...making excellence a habit.™

ISO/IEC FDIS 27001:2022

Information security, cybersecurity and privacy protection - Information security management systems

(Rev 11/09/2022)

Just for Customer
Guide Series

BSI, a Royal Charter Company

4 Context of the organization (บริบทขององค์กร)	
4.1 Understanding the organization and its context The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system. NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.4.1 of ISO 31000:2018[5].	**4.1 ความเข้าใจองค์กรและบริบทขององค์กร** องค์กรต้องกำหนดประเด็นภายนอกและภายในที่เกี่ยวข้องกับวัตถุประสงค์และที่ส่งผลต่อความสามารถในการบรรลุผลลัพธ์ตามที่ตั้งใจไว้ของระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ **หมายเหตุ** การกำหนดประเด็นเหล่านี้ อ้างถึงการจัดทำบริบทภายนอกและภายในขององค์กร ซึ่งพิจารณาตามข้อกำหนด 5.4.1 ของมาตรฐาน ISO 31000:2018[5].
4.2 Understanding the needs and expectations of interested parties The organization shall determine: a) interested parties that are relevant to the information security management system; b) the relevant requirements of these interested parties; c) which of these requirements will be addressed through the information security management system. NOTE The requirements of interested parties can include legal and regulatory requirements and contractual obligations.	**4.2 ความเข้าใจความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย** องค์กรต้องกำหนด: a) ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ b) ข้อกำหนดที่เกี่ยวข้องของผู้มีส่วนได้ส่วนเสียเหล่านี้ c) ข้อกำหนดเหล่านี้จะจัดการผ่านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ **หมายเหตุ** ข้อกำหนดของผู้มีส่วนได้ส่วนเสีย อาจรวมถึงกฎหมาย ข้อกำหนด กฎระเบียบบังคับ และข้อผูกผันตามสัญญา
4.3 Determining the scope of the information security management system The organization shall determine the boundaries and applicability of the information security management system to establish its scope. When determining this scope, the organization shall consider: a) the external and internal issues referred to in 4.1; b) the requirements referred to in 4.2; c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations. The scope shall be available as documented information.	**4.3 การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ** องค์กรต้องกำหนดขอบเขตและการบังคับใช้ของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อจัดตั้งขอบเขต เมื่อกำหนดขอบเขตนี้ องค์กรต้องพิจารณา: a) ประเด็นภายนอกและภายในที่อ้างถึงในข้อ 4.1; b) ข้อกำหนดที่อ้างถึงในข้อ 4.2; c) ความสัมพันธ์เชื่อมโยงและขึ้นต่อกันระหว่างกิจกรรมที่องค์กรดำเนินงานเอง และกิจกรรมเหล่านั้น ที่ดำเนินงานโดยองค์กรอื่น ขอบข่ายต้องจัดทำเป็นเอกสารสารสนเทศ
4.4 Information security management system The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.	**4.4 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ** องค์กรต้องจัดตั้ง นำไปปฏิบัติ รักษาให้คงไว้ และปรับปรุงพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง รวมถึงกระบวนการที่จำเป็นและปฏิสัมพันธ์ของกระบวนการเหล่านั้น เพื่อให้สอดคล้องกับข้อกำหนดของเอกสารฉบับนี้

5 Leadership (ภาวะผู้นำ)	
5.1 Leadership and commitment Top management shall demonstrate leadership and commitment with respect to the information security management system by: a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization; b) ensuring the integration of the information security management system requirements into the organization's processes; c) ensuring that the resources needed for the information security management system are available; d) communicating the importance of effective information security management and of conforming to the information security management system requirements; e) ensuring that the information security management system achieves its intended outcome(s); f) directing and supporting persons to contribute to the effectiveness of the information security management system; g) promoting continual improvement; and h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility. NOTE Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.	**5.1 ภาวะผู้นำและพันธสัญญา** ผู้บริหารระดับสูงต้องแสดงให้เห็นถึงความเป็นผู้นำและพันธสัญญาที่มีต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดย a) ทำให้มั่นใจว่านโยบายความมั่นคงปลอดภัยสารสนเทศ และวัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศจัดตั้งขึ้น และสอดคล้องกับทิศทางเชิงกลยุทธ์ขององค์กร; b) ทำให้มั่นใจว่ามีการบูรณาการข้อกำหนดระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเข้าไปในกระบวนการต่างๆ ขององค์กร; c) ทำให้มั่นใจว่ามีทรัพยากรที่จำเป็นสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย; d) สื่อสารถึงความสำคัญของประสิทธิผลในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและความสอดคล้องกับข้อกำหนดของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ; e) ทำให้มั่นใจว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศบรรลุผลตามที่ตั้งใจไว้; f) การสั่งการและให้การสนับสนุนผู้ที่มีส่วนร่วมต่อประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ; g) ส่งเสริมการปรับปรุงพัฒนาอย่างต่อเนื่อง; และ h) สนับสนุนบทบาทการจัดการอื่นๆ ที่เกี่ยวข้อง เพื่อแสดงความเป็นผู้นำตามขอบเขตในส่วนที่รับผิดชอบ **หมายเหตุ** อ้างอิงคำว่า "ธุรกิจ" ในเอกสารฉบับนี้สามารถตีความกว้างๆ หมายรวมถึง กิจกรรมใดๆ ที่เป็นหลักของวัตถุประสงค์ในการดำรงอยู่ขององค์กร
5.2 Policy Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; d) includes a commitment to continual improvement of the information security management system. The information security policy shall: e) be available as documented information; f) be communicated within the organization; g) be available to interested parties, as appropriate.	**5.2 นโยบาย** ผู้บริหารระดับสูงต้องกำหนดนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ ซึ่ง: a) เหมาะสมต่อวัตถุประสงค์ขององค์กร; b) รวมถึงวัตถุประสงค์ความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information Security Objectives) (ดูข้อกำหนด 6.2) หรือมีเค้าโครงร่าง (Framework) เพื่อกำหนดวัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศ; c) รวมถึงพันธสัญญา (Commitment) เพื่อให้เป็นไปตามข้อกำหนดต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ; และ d) รวมถึงพันธสัญญา (Commitment) เพื่อการปรับปรุงอย่างต่อเนื่องของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ นโยบายความมั่นคงปลอดภัยสารสนเทศ ต้อง e) จัดทำเป็นเอกสารสารสนเทศ f) นำไปสื่อสารภายในองค์กร และ g) จัดให้มีพร้อมแก่ผู้มีส่วนได้ส่วนเสีย ตามความเหมาะสม

5.3 Organizational roles, responsibilities and authorities Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization. Top management shall assign the responsibility and authority for: a) ensuring that the information security management system conforms to the requirements of this document; b) reporting on the performance of the information security management system to top management. NOTE Top management can also assign responsibilities and authorities for reporting performance of the information security management system within the organization.	**5.3 บทบาท ความรับผิดชอบ และอำนาจหน้าที่** ผู้บริหารระดับสูงต้องมั่นใจว่า ความรับผิดชอบและอำนาจหน้าที่สำหรับบทบาทที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ได้มีการมอบหมายและมีการสื่อสารภายในองค์กร ผู้บริหารระดับสูงต้องมอบหมายความรับผิดชอบและอำนาจหน้าที่ สำหรับ: a) ทำให้มั่นใจได้ว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศสอดคล้องตามข้อกำหนดของเอกสารฉบับนี้; และ b) รายงานถึงประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต่อผู้บริหารระดับสูง **หมายเหตุ** ผู้บริหารระดับสูงอาจมอบหมายหน้าที่ความรับผิดชอบและอำนาจหน้าที่สำหรับการรายงานประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายในองค์กรได้เช่นกัน
6 Planning (การวางแผน)	
6.1 Actions to address risks and opportunities **6.1.1 General** When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; c) achieve continual improvement. The organization shall plan: d) actions to address these risks and opportunities; and e) how to 1. integrate and implement the actions into its information security management system processes; and 2. evaluate the effectiveness of these actions. **6.1.2 Information security risk assessment** The organization shall define and apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments; b) ensures that repeated information security risk assessments produce consistent, valid and comparable results; c) identifies the information security risks: 1. apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for	**6.1 การดำเนินการเพื่อจัดการความเสี่ยงและโอกาส** **6.1.1 ทั่วไป** เมื่อทำการวางแผนสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องพิจารณาถึงประเด็นต่าง ๆ ที่อ้างถึงในข้อกำหนด 4.1 และข้อกำหนดต่างๆ ที่อ้างถึงในข้อกำหนด 4.2 และกำหนดความเสี่ยงและโอกาสที่จำเป็นต้องได้รับการจัดการ เพื่อ: a) ให้มั่นใจว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศสามารถบรรลุผลตามผลลัพธ์ที่ตั้งใจไว้; b) ป้องกันหรือลดผลกระทบที่ไม่พึงปรารถณา; c) ให้บรรลุเป้าหมายของการปรับปรุงอย่างต่อเนื่อง. องค์กรต้องวางแผน d) ดำเนินการเพื่อจัดการความเสี่ยงและโอกาส; และ e) วิธีการ 1) บูรณาการและนำการดำเนินการไปปฏิบัติให้เข้ากับกระบวนการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และ 2) ประเมินประสิทธิผลของการดำเนินการดังกล่าว **6.1.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ** องค์กรต้องกำหนดและประยุกต์ใช้กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดย a) จัดตั้งและรักษาเกณฑ์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึง 1) เกณฑ์การยอมรับความเสี่ยง และ 2) เกณฑ์สำหรับดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ b) ทำให้มั่นใจว่าการประเมินความเสี่ยงดังกล่าวสามารถทำซ้ำและได้ผลลัพธ์ที่ตรงกัน ถูกต้องและสามารถเปรียบเทียบได้ C) ระบุความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ 1) ประยุกต์ใช้กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อระบุความเสี่ยงที่เกี่ยวข้องกับการสูญเสียความลับ ความถูกต้องสมบูรณ์ และความ

information within the scope of the information security management system; and 2. identify the risk owners; d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk; e) evaluates the information security risks: 1. compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2. prioritize the analysed risks for risk treatment. The organization shall retain documented information about the information security risk assessment process. **6.1.3 Information security risk treatment** The organization shall define and apply an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results; b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; NOTE 1 Organizations can design controls as required, or identify them from any source. c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted; NOTE 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked. NOTE 3 The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed. d) produce a Statement of Applicability that contains: — the necessary controls (see 6.1.3 b) and c)); — justification for their inclusion; — whether the necessary controls are implemented or not; and — the justification for excluding any of the Annex A controls. e) formulate an information security risk treatment plan; and	พร้อมใช้งาน ของสารสนเทศภายในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และ 2) ระบุผู้เป็นเจ้าของความเสี่ยง d) วิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ 1) ประเมินผลกระทบที่เป็นไปได้ ถ้าความเสี่ยงที่ระบุไว้ในข้อกำหนด 6.1.2 c) เกิดขึ้นจริง 2) ประเมินโอกาสที่สมเหตุผลของการเกิดความเสี่ยงที่ระบุไว้ในข้อกำหนด 6.1.2 c) และ 3) กำหนดระดับค่าความเสี่ยง e) ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ 1) เปรียบเทียบผลการวิเคราะห์ความเสี่ยงกับเกณฑ์ความเสี่ยงที่สร้างขึ้นในข้อกำหนด 6.1.2 a) และ 2) จัดลำดับความสำคัญของความเสี่ยงที่ได้วิเคราะห์แล้ว เพื่อการจัดการความเสี่ยง องค์กรต้องเก็บรักษาเอกสารสนเทศ เกี่ยวกับกระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ **6.1.3 การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ** องค์กรต้องกำหนดและประยุกต์ใช้กระบวนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อ a) เลือกตัวเลือกของการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เหมาะสม โดยพิจารณาจากผลประเมินความเสี่ยง b) กำหนดมาตรการควบคุมทั้งหมดที่จำเป็น เพื่อนำไปใช้ตามตัวเลือกการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่ได้เลือกไว้ **หมายเหตุ 1** องค์กรสามารถออกแบบมาตรการควบคุมตามที่ต้องการ หรือระบุมาตรการควบคุมจากแหล่งอ้างอิงใด ๆ c) เปรียบเทียบมาตรการควบคุมที่กำหนดไว้ในข้อกำหนด 6.1.3 b) กับมาตรการควบคุมใน Annex A และทวนสอบว่าไม่มีมาตรการควบคุมที่จำเป็นใด ๆ ได้ละเว้นออกไป **หมายเหตุ 2** Annex A ประกอบด้วย รายการมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศที่เป็นไปได้ ผู้ใช้เอกสารฉบับนี้ ได้รับการชี้แนะไปที่ Annex A เพื่อให้มั่นใจว่าไม่มีมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศที่จำเป็นใด ๆ ถูกมองข้ามไป **หมายเหตุ 3** รายการมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศที่ระบุไว้ใน Annex A ไม่ใช่มาตรการควบคุมทั้งหมดทั้งสิ้น และสามารถเพิ่มเติมมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศอื่นๆ ได้หากจำเป็น d) จัดทำเอกสารแสดงการประยุกต์ใช้ ประกอบด้วย • มาตรการควบคุมที่จำเป็น (ดูข้อกำหนด 6.1.3 b) และ c)) • เหตุผลของการนำมาใช้ • ไม่ว่ามาตรการควบคุมที่จำเป็นได้นำไปปฏิบัติแล้วหรือไม่ก็ตาม และ • เหตุผลของการละเว้นมาตรการควบคุมใด ๆ ใน Annex A

f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization shall retain documented information about the information security risk treatment process. NOTE 4 The information security risk assessment and treatment process in this document aligns with the principles and generic guidelines provided in ISO 31000[5].	e) จัดทำแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และ f) ขออนุมัติแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และการยอมรับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่หลงเหลืออยู่ จากผู้เป็นเจ้าของความเสี่ยง องค์กรต้องเก็บรักษาเอกสารสนเทศ เกี่ยวกับกระบวนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ **หมายเหตุ 4** กระบวนการประเมินความเสี่ยงและกระบวนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศในเอกสารฉบับนี้ สอดคล้องกลับหลักการและแนวทางโดยทั่วไปที่ระบุไว้ในมาตรฐาน ISO 31000[5].
6.2 Information security objectives and planning to achieve them The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and results from risk assessment and risk treatment; d) be monitored; e) be communicated; f) be updated as appropriate; g) be available as documented information. The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine: h) what will be done; i) what resources will be required; j) who will be responsible; k) when it will be completed; and l) how the results will be evaluated.	**6.2 วัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศ และการวางแผนเพื่อการบรรลุผล** องค์กรต้องจัดตั้งวัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศไปยังส่วนงานและระดับที่เกี่ยวข้อง วัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศ ต้อง: a) สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ; b) สามารถวัดผลได้ (ถ้าปฏิบัติได้); c) พิจารณาถึงข้อกำหนดต่างๆ ด้านความมั่นคงปลอดภัยสารสนเทศ และผลลัพธ์จากการประเมินความเสี่ยงและการจัดการความเสี่ยง; d) ได้รับการติดตาม; e) ได้รับการสื่อสาร; f) ได้รับการปรับปรุงตามความเหมาะสม; g) จัดทำเป็นเอกสารสารสนเทศ. องค์กรต้องเก็บรักษาเอกสารสนเทศ เกี่ยวกับวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ เมื่อวางแผนวิธีการเพื่อให้บรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องกำหนด: h) กิจกรรมที่จะทำให้เสร็จ i) ทรัพยากรอะไรที่ต้องการ j) ใครเป็นผู้รับผิดชอบ k) เมื่อไหร่ที่จะแล้วเสร็จ และ l) ผลลัพธ์ที่ได้จะประเมินอย่างไร
6.3 Planning of changes When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.	**6.3 การวางแผนของการเปลี่ยนแปลง** เมื่อองค์กรกำหนดความจำเป็นในการเปลี่ยนแปลงระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ การเปลี่ยนแปลงต้องดำเนินการตามแผนที่วางไว้
7. Support (การสนับสนุน)	

7.1 Resources The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	**7.1 ทรัพยากร** องค์กรต้องกำหนด และจัดหาทรัพยากรที่จำเป็นในการจัดตั้ง การนำไปปฏิบัติ และการรักษาให้คงไว้ และการปรับปรุงพัฒนาอย่างต่อเนื่อง ของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
7.2 Competence The organization shall: a) determine the necessary competence of person(s) doing work under its control that affects its information security performance; b) ensure that these persons are competent on the basis of appropriate education, training, or experience; c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d) retain appropriate documented information as evidence of competence. NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the reassignment of current employees; or the hiring or contracting of competent persons.	**7.2 ความสามารถ** องค์กรต้อง a) กำหนดความสามารถที่จำเป็นของบุคลากรที่ปฏิบัติงานอยู่ภายใต้การควบคุมขององค์กร ซึ่งส่งผลต่อประสิทธิภาพด้านความมั่นคงปลอดภัยสารสนเทศ b) ทำให้มั่นใจว่าบุคลากรดังกล่าวมีความสามารถจากพื้นฐานทางการศึกษา การฝึกอบรม หรือประสบการณ์ทำงานที่เหมาะสม c) ถ้าเหมาะสม ดำเนินการเพื่อให้ได้มาซึ่งความสามารถที่จำเป็นนั้น และประเมินประสิทธิผลของการดำเนินการ และ d) เก็บรักษาเอกสารสนเทศ เพื่อเป็นหลักฐานแสดงความสามารถ **หมายเหตุ** การดำเนินการที่เหมาะสม อาจรวมถึง ตัวอย่างเช่น การจัดฝึกอบรม การมีพี่เลี้ยง หรือการมอบหมายงานใหม่ให้แก่พนักงานปัจจุบัน หรือ การว่าจ้างงาน หรือทำสัญญาจ้าง ผู้ที่มีความสามารถ
7.3 Awareness Persons doing work under the organization's control shall be aware of: a) the information security policy; b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c) the implications of not conforming with the information security management system requirements.	**7.3 ความตระหนัก** บุคลากรที่ปฏิบัติงานภายใต้การควบคุมขององค์กร ต้องตระหนักถึง: a) นโยบายความมั่นคงปลอดภัยสารสนเทศ; b) การมีส่วนร่วมต่อประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ รวมถึงประโยชน์ที่ได้จากการปรับปรุงประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ; และ c) ผลกระทบที่อาจตามมาของความไม่สอดคล้องกับข้อกำหนดของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
7.4 Communication The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; d) how to communicate.	**7.4 การสื่อสาร** องค์กรต้องกำหนดความจำเป็นของการสื่อสารที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ทั้งภายในและภายนอกองค์กร รวมถึง: a) สิ่งที่ต้องการสื่อสาร; b) เมื่อไรที่จะสื่อสาร; c) สื่อสารถึงใคร; d) วิธีการสื่อสาร;
7.5 Documented information **7.5.1 General** The organization's information security management system shall include: a) documented information required by this document; and b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.	**7.5 เอกสารสารสนเทศ** **7.5.1 ทั่วไป** ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ต้องรวมถึง a) เอกสารสารสนเทศที่กำหนดโดยเอกสารฉบับนี้ และ b) เอกสารสารสนเทศที่กำหนดโดยองค์กรว่าเป็นสิ่งที่จำเป็นต่อประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

NOTE The extent of documented information for an information security management system can differ from one organization to another due to:
1) the size of organization and its type of activities, processes, products and services;
2) the complexity of processes and their interactions; and
3) the competence of persons.

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:
a) identification and description (e.g. a title, date, author, or reference number);
b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and
c) review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the information security management system and by this document shall be controlled to ensure:
a) it is available and suitable for use, where and when it is needed; and
b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:
c) distribution, access, retrieval and use;
d) storage and preservation, including the preservation of legibility;
e) control of changes (e.g. version control); and
f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

หมายเหตุ ขอบเขตของเอกสารสารสนเทศที่มีการบันทึกสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศสามารถแตกต่างกันตามแต่ละองค์กร เนื่องจาก
1) ขนาดขององค์กร และประเภทของกิจกรรม กระบวนการ ผลิตภัณฑ์ และบริการ
2) ความซับซ้อนของกระบวนการ และปฏิสัมพันธ์ของกระบวนการเหล่านั้น และ
3) ความสามารถของบุคลากร

7.5.2 การจัดทำและการปรับปรุง

เมื่อจัดทำและปรับปรุงเอกสารสนเทศ องค์กรต้องมั่นใจว่ามีความเหมาะสมของ:
a) การชี้บ่งและคำอธิบาย (เช่น ชื่อเอกสาร วันที่ ผู้จัดทำ หรือเลขที่อ้างอิง);
b) รูปแบบ (เช่น ภาษาที่ใช้ เวอร์ชันของซอฟต์แวร์ กราฟิก) และสื่อบันทึก (เช่น กระดาษ อิเล็กทรอนิกส์); และ
c) การทบทวนและการอนุมัติอย่างเหมาะสม และเพียงพอ

7.5.3 การควบคุมเอกสารสารสนเทศ

เอกสารสารสนเทศที่กำหนดขึ้นโดยระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และตามเอกสารฉบับนี้ ต้องถูกควบคุม เพื่อให้มั่นใจว่า:
a) พร้อมใช้ และเหมาะสมต่อการนำไปใช้ ในสถานที่ และในเวลาที่จำเป็นต้องใช้ และ
b) ได้รับการปกป้องอย่างเพียงพอ (เช่น จากการสูญเสียความลับ การใช้งานที่ไม่เหมาะสม หรือการสูญเสียความถูกต้องสมบูรณ์)

สำหรับการควบคุมเอกสารสารสนเทศ องค์กรต้องจัดการ ดังต่อไปนี้ ตามความเหมาะสม
c) การแจกจ่าย การเข้าถึง การเรียกคืน และการนำไปใช้
d) การจัดเก็บ และการเก็บรักษา รวมถึง การคงไว้ให้สามารถอ่านออกได้
e) การควบคุมการเปลี่ยนแปลง (เช่น การควบคุมเวอร์ชัน) และ
f) การเก็บรักษา และการทำลาย

เอกสารสารสนเทศที่มาจากแหล่งภายนอก ที่กำหนดโดยองค์กรว่าเป็นสิ่งที่จำเป็นต่อการวางแผนและการดำเนินงานของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องได้รับการชี้บ่งตามความเหมาะสม และได้รับการควบคุม

หมายเหตุ การเข้าถึงสามารถรวมถึง การตัดสินใจเกี่ยวกับการได้รับอนุญาตให้เรียกดูข้อมูลเอกสารเท่านั้น หรือการได้รับอนุญาตและให้อำนาจในการเรียกดูและเปลี่ยนแปลงข้อมูล เป็นต้น

8. Operation (การดำเนินการ)

8.1 Operational planning and control The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by: — establishing criteria for the processes; — implementing control of the processes in accordance with the criteria. Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.	**8.1 การวางแผนปฏิบัติการและควบคุม** องค์กรต้องวางแผน นำไปปฏิบัติ และควบคุมกระบวนการที่จำเป็นเพื่อให้เป็นไปตามข้อกำหนด และปฏิบัติตามสิ่งที่กำหนดไว้ในข้อกำหนด 6 โดย: - จัดทำหลักเกณฑ์สำหรับกระบวนการ - ดำเนินการควบคุมกระบวนการตามหลักเกณฑ์ที่กำหนดไว้ เอกสารสารสนเทศจะต้องจัดเก็บไว้ตามปริมาณเท่าที่จำเป็นเพื่อให้มั่นใจว่ากระบวนการได้ดำเนินการตามแผนที่วางไว้ องค์กรต้องควบคุมการเปลี่ยนแปลงตามแผนที่ได้วางไว้ และทบทวนผลที่ตามมาของการเปลี่ยนแปลงที่ไม่ได้ตั้งใจ เพื่อดำเนินการลดผลกระทบด้านลบใด ๆ ตามความจำเป็น องค์กรต้องมั่นใจว่ามีการควบคุมกระบวนการ ผลิตภัณฑ์ หรือบริการจากภายนอกที่เกี่ยวข้องกับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ
8.2 Information security risk assessment The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). The organization shall retain documented information of the results of the information security risk assessments.	**8.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ** องค์กรต้องทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามช่วงเวลาที่ได้วางแผนไว้ หรือเมื่อการเปลี่ยนแปลงที่มีนัยสำคัญถูกเสนอให้พิจารณาหรือมีเกิดขึ้น โดยพิจารณาตามเกณฑ์ที่จัดทำขึ้นในข้อกำหนด 6.1.2 a) องค์กรต้องเก็บรักษาเอกสารสนเทศ ที่เป็นผลลัพธ์ของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
8.3 Information security risk treatment The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.	**8.3 การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ** องค์กรต้องปฏิบัติตามแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องเก็บรักษาเอกสารสนเทศ ที่เป็นผลลัพธ์ของการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
9. Performance evaluation (การประเมินผลการปฏิบัติงาน)	
9.1 Monitoring, measurement, analysis and evaluation The organization shall determine: a) what needs to be monitored and measured, including information security processes and controls; b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid; c) when the monitoring and measuring shall be performed; d) who shall monitor and measure; e) when the results from monitoring and measurement shall be analysed and evaluated; f) who shall analyse and evaluate these results.	**9.1 การเฝ้าติดตาม ตรวจวัด วิเคราะห์ และประเมินผล** องค์กรต้องกำหนด a) สิ่งที่ต้องได้รับการเฝ้าติดตามและตรวจวัด ซึ่งรวมถึงกระบวนการและมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ b) วิธีการสำหรับการเฝ้าติดตาม ตรวจวัด วิเคราะห์ การประเมินผลที่เหมาะสม เพื่อให้มั่นใจว่าผลที่ได้ถูกต้อง วิธีการที่เลือกใช้ควรให้ผลลัพธ์ที่ถูกต้องที่สามารถเปรียบเทียบได้ และทำซ้ำได้ c) เมื่อไรที่ต้องเฝ้าติดตามและวัดผล d) ใครต้องเฝ้าติดตามและวัดผล e) เมื่อไรที่ผลที่ได้จากการเฝ้าติดตามและวัดผลต้องนำมาวิเคราะห์และประเมินผล และ f) ใครต้องวิเคราะห์และประเมินผลดังกล่าว

Documented information shall be available as evidence of the results. The organization shall evaluate the information security performance and the effectiveness of the information security management system.	เอกสารสารสนเทศจะต้องจัดทำเพื่อเป็นหลักฐานแสดงผลลัพธ์ องค์กรต้องประเมินประสิทธิภาพด้านความมั่นคงปลอดภัยสารสนเทศและประสิทธิภาพของระบบการจัดการด้านความมั่นคงปลอดภัยสารสนเทศ
9.2 Internal audit **9.2.1 General** The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system: a) conforms to 1) the organization's own requirements for its information security management system; 2) the requirements of this document; b) is effectively implemented and maintained. **9.2.2 Internal audit programme** The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits. The organization shall: a) define the audit criteria and scope for each audit; b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process; c) ensure that the results of the audits are reported to relevant management; Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.	**9.2 การตรวจประเมินภายใน** **9.2.1 ทั่วไป** องค์กรต้องดำเนินการตรวจประเมินภายในตามรอบระยะเวลาที่กำหนด เพื่อให้ข้อมูลที่แสดงว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ: a) สอดคล้องกับ 1) ข้อกำหนดขององค์กรเอง สำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ; 2) ข้อกำหนดของเอกสารฉบับนี้; b) ได้นำไปปฏิบัติและรักษาให้คงไว้อย่างมีประสิทธิผล **9.2.2 โปรแกรมตรวจสอบภายใน** องค์กรต้องวางแผน จัดตั้ง นำไปปฏิบัติ และรักษาให้คงไว้ของโปรแกรมการตรวจประเมิน (Audit Programme) ซึ่งรวมถึงความถี่ วิธีการ หน้าที่ความรับผิดชอบ ข้อกำหนดของการวางแผน และการรายงาน เมื่อจัดตั้งโปรแกรมการตรวจประเมินภายใน องค์กรต้องพิจารณาถึงความสำคัญของกระบวนการที่เกี่ยวข้องและผลการตรวจประเมินครั้งก่อน องค์กรต้อง a) กำหนดเกณฑ์การตรวจประเมิน และขอบเขตสำหรับการตรวจประเมินแต่ละครั้ง b) คัดเลือกผู้ตรวจประเมินและดำเนินการตรวจประเมิน เพื่อให้มั่นใจได้ถึงความเป็นกลาง และความเป็นธรรมของกระบวนการตรวจประเมิน c) มั่นใจว่าผลที่ได้จากการตรวจประเมินได้นำไปรายงานต่อผู้บริหารที่เกี่ยวข้อง; เอกสารสารสนเทศจะต้องจัดทำเพื่อเป็นหลักฐานของการดำเนินการตามโปรแกรมการตรวจประเมินและผลการตรวจประเมิน

9.3 Management review **9.3.1 General** Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. **9.3.2 Management review inputs** The management review shall include consideration of: a) the status of actions from previous management reviews; b) changes in external and internal issues that are relevant to the information security management system; c) changes in needs and expectations of interested parties that are relevant to the information security management system; d) feedback on the information security performance, including trends in: 1) nonconformities and corrective actions; 2) monitoring and measurement results; 3) audit results; 4) fulfilment of information security objectives; e) feedback from interested parties; f) results of risk assessment and status of risk treatment plan; g) opportunities for continual improvement. **9.3.3 Management review results** The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. Documented information shall be available as evidence of the results of management reviews.	**9.3 การทบทวนของฝ่ายบริหาร** **9.3.1 ทั่วไป** ผู้บริหารระดับสูงต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรตามรอบระยะเวลาที่กำหนด เพื่อให้มั่นใจถึงความเหมาะสม เพียงพอ และประสิทธิผล ของระบบ **9.3.2 ผู้บริหารทบทวนปัจจัยการผลิต** การทบทวนของฝ่ายบริหาร ต้องรวมถึงการพิจารณา a) สถานะของการดำเนินงานจากการทบทวนของฝ่ายบริหารครั้งก่อน; b) การเปลี่ยนแปลงของประเด็นภายในและภายนอกที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ; c) การเปลี่ยนแปลงความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ; d) ผลตอบกลับจากประสิทธิภาพของความมั่นคงปลอดภัยสารสนเทศ รวมถึงแนวโน้ม; 1) ความไม่สอดคล้อง และการดำเนินการแก้ไข; 2) ผลลัพธ์ของการเฝ้าติดตามและวัดผล; 3) ผลลัพธ์จากการตรวจประเมิน; 4) ความสำเร็จของวัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศ; e) ผลตอบกลับจากผู้มีส่วนได้ส่วนเสีย; f) ผลลัพธ์จากการประเมินความเสี่ยง และสถานะของแผนการจัดการความเสี่ยง; g) โอกาสสำหรับการปรับปรุงพัฒนาอย่างต่อเนื่อง **9.3.3 ผลการทบทวนของฝ่ายบริหาร** ผลลัพธ์การทบทวนของฝ่ายบริหาร ต้องรวมถึง การตัดสินใจที่เกี่ยวกับการปรับปรุงพัฒนาอย่างต่อเนื่อง และความจำเป็นใด ๆ เพื่อการเปลี่ยนแปลงต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เอกสารสารสนเทศจะต้องจัดทำเพื่อเป็นหลักฐานแสดงผลลัพธ์การทบทวนของฝ่ายบริหาร
10. Improvement (การปรับปรุง)	
10.1 Continual improvement The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.	**10.1 การปรับปรุงอย่างต่อเนื่อง** องค์กรต้องทำการปรับปรุงความเหมาะสม ความเพียงพอ และประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

10.2 Nonconformity and corrective action When a nonconformity occurs, the organization shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it; 2) deal with the consequences; b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur; c) implement any action needed; d) review the effectiveness of any corrective action taken; and e) make changes to the information security management system, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. Documented information shall be available as evidence of: f) the nature of the nonconformities and any subsequent actions taken, g) the results of any corrective action.	**10.2 ความไม่สอดคล้องและการปรับปรุงแก้ไข** เมื่อความไม่สอดคล้องเกิดขึ้น องค์กรต้อง: a) ตอบสนองต่อความไม่สอดคล้อง และตามความเหมาะสม 1) ดำเนินการเพื่อควบคุมและแก้ไข; 2) รับมือกับผลกระทบที่ตามมา b) ประเมินความจำเป็นสำหรับดำเนินการขจัดสาเหตุของความไม่สอดคล้อง เพื่อไม่ให้ความไม่สอดคล้องเกิดขึ้นซ้ำ หรือไม่เกิดขึ้นที่อื่น ๆ โดย 1) ทบทวนความไม่สอดคล้อง 2) ระบุสาเหตุของความไม่สอดคล้อง และ 3) ระบุ ถ้าความไม่สอดคล้องที่คล้ายกันมีอยู่ หรือสามารถมีโอกาสเกิดขึ้นได้ c) ดำเนินการปฏิบัติที่จำเป็น d) ทบทวนประสิทธิผลของการปฏิบัติการแก้ไข และ e) ทำการเปลี่ยนแปลงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ถ้าจำเป็น การปฏิบัติการแก้ไขต้องเหมาะสมต่อผลกระทบของความไม่สอดคล้องที่พบ เอกสารสารสนเทศจะต้องจัดทำเพื่อเป็นหลักฐานแสดง f) ลักษณะของความไม่สอดคล้อง และการปฏิบัติใดๆ ที่ได้ดำเนินการ และ g) ผลลัพธ์ของการปฏิบัติการแก้ไข
Annex A	
Table A.1 — Information security controls **A.5 Organizational controls** **A.5.1 Policies for information security** **Control** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur. **A.5.2 Information security roles and responsibilities** **Control** Information security roles and responsibilities shall be defined and allocated according to the organization needs. **A.5.3 Segregation of duties** **Control** Conflicting duties and conflicting areas of responsibility shall be segregated. **A.5.4 Management responsibilities** **Control**	**ตาราง A.1 — การควบคุมความมั่นคงปลอดภัยสารสนเทศ** **A.5 มาตรการควบคุมขององค์กร** **A.5.1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ** **มาตรการควบคุม** นโยบายความมั่นคงปลอดภัยสารสนเทศและนโยบายเฉพาะเรื่องต้องมีการกำหนด อนุมัติโดยผู้บริหาร, เผยแพร่, สื่อสาร และบุคลากรที่เกี่ยวข้องและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องรับทราบ และทบทวนตามอบระยะเวลาที่กหนดและเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้น **A.5.2 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ** **มาตรการควบคุม** บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศต้องถูกกำหนดและมอบหมายงานตามความต้องการขององค์กร **A.5.3 การแบ่งงานและหน้าที่ความรับผิดชอบ** **มาตรการควบคุม** งานและหน้าที่รับผิดชอบที่ขัดแย้งกันต้องแบ่งแยกออกจากกัน **A.5.4 หน้าที่ความรับผิดชอบของผู้บริหาร** **มาตรการควบคุม**

Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	ผู้บริหารต้องกำหนดให้บุคลากรทุกคนใช้ความมั่นคงปลอดภัยสารสนเทศตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายเฉพาะเรื่อง และขั้นตอนปฏิบัติขององค์กรที่จัดทำขึ้น
A.5.5 Contact with authorities **Control** The organization shall establish and maintain contact with relevant authorities.	**A.5.5 การติดต่อหน่วยงานผู้มีอำนาจ** **มาตรการควบคุม** องค์กรต้องจัดทำและรักษาไว้ซึ่งการติดต่อกับหน่วยงานผู้มีอำนาจที่เกี่ยวข้อง
A.5.6 Contact with special interest groups **Control** The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	**A.5.6 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ** **มาตรการควบคุม** องค์กรต้องจัดทำและรักษาไว้ซึ่งการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกันหรือกลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย และสมาคมวิชาชีพ
A.5.7 Threat intelligence **Control** Information relating to information security threats shall be collected and analysed to produce threat intelligence.	**A.5.7 ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม** **มาตรการควบคุม** ข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศจะถูกรวบรวมและวิเคราะห์เพื่อสร้างข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม
A.5.8 Information security in project management **Control** Information security shall be integrated into project management.	**A.5.8 ความมั่นคงปลอดภัยสารสนเทศในการบริการโครงการ** **มาตรการควบคุม** ความมั่นคงปลอดภัยสารสนเทศจะถูกผนวกรวมเข้ากับการบริหารโครงการ
A.5.9 Inventory of information and other associated assets **Control** An inventory of information and other associated assets, including owners, shall be developed and maintained.	**A.5.9 บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ** **มาตรการควบคุม** บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ รวมถึงความเป็นเจ้าของ ต้องได้รับการพัฒนาและรักษาให้คงไว้
A.5.10 Acceptable use of information and other associated assets **Control** Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	**A.5.10 การใช้งานข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ อย่างเหมาะสม** **มาตรการควบคุม** หลักเกณฑ์การใช้งานอย่างเหมาะสมและขั้นตอนปฏิบัติสำหรับการจัดการข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ จะต้องถูกกำหนด จัดทำเป็นเอกสาร และนำไปปฏิบัติ
A.5.11 Return of assets **Control** Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	**A.5.11 การคืนทรัพย์สิน** **มาตรการควบคุม** บุคลากรและผู้มีส่วนได้ส่วนเสียตามความเหมาะสม ต้องคืนทรัพย์สินทั้งหมดขององค์กรที่ตนถือครองไว้ เมื่อมีการเปลี่ยนแปลงหรือสิ้นสภาพการว่าจ้างงาน สิ้นสุดสัญญาหรือข้อตกลง
A.5.12 Classification of information **Control** Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	**A.5.12 การจัดหมวดหมู่ของสารสนเทศ** **มาตรการควบคุม** สารสนเทศต้องได้รับการแยกหมวดหมู่ตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรตามการรักษาความลับ ความถูกต้องสมบูรณ์ ความพร้อมใช้งาน และข้อกำหนดของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง

A.5.13 Labelling of information
Control
An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

A.5.14 Information transfer
Control
Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.

A.5.15 Access control
Control
Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.

A.5.16 Identity management
Control
The full life cycle of identities shall be managed.

A.5.17 Authentication information
Control
Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.

A.5.18 Access rights
Control
Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.

A.5.19 Information security in supplier relationships
Control
Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.

A.5.20 Addressing information security within supplier agreements
Control

A.5.13 การทำป้ายชี้บ่งสารสนเทศ
มาตรการควบคุม
ชุดขั้นตอนปฏิบัติงานที่เหมาะสมสำหรับการทำป้ายชี้บ่งสารสนเทศ ต้องจัดทำและนำไปปฏิบัติตามให้สอดคล้องกับวิธีการจัดหมวดหมู่สารสนเทศที่องค์กรกำหนดไว้

A.5.14 การถ่ายโอนข้อมูล
มาตรการควบคุม
หลักเกณฑ์การถ่ายโอนข้อมูล, ขั้นตอนปฏิบัติ, หรือข้อตกลงในการถ่ายโอนข้อมูล ต้องถูกนำมาใช้สำหรับการถ่ายโอนข้อมูลทุกประเภทภายในองค์กร และระหว่างองค์กรกับหน่วยงานภายนอก

A.5.15 การควบคุมการเข้าถึง
มาตรการควบคุม
ข้อบังคับในการควบคุมการเข้าถึงสารสนเทศและทรัพย์สินที่เกี่ยวข้องอื่น ๆ ทางกายภาพและทางตรรกะ จะต้องจัดทำขึ้นและนำไปปฏิบัติตามข้อกำหนดทางธุรกิจและข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

A.5.16 การบริหารจัดการพิสูจน์ตัวตน
มาตรการควบคุม
วงจรชีวิตของการพิสูจน์ตัวตนจะต้องได้รับการจัดการ

A.5.17 ข้อมูลในการพิสูจน์ตัวตน
มาตรการควบคุม
การจัดสรรและการจัดการข้อมูลในการพิสูจน์ตัวตนจะต้องถูกควบคุมโดยกระบวนการบริหารจัดการ รวมถึงการให้คำแนะนำบุคลากรในการจัดการข้อมูลการพิสูจน์ตัวตนอย่างเหมาะสม

A.5.18 สิทธิ์การเข้าถึง
มาตรการควบคุม
สิทธิ์การเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ จะต้องมีการให้สิทธิ์ การทบทวน การแก้ไข และการถอดถอนตามนโยบายเฉพาะขององค์กรและข้อบังคับสำหรับการควบคุมการเข้าถึง

A.5.19 ความมั่นคงปลอดภัยสารสนเทศในความสัมพันธ์กับผู้ให้บริการภายนอก
มาตรการควบคุม
กระบวนการและขั้นตอนปฏิบัติจะต้องกำหนดและนำไปปฏิบัติเพื่อจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการใช้ผลิตภัณฑ์หรือบริการของผู้ให้บริการภายนอก

A.5.20 การระบุความมั่นคงปลอดภัยสารสนเทศในข้อตกลงของผู้ให้บริการภายนอก
มาตรการควบคุม
ข้อกำหนดที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ ต้องจัดทำขึ้นและตกลงร่วมกันกับผู้ให้บริการภายนอกแต่ละรายตามประเภทของความสัมพันธ์กับผู้ให้บริการภายนอก

Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship. **A.5.21 Managing information security in the information and communication technology (ICT) supply chain** **Control** Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain. **A.5.22 Monitoring, review and change management of supplier services** **Control** The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery. **A.5.23 Information security for use of cloud services** **Control** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements. **A.5.24 Information security incident management planning and preparation** **Control** The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. **A.5.25 Assessment and decision on information security events** **Control** The organization shall assess information security events and decide if they are to be categorized as information security incidents. **A.5.26 Response to information security incidents** **Control** Information security incidents shall be responded to in accordance with the documented procedures. **A.5.27 Learning from information security incidents** **Control** Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	**A.5.21 การจัดการด้านความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่อุปทานเทคโนโลยีสารสนเทศและการสื่อสาร (ICT)** **มาตรการควบคุม** กระบวนการและขั้นตอนปฏิบัติจะต้องกำหนดและนำไปปฏิบัติเพื่อจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับห่วงโซ่อุปทานของผลิตภัณฑ์และบริการด้าน ICT **A.5.22 การติดตาม การทบทวน และการเปลี่ยนแปลงการจัดการบริการของผู้ให้บริการภายนอก** **มาตรการควบคุม** องค์กรต้องเฝ้าติดตาม ทบทวน ประเมินและบริหารจัดการการเปลี่ยนแปลงไว้ในแนวทางปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการภายนอกและการส่งมอบบริการอย่างสม่ำเสมอ **A.5.23 ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์** **มาตรการควบคุม** กระบวนการในการจัดหา การใช้ การจัดการ และการยกเลิกการใช้บริการคลาวด์ จะต้องจัดทำขึ้นตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร **A.5.24 การวางแผนและการเตรียมการ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ** **มาตรการควบคุม** องค์กรต้องวางแผนและเตรียมพร้อมสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศโดยการกำหนด จัดทำ และสื่อสารกระบวนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึง บทบาท และความรับผิดชอบ **A.5.25 การประเมินและการตัดสินใจต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ** **มาตรการควบคุม** องค์กรต้องประเมินและตัดสินใจต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ถ้าเหตุการณ์ดังกล่าวถูกจัดหมวดหมู่เป็นเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ **A.5.26 การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ** **มาตรการควบคุม** เหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ต้องได้รับการตอบสนองตามเอกสารขั้นตอนปฏิบัติ **A.5.27 การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ** **มาตรการควบคุม** ความรู้ที่ได้รับจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ต้องถูกนำไปใช้เพื่อเสริมสร้างควววามแข็งแกร่งและปรับปรุงมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ

A.5.28 Collection of evidence **Control** The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	**A.5.28 การเก็บรวบรวมหลักฐาน** **มาตรการควบคุม** องค์กรต้องจัดทำและดำเนินการตามขั้นตอนปฏิบัติ ในการระบุ การเก็บรวบรวม การจัดหา การเก็บรักษาหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
A.5.29 Information security during disruption **Control** The organization shall plan how to maintain information security at an appropriate level during disruption.	**A.5.29 ความมั่นคงปลอดภัยสารสนเทศระหว่างการหยุดชะงัก** **มาตรการควบคุม** องค์กรต้องวางแผนถึงวิธีการรักษาความมั่นคงปลอดภัยสารสนเทศในระดับที่เหมาะสมระหว่างการหยุดชะงัก
A.5.30 ICT readiness for business continuity **Control** ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	**A.5.30 ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ** **มาตรการควบคุม** ความพร้อมด้าน ICT จะต้องวางแผน ดำเนินการ รักษาไว้ และทดสอบตามวัตถุประสงค์ความต่อเนื่องทางธุรกิจและข้อกำหนดความต่อเนื่องด้าน ICT
A.5.31 Legal, statutory, regulatory and contractual requirements **Control** Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	**A.5.31 กฎหมาย ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญา** **มาตรการควบคุม** กฎหมาย ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และวิธีการขององค์กรเพื่อให้เป็นไปตามข้อกำหนดดังกล่าวจะต้องได้รับการระบุ จัดทำเป็นเอกสาร และปรับปรุงให้เป็นปัจจุบัน
A.5.32 Intellectual property rights **Control** The organization shall implement appropriate procedures to protect intellectual property rights.	**A.5.32 สิทธิในทรัพย์สินทางปัญญา** **มาตรการควบคุม** องค์กรต้องดำเนินการตามขั้นตอนที่เหมาะสมเพื่อปกป้องสิทธิในทรัพย์สินทางปัญญา
A.5.33 Protection of records **Control** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	**A.5.33 การป้องกันบันทึก** **มาตรการควบคุม** บันทึกต้องได้รับการป้องกันการสูญหาย การทำลาย การปลอมแปลง การเข้าถึงโดยไม่ได้รับอนุญาต และการเผยแพร่ออกไปโดยไม่ได้รับอนุญาต
A.5.34 Privacy and protection of personal identifiable information (PII) **Control** The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	**A.5.34 ความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล (PII)** **ควบคุม** องค์กรต้องระบุและปฏิบัติตามข้อกำหนดที่เกี่ยวกับการรักษาความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล (PII) ตามกฎหมาย ระเบียบข้อบังคับ และข้อกำหนดตามสัญญา
A.5.35 Independent review of information security **Control** The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	**A.5.35 การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ** **มาตรการควบคุม** วิธีการขององค์กรที่ใช้เพื่อบริการจัดการความมั่นคงปลอดภัยสารสนเทศ และการนำไปปฏิบัติรวมถึงบุคลากร กระบวนการ และเทคโนโลยีจะต้องได้รับการทบทวนอย่างเป็นอิสระตามช่วงเวลาที่วางแผนไว้ หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

A.5.36 Compliance with policies, rules and standards for information security **Control** Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed. **A.5.37 Documented operating procedures** **Control** Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	**A.5.36 การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ** **มาตรการควบคุม** การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร นโยบายเฉพาะ กฎระเบียบ และมาตรฐาน ต้องได้รับการทบทวนอย่างสม่ำเสมอ **A.5.37 เอกสารขั้นตอนการปฏิบัติงาน** **มาตรการควบคุม** ขั้นตอนการปฏิบัติสำหรับสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ จะต้องจัดทำเป็นเอกสารและมีพร้อมใช้แก่ผู้ใช้งานทุกคนที่จำเป็นต้องใช้
6 People control **A.6.1 Screening** **Control** Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. **A.6.2 Terms and conditions of employment** **Control** The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security. **A.6.3 Information security awareness, education and training** **Control** Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function. **A.6.4 Disciplinary process** **Control** A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation. **A.6.5 Responsibilities after termination or change of employment** **Control**	**6. ผู้ควบคุม** **A.6.1 การคัดกรอง** **มาตรการควบคุม** การตรวจสอบประวัติความเป็นมาของผู้สมัครงานทั้งหมดเพื่อเป็นพนักงานต้องดำเนินการก่อนเข้าร่วมองค์กรและดำเนินการอย่างต่อเนื่องโดยให้สอดคล้องตามกฎหมาย ระเบียบข้อบังคับ และจริยธรรมที่เกี่ยวข้องและเหมาะสมต่อข้อกำหนดทางธุรกิจ ชั้นความลับข้อมูลที่จะเข้าถึง และความเสี่ยงที่เกี่ยวข้อง **A.6.2 ข้อตกลงและเงื่อนไขการจ้างงาน** **มาตรการควบคุม** ข้อตกลงในสัญญาจ้างงานต้องกล่าวถึงหน้าที่ความรับผิดชอบของบุคลากรและขององค์กรในด้านความมั่นคงปลอดภัยสารสนเทศ **A.6.3 ความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ** **มาตรการควบคุม** บุคลากรขององค์กรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องจะต้องได้รับการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ การให้ความรู้ การฝึกอบรม และการปรับปรุงอย่างสม่ำเสมอถึงนโยบายขององค์กร นโยบายเฉพาะ และขั้นตอนปฏิบัติ ที่เกี่ยวกับด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร ที่เกี่ยวข้องกับงานที่นับผิดชอบอย่างสม่ำเสมอ **A.6.4 กระบวนการทางวินัย** **มาตรการควบคุม** กระบวนการทางวินัยจะต้องเป็นทางการและสื่อสารให้รับทราบ เพื่อลงโทษบุคลากรและผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่ฝ่าฝืน ละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ **A.6.5 ความรับผิดชอบหลังการสิ้นสภาพหรือการเปลี่ยนแปลงการจ้างงาน** **มาตรการควบคุม** ความรับผิดชอบและหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศที่ยังคงหลังการสิ้นสภาพหรือการเปลี่ยนแปลงการจ้างงาน ต้องกำหนดไว้ บังคับใช้ และสื่อสารกับบุคลากรที่เกี่ยวข้องและผู้มีส่วนได้ส่วนเสียอื่นๆ ทราบ

Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties. **A.6.6 Confidentiality or non-disclosure agreements** **Control** Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties. **A.6.7 Remote working** **Control** Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises. **A.6.8 Information security event reporting** **Control** The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	**A.6.6 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ** **มาตรการควบคุม** ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับสะท้อนให้เห็นถึงความต้องการขององค์กรในการปกป้องข้อมูล จะต้องกำหนด จัดทำเป็นเอกสาร ทบทวนอย่างสม่ำเสมอ และลงนามโดยบุคลากรและผู้มีส่วนได้ส่วนเสียอื่นๆ **A.6.7 การปฏิบัติงานจากระยะไกล** **มาตรการควบคุม** มาตรการรักษาด้านความมั่นคงปลอดภัยจะต้องนำไปปฏิบัติ เมื่อบุคลากรปฏิบัติงานจากระยะไกล เพื่อปกป้องข้อมูลที่ถูกเข้าถึง การประมวลผล หรือจัดเก็บจากภายนอกองค์กร **A.6.8 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ** **มาตรการควบคุม** องค์กรต้องจัดให้มีกลไกสำหรับบุคลากรในการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่สังเกตพบหรือต้องสงสัยผ่านช่องทางที่เหมาะสมในเวลาที่เหมาะสม
7 Physical controls **A.7.1 Physical security perimeters** **Control** Security perimeters shall be defined and used to protect areas that contain information and other associated assets. **A.7.2 Physical entry** **Control** Secure areas shall be protected by appropriate entry controls and access points. **A.7.3 Securing offices, rooms and facilities** **Control** Physical security for offices, rooms and facilities shall be designed and implemented. **A.7.4 Physical security monitoring** **Control** Premises shall be continuously monitored for unauthorized physical access. **A.7.5 Protecting against physical and environmental threats** **Control**	**7 ตัวควบคุมทางกายภาพ** **A.7.1 อาณาเขตความมั่นคงปลอดภัยทางกายภาพ** **มาตรการควบคุม** อาณาเขตความมั่นคงปลอดภัย ต้องถูกกำหนด และนำไปใช้เพื่อปกป้องพื้นที่ที่มีสารสนเทศและทรัพย์สินที่เกี่ยวข้องอื่น ๆ **A.7.2 การเข้า-ออกพื้นที่** **มาตรการควบคุม** บริเวณที่ต้องรักษาความมั่นคงปลอดภัยต้องได้รับการปกป้องโดยมาตรการควบคุมการเข้า-ออกและจุดที่เข้าถึงได้อย่างเหมาะสม **A.7.3 ความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวก** **มาตรการควบคุม** ความมั่นคงปลอดภัยทางกายภาพของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวกต่างๆ ต้องได้รับการออกแบบและนำไปประยุกต์ใช้ **A.7.4 การเฝ้าติดตามความมั่นคงปลอดภัยทางกายภาพ** **มาตรการควบคุม** สถานที่จะต้องได้รับการเฝ้าติดตามสำหรับการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาตอย่างต่อเนื่อง **A.7.5 การป้องกันภัยคุกคามทางกายภาพและสภาพแวดล้อม**

Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical.	**มาตรการควบคุม** การป้องกันภัยคุกคามทางกายภาพและสภาพแวดล้อม เช่น ภัยพิบัติทางธรรมชาติ และทางกายภาพอื่น ๆ โดยตั้งใจหรือไม่ตั้งใจ
A.7.6 Working in secure areas **Control** Security measures for working in secure areas shall be designed and implemented.	**A.7.6 การปฏิบัติงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัย** **มาตรการควบคุม** มาตรการรักษาด้านความมั่นคงปลอดภัยสำหรับการทำงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัยต้องได้รับการออกแบบและนำไปประยุกต์ใช้
A.7.7 Clear desk and clear screen **Control** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	**A.7.7 การจัดเก็บโต๊ะทำงาน และจัดการหน้าจอ** **มาตรการควบคุม** กฎเกณฑ์การจัดเก็บโต๊ะทำงานสำหรับกระดาษและสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ และกฎเกณฑ์การจัดการหน้าจอสำหรับสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ ต้องกำหนดและบังคับใช้อย่างเหมาะสม
A.7.8 Equipment siting and protection **Control** Equipment shall be sited securely and protected.	**A.7.8 การจัดวางและการป้องกันอุปกรณ์** **มาตรการควบคุม** อุปกรณ์ต้องได้รับการจัดวางอย่างปลอดภัยและได้รับการป้องกัน
A.7.9 Security of assets off-premises **Control** Off-site assets shall be protected.	**A.7.9 ความมั่นคงปลอดภัยของทรัพย์สินที่ใช้งานนอกสำนักงาน** **มาตรการควบคุม** ทรัพย์สินที่นำออกไปใช้งานนอกสำนักงานจะต้องได้รับการป้องกัน
A.7.10 Storage media **Control** Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	**A.7.10 สื่อบันทึกข้อมูล** **มาตรการควบคุม** สื่อบันทึกข้อมูลต้องได้รับการบริหารจัดการตลอดวงจรชีวิตของการจัดหา การใช้งาน การขนส่ง และการจำหน่ายตามการจัดระดับชั้นความลับขององค์กรและข้อกำหนดในการจัดการ
A.7.11 Supporting utilities **Control** Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	**A.7.11 ระบบสาธารณูปโภคสนับสนุน** **มาตรการควบคุม** สิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ ต้องได้รับการป้องกันจากความล้มเหลวของกระแสไฟฟ้า และการหยุดชะงักอื่น ๆ ที่มีสาเหตุมาจากความผิดพลาดของระบบสาธารณูปโภคสนับสนุน
A.7.12 Cabling security **Control** Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	**A.7.12 ความมั่นคงปลอดภัยของการเดินสาย** **มาตรการควบคุม** สายเคเบิลที่นำไฟฟ้า,ข้อมูล หรือสนับสนุนบริการทางข้อมูลจะต้องได้รับการปกป้องจากการขัดขวางการทำงาน การแทรกแซงสัญญาณ หรือการทำให้เสียหาย
A.7.13 Equipment maintenance **Control** Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	**A.7.13 การบำรุงรักษาอุปกรณ์** **มาตรการควบคุม** อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้อง เพื่อให้มั่นใจถึงความพร้อมใช้งาน ความถูกต้องในการทำงาน และการรักษาความลับของข้อมูล
A.7.14 Secure disposal or re-use of equipment **Control**	

Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	**A.7.14 การจำหน่ายหรือนำอุปกรณ์มาใช้ซ้ำอย่างมั่นคงปลอดภัย** **มาตรการควบคุม** อุปกรณ์ที่มีสื่อบันทึกข้อมูลจะต้องได้รับการตรวจสอบ เพื่อให้มั่นใจว่าข้อมูลที่ละเอียดอ่อนและซอฟต์แวร์ลิขสิทธิ์ที่ติดตั้งอยู่ ได้ถูกลบออก หรือเขียนทับอย่างมั่นคงปลอดภัย ก่อนนำไปจำหน่าย หรือนำมาใช้ซ้ำ
8. Technological controls **A.8.1 User end point devices** **Control** Information stored on, processed by or accessible via user end point devices shall be protected. **A.8.2 Privileged access rights** **Control** The allocation and use of privileged access rights shall be restricted and managed. **A.8.3 Information access restriction** **Control** Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control. **A.8.4 Access to source code** **Control** Read and write access to source code, development tools and software libraries shall be appropriately managed. **A.8.5 Secure authentication** **Control** Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control. **A.8.6 Capacity management** **Control** The use of resources shall be monitored and adjusted in line with current and expected capacity requirements. **A.8.7 Protection against malware** **Control** Protection against malware shall be implemented and supported by appropriate user awareness. **A.8.8 Management of technical vulnerabilities**	**8. ตัวควบคุมทางเทคโนโลยี** **A.8.1 อุปกรณ์ปลายทางของผู้ใช้** **มาตรการควบคุม** ข้อมูลที่จัดเก็บ ประมวลผลหรือเข้าถึงได้ผ่านอุปกรณ์ปลายทางของผู้ใช้ ต้องได้รับการปกป้อง **A.8.2 สิทธิพิเศษในการเข้าถึง** **มาตรการควบคุม** การจัดสรรและใช้สิทธิ์การเข้าถึงที่เป็นสิทธิพิเศษต้องถูกจำกัดและบริหารจัดการ **A.8.3 การจำกัดการเข้าถึงสารสนเทศ** **มาตรการควบคุม** การเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ ต้องถูกจำกัดตามนโยบายเฉพาะที่จัดทำไว้ในการควบคุมการเข้าถึง **A.8.4 การเข้าถึงซอร์สโค้ด** **มาตรการควบคุม** การเข้าถึงซอร์สโค้ดโดยการอ่านและเขียน เครื่องมือในการพัฒนา และซอฟต์แวร์ไลบรารี ต้องได้รับการจัดการอย่างเหมาะสม **A.8.5 การพิสูจน์ตัวตนอย่างมั่นคงปลอดภัย** **มาตรการควบคุม** เทคโนโลยีของการพิสูจน์ตัวตนอย่างมั่นคงปลอดภัยและขั้นตอนปฏิบัติ ต้องดำเนินการตามข้อจำกัดการเข้าถึงสารสนเทศและนโยบายเฉพาะเกี่ยวกับการควบคุมการเข้าถึง **A.8.6 การบริหารจัดการขีดความสามารถ** **มาตรการควบคุม** การใช้ทรัพยากรต้องได้รับการเฝ้าระวังและปรับให้สอดคล้องกับความต้องการในปัจจุบันและที่คาดการณ์ไว้ **A.8.7 การป้องกันจากโปรแกรมไม่พึงประสงค์** **มาตรการควบคุม** การป้องกันจากโปรแกรมไม่พึงประสงค์จะต้องดำเนินการและสนับสนุนโดยการสร้างความตระหนักแก่ผู้ใช้งานอย่างเหมาะสม **A.8.8 การบริหารจัดการช่องโหว่ทางเทคนิค** **มาตรการควบคุม**

Control Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	ต้องได้รับข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบสารสนเทศที่ใช้งาน, ช่องโหว่ดังกล่าวขององค์กร ต้องได้รับการประเมินและระบุมาตรการที่เหมาะสม
A.8.9 Configuration management **Control** Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	**A.8.9 การจัดการองค์ประกอบ** **มาตรการควบคุม** องค์ประกอบ รวมถึงความมั่นคงปลอดภัยขององค์ประกอบ ของฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่าย ต้องจัดทำ ทำเป็นเอกสาร นำไปปฏิบัติ เฝ้าติดตามและทบทวน
A.8.10 Information deletion **Control** Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	**A.8.10 การลบข้อมูล** **มาตรการควบคุม** ข้อมูลที่จัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์หรือสื่อบันทึกข้อมูลอื่น ๆ ต้องถูกลบออกเมื่อไม่มีความจำเป็นต้องใช้งานข้อมูลนั้นอีก
A.8.11 Data masking **Control** Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	**A.8.11 การปิดบังข้อมูล** **มาตรการควบคุม** การปิดบังข้อมูล ต้องใช้ตามนโยบายเฉพาะขององค์กรที่เกี่ยวกับการควบคุมการเข้าถึงและนโยบายเฉพาะอื่น ๆ ที่เกี่ยวข้อง และข้อกำหนดทางธุรกิจ โดยนำกฎหมายที่บังคับใช้มาพิจารณา
A.8.12 Data leakage prevention **Control** Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	**A.8.12 การป้องกันข้อมูลรั่วไหล** **มาตรการควบคุม** มาตรการป้องกันข้อมูลรั่วไหล ต้องนำไปใช้กับระบบ เครือข่าย และอุปกรณ์อื่นๆ ที่ใช้ประมวลผล จัดเก็บ หรือมีการส่งข้อมูลที่ละเอียดอ่อน
A.8.13 Information backup **Control** Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	**A.8.13 การสำรองข้อมูล** **มาตรการควบคุม** การสำรอง ข้อมูลสารสนเทศ, ซอฟต์แวร์ และระบบ ต้องได้รับการบำรุงรักษาและทดสอบอย่างสม่ำเสมอ สอดคล้องกับนโยบายเฉพาะที่ตกลงกันในการสำรองข้อมูล
A.8.14 Redundancy of information processing facilities **Control** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	**A.8.14 อุปกรณ์สำรองของสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ** **มาตรการควบคุม** สิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ ต้องดำเนินการสำรองไว้อย่างเพียงพอเพื่อให้เป็นไปตามข้อกำหนดด้านความพร้อมใช้งาน
A.8.15 Logging **Control** Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	**A.8.15 การบันทึกล็อก** **มาตรการควบคุม** ล็อกที่บันทึกกิจกรรม ข้อยกเว้น ข้อผิดพลาด และเหตุการณ์ที่เกี่ยวข้องอื่น ๆ จะต้องมีการจัดทำขึ้น จัดเก็บ ป้องกัน และวิเคราะห์

A.8.16 Monitoring activities **Control** Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	**A.8.16 การเฝ้าติดตามกิจกรรม** **มาตรการควบคุม** เครือข่าย ระบบ และแอปพลิเคชัน ต้องได้รับการเฝ้าติดตามพฤติกรรมที่ผิดปกติและการดำเนินการที่เหมาะสม เพื่อประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้น
A.8.17 Clock synchronization **Control** The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	**A.8.17 การตั้งค่านาฬิกาให้ตรงกัน** **มาตรการควบคุม** นาฬิกาของระบบประมวลผลสารสนเทศที่องค์กรใช้งาน ต้องได้รับการตั้งค่าเวลาให้ตรงกับแหล่งเทียบเวลาที่ได้รับการรับรอง
A.8.18 Use of privileged utility programs **Control** The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	**A.8.18 การใช้งานโปรแกรมยูทิลิตี้ที่ได้รับสิทธิพิเศษ** **มาตรการควบคุม** การใช้งานโปรแกรมยูทิลิตี้ ที่สามารถข้ามผ่านมาตรการควบคุมของระบบและแอพลิเคชั่นได้ ต้องถูกจำกัดและควบคุมอย่างเคร่งครัด
A.8.19 Installation of software on operational systems **Control** Procedures and measures shall be implemented to securely manage software installation on operational systems.	**A.8.19 การติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ** **มาตรการควบคุม** ต้องดำเนินการตามขั้นตอนปฏิบัติและมาตรการเพื่อจัดการการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการอย่างมั่นคงปลอดภัย
A.8.20 Networks security **Control** Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	**A.8.20 ความมั่นคงปลอดภัยของเครือข่าย** **มาตรการควบคุม** เครือข่ายและอุปกรณ์เครือข่ายต้องได้รับการรักษาความมั่นคงปลอดภัย บริหารจัดการ และควบคุมเพื่อปกป้องข้อมูลในระบบและแอปพลิเคชัน
A.8.21 Security of network services **Control** Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	**A.8.21 ความมั่นคงปลอดภัยของบริการเครือข่าย** **มาตรการควบคุม** กลไกด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดของบริการเครือข่าย ต้องได้รับการระบุ นำไปปฏิบัติ และเฝ้าติดตาม
A.8.22 Segregation of networks **Control** Groups of information services, users and information systems shall be segregated in the organization's networks.	**A.8.22 การแบ่งแยกเครือข่าย** **มาตรการควบคุม** กลุ่มบริการข้อมูลสารสนเทศ ผู้ใช้ และระบบสารสนเทศต่างๆ ต้องได้รับการแบ่งแยกออกจากเครือข่ายขององค์กร
A.8.23 Web filtering **Control** Access to external websites shall be managed to reduce exposure to malicious content.	**A.8.23 การกรองเว็บ** **มาตรการควบคุม** การเข้าถึง การเปิดเว็บไซต์ภายนอก ต้องได้รับการจัดการเพื่อลดปัจจัยเสี่ยงในการเข้าถึงเนื้อหาที่เป็นอันตราย
A.8.24 Use of cryptography **Control**	**A.8.24 กการเข้ารหัสข้อมูล** **มาตรการควบคุม**

Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	หลักเกณฑ์สำหรับการใช้งานการเข้ารหัสข้อมูลอย่างมีประสิทธิภาพ รวมถึงการบริหารจัดการกุญแจการเข้ารหัสข้อมูล ต้องได้รับการกำหนดและนำไปปฏิบัติ
A.8.25 Secure development life cycle **Control** Rules for the secure development of software and systems shall be established and applied.	**A.8.25 วงจรชีวิตการพัฒนาอย่างมั่นคงปลอดภัย** **มาตรการควบคุม** หลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบอย่างมั่นคงปลอดภัย ต้องได้รับการกำหนดและนำไปปฏิบัติ
A.8.26 Application security requirements **Control** Information security requirements shall be identified, specified and approved when developing or acquiring applications.	**A.8.26 ข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชัน** **มาตรการควบคุม** หลักเกณฑ์ด้านความมั่นคงปลอดภัยสารสนเทศจะต้องกำหนด ระบุ และอนุมัติเมื่อพัฒนาหรือจัดหาแอปพลิเคชัน
A.8.27 Secure system architecture and engineering principles **Control** Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	**A.8.27 สถาปัตยกรรมระบบและหลักการทางวิศวกรรมที่มั่นคงปลอดภัย** **มาตรการควบคุม** หลักการด้านความมั่นคงปลอดภัยทางวิศวกรรมระบบ ต้องจัดทำ ทำเป็นเอกสาร บำรุงรักษา และนำไปประยุกต์ใช้กับทุกกิจกรรมของการพัฒนาระบบสารสนเทศ
A.8.28 Secure coding **Control** Secure coding principles shall be applied to software development.	**A.8.28 การเขียนชุดคำสั่งอย่างมั่นคงปลอดภัย** **มาตรการควบคุม** หลักการในการเขียนชุดคำสั่งอย่างมั่นคงปลอดภัยเข้ารหัสที่ ต้องนำไปใช้กับการพัฒนาซอฟต์แวร์
A.8.29 Security testing in development and acceptance **Control** Security testing processes shall be defined and implemented in the development life cycle.	**A.8.29 การทดสอบความมั่นคงปลอดภัยในการพัฒนาและการยอมรับ** **มาตรการควบคุม** การทดสอบความมั่นคงปลอดภัย ต้องได้รับการกำหนดและนำไปประยุกต์ใช้ในวงจรชีวิตของการพัฒนา
A.8.30 Outsourced development **Control** The organization shall direct, monitor and review the activities related to outsourced system development.	**A.8.30 การพัฒนาโดยหน่วยงานภายนอก** **มาตรการควบคุม** องค์กรต้องกำกับดูแล เฝ้าติดตาม และทบทวนกิจกรรมที่เกี่ยวข้องกับการพัฒนาระบบจากหน่วยงานภายนอก
A.8.31 Separation of development, test and production environments **Control** Development, testing and production environments shall be separated and secured.	**A.8.31 การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริงออกจากกัน** **มาตรการควบคุม** สภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริงต้องถูกแบ่งแยกออกจากกันและรักษาความมั่นคงปลอดภัย
A.8.32 Change management **Control** Changes to information processing facilities and information systems shall be subject to change management procedures.	**A.8.32 การบริหารจัดการการเปลี่ยนแปลง** **มาตรการควบคุม** การเปลี่ยนแปลงถึงสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ และระบบสารสนเทศต้องเป็นไปตามขั้นตอนการจัดการการเปลี่ยนแปลง
A.8.33 Test information	

Control Test information shall be appropriately selected, protected and managed. **A.8.34 Protection of information systems during audit testing** **Control** Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	**A.8.33 ข้อมูลในการทดสอบ** **มาตรการควบคุม** ข้อมูลในการทดสอบต้องได้รับการคัดเลือก ปกป้อง และบริหารจัดการอย่างเหมาะสม **A.8.34 การปกป้องระบบสารสนเทศระหว่างการทดสอบในการตรวจประเมิน** **มาตรการควบคุม** การทดสอบในการตรวจประเมินและกิจกรรมการรับประกันอื่น ๆ ที่เกี่ยวข้องกับการตรวจประเมินระบบปฏิบัติการ ต้องมีการวางแผนและตกลงร่วมกันระหว่างผู้ทดสอบและผู้บริหารอย่างเหมาะสม