่ยอมรับได้ของขีดความสามารถของระบบทั้งทางด้านอุปกรณ์ระบบคอมพิวเตอร์ และระบบเครือข่าย อย่างน้อยการประเมินค่า CPU, RAM, Storage, Network Utilization

ดำเนินการตรวจสอบประเมินขีดความสามารถของระบบดังระบุข้างต้น

ดำเนินการวิเคราะห์ ประมวลผล ขีดสมรรถนะของระบบเพื่อค้นหาสาเหตุและปัญหารวมทั้งแนวทางการแก้ไขอย่างเป็นระบบ รวมทั้ง ติดตาม ปรับปรุง และคาดการความต้องการเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพ

สรุปผลการบริหารจัดการขีดสมรรถนะของระบบ

8.1.7. การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, testing and operational environments)

ต้องมีการแยกเครื่องมือในการประมวลผลสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) ในการพัฒนาและทดสอบ อาทิ การพัฒนาซอฟต์แวร์ควรมีการแยกเครื่องที่ใช้ในการพัฒนาและทดสอบ ออกจากกับเครื่องที่ใช้งานจริงหากจำเป็นระบบเครือข่ายของการพัฒนาควรแยกออกจากระบบที่ใช้งานจริงด้วย

8.2. การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

8.2.1. มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware)

เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์แบบพกพา ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัส รุ่นล่าสุดที่ได้รับการอนุมัติจาก บริษัท และต้องเปิดใช้งานตลอดเวลาที่ใช้งานเครื่อง

เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุด (Update Latest Pattern) อยู่เสมอ เครื่องให้บริการ เครื่องตั้งโต๊ะ และโน้ตบุ๊คทุกเครื่องต้องได้รับการปรับปรุงข้อมูลล่าสุดจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส

เอกสารการติดตั้งค่าของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัส ต้องได้รับการตรวจสอบทุก 6 เดือน และต้องจัดทำเอกสาร Checklist ประกอบการตรวจสอบด้วย

ห้ามพนักงานทำการดาวน์โหลด แชร์แวร์(ทดลองใช้) หรือฟรีแวร์ โดยตรงจากอินเทอร์เน็ต โดยปราศจากการอนุมัติ หลังจากการอนุมัติแล้ว เจ้าหน้าที่ต้องทำการสแกนซอฟต์แวร์ด้วยโปรแกรมตรวจหาไวรัส ก่อนการใช้งาน

ไฟล์ทุกไฟล์ที่ดาวน์โหลดในหน่วยงานเป็นไฟล์แนบของอีเมล์ สำเนาจากแผ่นดิสก์ หรือไฟล์แชร์ต่าง ๆ ต้องได้รับการสแกนหาไวรัส

ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมมุ่งร้ายใด ๆ ตัวอย่างเช่น ไวรัส หนอนอินเทอร์เน็ตโปรแกรมแฝง (ม้าโทรจัน) อีเมล์บอมบ์ ฯลฯ เข้าสู่ระบบคอมพิวเตอร์ของบริษัท

ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

ไฟล์ที่เกี่ยวข้องกับการทำงานเท่านั้น ที่ได้รับอนุญาตให้สามารถรับ - ส่งผ่านระบบเครือข่ายของบริษัท ได้ ทั้งนี้ผู้ใช้งานควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จัก และจากช่องทางการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้น นอกจากนี้ผู้ใช้งานต้องทำการสแกนไวรัสในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันไวรัสของบริษัท ก่อนเปิดใช้งานเสมอ

เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชันการทำงานเชื่อมต่อกับอินเทอร์เน็ตยกเว้นในกรณีที่จำเป็นต้องใช้เท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดีมีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้

มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against malware) มาตรการตรวจหา การป้องกัน และการกู้คืนจากโปรแกรมไม่ประสงค์ดี ต้องมีการดำเนินการร่วมกับการสร้างความตระหนักผู้ใช้งานที่เหมาะสม

ตั้งค่าให้ซอฟต์แวร์ Anti-malware อัปเดตซอฟต์แวร์ และปรับปรุงค่า Signature ทุกวัน

8.2.2. การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical Vulnerability)

เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งานและประเมินความเสี่ยงของช่องโหว่เหล่านั้น รวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

ต้องอัพเดทระบบซอฟต์แวร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยให้เป็นปัจจุบันเพื่ออุดช่องโหว่ ต่าง ๆ อย่างสม่ำเสมอรวมถึงต้องกำหนดและจำกัดรายการของซอฟต์แวร์ ที่ติดตั้งบนเครื่อง คอมพิวเตอร์ลูกข่าย

8.2.3. การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

ต้องจัดให้มีการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งานหรือให้บริการอยู่แล้ว ตามระยะเวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยสารสนเทศและงานบริการเทคโนโลยีอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่า ระบบสามารถถูกบุกรุกได้หรือไม่การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งาน เป็นไปอย่างปลอดภัยหรือไม่รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบด้วย

8.2.4. การจัดการการตั้งค่า (Configuration Management)

ต้องกำหนดให้บริษัทฯ ต้องบริหารจัดการวงจรทั้งหมดของการกำหนดค่าความปลอดภัยสำหรับ เทคโนโลยีสารสนเทศ เพื่อให้แน่ใจว่ามีระดับความปลอดภัยที่เหมาะสม และเพื่อหลีกเลี่ยงการเปลี่ยนแปลง ที่ไม่ได้รับอนุญาต ซึ่งรวมถึงการกำหนด Configuration การนำไปใช้ การมอนิเตอร์ และการทบทวน

บริษัทฯ มีการจัดทำกระบวนการ สำหรับการเสนอ ตรวจสอบ และอนุมัติการกำหนดค่า ความปลอดภัยตลอดจนกระบวนการสำหรับจัดการและตรวจสอบการกำหนดค่าต้องมีการทบทวน การเปลี่ยนแปลงการกำหนดค่าทั้งหมดอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

8.2.5. การลบข้อมูล (Information deletion control)

ควรลบสารสนเทศที่จัดเก็บไว้ในระบบสารสนเทศอุปกรณ์หรือสื่อจัดเก็บข้อมูลอื่น ๆ ทิ้งเมื่อไม่ต้องการใช้อีกต่อไป และเพื่อป้องกันการเปิดเผยสารสนเทศที่ละเอียดอ่อนโดยไม่จำเป็นและเพื่อให้สอดคล้องกับ ข้อกำหนด พรบ. คุ้มครองข้อมูลส่วนบุคคล สำหรับการลบข้อมูลสารสนเทศ

เมื่อใช้บริการระบบคลาวด์บริษัทฯ ควรทวนสอบว่าวิธีการลบที่ผู้ให้บริการคลาวด์ให้มานั้นสามารถยอมรับได้หรือไม่ และหากเป็นกรณีเช่นนี้บริษัทฯ ควรใช้หรือขอ ให้ผู้ให้บริการคลาวด์ลบสารสนเทศกระบวนการลบเหล่านี้ควรเป็นแบบอัตโนมัติตามนโยบายหากมีและนำไปใช้ได้บันทึกสามารถติดตามหรือทวนสอบว่ามีกระบวนการลบสารสนเทศเกิดขึ้นทั้งนี้ขึ้นอยู่กับความละเอียดอ่อนของสารสนเทศที่ถูกลบ

เพื่อหลีกเลี่ยงการเปิดเผยสารสนเทศที่ละเอียดอ่อนโดยไม่ได้ตั้งใจเมื่ออุปกรณ์ถูกส่งกลับไปให้ ผู้ขายควรคุ้มครองข้อมูลสารสนเทศที่ละเอียดอ่อนโดยการนำที่เก็บข้อมูล ฮาร์ดดิสก์ไดรฟ์และหน่วยความจำ ออกก่อนที่จะส่งอุปกรณ์ออกนอกบริษัทฯ

8.2.6. การซ่อนข้อมูล (Data Marking)

- ควรใช้การปิดบังข้อมูลตามนโยบายเฉพาะหัวข้อของบริษัทฯเกี่ยวกับการควบคุมการเข้าถึงและข้อกำหนดทางธุรกิจเฉพาะหัวข้ออื่น ๆ ที่เกี่ยวข้องโดยคำนึงถึงกฎหมายที่บังคับใช้และเพื่อจำกัด การเปิดเผยข้อมูลที่ละเอียดอ่อน รวมถึงข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้และเพื่อให้ เป็นไปตามข้อกำหนดทางกฎหมาย พรบ. คุ้มครองข้อมูลส่วนบุคคล ระเบียบข้อบังคับ และสัญญา

- ในกรณีที่มีความกังวลเรื่องการคุ้มครองข้อมูลที่ละเอียดอ่อน (Sensitive personal data) บริษัทฯ ควรพิจารณาซ่อนข้อมูลดังกล่าวโดยใช้มาตรการทางเทคนิคต่าง ๆ เช่น การปิดบังข้อมูลโดยขีดฆ่าบนเอกสาร การแฝงข้อมูล (Pseudonymization) การทำข้อมูลนิรนาม (Anonymization)

- เมื่อใช้เทคนิคการแฝงข้อมูลหรือเทคนิคการทำข้อมูลนิรนามควรทวนสอบว่าเพียงพอและเหมาะสม ควรพิจารณาองค์ประกอบทั้งหมดของข้อมูลที่ละเอียดอ่อน เพื่อให้มีประสิทธิภาพของข้อมูลที่ละเอียดอ่อนเพื่อให้มีประสิทธิภาพตัวอย่างเช่นหากพิจารณาอย่างไม่ถูกต้องก็จะสามารถระบุตัวตนของบุคคลได้แม้ว่าข้อมูลที่สามารถระบุตัวบุคคลนั้น ได้โดยตรงนั้นจะไม่ได้ระบุชื่อก็ตาม โดยการมีข้อมูลเพิ่มเติมซึ่งทำให้สามารถระบุตัวบุคคลได้ทางอ้อม

8.2.7. การป้องกันข้อมูลรั่วไหล (Data Leakage prevent control)

ต้องมีมาตรการป้องกันการรั่วไหลของข้อมูลต่าง ๆ เพื่อหลีกเลี่ยงการเปิดเผยข้อมูลที่ละเอียดอ่อน โดยไม่ได้รับอนุญาตและหากเกิดเหตุการณ์การรั่วไหลของข้อมูลและสามารถที่จะตรวจจับได้อย่างทันท่วงที ซึ่งรวมถึงข้อมูลในระบบ เทคโนโลยีสารสนเทศ เครือข่าย หรืออุปกรณ์อื่น ๆ

บริษัทฯ มีการกำหนดกระบวนการจัดการชั้นความลับของข้อมูล และประเมินความเสี่ยง ด้านเทคโนโลยีสารสนเทศและตรวจสอบช่องโหว่ที่มีโอกาสเกิดการรั่วไหลของข้อมูล และมีมาตรการ ปกป้องข้อมูล

8.2.8. การสำรองข้อมูล (Information backup)

ต้องกำหนดความถี่ในการทำการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล

ต้องจัดให้มีการดูแลอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิภาพ สามารถใช้งานได้ตลอดเวลา

ต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ

ต้องกำหนดระยะเวลาในการสำรองข้อมูลตามระดับการบริหารความเสี่ยง

ต้องมีกระบวนการสำรองข้อมูลและการกู้ข้อมูลของทุกระบบ ต้องมีการทำเอกสาร และมีการตรวจสอบเป็นระยะ ๆ

ต้องจัดให้มีทะเบียนการบันทึกข้อมูลการสำรองข้อมูล และการเรียกคืนข้อมูลในแต่ละครั้ง

ข้อมูลสำรองต้องได้รับการทดสอบเป็นระยะ ๆ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

ต้องลงบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูล ต้องได้รับการตรวจสอบเป็นประจำทุกปี

กระบวนการในการเก็บข้อมูลระหว่างสถานที่ระบบคอมพิวเตอร์และสถานที่เก็บข้อมูลต้องได้รับการตรวจสอบอย่างน้อยปีละ 1 ครั้ง

สื่อที่ใช้เก็บข้อมูลต้องมีป้ายบอกรายละเอียด ซึ่งประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

- ชื่อระบบ
- วันสร้าง
- ระดับความสำคัญของข้อมูล
- รายละเอียดติดต่อผู้ดูแลข้อมูล
- วิธีการเก็บรักษาสื่อบันทึก เช่น สำรอง online /Hard copy

8.2.9. การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies)

สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)

มีการจัดลำดับความสำคัญของระบบงาน/กระบวนงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงานด้วยการประเมินความเสี่ยง (Risk Assessment) และ/หรือ การประเมินผลกระทบของกระบวนงานหลัก

มีการกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา

มีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

มีการกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ

มีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน

หน่วยงานที่เป็นหน่วยสำรองข้อมูลหรือจัดเก็บข้อมูลก็ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน

มีการทบทวนหรือปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ (ทุก 6 เดือน) และเก็บแผนฉุกเฉินไว้ในสถานที่มั่นคงปลอดภัย

ทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 2 ครั้ง โดยต้องเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง

ต้องสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องทุกระดับได้รับทราบเฉพาะเท่าที่จำเป็นและควรป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้รับทราบ

กรณีที่เกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหาไว้ด้วย

8.3. การบันทึกข้อมูลการใช้งาน และการเฝ้าระวัง (Logging and Monitoring)

8.3.1. การบันทึกข้อมูลเหตุการณ์ (Event logging)

มีการบันทึกการทำงานของระบบที่ไม่เป็นไปตามปกติ ความผิดพลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัย ต้องมีการบันทึกไว้ จัดเก็บและทบทวนอย่างสม่ำเสมอ รวมทั้งกำหนดวิธีการและระยะเวลาในการจัดเก็บให้สอดคล้องกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์โดยกำหนดเงื่อนไขขั้นต่ำ ดังนี้

ระบบที่สำคัญต้องบันทึกเหตุการณ์อย่างน้อย: การเข้าสู่ระบบ/ ออกจากระบบ, ความล้มเหลวในการพิสูจน์ตัวตน, การเปลี่ยนแปลงสิทธิ, การเข้าถึงข้อมูลสำคัญ, การเปลี่ยนค่า config" ทั้งนี้ต้องคงสภาพความถูกต้อง (Integrity) และจำกัดการเข้าถึง Log"

เวลาระบบต้องซิงค์เวลา (NTP) เพื่อความเที่ยงตรงในการสืบสวน

8.3.2. การป้องกันข้อมูลล็อก (Protection of log information)

กำหนดข้อกำหนดในการปกป้อง "ข้อมูลล็อก" ของระบบสารสนเทศและโครงสร้างพื้นฐานของบริษัท ให้มีความถูกต้องครบถ้วน (Integrity) ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต (Confidentiality) และพร้อมใช้เมื่อต้องตรวจสอบเหตุการณ์ (Availability) รวมถึงรองรับการตรวจสอบตาม ISO/IEC 27001, PDPA และ PCI DSS (ถ้ามี)

- ระบบงาน (Web/ Mobile/ Backend/ API), ฐานข้อมูล, ระบบปฏิบัติการ, อุปกรณ์เครือข่าย/ Firewall/ WAF, IAM/ SSO, Cloud (AWS)
- เครื่องมือ DevOps/ CI/ CD ที่เกี่ยวข้องกับการปล่อยระบบ (เช่น GitHub/ GitLab audit logs, pipeline logs)
- Log ที่ถูกจัดเก็บทั้งแบบศูนย์กลาง (Centralized Logging/SIEM) และบนระบบปลายทาง

การจัดชั้นความลับและการลดข้อมูลอ่อนไหวใน ล็อก

1. ล็อกต้องถูกจัดชั้นความลับตามการจัดชั้นข้อมูลของบริษัท
2. ห้ามบันทึกข้อมูลต่อไปนี้ลงใน ล็อกโดยไม่จำเป็น:
   - รหัสผ่าน/ รหัส PIN
   - ข้อมูลบัตร (เช่น PAN แบบเต็ม), CVV/CVC หรือ SAD ตามนิยาม PCI DSS
   - secret/ key/ token ที่สามารถนำไปเข้าระบบได้
3. หากหลีกเลี่ยงไม่ได้ ต้องใช้การ masking/ redaction (เช่น แสดงเฉพาะบางส่วน) และจำกัดสิทธิ์การเข้าถึงแบบเข้มงวด

การควบคุมการเข้าถึงและการแยกหน้าที่ (Access Control & SoD)

1. การเข้าถึงระบบจัดเก็บล็อก/ เครื่องมือค้นหาล็อก ต้องใช้หลัก Least Privilege และต้องกำหนดบทบาท (Role-based) ชัดเจน เช่น:
   - Viewer (อ่านอย่างเดียว)
   - Analyst (ค้นหา/สืบค้น)
   - Admin (จัดการระบบล็อก)
2. บุคลากรที่มีสิทธิ "แก้ไข/ ลบ/ เปลี่ยนการตั้งค่าล็อก" ต้องถูกจำกัดเฉพาะผู้ดูแลที่ได้รับอนุมัติ และต้องมีการแยกหน้าที่จากผู้พัฒนา/ผู้ใช้งานระบบเมื่อเหมาะสม

3. การเข้าถึงต้องใช้บัญชีรายบุคคล และ MFA และมีการทบทวนสิทธิ์เป็นระยะ (เช่น รายไตรมาส/ ครึ่งปี ตามความเสี่ยง)

การปกป้องความถูกต้องครบถ้วนของล็อก (Integrity / Anti-tampering)

1. ล็อกที่ส่งเข้าศูนย์กลางต้องถูกป้องกันการแก้ไข/ปลอมแปลง โดยใช้แนวทางอย่างน้อยหนึ่งข้อ:
   - การเก็บแบบ append-only / immutable (เช่น WORM หรือ Object Lock)
   - การทำ hash/signature/chain เพื่อให้ตรวจสอบการถูกแก้ไขได้
2. ต้องจำกัดหรือปิดความสามารถในการ “ลบล็อก” สำหรับผู้ใช้งานทั่วไป และการลบต้องทำได้เฉพาะตามกระบวนการที่อนุมัติ พร้อมมีหลักฐาน

การเข้ารหัสและการส่งผ่านอย่างปลอดภัย (Confidentiality)

1. ล็อกต้องถูกส่งผ่านช่องทางที่ปลอดภัย (เช่น TLS) ระหว่างแหล่งกำเนิดไปยังระบบจัดเก็บ
2. ล็อกที่จัดเก็บต้องเข้ารหัส (encryption at rest) ตามมาตรฐานบริษัท โดยเฉพาะ ล็อกที่มีข้อมูลส่วนบุคคล/ข้อมูลสำคัญ/ อยู่ใน PCI scope
3. กุญแจเข้ารหัสต้องถูกจัดการผ่านระบบบริหารจัดการกุญแจที่องค์กรอนุมัติ และจำกัดผู้เข้าถึง

การเก็บรักษา (Retention) และการทำลายอย่างปลอดภัย (Disposal)

1. กำหนดระยะเวลาเก็บรักษา ล็อกตามประเภทระบบ/ข้อกำกับ/ความเสี่ยง และสอดคล้อง PDPA
2. Log การใช้อินเทอร์เน็ต: Retention อย่างน้อย 90 วัน (เพื่อการตรวจสอบตามข้อกำหนดที่เกี่ยวข้อง)
3. Security/ Audit log ระบบสำคัญ: Retention 1 ปี เพื่อสืบสวนเหตุการณ์ย้อนหลัง

ความพร้อมใช้งานและการสำรอง (Availability / Backup)

1. ระบบจัดเก็บ ล็อกต้องมีความทนทาน/ สำรองตามความสำคัญของระบบ (เช่น replication/backup)
2. ต้องทดสอบการกู้คืนล็อก (log restore) ตามรอบที่กำหนด เพื่อให้ใช้ในการสืบสวนเหตุได้จริง

การเฝ้าระวังและการแจ้งเตือน (Monitoring & Alerting)

1. ต้องกำหนด use case การตรวจจับเหตุผิดปกติอย่างน้อย:
   - การ login ล้มเหลวจำนวนมาก, brute force
   - การยกระดับสิทธิ์/เปลี่ยน role/policy
   - การเปลี่ยนค่าระบบ logging/ปิด logging
   - การเข้าถึงข้อมูลอ่อนไหวผิดปกติ
2. การแจ้งเตือนเหตุสำคัญต้องส่งถึงทีมที่รับผิดชอบ (SOC/IT/InfoSec) และผูกกับกระบวนการ Incident Response

การคุ้มครองข้อมูลส่วนบุคคลใน ล็อก (PDPA)

1. ล็อกถือเป็นข้อมูลที่อาจระบุตัวบุคคลได้ (เช่น user ID, IP, device ID) ต้องควบคุมการเข้าถึงและใช้ตามวัตถุประสงค์
2. ห้ามนำ ล็อกไปใช้เกินวัตถุประสงค์ด้านความมั่นคงปลอดภัย/ตรวจสอบ/การปฏิบัติงาน เว้นแต่ได้รับอนุมัติตามกระบวนการ

3. ต้องมีมาตรการป้องกันการเปิดเผยโดยไม่จำเป็น (masking, จำกัด field, จำกัดผู้เข้าถึง)

ข้อกำหนดสำหรับผู้ให้บริการ/ บุคคลที่สาม หากมีผู้รับจ้าง/ ผู้ให้บริการที่เข้าถึง ล็อกหรือระบบ logging ต้อง:

- ได้รับอนุมัติเป็นลายลักษณ์อักษร
- จำกัดสิทธิ์แบบชั่วคราว/ ตามงาน
- บันทึกกิจกรรมของผู้รับจ้าง และเพิกถอนสิทธิ์ทันทีเมื่อจบงาน
- ผูกข้อกำหนดนี้ไว้ในสัญญา/ NDA/ DPA (กรณีมีข้อมูลส่วนบุคคล)

การบังคับใช้และข้อยกเว้น

- การละเมิดนโยบายนี้อาจนำไปสู่การดำเนินการตามระเบียบวินัย/สัญญา
- ข้อยกเว้น (Exception) ต้องทำเป็นเอกสาร ระบุเหตุผล ระยะเวลา มาตรการชดเชยความเสี่ยง และได้รับอนุมัติจากผู้มีอำนาจ (System Owner + InfoSec)

8.3.3. ข้อมูล ล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs)

กิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการต้องมีการบันทึกไว้เป็นข้อมูล ล็อกข้อมูลดังกล่าวต้องมีการป้องกันและทบทวนอย่างสม่ำเสมอ

8.3.4. การเฝ้าติดตามกิจกรรม (Monitoring activities)

- บริษัทฯ มีกระบวนการสอบทานและพิจารณาการดำเนินงานตามระบบการควบคุมภายใน ที่กำหนดขึ้นของหน่วยงานว่าอยู่ในระดับที่เหมาะสมเป็นไปตามวัตถุประสงค์การควบคุม ภายในอย่างมีประสิทธิภาพ ประสิทธิผล คุ้มค่า และมีการปรับปรุงให้สอดคล้องกับสถานการณ์ ในปัจจุบัน

- ควรเฝ้าติดตามเครือข่ายระบบและแอปพลิเคชันเพื่อหาพฤติกรรมที่ผิดปกติและการดำเนินการ เหมาะสมเพื่อประเมินอุบัติการณ์ด้านการรักษาความปลอดภัยของสารสนเทศที่อาจเกิดขึ้นและเพื่อตรวจจับพฤติกรรมที่ผิดปกติและอุบัติการณ์ด้านการรักษาความปลอดภัยของสารสนเทศที่อาจเกิดขึ้น

- ควรกำหนดขอบเขตและระดับการเฝ้าติดตามตามข้อกำหนดทางธุรกิจและการรักษา ความปลอดภัยของ สารสนเทศและคำนึงถึงกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง ควรดูแลเก็บรักษาบันทึกการเฝ้าติดตามตาม ระยะเวลาการเก็บรักษาที่กำหนดไว้

8.3.5. การตั้งเวลาให้ถูกต้อง (Clock Synchronization)

ระบบทุกประเภทต้องซิงโครไนซ์เวลาจากแหล่งเวลา (Time Source) ที่บริษัทกำหนดเท่านั้น เช่น NTP Server ภายในองค์กร หรือบริการเวลาในคลาวด์ที่ได้รับอนุมัติ

ต้องกำหนด Time Zone มาตรฐาน ขององค์กร (เช่น Asia/Bangkok) ให้สอดคล้องกันในทุกระบบ และห้ามผู้ใช้ทั่วไปแก้ไขเวลาเอง

ระบบที่มีความสำคัญ/ เกี่ยวข้องกับความปลอดภัย (เช่น AD/Directory, SIEM, Firewall, VPN, EDR, Database, Application สำคัญ) ต้องตั้งค่าให้ซิงโครไนซ์เวลาแบบอัตโนมัติและต่อเนื่อง และมีการตรวจสอบสถานะการซิงโครไนซ์

ต้องกำหนด แหล่งเวลาแบบสำรอง (Redundancy) อย่างน้อย 2 แหล่ง/ 2 เซิร์ฟเวอร์ (Primary/ Secondary) เพื่อรองรับกรณีแหล่งเวลาหลักขัดข้อง

ต้องจำกัดการเข้าถึงการตั้งค่าเวลาและการกำหนด NTP ให้เฉพาะผู้มีสิทธิ (Administrator) และต้องบันทึกการเปลี่ยนแปลงผ่านกระบวนการ Change Management (ยกเว้นกรณีฉุกเฉิน)

ต้องมีการเฝ้าระวัง/ แจ้งเตือนเมื่อเกิดความคลาดเคลื่อนของเวลาเกินเกณฑ์ที่กำหนด (เช่น เกิน X วินาที/ นาที ตามที่บริษัทกำหนดสำหรับแต่ละประเภทระบบ) และต้องดำเนินการแก้ไขภายในระยะเวลาที่กำหนด

ในกรณีใช้งานระบบคลาวด์ ให้ปฏิบัติตามแนวทางของผู้ให้บริการคลาวด์ และกำหนดมาตรฐานเวลาขององค์กรให้สอดคล้องกับการบันทึก log/monitoring ของบริษัท

8.3.6. การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operation software)

การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operation systems)

วิเคราะห์วางแผนการติดตั้งซอฟต์แวร์บนระบบการให้บริการเพื่อป้องกันความเสี่ยงต่อผลกระทบในการติดตั้งซอฟต์แวร์ระบบให้บริการที่อาจเกิดความล้มเหลว

มีขั้นตอนปฏิบัติสำหรับการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการต้องมีการปฏิบัติตามให้สอดคล้อง

สรุปวิเคราะห์ประเมินผล การติดตั้งซอฟต์แวร์ เพื่อนำไปสู่การปรับปรุงวางแผนการติดตั้งซอฟต์แวร์

8.3.7. การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation)

บริษัท ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานสินทรัพย์ทางปัญญาที่หน่วยงานจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด

บริษัท ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด(Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่

ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัท โดยเด็ดขาด

เพื่อที่จะให้เกิดความแน่ใจว่าเจ้าหน้าที่บริษัท มิได้ละเมิดลิขสิทธิ์โดยไม่ได้ตั้งใจ หรือพลั้งเผลอจึงไม่ควรจะทำสำเนาซอฟต์แวร์ใด ๆ ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของบริษัท เพื่อจุดประสงค์ใด ๆ ก็ตาม โดยที่ไม่ได้รับอนุญาตและในขณะเดียวกันไม่ควรจะติดตั้งโปรแกรมใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัท โดยไม่ได้รับการอนุญาต ทั้งนี้เพื่อที่จะให้แน่ใจว่ามีใบอนุญาตที่ครอบคลุมการติดตั้งดังกล่าว

บริษัท กำหนดให้มีการตรวจสอบเครื่องคอมพิวเตอร์อย่างน้อยปีละ 2 ครั้ง เพื่อตรวจดูรายการของซอฟต์แวร์ในเครื่องคอมพิวเตอร์ และเพื่อให้แน่ใจว่าบริษัท มีใบอนุญาตการใช้งานสำหรับผลิตภัณฑ์ซอฟต์แวร์แต่ละตัวในเครื่องคอมพิวเตอร์ ถ้าพบว่ามีซอฟต์แวร์ที่ไม่ได้รับอนุญาต ซอฟต์แวร์เหล่านั้นจะถูกลบทิ้ง และถ้าหากมีความจำเป็น สำนักงานอาจจะมีการพิจารณาให้นำซอฟต์แวร์ที่มีใบอนุญาตอย่างถูกต้องอื่นมาใช้แทนซอฟต์แวร์ดังกล่าวได้

8.4. ความมั่นคงปลอดภัยระบบเครือข่าย (Network Security)

8.4.1. การควบคุมการเข้าถึงเครือข่าย (Network Control)

- ผู้ดูแลระบบเครือข่ายต้องจำกัดการเข้าถึงระบบเครือข่ายและระบบเทคโนโลยี สารสนเทศที่เชื่อมต่อ อยู่กับระบบเครือข่ายโดยกำหนดให้ผู้ใช้งานในเครือข่าย สามารถเข้าถึงระบบเทคโนโลยีสารสนเทศ ผ่านทางระบบการพิสูจน์ตัวตน

- ผู้ดูแลระบบเครือข่ายต้องทดสอบความปลอดภัยทุกครั้งที่จะเชื่อมต่อกับระบบเครือข่ายของบุคคล ภายนอก เพื่อให้มั่นใจว่าไม่มีการเข้าถึงทรัพยากรที่ไม่ได้รับอนุญาต

- ผู้ดูแลระบบเครือข่ายต้องควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดย ไม่ได้รับอนุญาต

- การเข้าถึงอุปกรณ์เครือข่ายเพื่อการตรวจสอบและปรับแต่งระบบทั้งทางกายภาพ และการเข้าถึง จากระยะไกลต้องมีการควบคุม และทำได้เพียงแต่เฉพาะผู้ดูแลระบบ เครือข่ายที่ได้รับอนุญาต

- ในกรณีที่ต้องกำหนดสิทธิการเข้าถึงแบบชั่วคราวแก่บุคคลภายนอก

- ผู้ดูแลระบบเครือข่ายต้องให้มีผู้ควบคุม ตรวจสอบ และยกเลิกสิทธิการเข้าถึงทันที ที่ปฏิบัติงานเสร็จ

- ผู้ดูแลระบบเครือข่ายต้องตรวจสอบ และปิดพอร์ตของอุปกรณ์เครือข่ายที่ไม่ใช้งาน

- การให้บริการทางเครือข่ายสำหรับเครื่องคอมพิวเตอร์แม่ข่าย ผู้ดูแลระบบเครือข่าย ต้องอนุญาตเฉพาะพอร์ต (Port) การเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

- ผู้ดูแลระบบเครือข่ายต้อง Update Security Patch ของอุปกรณ์เครือข่ายอย่างสม่ำเสมอ

- ผู้ดูแลระบบเครือข่ายต้องจัดทำแผนผังเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในบริษัทฯ พร้อมทั้งปรับปรุงให้ เป็นปัจจุบันอยู่เสมอ

- ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องกับกฎหมาย

8.4.2. ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Service)

- ผู้ใช้งานต้องใช้บริการระบบเครือข่ายตามที่ผู้ดูแลระบบเครือข่ายอนุญาตเท่านั้น

- ผู้ใช้งานต้องใช้ระบบเครือข่ายที่ไม่กระทบต่อประสิทธิภาพการใช้งานเครือข่ายโดยรวม เช่น การรับ-ส่งไฟล์ขนาดใหญ่ การดาวน์โหลด หรือการอัปโหลดไฟล์ที่มีขนาดใหญ่ เป็นต้น

- ห้ามผู้ใช้งานอุปกรณ์เครือข่ายเชื่อมต่อกับระบบเครือข่ายของบริษัทก่อนได้รับอนุญาตจากผู้ดูแล ระบบเครือข่าย

- ห้ามใช้เครือข่ายเพื่อกระทำสิ่งที่ผิดกฎหมาย

- ผู้ใช้งานต้องเข้าใช้ระบบเครือข่ายด้วยบัญชีผู้ใช้งานของตนเองเท่านั้น

- ห้ามเผยแพร่ข้อมูลของผู้อื่นหรือของหน่วยงาน โดยไม่ได้รับอนุญาต

- ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ จากภายนอกเข้ากับ ระบบคอมพิวเตอร์และระบบเครือข่ายโดยเด็ดขาดหากมีความจำเป็นต้องใช้งานต้องดำเนิน การขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง

- ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่าง เช่น Router Switch Hub และ Wireless Access Point ฯลฯ โดยไม่ได้รับอนุญาตเด็ดขาด

8.4.3. การจัดแบ่งเครือข่ายภายในสำนักงานฯ (Segregation in Network)

- กลุ่มที่ให้บริการระบบเทคโนโลยีสารสนเทศเป็นระบบเครือข่ายที่สามารถเข้าถึง และใช้งานโดย ผู้ใช้งาน เช่น ระบบอินทราเน็ต ระบบจดหมายอิเล็กทรอนิกส์ เป็นต้น

- กลุ่มที่ให้บริการระบบเทคโนโลยีสารสนเทศ เป็นระบบเครือข่ายที่เข้าถึง และใช้งานโดยระบบ เทคโนโลยีสารสนเทศ ซึ่งต้องไม่ถูกเข้าถึงจากผู้ใช้งานโดยตรง เช่น ระบบฐานข้อมูล ระบบ Directory Service ระบบ Domain Name System (DNS) ระบบ Printer Service เป็นต้น

- กลุ่มที่ให้บริการผู้ใช้งานเป็นระบบเครือข่ายที่สามารถเข้าถึง และใช้งานโดยเครื่องคอมพิวเตอร์ ของผู้ใช้งาน

- กลุ่มที่ให้บริการผู้ใช้งานแบบไร้สายเป็นเครือข่ายสามารถเข้าถึง และใช้งานโดยเครื่อง คอมพิวเตอร์พกพา แท็บเล็ต และสมาร์ทโฟนของผู้ใช้งาน

- ต้องออกแบบระบบเครือข่ายตามกลุ่มของการบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน โดยแบ่งตามกลุ่มของผู้ใช้และกลุ่มของระบบเทคโนโลยีสารสนเทศโดยแบ่งเป็น โซนภายใน (Internal Zone) และโซนภายนอก

(External Zone) เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายใน และเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

8.4.4. การกรองเว็บ (Web Filtering)

บริษัทฯ มีการควบคุมการเข้าถึง กรองข้อมูล/บล็อกและจำกัดสิทธิการเข้าถึงเว็บไซต์ที่ไม่ปลอดภัยหรือเว็บเสี่ยง แบบอัตโนมัติ User ไม่สามารถทราบได้ว่าเว็บไซต์ไหนปลอดภัย หรือเว็บไซต์ ไหนเป็นอันตราย แผนกเทคโนโลยีสารสนเทศจะเป็นผู้ตรวจสอบและกำหนดนโยบายการกรองเว็บ (Web Filtering) และทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

อุปกรณ์ของบริษัทต้องถูกกำหนดให้ส่ง ทราฟฟิกเว็บผ่านระบบ Web Filtering และไม่อนุญาตให้ผู้ใช้หลีกเลี่ยงการกรองเว็บ (เช่น เปลี่ยนค่า Proxy เอง/ใช้เครื่องมือ bypass)

สำหรับการทำงานนอกสถานที่ (Remote work) ต้องมีวิธีบังคับใช้นโยบายเทียบเท่า (เช่น ผ่าน VPN, Agent ของ SWG, หรือ DNS filtering ที่องค์กรอนุมัติ)

หมวดหมู่เว็บไซต์/เนื้อหาที่ต้องควบคุม

บริษัทต้อง “ปิดกั้น (Block)” เว็บไซต์/ หมวดหมู่ที่มีความเสี่ยงหรือไม่สอดคล้องกับการใช้งานขององค์กรตามที่กำหนดอย่างน้อย ได้แก่

- มัลแวร์/ ฟิชชิง/ โดเมนอันตราย/ Command & Control
- เว็บไซต์ที่มีการดาวน์โหลดไฟล์อันตรายหรือไม่ปลอดภัย
- เนื้อหาผิดกฎหมายหรือไม่เหมาะสม (เช่น สื่อลามก การพนัน ยาเสพติด ความรุนแรง) ตามบริบทองค์กรและกฎหมาย
- Anonymizer/ Proxy/ VPN ที่ไม่ได้รับอนุญาต (เพื่อป้องกันการหลีกเลี่ยงการควบคุม)

บริษัทอาจกำหนด “การจำกัด (Restrict/ Allow with warning)” สำหรับหมวดหมู่ที่กระทบประสิทธิภาพงานหรือมีความเสี่ยงปานกลาง (เช่น Streaming/ Cloud storage ส่วนบุคคล/ Social media) โดยอิงตามความจำเป็นทางธุรกิจ

การอนุญาตใช้งานเฉพาะที่จำเป็น (Allow-list / Exception)

การอนุญาตเว็บไซต์/ บริการที่ถูกบล็อกต้องทำผ่านกระบวนการขอยกเว้น/ ขอปลดบล็อก โดยระบุเหตุผลทางธุรกิจ ระยะเวลา และเจ้าของระบบ/ ผู้รับผิดชอบ

การยกเว้นต้องได้รับการอนุมัติตามลำดับอำนาจ (เช่น หัวหน้างาน + IT Security) และต้องกำหนดมาตรการทดแทนความเสี่ยง (Compensating controls) ตามความเหมาะสม

บริษัทสงวนสิทธิในการเพิกถอนการยกเว้นเมื่อพบความเสี่ยงหรือการใช้งานไม่เป็นไปตามวัตถุประสงค์

การตรวจสอบ HTTPS/การคุ้มครองข้อมูลส่วนบุคคล

การกรองเว็บต้องคำนึงถึงความเป็นส่วนตัวและข้อกฎหมายที่เกี่ยวข้อง (เช่น PDPA) และใช้เฉพาะเท่าที่จำเป็นเพื่อความมั่นคงปลอดภัย

หากมีการทำ SSL/ TLS Inspection (การถอดรหัสเพื่อตรวจสอบ) ต้องได้รับอนุมัติจากฝ่ายที่เกี่ยวข้อง และต้องกำหนดข้อยกเว้นสำหรับข้อมูลอ่อนไหว/บริการที่ไม่ควรถอดรหัสตามความเหมาะสม (เช่น หมวดสุขภาพ/ธนาคาร/บริการที่กำหนด) รวมถึงต้องมีการควบคุมการเข้าถึงข้อมูลที่ได้จากการตรวจสอบอย่างรัดกุม

การบันทึกเหตุการณ์และการเฝ้าระวัง (Logging & Monitoring)

ระบบ Web Filtering ต้องบันทึกข้อมูลที่จำเป็นต่อการตรวจสอบ เช่น ผู้ใช้/ อุปกรณ์ เวลา URL/Domain หมวดหมู่ การอนุญาต/ปฏิเสธ และเหตุผลการบล็อก

ต้องกำหนดระยะเวลาเก็บรักษา Log ตามข้อกำหนดของบริษัท/ กฎหมาย และจำกัดการเข้าถึง Log เฉพาะผู้มีหน้าที่เกี่ยวข้อง

เหตุการณ์เสี่ยงสูง (เช่น การเข้าถึงเว็บไซต์ฟิชชิง/ มัลแวร์ซ้ำ ๆ) ต้องมีการแจ้งเตือนและดำเนินการตามกระบวนการ Incident Response

ความรับผิดชอบผู้ใช้งานและการบังคับใช้

ผู้ใช้งานต้องใช้อินเทอร์เน็ตตามนโยบายการใช้งานที่ยอมรับได้ (Acceptable Use) และต้องไม่พยายามหลีกเลี่ยงการกรองเว็บ

การฝ่าฝืนอาจนำไปสู่การระงับการใช้งาน การดำเนินการทางวินัย หรือมาตรการอื่นตามระเบียบบริษัทและกฎหมาย

8.5. การกำหนดการควบคุมการเข้ารหัสข้อมูล (Use of Cryptography)

เพื่อให้มั่นใจว่ามีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสม เข้าใจในกระบวนการเข้ารหัสลับ ซึ่งเป็นกระบวนการสำหรับแปรรูปข้อมูลธรรมดาให้อยู่ในรูปที่บุคคลทั่วไปไม่สามารถอ่านได้ถ้าจะอ่านต้องเข้าใจในวิธีการอ่าน รู้ช่องทางในการรับเข้า ในการถอดรหัสที่ตรงกันจึงจะสามารถถอดรหัสได้ และได้ผลและป้องกันความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

เพื่อกำหนดแนวทางการเข้ารหัสลับข้อมูลและทำให้ระบบสารสนเทศรักษาไว้ซึ่งความลับของข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานระบบสารสนเทศ และ/หรือ ป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาตอย่างมีประสิทธิภาพและความเหมาะสม

8.5.1. มาตรการการเข้ารหัสลับข้อมูล (Cryptographic Controls)

ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารต้องกำหนดมาตรการการเข้ารหัสลับข้อมูล และแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยกำหนดกลุ่มผู้ใช้งานอย่างเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้ แต่กรณีที่ไม่สามารถเข้ารหัสได้ ต้องควบคุมการเข้าถึงอย่างเหมาะสมตามหน้าที่และความรับผิดชอบ

การบริหารจัดการกุญแจเข้ารหัสลับข้อมูลฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารต้องกำหนดวิธีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัสลับข้อมูล ซึ่งประกอบไปด้วย

การพิจารณาประเภทกลุ่มข้อมูลที่นำมาใช้เข้ารหัสว่าสอดคล้องกับการจัดระดับชั้นความลับของข้อมูล และแนวทางการดำเนินการกำกับข้อมูล

การเลือกใช้การเข้ารหัสข้อมูลให้สามารถดำเนินการได้ 2 แบบ ดังนี้

- แบบ Symmetric คือการเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสเดียวกัน (Secret Key)
- แบบ Asymmetric คือการเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสคู่ (Public/ Private Key)

โดยพิจารณาวิธีการเข้ารหัสแต่ละรูปแบบ อ้างอิง “รูปแบบการเข้ารหัสข้อมูล” รวมทั้ง ใช้อัลกอริทึมที่เหมาะสม

8.5.2. การบริหารจัดการกุญแจในการเข้ารหัสข้อมูล (Key Management)

กุญแจรหัสลับที่ใช้ในการเข้ารหัสลับสำหรับระบบเครือข่ายคอมพิวเตอร์ภายใน บริษัทฯ ต้องได้รับการควบคุมดูแลการกำหนดกุญแจรหัสลับ การจัดเก็บกุญแจรหัสลับ การเปลี่ยนกุญแจรหัสลับ และการครอบครองกุญแจรหัสลับ

8.6. ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)

8.6.1. นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

ต้องมีการกำหนดหลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์ และมีการปฏิบัติตามนโยบายหรือข้อกำหนดที่บริษัทกำหนดขึ้นมา เช่น การพัฒนาซอฟต์แวร์ควรคำนึงความปลอดภัยในทุกขั้นตอนของการพัฒนา และนักพัฒนา (Developer) ควรมีความสามารถในการหลีกเลี่ยงไม่ให้โปรแกรมที่พัฒนาตรวจพบช่วงโหว่ และต้องสามารถแก้ไขช่องโหว่ที่ตรวจพบได้

8.6.2. ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System change control procedures)

- แต่งตั้งคณะทำงานดูแลการเข้าใช้งานระบบ และตั้งข้อปฏิบัติในการเข้าใช้งาน
- ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง หรือให้บริการอยู่แล้ว เช่น
- คำขอ ให้แก้ไขต้องมาจากผู้ที่มีสิทธิ
- ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
- ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
- เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ
- ต้องเก็บรายละเอียดของคำขอไว้ เป็นต้น

8.6.3. การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes)

ทำการทดสอบระบบทุกครั้งเมื่อมีการเปลี่ยนแปลงโครงสร้าง เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบซอฟต์แวร์ต่าง ๆ ที่ใช้งานว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

8.6.4. การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)

การใช้ซอฟต์แวร์ของผู้ผลิตจะใช้การแก้ไขโดยผ่านทาง firewall และกำหนดให้มีการ Update firewall ต่าง ๆ ให้เป็นแบบ Manual เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

8.6.5. หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

- มีคำสั่งจัดตั้งคณะกรรมการระบบด้านความมั่นคงปลอดภัย เพื่อให้เกิดความมั่นคงปลอดภัยทางด้านวิศวกรรมระบบ ต้องมีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร โดยมีการปรับปรุงอย่างต่อเนื่อง และมีการประยุกต์ใช้กับงานพัฒนาระบบ
- จัดทำแบบแปลนโครงสร้างทางวิศวกรรมและสามารถรองรับการแก้ไขเพิ่มเติมในอนาคตได้
- ตรวจทาน ปรับปรุง แก้ไขและทดสอบระบบทุก ๆ จุดและกระจายการออกแบบไปยังส่วนกลาง

8.6.6. สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)

- แต่งตั้งคณะกรรมการเพื่อศึกษาสภาพแวดล้อมของการพัฒนาระบบ
- จ้างบริษัทที่มีมาตรฐานเพื่อเข้ามาจัดทำระบบ

8.6.7. การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development)

การประเมินผู้รับจ้าง (Third-party Due Diligence)

ก่อนเริ่มงานต้องมี:

- Risk Assessment ของโครงการ (ตามระดับข้อมูล/การเชื่อมต่อ/ผลกระทบต่อการปฏิบัติงานสนามบิน)
- การประเมินความสามารถด้านความปลอดภัยของผู้รับจ้าง เช่น Secure SDLC, vulnerability management, incident response
- หากเกี่ยวข้องกับ PCI DSS ต้องยืนยันขอบเขต PCI (PCI scope) และบทบาทผู้รับจ้าง (service provider/third party) ชัดเจน
- เอกสารขั้นต่ำที่ต้องขอ: security policy/SDL practice, รายการพนักงานที่เข้าถึง, ตัวอย่างรายงาน Pentest/ VA (ปกปิดข้อมูลได้), แผน IR เบื้องต้น

ข้อกำหนดใน TOR/SOW และสัญญา (ต้องมีทุกงาน)

สัญญาต้องระบุอย่างน้อย:

- ขอบเขตข้อมูล ที่ผู้รับจ้างเข้าถึงได้/ วัตถุประสงค์/ ระยะเวลา
- การห้ามใช้ข้อมูลจริง ใน dev/test เว้นแต่ได้รับอนุมัติเป็นลายลักษณ์อักษรและทำ masking/anonymization
- Secure SDLC & Secure Coding อ้างอิง OWASP (Top 10/ASVS ตามความเหมาะสม)
- Vulnerability Fix SLA และเกณฑ์ “ห้ามขึ้นระบบจริง” หากยังมีช่องโหว่รุนแรง
- Incident/ Breach Notification ระยะเวลาแจ้ง (เช่น ภายใน 24 ชม. หลังพบเหตุ/ สงสัย) และความร่วมมือในการสืบสวน
- สิทธิการตรวจประเมิน (Audit right) รวมถึงการขอหลักฐานการควบคุม/รายงานทดสอบ
- การควบคุม Subcontractor: ห้ามจ้างช่วงโดยไม่ได้รับอนุมัติ และต้องผูกข้อกำหนดเดียวกัน
- IP Ownership & Deliverables: source code, IaC, เอกสาร, runbook, test evidence, pipeline
- Maintenance/ SLA: เวลาตอบสนอง, การ patching, on-call, การสนับสนุน incident

การควบคุมการเข้าถึง (Access Control) สำหรับ GitHub/ GitLab และ AWS

- ใช้บัญชี รายบุคคลเท่านั้น ห้ามแชร์บัญชี
- บังคับใช้ MFA สำหรับ GitHub/ GitLab, AWS IAM/ SSO และเครื่องมือสำคัญทั้งหมด
- การให้สิทธิต้องผ่านการอนุมัติ และใช้หลัก Least Privilege + กำหนดอายุสิทธิ (time-bound access) เมื่อเหมาะสม
- ห้ามใช้ access key แบบถาวรโดยไม่จำเป็น; ให้ใช้ SSO/ role assumption เป็นหลัก
- ต้องมีขั้นตอน Joiner–Mover–Leaver: เพิ่ม/ เปลี่ยน/ ถอนสิทธิทันทีเมื่อเปลี่ยนหน้าที่หรือสิ้นสุดสัญญา

- Production access ต้องจำกัดเฉพาะกรณีจำเป็น มีการบันทึก (logging) และอนุมัติเป็นครั้งคราว (break-glass)

ข้อกำหนดเฉพาะ PDPA (ข้อมูลส่วนบุคคล)

- ต้องจัดทำ DPA (Data Processing Agreement) ระบุบทบาท (ผู้ควบคุม/ผู้ประมวลผล), วัตถุประสงค์, มาตรการความปลอดภัย, ระยะเวลาเก็บ, การลบ/คืนข้อมูล
- ห้ามโอน/ เปิดเผยข้อมูลส่วนบุคคลให้บุคคลอื่นโดยไม่ได้รับอนุมัติ

การส่งมอบและการสิ้นสุดสัญญา (Exit)

เมื่อจบโครงการ/ ยกเลิกสัญญา:

- ส่งมอบ source code, IaC, pipeline, เอกสารสถาปัตยกรรม, runbook, คู่มือ admin, รายงานทดสอบ
- โอนความเป็นเจ้าของ repo/ project และปิด/ ถอนสิทธิผู้รับจ้างทั้งหมด
- คืน/ ลบข้อมูลบริษัท และออกหนังสือรับรองการลบ/ทำลายข้อมูล (เมื่อร้องขอ)
- จัดทำ knowledge transfer ให้ทีมภายใน

8.7.8. การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

ข้อกำหนดที่อย่างน้อยต้องมี 2 ข้อในการตรวจสอบ

- SAST/ SCA/ Secret/ IaC/ Container scan: ทุกครั้งใน CI/ CD (ทุก PR/ ทุก build อย่างน้อย)
- DAST: อย่างน้อยราย release หรือรายเดือน (ตามความเสี่ยง)
- Vulnerability scan (infra): อย่างน้อยรายเดือน และหลัง patch รอบใหญ่
- Penetration test: อย่างน้อยปีละ 1 ครั้งสำหรับระบบเสี่ยงสูง/ ระบบที่เปิดสาธารณะ และทุกครั้งหลัง major change
- PCI DSS (ถ้าเกี่ยวข้อง): ให้ทำตามความถี่/ ข้อกำหนดของ PCI ในส่วนที่เกี่ยวข้อง (เช่น การทดสอบ/สแกนตามเกณฑ์ของมาตรฐาน)
- เกณฑ์ “ผ่านก่อนขึ้นระบบจริง” (Go-Live Security Gate) ระบบจะขึ้น Production ได้เมื่อ:
- ช่องโหว่ระดับ Critical/High = 0 (หรือได้รับอนุมัติ Risk Acceptance เป็นลายลักษณ์อักษรจากผู้มีอำนาจ)
- มีหลักฐานการแก้ไขและ re-test สำหรับประเด็นสำคัญ
- Logging/Monitoring ที่จำเป็นเปิดใช้งานแล้ว (รวมถึง audit trail การเข้าถึงข้อมูลสำคัญ)

8.7.9. การทดสอบเพื่อรับรองระบบ (System acceptance testing)

- มีการจัดทำแผนการทดสอบหรือเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ โดยต้องมีการจัดทำทั้งสำหรับระบบใหม่และระบบที่ปรับปรุง
- ต้องจัดให้มีเกณฑ์ในการยอมรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือทรัพยากรสารสนเทศอื่น ๆ ก่อนการใช้งาน รวมทั้งต้องจัดทำเอกสาร Checklist หัวข้อที่ทำการทดสอบระบบก่อนที่จะตรวจรับระบบนั้น และให้มีการเซ็นชื่อเจ้าหน้าที่ทำการทดสอบและลายเซ็นผู้ส่งมอบ

8.8. ข้อมูลสำหรับการทดสอบ (Test data)

8.8.1. การป้องกันข้อมูลสำหรับการทดสอบ (Protection of test data)

ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบ จะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อนเมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ แจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

8.9. การบริหารการเปลี่ยนแปลง (Change Management)

8.9.1. นโยบายการบริหารการเปลี่ยนแปลง (Change Management)

- ก่อนทำการเปลี่ยนแปลงกับระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายระบบ คอมพิวเตอร์ซอฟต์แวร์ หรือฐานข้อมูลโดยผู้ดูแลระบบฯ หรือผู้ให้บริการภายนอกต้อง ดำเนินการขออนุมัติการดำเนินการ เปลี่ยนแปลงจากแผนกเทคโนโลยีสารสนเทศ อย่างเป็นลายลักษณ์อักษร
- การเปลี่ยนแปลงกับระบบเครือข่ายระบบคอมพิวเตอร์ซอฟต์แวร์หรือฐานข้อมูลโดย ผู้ให้บริการภายนอกต้องได้รับการควบคุมดูแลจากผู้ดูแลระบบเทคโนโลยีสารสนเทศ
- ผู้ดูแลระบบเทคโนโลยีสารสนเทศต้องแจ้งให้ผู้ใช้งานทราบก่อนทุกครั้งก่อนทำการเปลี่ยนแปลงระบบ
- ผู้ดูแลระบบเทคโนโลยีสารสนเทศหรือผู้ให้บริการภายนอกต้องมีการประเมินผลกระทบ ของการเปลี่ยนแปลงระบบก่อนที่จะทำการเปลี่ยนแปลงนั้นเพื่อป้องกันผลกระทบกับ การทำงานของระบบที่ใช้ ดำเนินงานอยู่ในปัจจุบัน
- ผู้ดูแลระบบเทคโนโลยีสารสนเทศต้องบันทึกรายละเอียดการเปลี่ยนแปลงระบบ เทคโนโลยีสารสนเทศ
- ผู้ดูแลระบบเทคโนโลยีสารสนเทศหรือผู้ให้บริการภายนอกต้องมีการทดสอบการเปลี่ยน แปลงนั้นก่อนเสมอ โดยเฉพาะอย่างในกรณีเป็นระบบเทคโนโลยีสารสนเทศที่สำคัญ
- ผู้ดูแลระบบเทคโนโลยีสารสนเทศ หรือผู้ให้บริการภายนอกต้องกำหนดแผนย้อนคืน (Fallback Plan) เพื่อรองรับหากการเปลี่ยนแปลงไม่เป็นไปตามที่คาดคิด
- ผู้ดูแลระบบเทคโนโลยีสารสนเทศหรือผู้ให้บริการจากภายนอกต้องกำหนดระยะเวลาในการติดตาม การเปลี่ยนแปลงนั้นเพื่อตรวจสอบผลกระทบที่อาจเกิดขึ้นกับระบบหลังจาก การเปลี่ยนแปลง

8.9.2. กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (System Change Control Procedures)

- ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ สำหรับระบบสารสนเทศที่ใช้งานจริง หรือให้บริการอยู่แล้ว เช่น

  - คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ
  - ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
  - ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
  - เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ
  - ต้องเก็บรายละเอียดของคำขอไว้ เป็นต้น

8.9.3. การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating Platform Changes)

เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบซอฟต์แวร์ต่าง ๆ ที่ใช้งานว่าไม่มีผลกระทบต่อการทำงาน และความมั่นคงปลอดภัย

8.9.4. การควบคุมการเปลี่ยนแปลงของซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)

เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็นและการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบ และจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้ เมื่อมี การปรับปรุงซอฟต์แวร์ในอนาคต

9. ข้อปฏิบัติและข้อบังคับตามกฎหมาย

บริษัท มีการจัดทำการตรวจสอบความปลอดภัยข้อมูลเพื่อให้ถูกต้องและตรงกับนโยบาย ระเบียบและกฎหมายอย่างต่อเนื่อง

การปฏิบัติตามนโยบายและระเบียบ

พนักงานทุกคนต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลและเอกสารที่เกี่ยวข้องกับนโยบายนี้ รวมถึงนโยบายอื่น ๆ ที่เกี่ยวข้อง อย่างเคร่งครัด เช่น นโยบายการคุ้มครองข้อมูลส่วนบุคคล พนักงานท่านใดที่ละเลย หรือมีเจตนาที่จะไม่ปฏิบัติตาม ถือว่ามีการละเมิดนโยบายดังกล่าว จะได้รับบทลงโทษหรืออาจจะร้ายแรงถึงขั้นไล่ออก

การปฏิบัติตามกฎหมายและข้อบังคับต่าง ๆ

นโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลจะต้องเป็นไปตามข้อบังคับทางกฎหมาย เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 (PDPA) กฎหมายที่เกี่ยวกับการป้องกันข้อมูล การเข้าถึงข้อมูล การป้องกันข้อมูลส่วนตัวและเอกสารอิเล็กทรอนิกส์ต่าง ๆ เป็นต้น

ตามระเบียบข้อบังคับของพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550 นั้นถือว่าบริษัทฯ เป็นผู้ให้บริการเข้าถึงอินเทอร์เน็ต ซึ่งต้องมีการบันทึกและเก็บการบันทึกข้อมูลจราจรทางอินเทอร์เน็ตทั้งหมดตามวันและเวลาที่เข้าถึง ย้อนหลังอย่างน้อย 90 วัน หรือมากกว่านั้น

10. ระเบียบและบทลงโทษ

10.1. การกระทำที่สงสัยว่าจะละเมิดนโยบายการรักษาความปลอดภัย (การเจาะข้อมูล, การทำลายข้อมูลของไวรัสคอมพิวเตอร์) หรือสงสัยว่ามีการล่วงละเมิดหรือแทรกแซงระบบข้อมูล ต้องแจ้งให้กับผู้บริหาร และเจ้าหน้าที่รักษาความปลอดภัยข้อมูลทราบทันที

10.2. การกระทำที่สงสัยว่าจะละเมิดข้อมูลส่วนบุคคล ต้องดำเนินการแจ้งให้กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทันที โดยอ้างอิงจาก "นโยบายการคุ้มครองข้อมูลส่วนบุคคล"

10.3. การละเมิดหรือการไม่ปฏิบัติตามนโยบายการรักษาความปลอดภัยของข้อมูล มีบทลงโทษต่อผู้ละเมิดอย่างร้ายแรง ระเบียบการลงโทษมีความรุนแรงขึ้นอยู่กับการกระทำ และสามารถรุนแรงถึงขั้นไล่ออก

10.4. การทำตามระเบียบของพนักงานทั้งหมดที่อยู่ภายใต้การดูแลของหัวหน้าฝ่ายหรือผู้มีระดับที่สูงกว่า เมื่อพนักงานทำผิดหรือละเมิดกฎหัวหน้าฝ่ายหรือผู้มีระดับที่สูงกว่าจะเป็นผู้พิจารณาลงโทษ

10.5. การกระทำที่ถือว่าเป็นการละเมิดกฎมีดังนี้

10.5.1. การเปลี่ยนแปลงแก้ไขข้อมูลภายในระบบโดยไม่ได้รับอนุญาตจากผู้มีอำนาจหรือหัวหน้างานก่อน

10.5.2. การปลอมแปลง ขโมย ชื่อผู้ใช้งานและรหัสผ่านเพื่อเข้าใช้งานในระบบแอปพลิเคชันใด ๆ โดยตั้งใจหรือไม่ตั้งใจก็ตาม

10.5.3. การใช้บัญชีผู้ใช้งานและรหัสผ่านของผู้อื่นในการเข้าใช้งานระบบคอมพิวเตอร์เพื่ออ่าน คัดลอกหรือทำสำเนา เปลี่ยนแปลงหรือลบข้อมูลไม่ว่าจะด้วยเหตุผลใด ๆ ก็ตาม

10.5.4. การละเลยและอนุญาตให้ผู้อื่นใช้บัญชีผู้ใช้งานและรหัสผ่านของตัวเองในการเข้าใช้งานระบบคอมพิวเตอร์ รวมถึงให้ใช้สิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์นั้น ๆ ด้วย

10.5.5. ทำการพยายามเปิดเผย ขาย และกระจายข้อมูลของบริษัทฯ

10.5.6 การพยายามเข้าใช้งานระบบและแอพลิเคชันใด ๆ โดยไม่มีสิทธิในการใช้งาน

10.5.7. การติดตั้ง ตรวจสอบ เฝ้าดู และใช้เครื่องมือหรือซอฟต์แวร์ในการเจาะข้อมูล (hacking tools) หรือโปรแกรมที่เกี่ยวกับตรวจสอบความปลอดภัยของระบบคอมพิวเตอร์ ยกเว้นผู้ที่มีหน้าที่รับผิดชอบในด้านในการทำการดังกล่าวเท่านั้น

10.5.8. ติดตั้งและทำการเปลี่ยนแปลงหมายเลขของเครื่องคอมพิวเตอร์ (IP address) โดยไม่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ (IT) ก่อน

10.5.9. การเปลี่ยนแปลง โอนย้าย หรือติดตั้ง ส่วนใดส่วนหนึ่งในระบบคอมพิวเตอร์โดยไม่ได้รับการอนุญาตจากฝ่าย IT ก่อน

10.5.10. การร่วมมือกับบุคคลภายนอกเพื่อให้เข้ามาใช้งานระบบคอมพิวเตอร์หรือโปรแกรมแอปพลิเคชันใด ๆ หรือทำลายการรักษาความปลอดภัยของข้อมูลหรือระบบของบริษัทฯ

10.6. บทลงโทษการฝ่าฝืนและละเลย

10.6.1. การกล่าวตักเตือน

10.6.2. ออกจดหมายเตือน

10.6.3. ได้รับการพักงานชั่วคราว

10.6.4. พ้นสภาพจากการเป็นพนักงานของบริษัท

10.6.5. บริษัทฯ จะพิจารณาและใช้ความละเอียดรอบคอบในการลงโทษพนักงานที่ทำผิดหรือละเมิดนโยบายฉบับนี้

บทสรุป

บริษัท โปร อินไซด์ จำกัด (มหาชน) จำเป็นต้องมีการพัฒนานโยบาย ระเบียบขั้นตอน ข้อแนะนำ และมาตรฐานต่าง ๆ ขึ้นมาเพื่อให้การสนับสนุนการทำงานในส่วนนโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลนี้ ซึ่งมีการประกาศใช้อย่างเป็นทางการให้ได้รับทราบภายในบริษัท คู่มือของนโยบายการรักษาความปลอดภัย สามารถใช้อ้างอิงถึงมาตรฐานหรือนโยบายย่อยที่ใช้ควบคุมระบบต่าง ๆ ภายในบริษัทและมีการปรับปรุงอย่างต่อเนื่อง

มีผลตั้งแต่วันที่ 26 มิถุนายน 2569 เป็นต้นไป

-นายวิสุทธิ์ ศรีสุพรรณ-

(นายวิสุทธิ์ ศรีสุพรรณ)

ประธานกรรมการ

อนุมัติโดยที่ประชุมคณะกรรมการบริษัท

ครั้งที่ 4/2569

เมื่อวันที่ 25 มิถุนายน 2569