ISO/IEC 27001:2022

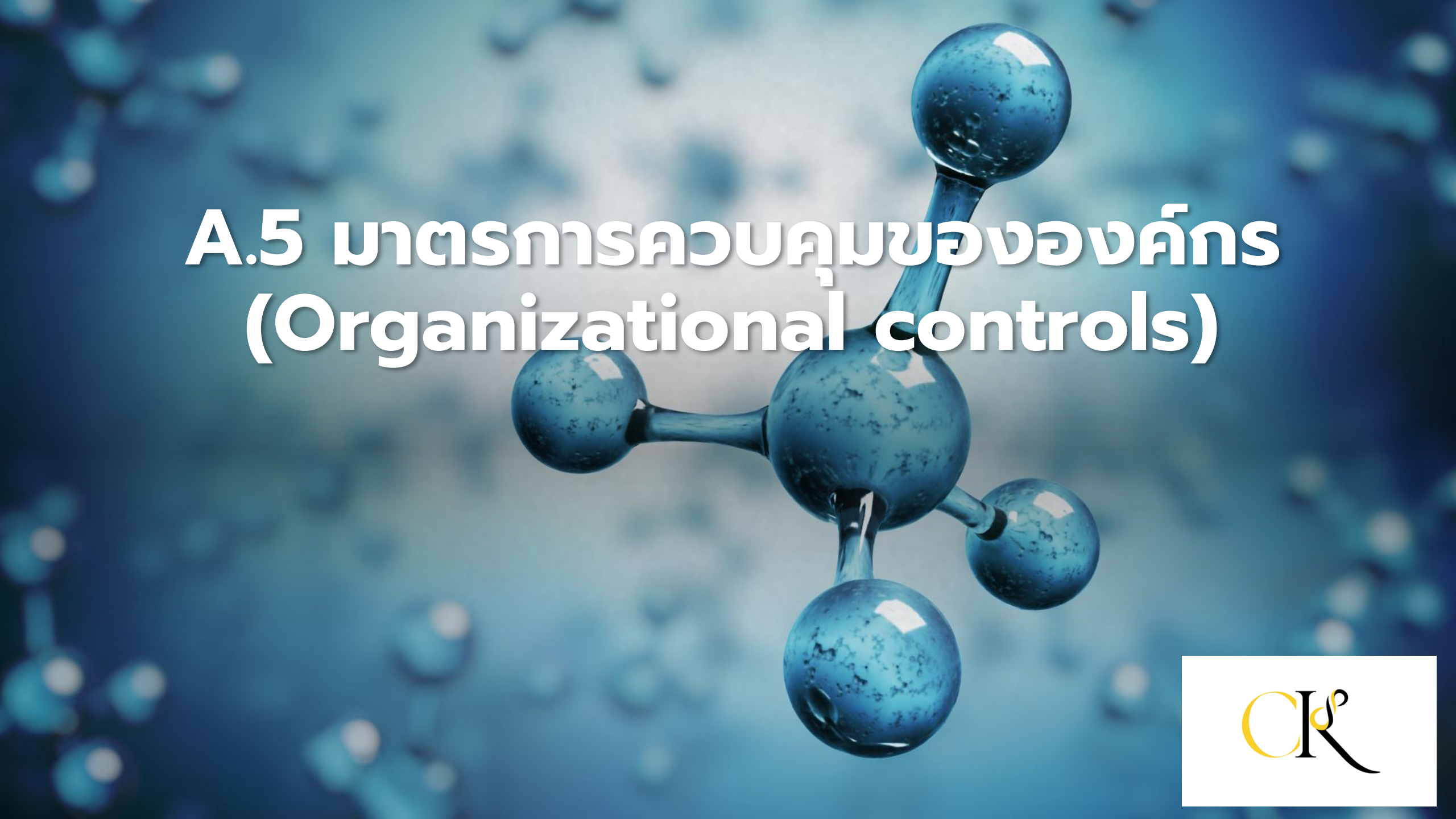
- Information security, cybersecurity and privacy protection - Information security management systems

BY: Dr.Chakkrit Khamsom
Mobile : 083-435-8785

การควบคุมความมั่นคงปลอดภัยสารสนเทศ

Information security controls

Dr.Krit
083-4358785
drchakkrit@gmail.com



A.5 มาตรการควบคุมขององค์กร (Organizational controls)

A.5 มาตรการควบคุมขององค์กร (Organizational controls)

A.5.1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ
มาตรการควบคุม : (Policies for information)
นโยบายความมั่นคงปลอดภัยสารสนเทศและนโยบายเฉพาะเรื่องต้องมีการกำหนดและถูกอนุมัติโดยผู้บริหาร แล้วถูกเผยแพร่, สื่อสาร, บุคลากรและผู้มีส่วนได้เสียที่เกี่ยวข้องรับทราบ และถูกทบทวนตามรอบระยะเวลาที่กำหนดและเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้น

A.5.2 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ : (Information security roles and responsibilities)
มาตรการควบคุม
บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศต้องถูกกำหนดและมอบหมายงานตามความต้องการขององค์กร

A.5.3 การแบ่งงานและหน้าที่ความรับผิดชอบ (Segregation of duties)
มาตรการควบคุม
งานและหน้าที่รับผิดชอบที่ขัดแย้งกันต้องแบ่งแยกออกจากกัน

A.5.4 หน้าที่ความรับผิดชอบของผู้บริหาร
มาตรการควบคุม(Management responsibilities)
ผู้บริหารต้องกำหนดให้บุคลากรทุกคนใช้สารสนเทศที่มีความมั่นคงปลอดภัยตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายเฉพาะเรื่อง และขั้นตอนปฏิบัติขององค์กรที่จัดทำขึ้น

A.5 มาตรการควบคุมขององค์กร (Organizational controls)

A.5.5 การติดต่อหน่วยงานผู้มีอำนาจ
มาตรการควบคุม(Contact with authorities)
องค์กรต้องจัดทำและรักษาไว้ซึ่งการติดต่อกับหน่วยงานผู้มีอำนาจที่เกี่ยวข้อง

A.5.6 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ(Contact with special interest groups)
มาตรการควบคุม
องค์กรต้องจัดทำและรักษาไว้ซึ่งการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกันหรือกลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย และสมาคมวิชาชีพ

A.5.7 ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม(Threat intelligence)
มาตรการควบคุม
ข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศจะถูกรวบรวมและวิเคราะห์เพื่อสร้างข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม

A.5.8 ความมั่นคงปลอดภัยสารสนเทศในการบริการโครงการ(Information security in project management)
มาตรการควบคุม
ความมั่นคงปลอดภัยสารสนเทศจะถูกผนวกรวมเข้ากับการบริหารโครงการ

A.5 มาตรการควบคุมขององค์กร (Organizational controls)

A.5.9 บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ

มาตรการควบคุม(Inventory of information and other associated assets)

บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ รวมถึงความเป็นเจ้าของ ต้องได้รับการพัฒนาและรักษาให้คงไว้

A.5.10 การใช้งานข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ อย่างเหมาะสม(Acceptable use of information and other associated assets)

มาตรการควบคุม

หลักเกณฑ์การใช้งานอย่างเหมาะสมและขั้นตอนปฏิบัติสำหรับการจัดการข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ จะต้องถูกกำหนด จัดทำเป็นเอกสาร และนำไปปภิบัติ

A.5.11 การคืนทรัพย์สิน(Return of assets)

มาตรการควบคุม

บุคลากรและผู้มีส่วนได้ส่วนเสียตามความเหมาะสม ต้องคืนทรัพย์สินทั้งหมดขององค์กรที่ตนถือครองไว้

เมื่อมีการเปลี่ยนแปลงหรือสิ้นสภาพการว่าจ้างงาน สัญญาหรือข้อตกลง

A.5.12 การจัดหมวดหมู่ของสารสนเทศ

มาตรการควบคุม (Classification of information)

สารสนเทศต้องได้รับการแยกหมวดหมู่ตามความต้องการ

ด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรตามการรักษาความลับ ความถูกต้องสมบูรณ์ ความพร้อมใช้งาน และข้อกำหนดของผู้มีส่วนได้เสียที่เกี่ยวข้อง

A.5 มาตรการควบคุมขององค์กร (Organizational controls)

A.5.13 การทำป้ายชี้บ่งสารสนเทศ(Labelling of information)

มาตรการควบคุม

ชุดขั้นตอนปฏิบัติงานที่หมาะสมสำหรับการทำป้ายชี้บ่งสารสนเทศ ต้องจัดทำและนำไปปฏิบัติตามให้สอดคล้องกับวิธีการจัดหมวดหมู่สารสนเทศที่องค์กรกำหนดไว้

A.5.14 การถ่ายโอนข้อมูล(Information transfer)

มาตรการควบคุม

หลักเกณฑ์การถ่ายโอนข้อมูล, ขั้นตอนปฏิบัติ, หรือข้อตกลงในการถ่ายโอนข้อมูล ต้องถูกนำมาใช้สำหรับการถ่ายโอนข้อมูลทุกประเภทภายในองค์กร และระหว่างองค์กรกับหน่วยงานภายนอก

A.5.15 การควบคุมการเข้าถึง(Access control)

มาตรการควบคุม

ข้อบังคับในการควบคุมการเข้าถึงสารสนเทศและทรัพย์สินที่เกี่ยวข้องอื่น ๆ ทางกายภาพและทางตรรกะ จะต้องจัดทำขึ้นและนำไปปฏิบัติตามข้อกำหนดทางธุรกิจและข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

A.5.16 การบริหารจัดการพิสูจน์ตัวตน(Identity management)

มาตรการควบคุม

ทั้งวงจรของกระบวนการพิสูจน์ตัวตนจะต้องได้รับ

การบริหารจัดการ

A.5 มาตรการควบคุมขององค์กร (Organizational controls)

A.5.17 ข้อมูลในการพิสูจน์ตัวตน(Authentication information)

มาตรการควบคุม

การจัดสรรและการจัดการข้อมูลในการพิสูจน์ตัวตนจะต้องถูกควบคุมโดยกระบวนการบริหารจัดการ รวมถึงการให้คำแนะนำบุคลากรในการจัดการข้อมูลการพิสูจน์ตัวตนอย่างเหมาะสม

A.5.18 สิทธิ์การเข้าถึง(Access rights)

มาตรการควบคุม

สิทธิ์การเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ จะต้องมีการให้สิทธิ์ การทบทวน การแก้ไข และการถอดถอนตามนโยบายเฉพาะขององค์กรและข้อบังคับสำหรับการควบคุมการเข้าถึง

A.5.19 ความมั่นคงปลอดภัยสารสนทศในความสัมพันธ์กับ

ผู้ให้บริการภายนอก(Information security in supplier relationships)

มาตรการควบคุม

กระบวนการและขั้นตอนปฏิบัติจะต้องกำหนดและนำไปปฏิบัติเพื่อจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการใช้ผลิตภัณฑ์หรือบริการ

A.5.20 การระบุความมั่นคงปลอดภัยสารสนเทศในข้อตกลงของผู้ให้บริการภายนอก(Addressing information security within supplier agreements)

มาตรการควบคุม

ข้อกำหนดที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ ต้องจัดทำขึ้นและตกลงร่วมกันกับผู้ให้บริการภายนอกแต่ละรายตามประเภทของความสัมพันธ์กับผู้ให้บริการภายนอก

A.5 มาตรการควบคุมขององค์กร (Organizational controls)

A.5.21 การจัดการด้านความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่อุปทานเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ICT (Managing information security in the information and communication technology (ICT) supply chain)

มาตรการควบคุม

กระบวนการและขั้นตอนปฏิบัติจะต้องกำหนดและนำไปปฏิบัติเพื่อจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับห่วงโซ่อุปทานของผลิตภัณฑ์และบริการด้าน ICT

A.5.22 การติดตาม การทบทวน และการเปลี่ยนแปลงการจัดการบริการของผู้ให้บริการภายนอก(Monitoring, review and change management of supplier services)

มาตรการควบคุม

องค์กรต้องเฝ้าติดตาม ทบทวน ประเมินและบริหารจัดการการเปลี่ยนแปลงตามแนวทางปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการภายนอกและการส่งมอบบริการอย่างสม่ำเสมอ

A.5.23 ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์(Information security for use of cloud services)

มาตรการควบคุม

กระบวนการในการจัดหา การใช้ การจัดการ และการยกเลิกการใช้บริการคลาวด์ จะต้องจัดทำขึ้นตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

A.5.24 การวางแผนและการเตรียมการการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ(Information security incident management planning and preparation)

มาตรการควบคุม

องค์กรต้องวางแผนและเตรียมพร้อมสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนทศ โดยการกำหนด จัดทำ และสื่อสารกระบวนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ถึงบทบาทและความรับผิดชอบ

A.5 มาตรการควบคุมขององค์กร (Organizational controls)

A.5.25 การประเมินและการตัดสินใจต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ(Assessment and decision on information security events)

มาตรการควบคุม

องค์กรต้องประเมินและตัดสินใจต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ถ้าเหตุการณ์ดังกล่าวถูกจัดหมวดหมู่เป็นเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

A.5.26 การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ(Response to information security incidents)

มาตรการควบคุม

เหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองตามเอกสารขั้นตอนปฏิบัติ

A.5.27 การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)

มาตรการควบคุม

ความรู้ที่ได้รับจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ต้องถูกนำไปใช้เพื่อเสริมสร้างความแข็งแกร่งและปรับปรุงมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ

A.5.28 การเก็บรวบรวมหลักฐาน (Collection of evidence)

มาตรการควบคุม

องค์กรต้องจัดทำและดำเนินการตามขั้นตอนปฏิบัติใน
การระบุ การเก็บรวบรวม การจัดหา การเก็บรักษาหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

A.5 มาตรการควบคุมขององค์กร (Organizational controls)

A.5.29 ความมั่นคงปลอดภัยสารสนเทศระหว่างการหยุดชะงัก (Information security during disruption)

มาตรการควบคุม

องค์กรต้องวางแผนถึงวิธีการรักษาความมั่นคงปลอดภัยสารสนเทศในระดับที่เหมาะสมระหว่างการหยุดชะงัก

A.5.30 ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity) มาตรการควบคุม

ความพร้อมด้าน ICT จะต้องวางแผน ดำเนินการ รักษาไว้ และทดสอบตามวัตถุประสงค์ความต่อเนื่องทางธุรกิจและข้อกำหนดความต่อเนื่องด้าน ICT

A.5.31 กฎหมาย ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญามาตรการควบคุม (Legal, statutory, regulatory and contractual requirements)

มาตรการควบคุม

กฎหมาย ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและวิธีการขององค์กร เพื่อให้เป็นไปตามข้อกำหนดดังกล่าวจะต้องได้รับการระบุ จัดทำเป็นเอกสาร และปรับปรุงให้เป็นปัจจุบัน

A.5.32 สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)

มาตรการควบคุม

องค์กรต้องดำเนินการตามขั้นตอนที่เหมาะสมเพื่อปกป้องสิทธิในทรัพย์สินทางปัญญา

A.5 มาตรการควบคุมขององค์กร (Organizational controls)

A.5.33 การป้องกันบันทึก **(Protection of records)**

มาตรการควบคุม

บันทึกต้องได้รับการป้องกันการสูญหาย การทำลาย

การปลอมแปลง การเข้าถึงโดยไม่ได้รับอนุญาต และการเผยแพร่ออกไปโดยไม่ได้รับอนุญาต

A.5.34 ความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล **(PII) (Privacy and protection of personal identifiable information (PII)**

มาตรการควบคุม

องค์กรต้องระบุและปฏิบัติตามข้อกำหนดที่เกี่ยวกับการรักษาความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล (PII) ตามกฎหมาย ระเบียบข้อบังคับ และข้อกำหนดตามสัญญา

A.5.35 การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ **(Independent review of information security)**

มาตรการควบคุม

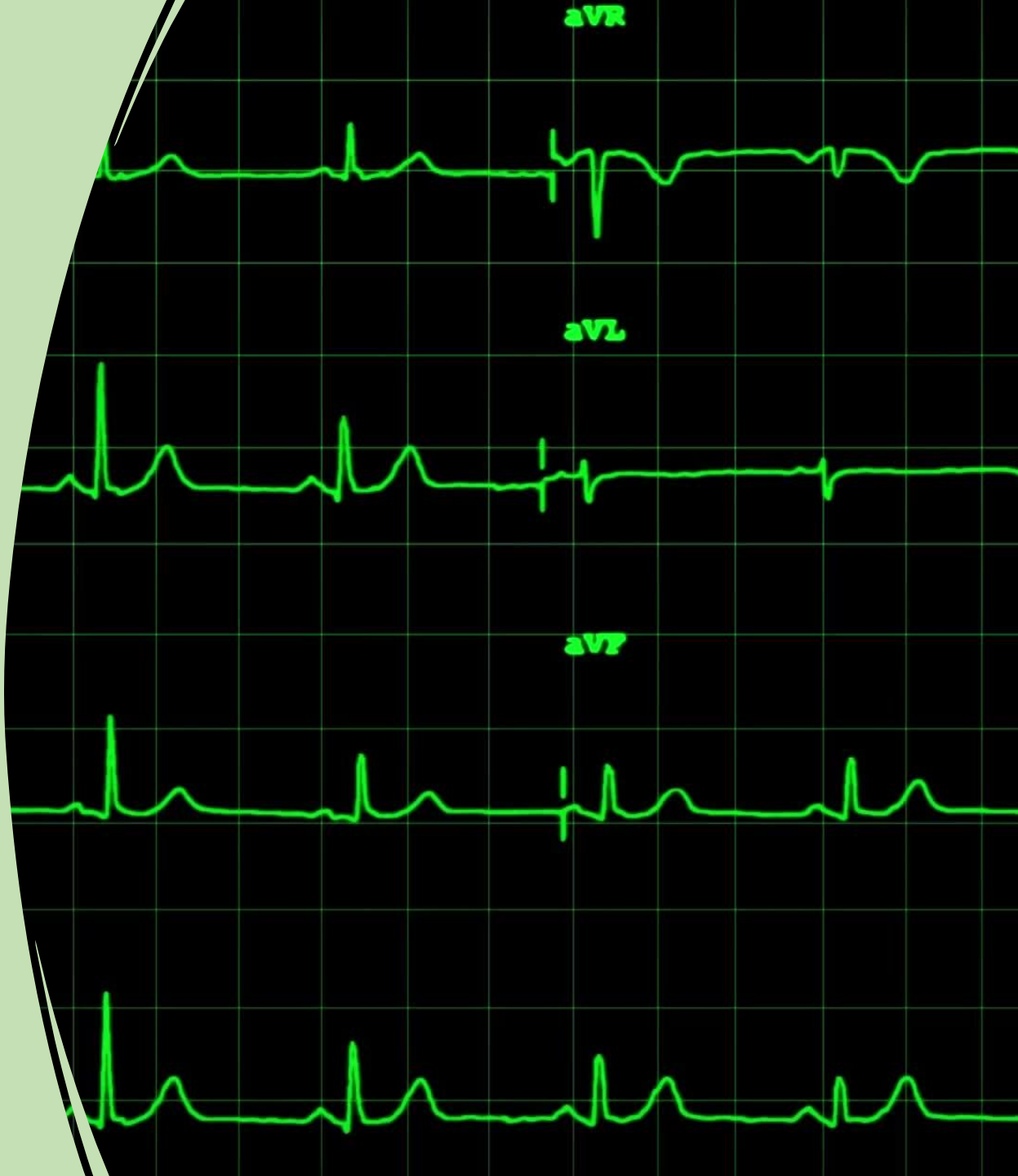
วิธีการขององค์กรที่ใช้เพื่อบริการจัดการความมั่นคงปลอดภัยสารสนเทศ และการนำไปปฏิบัติ รวมถึงบุคลากร กระบวนการ และเทคโนโลยีจะต้องได้รับการทบทวนอย่างเป็นอิสระตามช่วงเวลาที่วางแผนไว้ หรือเมื่อมีการเปลี่ยแปลงอย่างมีนัยสำคัญ

A.5.36 การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ **(Compliance with policies, rules and standards for information security)**

มาตรการควบคุม

การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร นโยบายเฉพาะกฎระเบียบ และมาตรฐาน ต้องได้รับการทบทวนอย่างสม่ำเสมอ

A.5 มาตรการควบคุมขององค์กร (Organizational controls)

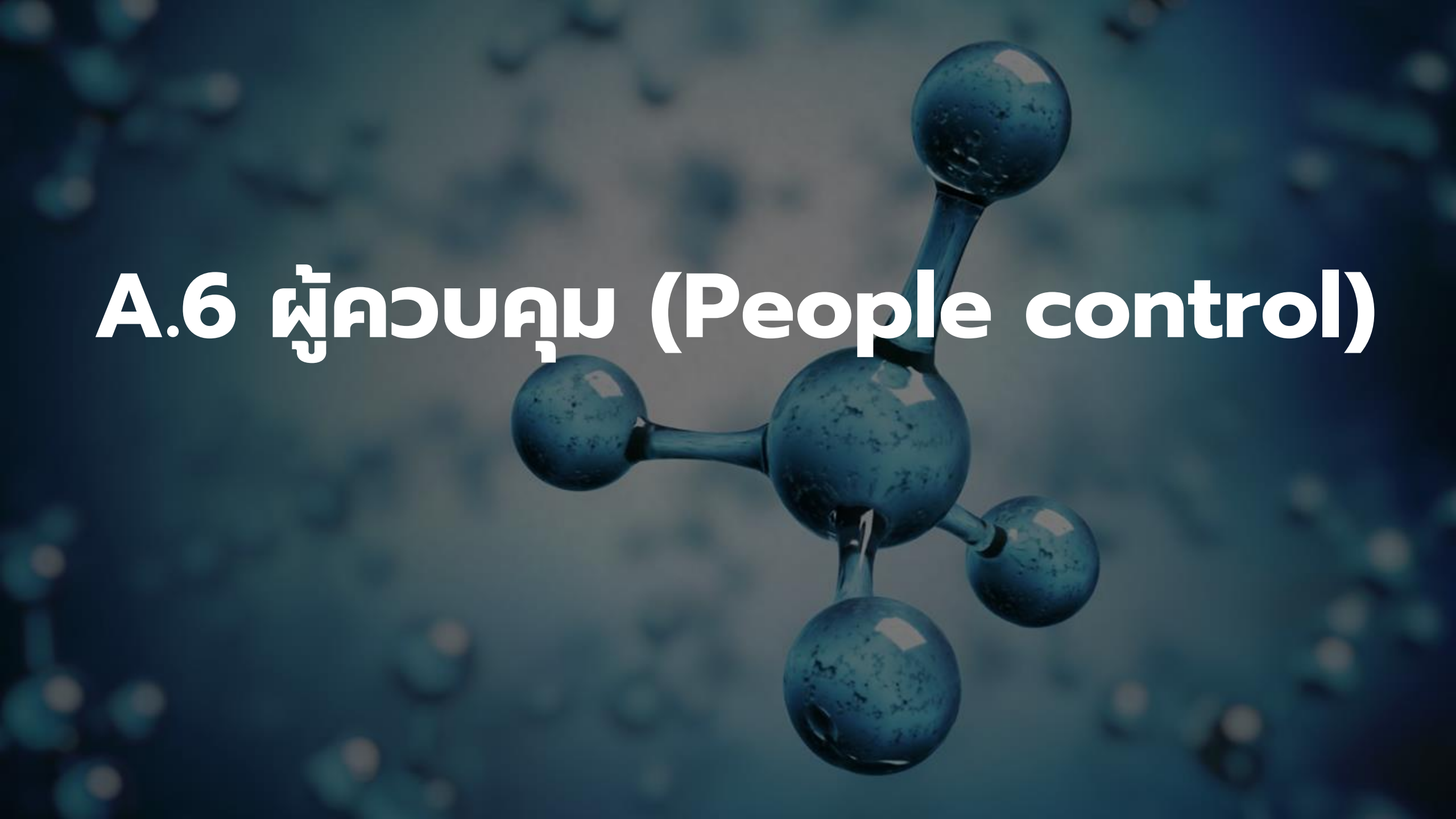


A.5.37 เอกสารขั้นตอนการปฏิบัติงาน (Documented operating procedures)

มาตรการควบคุม

ขั้นตอนการปฏิบัติสำหรับสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ จะต้องจัดทำเป็นเอกสารและมีพร้อมใช้แก่ผู้ใช้งานทุกคนที่จำเป็นต้องใช้

A.6 ผู้ควบคุม (People control)



A.6 ผู้ควบคุม (People control)

A.6.1 การคัดกรอง (Screening)

<u>มาตรการควบคุม</u>

การตรวจสอบประวัติความเป็นมาของผู้สมัครงานทั้งหมดเพื่อเป็นพนักงาน ต้องดำเนินการก่อนเข้าร่วมองค์กรและดำเนินการอย่างต่อเนื่องโดยให้สอดคล้องตามกฎหมาย ระเบียบข้อบังคับและจริยธรรมที่เกี่ยวข้องและเหมาะสมต่อข้อกำหนดทางธุรกิจ ชั้นความลับข้อมูลที่จะเข้าถึงและความเสี่ยงที่เกี่ยวข้อง

A.6.2 ข้อตกลงและเงื่อนไขการจ้างงาน(Terms and conditions of employment)

<u>มาตรการควบคุม</u>

ข้อตกลงในสัญญาจ้างงานต้องกล่าวถึงหน้าที่ความรับผิดชอบของบุคลากรและขององค์กรในด้านความมั่นคงปลอดภัยสารสนเทศ

A.6.3 ความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ(Information security awareness, education and training)

<u>มาตรการควบคุม</u>

บุคลากรขององค์กรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องจะต้องได้รับการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ

การให้ความรู้ การฝึกอบรม และการปรับปรุงอย่างสม่ำเสมอ ถึงนโยบายขององค์กร นโยบายเฉพาะ และขั้นตอนปฏิบัติที่เกี่ยวกับด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร ที่เกี่ยวข้องกับงานที่รับผิดชอบอย่างสม่ำเสมอ

A.6 ผู้ควบคุม (People control)

A.6.4 กระบวนการทางวินัย(Disciplinary process)

<u>มาตรการควบคุม</u>

กระบวนการทางวินัยจะต้องเป็นทางการและสื่อสารให้รับทราบ เพื่อลงโทษบุคลากรและผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่ฝ่าฝืนละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ

A.6.5 ความรับผิดชอบหลังการสิ้นสภาพหรือการเปลี่ยนแปลงการจ้างงาน(Responsibilities after termination or change of employment)

<u>มาตรการควบคุม</u>

ความรับผิดชอบและหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศที่ยังคงมีอยู่ หลังการสิ้นสภาพหรือการเปลี่ยนแปลง
การจ้างงาน ต้องกำหนดไว้ บังคับใช้ และสื่อสารกับบุคลากรที่เกี่ยวข้องและผู้มีส่วนได้ส่วนเสียอื่น ๆ ให้ทราบ

A.6.6 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ(Confidentiality or non-disclosure agreements)

<u>มาตรการควบคุม</u>

ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับสะท้อนให้เห็นถึงความต้องการขององค์กรในการปกป้องข้อมูล จะต้องกำหนด จัดทำเป็นเอกสาร ทบทวนอย่างสม่ำเสมอ และลงนามโดยบุคลากรและผู้มีส่วนได้ส่วนเสียอื่น ๆ

A.6 ผู้ควบคุม (People control)

A.6.7 การปฏิบัติงานจากระยะไกล (Remote working)

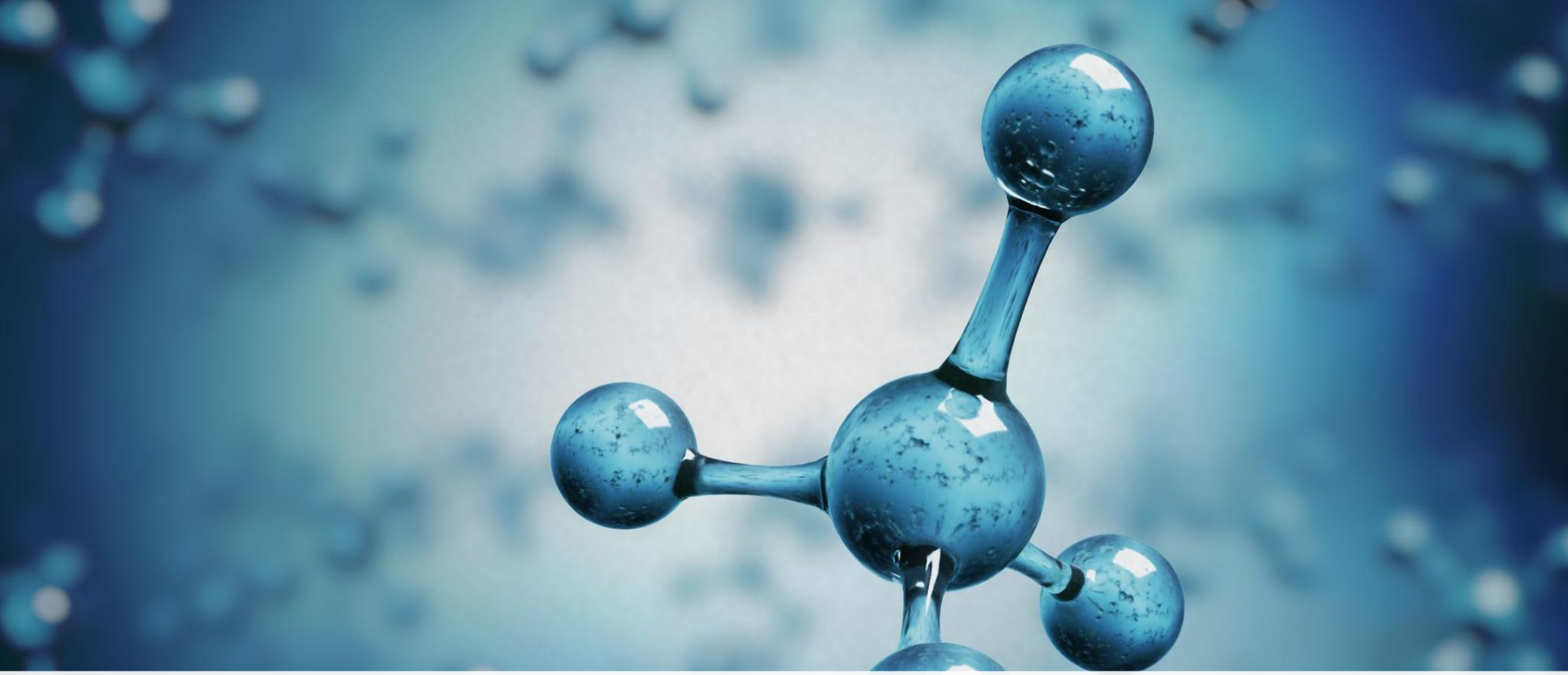
<u>มาตรการควบคุม</u>

มาตรการรักษาด้านความมั่นคงปลอดภัยจะต้องนำไปปฏิบัติ เมื่อบุคลากรปฏิบัติงานจากระยะไกล เพื่อปกป้องข้อมูลที่ถูกเข้าถึง การประมวลผล หรือจัดเก็บจากภายนอกองค์กร

A.6.8 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ(Information security event reporting)

<u>มาตรการควบคุม</u>

องค์กรต้องจัดให้มีกลไกสำหรับบุคลากรในการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่สังเกตพบหรือต้องสงสัยผ่านช่องทางที่เหมาะสมในเวลาที่เหมาะสม



A.7 ตัวควบคุมทางกายภาพ (Physical controls)

Dr.Krit
083-4358785
drchakkrit@gmail.com

A.7 ตัวควบคุมทางกายภาพ (Physical controls)

A.7.1 อาณาเขตความมั่นคงปลอดภัยทางกายภาพ(Physical security perimeters)

มาตรการควบคุม

อาณาเขตความมั่นคงปลอดภัย ต้องถูกกำหนด และนำไปใช้เพื่อปกป้องพื้นที่ที่มีสารสนเทศและทรัพย์สินที่เกี่ยวข้องอื่น ๆ

A.7.2 การเข้า-ออกพื้นที่(Physical security perimeters)

มาตรการควบคุม

บริเวณที่ต้องรักษาความมั่นคงปลอดภัยต้องได้รับการปกป้องโดยมาตรการควบคุมการเข้า-ออก และจุดที่เข้าถึงได้อย่างเหมาะสม

A.7.3 ความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวก(Securing offices, rooms and facilities)

มาตรการควบคุม

ความมั่นคงปลอดภัยทางกายภาพของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวกต่าง ๆ ต้องได้รับการออกแบบและนำไปประยุกต์ใช้

A.7 ตัวควบคุมทางกายภาพ (Physical controls)

A.7.4 การเฝ้าติดตามความมั่นคงปลอดภัยทางกายภาพ(Physical security monitoring)

มาตรการควบคุม

สถานที่จะต้องได้รับการเฝ้าติดตามสำหรับการเข้าถึงทางกายภาพโดย
ไม่ได้รับอนุญาตอย่างต่อเนื่อง

A. 7.5 การป้องกันภัยคุกคามทางกายภาพและสภาพแวดล้อม(Protecting against physical and environmental threat

มาตรการควบคุม

การป้องกันภัยคุกคามทางกายภาพและสภาพแวดล้อม เช่น ภัยพิบัติทางธรรมชาติ และ
อื่น ๆ โดยตั้งใจหรือไม่ตั้งใจ

A.7.6 การปฏิบัติงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัย(Working in secure areas)

มาตรการควบคุม

มาตรการรักษาด้านความมั่นคงปลอดภัยสำหรับการทำงานในบริเวณที่ต้องรักษา
ความมั่นคงปลอดภัยต้องได้รับการออกแบบและนำไปประยุกต์ใช้

A.7 ตัวควบคุมทางกายภาพ (Physical controls)

A.7.7 การจัดเก็บโต๊ะทำงาน และจัดการหน้าจอ (Clear desk and clear screen)

<u>มาตรการควบคุม</u>

กฎเกณฑ์การจัดเก็บโต๊ะทำงานสำหรับกระดาษและสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ และกฎเกณฑ์การจัดการหน้าจอสำหรับสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ ต้องกำหนดและบังคับใช้อย่างเหมาะสม

A.7.8 การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)

<u>มาตรการควบคุม</u>

อุปกรณ์ต้องได้รับการจัดวางอย่างปลอดภัยและได้รับการป้องกัน

A.7.9 ความมั่นคงปลอดภัยของทรัพย์สินที่ใช้นอกสำนักงาน(Security of assets off-premises)

<u>มาตรการควบคุม</u>

ทรัพย์ที่นำออกไปใช้งานนอกสำนักงานจะต้องได้รับการป้องกัน

A.7 ตัวควบคุมทางกายภาพ (Physical controls)

A.7.10 สื่อบันทึกข้อมูล (Storage media)

มาตรการควบคุม

สื่อบันทึกข้อมูลต้องได้รับการบริหารจัดการตลอดวงจรชีวิตของการจัดหา การใช้งาน การขนส่ง และการจำหน่ายตามการจัดระดับชั้นความลับขององค์กรและข้อกำหนดในการจัดการ

A.7.11 ระบบสาธารณูปโภคสนับสนุน(Supporting utilities)

มาตรการควบคุม

สิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ ต้องได้รับการป้องกันจากความล้มเหลว
ของกระแสไฟฟ้า และการหยุดชะงักอื่น ๆ ที่มีสาเหตุมาจากความผิดพลาดของระบบสาธารณูปโภคสนับสนุน

A.7.12 ความมั่นคงปลอดภัยของการเดินสาย(Cabling security)

มาตรการควบคุม

สายเคเบิลที่นำไฟฟ้า,ข้อมูล หรือสนับสนุนบริการทางข้อมูลจะต้องได้รับการปกป้องจากการขัดขวางการทำงาน การแทรกแซงสัญญาณ หรือการทำให้เสียหาย

A.7 ตัวควบคุมทางกายภาพ (Physical controls)

7.13 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

เพื่อป้องกันสารสนเทศและสินทรัพย์ที่เกี่ยวข้องอื่น ไม่ให้สูญเสีย เสียหาย ถูกโจรกรรม หรือตกอยู่ในความเสี่ยงและไม่ทำให้การดำเนินงานขององค์กรที่เกิดจากการขาดการบำรุงรักษาหยุดชะงัก

ควรดูแลรักษาอุปกรณ์อย่างถูกต้องเพื่อทำให้แน่ใจว่าพร้อมใช้งาน มีความสมบูรณ์ และรักษาความลับของสารสนเทศ

7.14 การกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย (Secure disposal or re-use of equipment)

เพื่อป้องกันสารสนเทศรั่วไหลออกจากอุปกรณ์ที่จะทิ้งหรือนำกลับมาใช้ใหม่ควรทวนสอบรายการต่าง ๆ ของอุปกรณ์ที่มีสื่อจัดเก็บข้อมูลเพื่อทำให้แน่ใจว่ามีการลบหรือเขียนทับข้อมูลที่ละเอียดอ่อนและซอฟต์แวร์ที่ได้รับอนุญาตอย่างปลอดภัยก่อนที่จะทิ้งหรือนำกลับมาใช้ใหม่

A.8 ตัวควบคุมทางเทคโนโลยี (Technological controls)

Dr.Krit
083-4358785
drchakkrit@gmail.com

A.8 ตัวควบคุมทางเทคโนโลยี (Technological controls)

A.8.1 อุปกรณ์ปลายทางของผู้ใช้(User end point devices)

มาตรการควบคุม

ข้อมูลที่จัดเก็บ ประมวลผลหรือเข้าถึงได้ผ่านอุปกรณ์ปลายทางของผู้ใช้ ต้องได้รับการปกป้อง

A.8.2 สิทธิพิเศษในการเข้าถึง(Privileged access rights)

มาตรการควบคุม

การจัดสรรและใช้สิทธิ์การเข้าถึงที่เป็นสิทธิพิเศษต้องถูกจำกัดและบริหารจัดการ

A.8.3 การจำกัดการเข้าถึงสารสนเทศ(Information access restriction)

มาตรการควบคุม

การเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ ต้องถูกจำกัดตามนโยบายเฉพาะ
ที่จัดทำไว้ในการควบคุมการเข้าถึง

A.8.4 การเข้าถึงซอร์สโค้ด(Access to source code)

มาตรการควบคุม

การเข้าถึงซอร์สโค้ดโดยการอ่านและเขียนเครื่องมือในการพัฒนา และซอฟต์แวร์ไลบรารีต้องได้รับการจัดการอย่างเหมาะสม

A.8.5 การพิสูจน์ตัวตนอย่างมั่นคงปลอดภัย(Secure authentication)

มาตรการควบคุม

เทคโนโลยีของการพิสูจน์ตัวตนอย่างมั่นคงปลอดภัยและขั้นตอนปฏิบัติ ต้องดำเนินการ
ตามข้อจำกัดการเข้าถึงสารสนเทศและนโยบายเฉพาะเกี่ยวกับการควบคุมการเข้าถึง

A.8.6 การบริหารจัดการขีดความสามารถ(Capacity management)

มาตรการควบคุม

การใช้ทรัพยากรต้องได้รับการเฝ้าระวังและปรับให้สอดคล้องกับความต้องการใน

A.8 ตัวควบคุมทางเทคโนโลยี (Technological controls)

A.8.7 การป้องกันจากโปรแกรมไม่พึงประสงค์(Protection against malware)

มาตรการควบคุม

การป้องกันจากโปรแกรมไม่พึงประสงค์จะต้องดำเนินการและสนับสนุนโดย
การสร้างความตระหนักแก่ผู้ใช้งานอย่างเหมาะสม

A.8.8 การบริหารจัดการช่องโหว่ทางเทคนิค(Management of technical vulnerabilities)

มาตรการควบคุม

ต้องได้รับข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบสารสนเทศที่ใช้งาน
ช่องโหว่ดังกล่าวขององค์กร ต้องได้รับการประเมินและระบุมาตรการที่เหมาะสม

A.8.9 การบริหารจัดการการกำหนดค่า (Configuration management)

มาตรการควบคุม

เพื่อตรวจสอบให้แน่ใจว่าฮาร์ดแวร์ ซอฟต์แวร์ บริการและเครือข่าย
ทำงานอย่างถูกต้องด้วยการกำหนดค่าการรักษาความปลอดภัยที่จำเป็น
และไม่เปลี่ยนแปลงการกำหนดค่าโดยการเปลี่ยนแปลงที่ไม่ได้รับ
อนุญาตหรือไม่ถูกต้อง เครือข่าย และจัดทำเป็นเอกสาร นำไปปฏิบัติ เฝ้า

A.8.10 การลบข้อมูล (Information deletion)

มาตรการควบคุม

ข้อมูลที่จัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์หรือสื่อบันทึกข้อมูลอื่น ๆ ต้องถูกลบออก
เมื่อไม่มีความจำเป็นต้องใช้งานข้อมูลนั้นอีก

A.8.11 การปิดบังข้อมูล(Data masking)

มาตรการควบคุม

การปิดขังข้อมูล ต้องใช้ตามนโยบายเฉพาะขององค์กรที่เกี่ยวกับการควบคุมการเข้าถึง
และนโยบายเฉพาะอื่น ๆ ที่เกี่ยวข้อง และข้อกำหนดทางธุรกิจ โดยนำกฎหมายที่บังคับใช้มาพิจารณา

A.8.12 การป้องกันข้อมูลรั่วไหล (Data leakage prevention)

มาตรการควบคุม เพื่อตรวจจับและป้องกันการเปิดเผยและดึงสารสนเทศโดยไม่ได้รับอนุญาตโดยบุคคลหรือระบบต่าง ๆ
มาตรการป้องกันข้อมูลรั่วไหล ต้องนำไปใช้กับระบบ เครือข่าย และอุปกรณ์อื่น ๆ ที่ใช้
ประมวลผล จัดเก็บ หรือมีการส่งข้อมูลที่ละเอียดอ่อน

A.8 ตัวควบคุมทางเทคโนโลยี (Technological controls)

A.8.13 การสำรองข้อมูล (Information backup)

<u>มาตรการควบคุม</u>

การสำรองข้อมูลสารสนเทศ, ซอฟต์แวร์ และระบบ ต้องได้รับการบำรุงรักษาและทดสอบอย่างสม่ำเสมอ สอดคล้องกับนโยบายเฉพาะที่ตกลงกันในการสำรองข้อมูล

A.8.14 อุปกรณ์สำรองของสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ (Redundancy of information processing facilities)

<u>มาตรการควบคุม</u>

สิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ ต้องดำเนินการสำรองไว้อย่างเพียงพอ เพื่อให้เป็นไปตามข้อกำหนดด้านความพร้อมใช้งาน

A.8.15 การบันทึกล็อก (Logging)

<u>มาตรการควบคุม</u>

ล็อกที่บันทึกกิจกรรม ข้อยกเว้น ข้อผิดพลาด และเหตุการณ์ที่เกี่ยวข้องอื่น ๆ จะต้องมีการ
จัดทำขึ้น จัดเก็บ ป้องกัน และวิเคราะห์

A.8.16 การเฝ้าติดตามกิจกรรม (Monitoring activities)

<u>มาตรการควบคุม</u>

เครือข่าย ระบบ และแอปพลิเคชัน ต้องได้รับการเฝ้าติดตามพฤติกรรมที่ผิดปกติ และ
การดำเนินการที่หมาะสม เพื่อประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
ที่อาจเกิดขึ้น

A.8.17 การตั้งค่านาฬิกาให้ตรงกัน (Clock synchronization)

<u>มาตรการควบคุม</u>

เพื่อให้เกิดความสัมพันธ์และการวิเคราะห์เหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยและข้อมูลที่บันทึกไว้อื่น ๆ และเพื่อสนับสนุนการสอบสวนอุบัติการณ์ด้านการรักษาความปลอดภัยของสารสนเทศ ควรซิงโครไนซ์นาฬิกาของระบบประมวลผลสารสนเทศที่องค์กรใช้กับแหล่งเวลาที่ได้รับอนุมัติ

A.8 ตัวควบคุมทางเทคโนโลยี (Technological controls)

A.8.18 การใช้งานโปรแกรมยูทิลิตี้ที่ได้รับสิทธิพิเศษ(Use of privileged utility programs)

<u>มาตรการควบคุม</u>

การใช้งานโปรแกรมยูทิลิตี้ ที่สามารถข้ามผ่านมาตรการควบคุมของระบบและแอพลิเคชันได้ ต้องถูกจำกัดและควบคุมอย่างเคร่งครัด

A.8.19 การติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ(Installation of software on operational systems)

<u>มาตรการควบคุม</u>

ต้องดำเนินการตามขั้นตอนปฏิบัติและมาตรการเพื่อจัดการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการอย่างมั่นคงปลอดภัย

A.8.20 ความมั่นคงปลอดภัยของเครือข่าย (Networks security)

<u>มาตรการควบคุม</u>

เครือข่ายและอุปกรณ์เครือข่ายต้องได้รับการรักษาความมั่นคงปลอดภัย บริหารจัดการ และควบคุมเพื่อปกป้องข้อมูลในระบบและแอปพลิเคชัน

A.8.21 ความมั่นคงปลอดภัยของบริการเครือข่าย (Security of network services)

<u>มาตรการควบคุม</u>

กลไกด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดของบริการเครือข่าย
ต้องได้รับการระบุ นำไปปฏิบัติ และเฝ้าติดตาม

A.8.22 การแบ่งแยกเครือข่าย(Segregation of networks)

<u>มาตรการควบคุม</u>

กลุ่มบริการข้อมูลสารสนเทศ ผู้ใช้ และระบบสารสนเทศต่าง ๆ ต้องได้รับการแบ่งแยก
ออกจากเครือข่ายขององค์กร

A.8.23 การกรองเว็บ เว็บ (Web filtering)

<u>มาตรการควบคุม</u>

การเข้าถึง การเปิดเว็บไซต์ภายนอก ต้องได้รับการจัดการเพื่อลดปัจจัยเสี่ยงในการเข้าถึง
เนื้อหาที่เป็นอันตราย

A.8 ตัวควบคุมทางเทคโนโลยี (Technological controls)

A.8.24 การเข้ารหัสข้อมูล(Use of cryptography)

<u>มาตรการควบคุม</u>

หลักเกณฑ์สำหรับการใช้งานการเข้ารหัสข้อมูลอย่างมีประสิทธิภาพ รวมถึงการบริหารจัดการกุญแจการเข้ารหัสข้อมูล ต้องได้รับการกำหนดและนำไปปฏิบัติ

A.8.25 วงจรชีวิตการพัฒนาอย่างมั่นคงปลอดภัย(Secure development life cycle)

<u>มาตรการควบคุม</u>

หลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบอย่างมั่นคงปลอดภัย ต้องได้รับ
การกำหนดและนำไปปฏิบัติ

A.8.26 ข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชั่น (Application security requirements)

<u>มาตรการควบคุม</u>

หลักกณฑ์ด้านความมั่นคงปลอดภัยสารสนเทศจะต้องกำหนด ระบุ และอนุมัติเพื่อ

A.8.27 สถาปัตยกรรมระบบและหลักการทางวิศวกรรมที่มั่นคงปลอดภัย (Secure system architecture and engineering principles)

<u>มาตรการควบคุม</u>

หลักการด้านความมั่นคงปลอดภัยทางวิศวกรรมระบบ ต้องจัดทำขึ้น บันทึกเป็นเอกสาร บำรุงรักษาและนำไปประยุกต์ใช้กับทุกกิจกรรมของการพัฒนาระบบสารสนเทศ

A.8.28 แนวทางการพัฒนาซอฟต์แวร์เพื่อความปลอดภัย(Secure coding)

<u>มาตรการควบคุม</u>

เพื่อตรวจสอบให้แน่ใจว่ามีการเขียนซอฟต์แวร์อย่างปลอดภัยโดยลดจำนวนช่องโหว่ด้านการรักษาความปลอดภัยของสารสนเทศที่อาจเกิดขึ้นในซอฟต์แวร์

A.8.29 การทดสอบความมั่นคงปลอดภัยในการพัฒนาและการยอมรับ (Security testing in development and acceptance)

<u>มาตรการควบคุม</u>

เพื่อตรวจสอบความถูกต้องว่าตรงตามข้อกำหนดด้านการรักษาความปลอดภัยของสารสนเทศหรือไม่เมื่อมีการปรับใช้แอปพลิเคชัน หรือรหัสกับสภาพแวดล้อมการผลิต

A.8 ตัวควบคุมทางเทคโนโลยี (Technological controls)

A.8.30 การพัฒนาโดยหน่วยงานภายนอก(Outsourced development)

มาตรการควบคุม

องค์กรต้องกำกับดูแล เฝ้าติดตาม และทบทวนกิจกรรมที่เกี่ยวข้องกับการพัฒนาระบบจากหน่วยงานภายนอก

A.8.31 การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริงออกจากกัน(Separation of development, test and production)

มาตรการควบคุม

สภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริงต้องถูกแบ่งแยกออกจากกันและถูกรักษาความปลอดภัย

A.8.32 การบริหารจัดการการเปลี่ยนแปลง(Change management)

มาตรการควบคุม

การเปลี่ยนแปลงถึงสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศและระบบสารสนเทศต้องเป็นไปตามขั้นตอนการจัดการการเปลี่ยนแปลง

A.8.33 ข้อมูลในการทดสอบ(Test information)

มาตรการควบคุม

เพื่อตรวจสอบให้มั่นใจว่าการทดสอบและการคุ้มครองสารสนเทศการปฏิบัติงานที่ใช้ในการทดสอบตรงประเด็น

ข้อมูลในการทดสอบต้องได้รับการคัดเลือก ปกป้อง และบริหารจัดการอย่างเหมาะสม

A.8.34 การปกป้องระบบสารสนเทศระหว่างการตรวจประเมิน (Protection of information systems during audit testing)

มาตรการควบคุม

การตรวจประเมินและกิจกรรมให้ความเชื่อมั่นอื่น ๆ ที่เกี่ยวข้องกับการตรวจประเมินระบบปฏิบัติการ ต้องมีการวางแผนและตกลงร่วมกันระหว่างผู้ทดสอบและผู้บริหารอย่างเหมาะสม

THANK YOU

083-4358785