ภาคผนวก

ก. ตัวอย่างแบบประเมินองค์กรเบื้องต้น ตามมาตรฐาน ISO/IEC 27001

แบบประเมินองค์การตาม ISO/IEC 27001	การดำเนินการ		
	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
หมวดที่ 1 : นโยบายความมั่นคงปลอดภัย (Security policy)			
1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)			
1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)			
1.1.2 การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)			
หมวดที่ 2 : โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)			
2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization)			
2.1.1 การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security)			
2.1.2 การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)			
2.1.3 การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)			
2.1.4 กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ (Authorization process for information processing facilities)			
2.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements)			
2.1.6 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with authorities)			
2.1.7 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)			
2.1.8 การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ (Independent review of information security)			
2.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties)			
2.2.1 การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก (Identification of risks related to external parties)			
2.2.2 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security when dealing with customers)			
2.2.3 การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security in third party agreements)			

แบบประเมินองค์การตาม ISO/IEC 27001	การดำเนินการ		
	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
หมวดที่ 3 การบริหารจัดการทรัพย์สินขององค์กร (Asset management)			
3.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets)			
3.1.1 การจัดทำบัญชีทรัพย์สิน (Inventory of assets)			
3.1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of assets)			
3.1.3 การใช้งานทรัพย์สินที่เหมาะสม (Acceptable use of assets)			
3.2 การจัดหมวดหมู่สารสนเทศ (Information classification)			
3.2.1 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification guidelines)			
3.2.2 การจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศ (Information labeling and handling)			
หมวดที่ 4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)			
4.1 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment)			
4.1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Roles and responsibilities)			
4.1.2 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)			
4.1.3 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment)			
4.2 การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment)			
4.2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsibilities)			
4.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education, and training)			
4.2.3 กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary process)			
4.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or change of employment)			
4.3.1 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination responsibilities)			
4.3.2 การคืนทรัพย์สินขององค์กร (Return of assets)			
4.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)			

แบบประเมินองค์การตาม ISO/IEC 27001	การดำเนินการ		
	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
หมวดที่ 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)			
5.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas)			
5.1.1 การจัดทำบริเวณล้อมรอบ (Physical security perimeter)			
5.1.2 การควบคุมการเข้า-ออก (Physical entry controls)			
5.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing offices, rooms and facilities)			
5.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats)			
5.1.5 การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)			
5.1.6 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, delivery, and loading areas)			
5.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security)			
5.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)			
5.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)			
5.2.3 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security)			
5.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)			
5.2.5 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of equipment off-premises)			
5.2.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)			
5.2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)			
หมวดที่ 6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)			
6.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational procedures and responsibilities)			
6.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)			
6.1.2 การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบหรืออุปกรณ์ ประมวลผลสารสนเทศ (Change management)			

แบบประเมินองค์การตาม ISO/IEC 27001	การดำเนินการ		
	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
6.1.3 การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)			
6.1.4 การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, test, and operational facilities)			
6.2 การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third party service delivery management)			
6.2.1 การให้บริการโดยหน่วยงานภายนอก (Service delivery)			
6.2.2 การตรวจสอบการให้บริการโดยหน่วยงานภายนอก (Monitoring and review of third party services)			
6.2.3 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ (Managing changes to third party services)			
6.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System planning and acceptance)			
6.3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)			
6.3.2 การตรวจรับระบบ (System acceptance)			
6.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection against malicious and mobile code)			
6.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)			
6.4.2 การป้องกันโปรแกรมชนิดเคลื่อนที่ (Controls against mobile code)			
6.5 การสำรองข้อมูล (Back-up/Housekeeping)			
6.5.1 การสำรองข้อมูล (Information back-up)			
6.6 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management)			
6.6.1 มาตรการทางเครือข่าย (Network controls)			
6.6.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)			
6.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media handling and security)			
6.7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)			
6.7.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of media)			
6.7.3 ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information handling procedures)			

แบบประเมินองค์การตาม ISO/IEC 27001	การดำเนินการ		
	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
6.7.4 การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system documentation)			
6.8 การแลกเปลี่ยนสารสนเทศ (Exchange of information)			
6.8.1 นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information exchange policies and procedures)			
6.8.2 ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange agreements)			
6.8.3 การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร (Physical media in transit)			
6.8.4 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)			
6.8.5 ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business information systems)			
6.9 การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services)			
6.9.1 การพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce)			
6.9.2 การทำธุรกรรมออนไลน์ (On-line transactions)			
6.9.3 สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ (Publicly available information)			
6.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)			
6.10.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging)			
6.10.2 การตรวจสอบการใช้งานระบบ (Monitoring system use)			
6.10.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of log information)			
6.10.4 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and operator logs)			
6.10.5 การบันทึกเหตุการณ์ข้อผิดพลาด (Fault logging)			
6.10.6 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock synchronization)			

แบบประเมินองค์การตาม ISO/IEC 27001	การดำเนินการ		
	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
หมวด 7 การควบคุมการเข้าถึง (Access control)			
7.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)			
7.1.1 นโยบายการควบคุมการเข้าถึงระบบ (Access control policy)			
7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)			
7.2.1 การลงทะเบียนพนักงาน (User registration)			
7.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)			
7.2.3 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)			
7.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)			
7.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)			
7.3.1 การใช้งานรหัสผ่าน (Password use)			
7.3.2 การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment)			
7.3.3 นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy)			
7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)			
7.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)			
7.4.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)			
7.4.3 การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks)			
7.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)			
7.4.5 การแบ่งแยกเครือข่าย (Segregation in networks)			
7.4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)			
7.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)			

แบบประเมินองค์การตาม ISO/IEC 27001	การดำเนินการ		
	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
7.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)			
7.5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)			
7.5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)			
7.5.3 ระบบบริหารจัดการรหัสผ่าน (Password management system)			
7.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)			
7.5.5 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)			
7.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)			
7.6 การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)			
7.6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)			
7.6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)			
7.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)			
7.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)			
7.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)			
หมวดที่ 8 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)			
8.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security requirements of information systems)			
8.1.1 การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security requirements analysis and specification)			
8.2 การประมวลผลสารสนเทศในแอพพลิเคชัน (Correct processing in applications)			
8.2.1 การตรวจสอบข้อมูลนำเข้า (Input data validation)			
8.2.2 การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of internal processing)			
8.2.3 การตรวจสอบความถูกต้องของข้อความ (Message integrity)			
8.2.4 การตรวจสอบข้อมูลนำออก (Output data validation)			

แบบประเมินองค์การตาม ISO/IEC 27001	การดำเนินการ		
	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
8.3 มาตรการการเข้ารหัสข้อมูล (Cryptographic controls)			
8.3.1 นโยบายการใช้งานการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)			
8.3.2 การบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key management)			
8.4 การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of system files)			
8.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)			
8.4.2 การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ (Protection of system test data)			
8.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)			
8.5 การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน (Security in development and support processes)			
8.5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change control procedures)			
8.5.2 การตรวจสอบการทำงานของแอพพลิเคชันภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes)			
8.5.3 การจำกัดการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต (Restrictions on changes to software packages)			
8.5.4 การป้องกันการรั่วไหลของสารสนเทศ (Information leakage)			
8.5.5 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)			
8.6.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)			
หมวดที่ 9 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)			
9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events and weaknesses)			
9.1.1 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events)			
9.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)			
9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of information security incidents and improvements)			
9.2.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)			

แบบประเมินองค์การตาม ISO/IEC 27001	การดำเนินการ		
	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
9.2.2 การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from security incidents)			
9.2.3 การเก็บรวบรวมหลักฐาน (Collection of evidence)			
หมวดที่ 10 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)			
10.1 หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Information security aspects of business continuity management)			
10.1.1 กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ (Including information security in the business continuity management process)			
10.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)			
10.1.3 การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ (Developing and implementing continuity plans including information security)			
10.1.4 การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity planning framework)			
10.1.5 การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ (Testing, maintaining and re-assessing business continuity plans)			
หมวดที่ 11 การปฏิบัติตามข้อกำหนด (Compliance)			
11.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirements)			
11.1.1 การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย (Identification of applicable legislation)			
11.1.2 การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual property rights (IRP))			
11.1.3 การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร (Protection of organizational records)			
11.1.4 การป้องกันข้อมูลส่วนตัว (Data protection and privacy of personal information)			
11.1.5 การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of misuse of information processing facilities)			
11.1.6 การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด (Regulation of cryptographic controls)			
11.2 การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with security policies and standards, and technical compliance)			
11.2.1 การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย (Compliance with security policies and standards)			
11.2.2 การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร (Technical compliance checking)			

แบบประเมินองค์การตาม ISO/IEC 27001	การดำเนินการ		
	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
11.3 การตรวจประเมินระบบสารสนเทศ (Information systems audit considerations)			
11.3.1 มาตรการการตรวจประเมินระบบสารสนเทศ (Information systems audit controls)			
11.3.2 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of information systems audit tools)			