การวิเคราะห์ความพร้อมในการขอรับรองมาตรฐาน ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 กรณีศึกษา สำนักเทคโนโลยีดิจิทัลและสารสนเทศ

กฤษณะ หล่อโลหพันธุ์

นักวิชาการคอมพิวเตอร์ปฏิบัติการ

สำนักเทคโนโลยีดิจิทัลและสารสนเทศ

คำนำ

การจัดทำเอกสารวิเคราะห์ความพร้อมในการขอรับรองมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO /IEC 27001:2022 กรณีศึกษา สำนักเทคโนโลยีดิจิทัลและสารสนเทศ ฉบับนี้ ได้นำผลการดำเนินงานของสำนักเทคโนโลยีสารสนเทศมาวิเคราะห์หาช่องว่าง (Gap analysis) โดยการรวบรวมข้อมูลจากเอกสารของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ รวมกับการสอบถามเพิ่มเติมจากบุคลากรภายในสำนักที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศของสำนัก เพื่อประเมินความพร้อมของการขอรับรองมาตรฐาน ISO/IEC 27001 ของสำนัก และเพื่อนำไปใช้ประกอบในการวางแผนและดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศอย่างมีประสิทธิภาพต่อเนื่อง

ผู้จัดทำต้องขอขอบพระคุณผู้อำนวยการสำนัก ผู้อำนวยการกองบริหารงานสำนัก และบุคลากรของสำนักเทคโนโลยีดิจิทัลและสารสนเทศที่เกี่ยวข้องทุกท่าน ที่ช่วยส่งเสริมการจัดทำงานวิเคราะห์ฉบับนี้ หวังเป็นอย่างยิ่งว่า เอกสารฉบับนี้จะเป็นประโยชน์ตามวัตถุประสงค์ดังกล่าว และเป็นแนวทางเพื่อใช้ต่อยอดในการนำไปใช้ในการวิเคราะห์สำหรับผู้สนใจต่อไป หากมีข้อบกพร่องประการใด ผู้จัดทำต้องขออภัยและขอรับผิดทุกประการ ทั้งนี้จะนำข้อคิดเห็นและข้อเสนอแนะทุกๆด้านนำไปปรับปรุงในโอกาสต่อไป

กฤษณะ หล่อโลหพันธุ์
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
สำนักเทคโนโลยีดิจิทัลและสารสนเทศ

สารบัญ

สารบัญตาราง

สารบัญภาพ

บทที่ 1. บทนำ

1.1. ความเป็นมาและความสำคัญ

เทคโนโลยีดิจิทัลมีบทบาทอย่างมากต่อการดำเนินงานขององค์กร มีการทำ Digital Transformation นำระบบเทคโนโลยีสารสนเทศมาช่วยสนับสนุนในการดำเนินงาน และมีการปรับเปลี่ยนการจัดเก็บข้อมูลให้มาอยู่ในรูปแบบดิจิทัลมากขึ้น ข้อมูลสารสนเทศในรูปแบบดิจิทัลซึ่งถือเป็นทรัพย์สินอย่างหนึ่งขององค์กรได้ถูกนำมาจัดเก็บไว้ในระบบเทคโนโลยีสารสนเทศเพื่อช่วยอำนวยความสะดวกในการสืบค้น ประมวลผล วิเคราะห์ และนำใช้ประโยชน์อื่นๆต่อได้ แต่หากระบบเทคโนโลยีสารสนเทศที่ใช้งานไม่มีการจัดการในด้านความมั่นคงปลอดภัยสารสนเทศที่เพียงพอก็มีความเสี่ยงต่อการถูกโจมตีไซเบอร์ซึ่งถือเป็นอาชญกรรมทางคอมพิวเตอร์อย่างหนึ่ง อาจจะทำให้ระบบเทคโนโลยีสารสนเทศไม่สามารถใช้การได้หรือทำให้ข้อมูลรั่วไหล สูญเสีย หรือถูกทำลาย ซึ่งอาจจะสร้างความเสียหายที่ไม่มากไปจนถึงระดับที่ร้ายแรงขึ้นอยู่กับความสำคัญของระบบว่ามีความจำเป็นต่อการดำเนินงานขององค์กรหรือไม่ และความสำคัญของข้อมูลว่าเป็นข้อมูลความลับหรือข้อมูลส่วนบุคคลหรือไม่ หลายองค์กรจึงเริ่มตระหนักถึงภัยคุกคามดังกล่าว และเริ่มมีการจัดการด้านความมั่นคงปลอดภัยต่อระบบเทคโนโลยีสารสนเทศอย่างจริงจัง

จากสถิติภัยคุกคามทางไซเบอร์ แยกตามภารกิจหรือบริการของหน่วยงานที่ถูกโจมตี ในปี พ.ศ. 2567 ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) (2568) พบว่ามีหน่วยงานที่ถูกโจมตีทางไซเบอร์จำนวน 2,135 เหตุการณ์ และหน่วยงานที่ถูกภัยคุกคามทางไซเบอร์มากที่สุด คือ หน่วยงานการศึกษามีถึง 555 เหตุการณ์ หรือคิดเป็นประมาณ 26% ของเหตุการณ์ที่ถูกภัยคุกคามทั้งหมด ดังนั้นสถาบันบัณฑิตพัฒนบริหารศาสตร์ซึ่งเป็นสถาบันการศึกษาที่มีการนำระบบเทคโนโลยีสารสนเทศมาช่วยสนับสนุนการดำเนินงานตามภารกิจของสถาบัน และมีการจัดเก็บข้อมูลสารสนเทศที่จำเป็นต่อการดำเนินงานในหลายๆด้านที่รวมถึงข้อมูลส่วนบุคคลและข้อมูลอ่อนไหว จำเป็นต้องมีการจัดการในการรักษาความมั่นคงปลอดภัยต่อข้อมูลสารสนเทศให้เป็นไปตามหลักการพื้นฐานความมั่นคงปลอดภัยสารสนเทศ CIA ที่มีองค์ประกอบ 3 ด้าน ได้แก่ ด้านการรักษาความลับ (Confidential) ด้านความถูกต้องสมบูรณ์ (Integrity) และด้านความพร้อมใช้งาน (Availability) ซึ่งถือว่าเป็นสิ่งสำคัญที่ไม่อาจมองข้ามได้

สำนักเทคโนโลยีดิจิทัลและสารสนเทศซึ่งเป็นหน่วยงานที่ควบคุมดูแลระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศหลักของสถาบัน และเป็นหน่วยงานสำคัญในการรักษาข้อมูลสารสนเทศให้ความมั่นคงปลอดภัย จึงต้องมีการบริหารจัดการด้านความมั่นคงปลอดภัยอย่างเป็นระบบ โดยสำนักได้เริ่มนำมาตรฐาน

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013 มาปรับปรุงการบริหารจัดการของสำนักให้มีประสิทธิภาพและมีการดำเนินงานอย่างเป็นระบบ ตั้งแต่การกำหนดนโยบาย แนวปฏิบัติ และมาตรการควบคุม การวางแผนการดำเนินงานและจัดสรรทรัพยากร การกำหนดขั้นตอนและการปฏิบัติงาน การกำกับติดตามและเฝ้าระวัง จนถึงการปรับปรุงอย่างต่อเนื่อง ซึ่งทำให้สำนักได้รับการรับรองมาตรฐาน ISO/IEC 27001:2013 ในปี พ.ศ. 2565

ปัจจุบันมาตรฐาน ISO/IEC 27001 ได้มีการปรับปรุงออกเป็นมาตรฐาน ISO/IEC 27001:2022 ซึ่งมีการปรับเปลี่ยนรายละเอียดและเพิ่มข้อกำหนดไว้ในมาตรฐานเพื่อให้สอดคล้องกระบวนการ ภัยคุกคาม และเทคโนโลยีดิจิทัลที่เปลี่ยนไป ทำให้กระบวนการทำงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศในปัจจุบันอาจจะไม่สอดคล้องหรือไม่รองรับการเปลี่ยนแปลงที่เกิดขึ้น ดังนั้นการประเมินความสอดคล้องของมาตรฐาน ISO/IEC 27001:2022 กับระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของสำนักจะช่วยทำให้เห็นช่องว่างที่เกิดขึ้นและนำไปใช้ในการวิเคราะห์วางแผนปรับปรุงการดำเนินงานของสำนักให้มีประสิทธิภาพสอดคล้องกับข้อกำหนด และพร้อมที่จะขอรับรองมาตรฐาน ISO/IEC 27001:2022 ต่อไป

1.2. วัตถุประสงค์ของการวิเคราะห์

(1) เพื่อศึกษาระบบบริหารความมั่นคงปลอดภัยสารสนเทศและมาตรการควบคุม (Control) ของมาตรฐาน ISO/IEC 27001:2022

(2) เพื่อประเมินความสอดคล้องและวิเคราะห์ช่องว่าง (Gap Analysis) ระหว่างข้อกำหนดของมาตรฐาน ISO/IEC 27001:2022 กับการดำเนินงานในการบริหารความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

(3) นำเสนอแนวทางในการปรับปรุงการดำเนินงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศให้สอดคล้องกับมาตรฐาน ISO/IEC 27001:2022

1.3. ประโยชน์ที่คาดว่าจะได้รับ

ประโยชนที่คาดว่าจะได้รับจากการศึกษาและวิเคราะห์นี้ ได้แก่ การรับรู้และความเข้าใจถึงการดำเนินงานในการบริหารความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัลและสารสนเทศในปัจจุบันเมื่อเทียบกับข้อกำหนดของมาตรฐาน ISO/IEC 27001:2022 และช่วยกำหนดแนวทางในการปรับปรุงนโยบาย แนวปฏิบัติ กระบวนการทำงานของระบบบริหารความมั่นคงปลอดภัยสารสนเทศของสำนัก ตั้งแต่การวางแผน การปฏิบัติ การประเมินผล และการปรับปรุงอย่างต่อเนื่อง เพื่อให้สอดคล้องกับข้อกำหนดของมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022

1.4. ขอบเขตการวิเคราะห์

ขอบเขตของการวิเคราะห์นี้จะเป็นการศึกษามาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 และทำการวิเคราะห์เปรียบเทียบข้อกำหนดของมาตรฐานกับการดำเนินการของสำนักเทคโนโลยีดิจิทัลและสารสนเทศตามขอบเขตการขอรับรองมาตรฐาน เพื่อหาช่องว่าง (Gap) สิ่งที่สำนักเทคโนโลยีดิจิทัลและสารสนเทศยังดำเนินการไม่ครบถ้วน พร้อมกับนำเสนอแนวทางในการปรับปรุงการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัลและสารสนเทศให้สอดคล้องกับมาตรฐาน ISO/IEC 27001:2022

1.5. นิยามศัพท์

สถาบัน หมายถึง สถาบันบัณฑิตพัฒนบริหารศาสตร์

สำนัก หมายถึง สำนักเทคโนโลยีดิจิทัลและสารสนเทศ

สารสนเทศ หมายถึง ข้อมูลที่ผ่านกระบวนการประมวลผล จัดระเบียบ ทำให้มีความหมายและคุณค่าเพิ่มขึ้น สามารถนำไปใช้ประโยชน์ในการตัดสินใจ วางแผน หรือดำเนินการต่าง ๆ ได้

ความมั่นคงปลอดภัยสารสนเทศ หมายถึง การปกป้องข้อมูลและระบบสารสนเทศจากภัยคุกคามต่างๆ เช่น การเข้าถึงหรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต การทำลายข้อมูล การทำให้ข้อมูลเสียหาย หรือการทำให้ระบบสารสนเทศใช้งานไม่ได้

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ หมายถึง กรอบการทำงานที่ประกอบด้วยนโยบาย กระบวนการ ขั้นตอนการปฏิบัติงาน และการควบคุมที่ออกแบบมาเพื่อจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรอย่างเป็นระบบและต่อเนื่อง

มาตรฐาน ISO/IEC 27001 หมายถึง มาตรฐานสากลที่มีข้อกำหนดในการจัดทำ การนำไปปฏิบัติ การรักษา และการปรับปรุง สำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

ความสอดคล้อง หมายถึง การปฏิบัติหรือการดำเนินการที่เป็นไปตามข้อกำหนด กฎหมาย ระเบียบข้อบังคับ นโยบายและแนวปฏิบัติ

บริการ VPS (Virtual Private Server) หมายถึง บริการให้ใช้เครื่องคอมพิวเตอร์เสมือน (Virtual machine) ที่มีการจัดสรรทรัพยากรเฉพาะให้กับผู้รับบริการแต่ละราย โดยใช้เทคโนโลยี Virtualization

บริการ Colocation หมายถึง บริการให้ใช้พื้นที่ในศูนย์ข้อมูล (Data Center) สำหรับติดตั้งเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายของผู้รับบริการ โดยสำนักจะจัดเตรียมทรัพยากรระบบโครงสร้าง

พื้นฐานที่จำเป็นไว้ให้ เช่น เครือข่ายอินเทอร์เน็ต ระบบไฟฟ้า การรักษาความมั่นคงปลอดภัยทางกายภาพ

บทที่ 2. เอกสารที่เกี่ยวข้องกับเรื่องที่จะวิเคราะห์

การศึกษาเพื่อวิเคราะห์ความพร้อมขององค์กรในการขอรับรองมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 กรณีศึกษาสำนักเทคโนโลยีดิจิทัลและสารสนเทศนั้น ผู้ศึกษาได้ทำการศึกษาเอกสารที่เกี่ยวข้องกับการวิเคราะห์ ดังนี้

(1) แนวคิดการรักษาความมั่นคงปลอดภัยสารสนเทศ

(2) มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

(3) การให้บริการ Colocation และ Virtual Private Server

(4) การวิเคราะห์ช่องว่าง (Gap Analysis)

(5) กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

(6) บทความ/งานวิจัยที่เกี่ยวข้อง

2.1. แนวคิดการรักษาความมั่นคงปลอดภัยสารสนเทศ

การปรับเปลี่ยนองค์กรโดยนำเทคโนโลยีดิจิทัลมาช่วยสนับสนุนการดำเนินงานและจัดเก็บข้อมูลให้อยู่ในรูปแบบดิจิทัลมีเพิ่มขึ้นอย่างต่อเนื่อง ซึ่งทำให้มีความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเพิ่มขึ้นตามมาด้วย ดังนั้นทรัพย์สินสารสนเทศขององค์กรจึงเป็นสิ่งสำคัญที่ต้องดูแลรักษาและมีการป้องกัน (Mirtsch et al., 2021) ซึ่งการรักษาความมั่นคงปลอดภัยสารสนเทศไม่ได้อาศัยความสามารถของซอฟต์แวร์และฮาร์ดแวร์เพียงอย่างเดียว เป็นเรื่องของกระบวนการที่ต้องมีการกำหนดนโยบายและมาตรการในการปฏิบัติ วิธีการจัดการเทคโนโลยีให้มีความปลอดภัย มีการป้องกัน มีการสำรองข้อมูล มีการรับมือ และการควบคุมกำกับติดตามอย่างเหมาะสม (สมศิริ พันธุ์ศักดิ์ศิริ และ เสาวนีย์ สมันต์ตรีพร, 2023)

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Techology, NIST) ของประเทศสหรัฐอเมริกา ได้นำเสนอหลักการพื้นฐานที่สำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ (The National Institute of Standards and Technology, 2020) ประกอบด้วย 3 องค์ประกอบหลัก ได้แก่ การรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) หรือที่รู้เรียกว่าแนวคิด CIA Triad

ภาพที่ 2-1 แผนภาพ CIA Triad (The National Institute of Standards and Technology, 2020)

(1) การรักษาความลับ (Confidentiality) เป็นการจำกัดการเข้าถึงและเปิดเผยข้อมูลเฉพาะผู้ที่ได้รับอนุญาต รวมถึงการป้องกันข้อมูลส่วนบุคคลและข้อมูลที่อ่อนไหว

(2) ความถูกต้องสมบูรณ์ (Integrity) เป็นการรับประกันว่าข้อมูลจะได้รับการป้องกันการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต และมั่นใจว่าเป็นข้อมูลที่ถูกต้องแท้จริง

(3) ความพร้อมใช้งาน (Availability) เป็นการรับรองความน่าเชื่อถือว่าข้อมูลสามารถเข้าถึงและใช้งานได้อย่างทันทีที่ต้องการ

การรักษาข้อมูลสารสนเทศให้มีความมั่นคงปลอดภัยตามแนวคิด CIA Triad ต้องมีการบริหารจัดการอย่างเป็นระบบและมีประสิทธิภาพ ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System, ISMS) จึงเป็นเครื่องมือที่จะมาช่วยจัดการและควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ มีกระบวนการทำงานที่เป็นระบบ มีการจัดทำเป็นเอกสาร และมีการสื่อสารให้รับรู้ทั้งองค์กร โดยกลยุทธและนโยบายต่างๆจะต้องถูกจัดทำขึ้นเพื่อให้ทรัพยสินสารสนเทศ มีการรักษาความลับ มีความถูกต้องสมบูรณ์ และมีความพร้อมใช้งาน พร้อมกับมีการจัดการให้ข้อมูลสารสนเทศมีความเสี่ยงด้านความมั่นคงปลอดภัยอยู่ในระดับต่ำที่องค์กรสามารถยอมรับได้ (Susanto & Almunawar, 2018 อ้างถึงใน Fonseca-Herrera, Rojas, & Florez, 2021)

ข้อมูลสารสนเทศเป็นเครื่องมือที่สำคัญในการบริหารจัดการและการดำเนินงานขององค์กร ความมั่นคงปลอดภัยสารสนเทศจึงไม่ใช่เป็นเรื่องแค่การจัดการเทคโนโลยีเพื่อปกป้องข้อมูลจากภัยคุกคามทางไซเบอร์ แต่ต้องรวมถึงการปกป้องข้อมูลไม่ให้เกิดการสูญเสียหรือสูญหายที่เกิดจากการก่อการร้าย อุบัติเหตุ หรือภัยพิบัติทางธรรมชาติ ซึ่งหมายถึงว่าแนวคิดการรักษาความมั่นคงปลอดภัยสารสนเทศต้องมีนโยบายและกระบวนจัดการที่ครอบคลุมถึงการบริหารจัดการให้เกิดความต่อเนื่องทางธุรกิจเพื่อปกป้องข้อมูลได้อย่างมีประสิทธิภาพตอบสนองความต้องการขององค์กร (Goodman และคนอื่นๆ, 2008)

2.2. มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) เป็นกรอบแนวทางในการทำงานที่ช่วยให้องค์กรสามารถจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัยในองค์รวมอย่างเป็นระบบ (Achmadi et al., 2018) ซึ่งมีกระบวนการทำงานและการจัดทำเอกสาร อย่างเป็นระบบ และรับทราบทั่วทั้งองค์กร ภายใต้นโยบายและกลยุทธ์ที่กำหนดเพื่อให้มีการรับประกันว่าสารสนเทศจะต้องมีการรักษาความลับ (Confidentiality) มีความถูกต้องสมบูรณ์ (Integrity) และมีความพร้อมใช้งาน (Availability) (Fonseca-Herrera et al., 2021)

ในส่วนมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) นั้น จุดเริ่มต้นมาจากชุดมาตรฐาน BS 7799 ซึ่งพัฒนาโดยสถาบันมาตรฐานแห่งประเทศอังกฤษ (British Standard Institution: BSI) ในปี ศ.ศ. 1995 โดย United Kingdom Government's Department of Trade and Industry (DTI) ซึ่งมาตรฐาน BS 7799-1 เป็นมาตรฐานที่เน้นทางด้านเทคนิค และ BS 7799-2 เป็นมาตรฐานที่เน้นระบบการจัดการตามหลัก PDCA (Plan-Do-Check-Act) โดยมีหลักการเพื่อปกป้องข้อมูลในด้านการรักษาความลับ (Confidential) ด้านความถูกต้องสมบูรณ์ (Integrity) และด้านความพร้อมใช้งาน (Availability) ต่อมาในปี ค.ศ. 2005 องค์กร ISO (International Organization for Standardization) ซึ่งเป็นองค์กรที่กำหนดมาตรฐานอุตสาหกรรมและการค้าระดับสากล ได้ร่วมกับคณะกรรมาธิการระหว่างประเทศว่าด้วยมาตรฐานอิเล็กทรอนิกส์ (International Electrotechnical Commission หรือ IEC) ได้นำมาตรฐานชุด BS 7799 มาจัดทำมาตรฐานระบบการบริหารจัดการความปลอดภัยสารสนเทศ ISO/IEC 27001 และ ISO/IEC 27002 (กิตติพงษ์ เกียรตินิยมรุ่, ม.ป.ป.) ซึ่งได้มีการปรับปรุงออกเป็นมาตรฐาน ISO/IEC 27001:2013 ในปี ค.ศ. 2013 และปรับปรุงล่าสุดเป็นมาตรฐาน ISO/IEC 27001:2022 ในปี ค.ศ. 2022

ภาพที่ 2-2 ความสัมพันธ์ของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Mataracioglu, 2017)

เอกสารมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 มีลักษณะตามโครงสร้างเอกสาร High-Level Structure (HLS) ตาม Annex SL ซึ่งสอดคล้องกับมาตรฐานระบบบริหารจัดการอื่นๆขององค์กร ISO ซึ่งประกอบด้วยข้อกำหนดหลัก 10 ข้อ ซึ่งเป็นข้อกำหนดที่เกี่ยวกับระบบบริหารจัดการด้านความปลอดภัยสารสนเทศขององค์กร และข้อกำหนด Annex A (normative) ในภาคผนวก ที่อธิบายถึงมาตรการการควบคุมการดำเนินงานขององค์กรให้มีความมั่นคงปลอดภัยสารสนเทศ

2.2.1. ข้อกำหนดระบบบริหารจัดการ (Management system requirements)

ข้อกำหนดระบบบริหารจัดการในมาตรฐาน ISO/IEC 27001:2002 ประกอบด้วยข้อกำหนดหลัก 10 ข้อ โดยข้อกำหนดที่ 1 - 3 เป็นข้อกำหนดทั่วไปของมาตรฐานอธิบายถึงขอบเขต (Scope) ของมาตรฐาน รูปแบบการอ้างอิง (Normative references) ในเอกสาร และคำศัพท์และนิยาม (Terms and definitions) ส่วนข้อกำหนดที่ 4 – 10 จะอธิบายถึงหลักการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC, 2022) ที่ประกอบด้วย 7 ข้อกำหนดหลัก ดังนี้

(1) ข้อกำหนดที่ 4 บริบทองค์กร (Context of the organization)

กำหนดให้องค์กรต้องทำความเข้าใจบริบทองค์กร และกำหนดประเด็นทั้งภายในและภายนอกที่ส่งผลต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศ รวมถึงความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย เพื่อนำไปกำหนดขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

(2) ข้อกำหนดที่ 5 ความเป็นผู้นำ (Leadership)

ผู้บริหารระดับสูงขององค์กรต้องแสดงความเป็นผู้นำและแสดงความมุ่งมั่นในการสนับสนุนระบบบริหารความมั่นคงปลอดภัยสารสนเทศ มีการกำหนดนโยบายและวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนการจัดสรรทรัพยากรที่จำเป็น มีการมอบหมายอำนาจ หน้าที่ ความรับผิดชอบตามบทบาทที่เกี่ยวข้อง และสื่อสารให้องค์กรทราบโดยทั่วกัน

(3) ข้อกำหนดที่ 6 การวางแผน (Planning)

องค์กรต้องวิเคราะห์ความเสี่ยงและโอกาสโดยพิจารณาประเด็นต่างๆที่กำหนดไว้ในข้อกำหนดที่ 4 รวมถึงวิเคราะห์และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และจัดทำแผนจัดการความเสี่ยง กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ และมีการวางแผนจัดการเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

(4) ข้อกำหนดที่ 7 การสนับสนุน (Support)

องค์กรต้องจัดเตรียมทรัพยากรที่จำเป็นต่อการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีการพัฒนาสมรรถนะบุคลากรให้มีสมรรถนะที่จำเป็นต่อการปฏิบัติงาน มีการสร้างความตระหนักถึงนโยบายและการจัดการขององค์กร มีการสื่อสารทั้งภายในและภายนอกองค์กรรับทราบ และมีการจัดการเอกสารสารสนเทศอย่างเหมาะสม

(5) ข้อกำหนดที่ 8 การดำเนินการ (Operation)

องค์กรต้องมีการวางแผน กำหนดกระบวนการ เกณฑ์ในการวัดผล การควบคุมกระบวนการให้เป็นแผนทีกำหนด มีการวิเคราะห์และประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และจัดการความเสี่ยงตาแผนที่กำหนดไว้ในการดำเนินการตามข้อกำหนดที่ 6

(6) ข้อกำหนดที่ 9 การประเมินสมรรถนะ (Performance evaluation)

องค์กรต้องประเมินสมรรถนะและประสิทธิผลของระบบบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร ด้วยการกำหนดสิ่งที่จำเป็น วิธีการ ระยะเวลา และผู้รับผิดชอบในการเฝ้าระวังและติดตามผล และต้องมีการตรวจประเมินภายใน (Internal audit) ตามระยะเวลาและแผนที่กำหนดไว้ และมีการทบทวนโดยฝ่ายบริหาร (Management review

(7) ข้อกำหนดที่ 10 การปรับปรุง (Improvement)

องค์กรต้องดำเนินการปรับปรุงระบบบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กรให้มีความเหมาะสม และมีประสิทธิภาพที่เพียงพออย่างต่อเนื่อง รวมถึงต้องมีการจัดการกับสิ่งที่ไม่เป็นไปตามข้อกำหนดหรือแผนดำเนินงานที่กำหนดไว้ (Nonconformity) โดยต้องมีการวิเคราะห์สาเหตุ ดำเนินการแก้ไข และติดตามผลการดำเนินการแก้ไข

การเปลี่ยนแปลงในข้อกำหนดระบบบริหารจัดการ (System management requirements) จากมาตรฐาน ISO/IEC 27001:2013 มาเป็น ISO/IEC 27001:2022 มีเพียงเล็กน้อย ซึ่งส่วนใหญ่จะเป็นการปรับรูปแบบและเนื้อหาในเอกสารให้สอดคล้องกับรูปแบบโครงสร้างเอกสาร High-Level Structure (HLS) ขององค์กร ISO และมีการปรับเปลี่ยนรายละเอียดในข้อกำหนดที่สำคัญดังนี้

(1) ขยายขอบเขตของมาตรฐานให้ครอบคลุมถึงประเด็นที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber security) และการปกป้องข้อมูลส่วนบุคคล (Privacy Protection)

(2) ข้อกำหนด 6.2 วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและแผนการบรรลุวัตถุประสงค์ (Information security objectives and plans to achieve them) มีการเพิ่มรายละเอียดให้มีการเฝ้าระวัง (Monitor) และบันทึกเป็นเอกสารที่สามารถตรวจสอบได้

(3) เพิ่มข้อกำหนด 6.3 การวางแผนการเปลี่ยนแปลง (Planning of changes) โดยกำหนดว่าหากองค์กรมีการเปลี่ยนแปลงระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ต้องมีการวางแผนในลักษณะเป็นแผนการดำเนินงาน

(4) ข้อกำหนด 7.4 การสื่อสาร (Communication) โดยปรับเปลี่ยนรายละเอียดที่ต้องกำหนดว่าใครเป็นผู้สื่อสาร เป็นต้องกำหนดว่ามีวิธีการอย่างไร (How to communicate)

(5) ข้อกำหนด 9.3 การทบทวนฝ่ายบริหาร (Management review) โดยเพิ่มรายละเอียดว่าต้องนำประเด็นการเปลี่ยนแปลงในความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมาพิจารณาด้วย

2.2.2. ข้อกำหนดการควบคุม Annex A (Normative)

ข้อกำหนดการควบคุม Annex A (Normative) เป็นข้อกำหนดที่อธิบายถึงมาตรการในการควบคุมการดำเนินงานให้มีความมั่นคงปลอดภัยสารสนเทศ โดยมีการเปลี่ยนแปลงจากมาตรฐาน ISO/IEC 27001:2013 ที่แบ่งเป็น 14 หมวด จำนวน 114 ข้อ มา ในฉบับปี 2022 ได้แบ่งออกเป็น 4 หมวด จำนวนทั้งหมด 93 ข้อ ดังนี้

(1) ข้อกำหนดการควบคุมด้านองค์กร (Organizational Controls)

ประกอบด้วย 37 ข้อกำหนด (ตั้งแต่ข้อ 5.1 – 5.37 ในข้อกำหนด Annex A) ที่ครอบคลุมในเรื่องนโยบายความมั่นคงปลอดภัยสารสนเทศ บทบาทและความรับผิดชอบ การแบ่งแยกหน้าที่ การติดต่อกับหน่วยงานที่มีอำนาจและกลุ่มผู้เชี่ยวชาญ การบริหารโครงการ การจัดการสารสนเทศและทรัพย์สินที่เกี่ยวข้อง การควบคุมการเข้าถึง การจัดการความสัมพันธ์กับผู้ให้บริการภายนอก การจัดการเหตุด้านความมั่นคงปลอดภัยสารสนเทศ และการปฏิบัติตามข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับและสัญญา

(2) ข้อกำหนดการควบคุมด้านบุคคล (People Controls)

ประกอบด้วย 8 ข้อกำหนด (ตั้งแต่ข้อ 6.1 – 6.8 ในข้อกำหนด Annex A) ที่เกี่ยวข้องกับการคัดกรองบุคลากร ข้อตกลงและเงื่อนไขการจ้างงาน การสร้างความตระหนักและการฝึกอบรม กระบวนการทางวินัย ความรับผิดชอบหลังการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ข้อตกลงการรักษาความลับ การปฏิบัติงานจากระยะไกล (Remote working) และการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

(3) ข้อกำหนดการควบคุมด้านกายภาพ (Physical Controls)

ประกอบด้วย 14 ข้อกำหนด (ตั้งแต่ข้อ 7.1 – 7.14 ในข้อกำหนด Annex A) ที่เกี่ยวข้องกับการกำหนดขอบเขตความมั่นคงปลอดภัยทางกายภาพ การควบคุมการเข้าถึงทางกายภาพ การรักษาความปลอดภัยในส่วนสำนักงาน ห้อง และสิ่งอำนวยความสะดวก การป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อม การบำรุงรักษาและจัดการกับอุปกรณ์ที่ใช้งาน การรักษาความปลอดภัยสำหรับทรัพย์สินที่อยู่นอกสถานที่ และการกำจัดหรือการนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย

(4) ข้อกำหนดควบคุมด้านเทคโนโลยี (Technology Controls)

ประกอบด้วย 34 ข้อกำหนด (ตั้งแต่ข้อ 8.1 – 8.34 ในข้อกำหนด Annex A) ที่ครอบคลุมการควบคุมอุปกรณ์ปลายทางของผู้ใช้งาน การจัดการสิทธิการเข้าถึงแบบพิเศษ การจำกัดการเข้าถึงข้อมูลและซอร์สโค้ด (Source code) เทคโนโลยีที่ใช้ในการพิสูจน์ยืนยันตัวตน การจัดการขีดความสามารถ (Capacity) ของทรัพยากร การป้องกันมัลแวร์ การจัดการช่องโหว่ทางเทคนิค การจัดการการตั้งค่า (Configuration) การลบข้อมูล การปกปิดข้อมูล การป้องกันการรั่วไหลของข้อมูล การสำรองข้อมูล การสำรองอุปกรณ์หรือสิ่งอำนวยความสะดวกที่สนับสนุนการประมวลผลข้อมูล กการตรวจสอบเฝ้าระวัง การเทียบเวลา การควบคุมการติดตั้ง

ซอฟต์แวร์และโปรแกรมอื่นๆ ความมั่นคงปลอดภัยของเครือข่าย การใช้เทคโนโลยีการเข้ารหัส และการพัฒนาซอฟต์แวร์อย่างปลอดภัย

การเปลี่ยนแปลงเนื้อหาในข้อกำหนดการควบคุม Annex A จากมาตรฐาน ISO/IEC 27001:2013 มาเป็น ISO/IEC 27001:2022 ที่สำคัญมีดังนี้

(1) การปรับเปลี่ยนข้อกำหนดโดยนำข้อกำหนดเดิมของฉบับปี 2013 มาบูรณาการจัดหมวดหมู่หรือรวมเป็นข้อเดียวกัน เพื่อให้เห็นถึงความสัมพันธ์และลดความซ้ำซ้อนของข้อกำหนด เช่น การนำข้อกำหนด A.5.1 นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศ (Policies for information security) และ A.5.1.2 การทบทวนนโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศ (Review of the policies for information security) ในมาตรฐาน ISO/IEC 27001:2013 มารวมเป็นข้อเดียวคือ ข้อกำหนด 5.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Policies for information security) ในมาตรฐาน ISO/IEC 27001:2022 โดยวัตถุประสงค์และความหมายของเนื้อหายังคงเดิม

(2) การเพิ่มข้อกำหนดใหม่เพื่อให้มีความทันสมัยสอดคล้องกับเทคโนโลยีและภัยคุกคามที่เปลี่ยนแปลงไปในปัจจุบัน เช่น ข้อกำหนด 5.23 ความมั่นคงปลอดภัยสารสนเทศในการใช้บริการคลาวด์ (Information security for use of cloud services) ที่เพิ่มมาตรการในการควบคุมในกรณีที่องค์กรมีการใช้บริการคลาวด์จากผู้ให้บริการภายนอก หรือ ข้อกำหนด 8.12 การป้องกันข้อมูลรั่วไหล (Data leakage prevention) ที่กำหนดให้องค์กรต้องมีการจัดการเพื่อป้องกันข้อมูลส่วนบุคคลหรือข้อมูลที่สำคัญมีการรั่วไหลไปยังภายนอกโดยไม่ได้รับอนุญาต

ดังนั้นการนำมาตรฐาน ISO/IEC 27001:2022 ที่มีการปรับปรุงให้สอดคล้องกับบริบทในโลกเทคโนโลยีดิจิทัลในปัจจุบันมาประยุกต์ใช้กับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร จะช่วยส่งเสริมให้องค์กรได้เตรียมความพร้อมรับมือกับการเปลี่ยนแปลงของเทคโนโลยีที่มาพร้อมกับภัยคุกคามทางไซเบอร์ที่ความซับซ้อนยิ่งขึ้น และก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่มากขึ้น รวมถึงการปรับเปลี่ยนขององค์กรเพื่อให้สอดคล้องกับกฎระเบียบที่มีการพัฒนาออกมาเพื่อรองรับการเปลี่ยนแปลงด้วย

2.3. การให้บริการ Colocation และ Virtual Private Server

บริการ Colocation เป็นบริการให้เช่าพื้นที่สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายไว้ในอาคารศูนย์ข้อมูล (Data Center) ของผู้ให้บริการ ที่มีการจัดเตรียมระบบไฟฟ้าและระบบปรับอากาศ มีการเชื่อมต่ออินเทอร์เน็ตความเร็วสูงเพื่อรองระบบ Web Server ของผู้ใช้บริการ และอาจมีให้บริการดูแลและแก้ไขปัญหา

เครื่องคอมพิวเตอร์แม่ข่ายด้วย (PCMag, n.d.) นอกจากนี้ในศูนย์ข้อมูล (Data Center) ก็ยังมีการรักษาความปลอดภัย เช่น มีระบบไฟฟ้าสำรอง มีระบบควบคุมการเข้าออก (Access Control) มีระบบกล้องวงจรปิด (CCTV) มีระบบแจ้งเตือนอัคคีภัย และมีระบบดับเพลิง (สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา, ม.ป.ป.)

บริการ Virtual Private Server เป็นการให้บริการเช่าคอมพิวเตอร์แม่ข่ายเสมือนที่ผู้ใช้เสมือนได้ใช้งานเครื่องคอมพิวเตอร์แม่ข่ายจริง ซึ่งเป็นการนำเทคโนโลยี Virtualization มาจำลองระบบปฏิบัติการ จำลองเครือข่าย และจัดสรรทรัพยากรในเครื่องคอมพิวเตอร์แม่ข่าย เสมือนมีเครื่องคอมพิวเตอร์หลายเครื่องที่ทำงานแยกอิสระต่อกัน แต่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แม่ข่ายเครื่องเดียวกัน (Almurayh, 2010) ซึ่ง Virtual Private Server จะช่วยให้สามารถจัดสรรทรัพยากรคอมพิวเตอร์ได้หลายวัตถุประสงค์ตามความต้องการ เช่น เพื่อรองรับเว็บไซต์ เพื่อใช้แสดงผลวิดีโอ หรือ เพื่อใช้เกมส์เซิร์ฟเวอร์ และยังมีความยืดหยุ่นในการปรับแต่งหรือขยายระบบได้ (BALEN et al., 2020)

โดยทั่วไปศูนย์ข้อมูล (Data Center) ที่ให้บริการทั้ง Virtual Private Server และ Colocation จะมีการขอการรับรองมาตรฐาน ISO/IEC 27001 ไม่ว่าจะเป็นองค์กรภาคเอกชน อย่าง TRUE IDC (True Internet Data Center) (True IDC, 2018) หรือ AIS Data Center (AIS, n.d.) และหน่วยงานภาครัฐอย่างสำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา ภายใต้สังกัดกระทรวงการอุดมศึกษาวิทยาศาสตร์ วิจัยและนวัตกรรม ที่มีการให้บริการ DATA CENTER & DISASTER RECOVERY CENTER (สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา, ม.ป.ป.) รวมถึงสถาบันการศึกษาอย่าง กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล (มหาวิทยาลัยมหิดล, 2025) ซึ่งองค์กรที่ให้บริการเหล่านี้มักจะมีการจัดการระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามหลักการ CIA และได้รับการรับรองมาตรฐาน ISO/IEC 27001 ซึ่งจะช่วยสร้างความมั่นใจให้กับลูกค้าที่จะมาใช้บริการว่ากระบวนการจัดการสารสนเทศของศูนย์ข้อมูลที่ใช้บริการจะมีความมั่นคงปลอดภัยสารสนเทศที่ได้มาตรฐานสากล

2.4. การวิเคราะห์ช่องว่าง (Gap Analysis)

การวิเคราะห์ช่องว่าง (Gap Analysis) คือวิธีการที่องค์กรใช้ประเมินช่องว่างความแตกต่างระหว่างสถานะที่เป็นอยู่ในปัจจุบันขององค์กรกับสถานะเป้าหมายที่องค์กรต้องการ เพื่อประเมินประสิทธิภาพขององค์กรว่าเพียงพอที่จะไปสู่เป้าหมายหรือต้องมีการดำเนินการเพิ่มเติม (Hanna & Sales, 2021) ซึ่งการวิเคราะห์ช่องว่างเป็นเครื่องมือที่มีประโยชน์ช่วยให้องค์กรสามารถมองเห็นภาพของตนเองได้ชัดเจนขึ้น ช่วยใน

การตัดสินใจวางแผนกลยุทธในการกำหนดเป้าหมาย ปรับปรุงกระบวนการ และประเมินผลการดำเนินงาน เพื่อให้บรรลุเป้าหมายที่วางไว้ (Einstein, 2024)

ในกระบวนการวิเคราะห์ช่องว่าง ประกอบด้วย 5 ขั้นตอนหลัก ดังนี้

(1) กำหนดวัตถุประสงค์ เป้าหมาย และขอบเขตที่จะประเมิน (Hanna & Sales, 2021)

(2) รวบรวมและทบทวนข้อมูลพื้นฐานจากเอกสารขององค์กร เช่น ผังกระบวนการ บทบาทหน้าที่ และข้อตกลงระดับบริการที่เกี่ยวข้อง (ดร.นิพนธ์ นาชิน, 2567)

(3) เก็บข้อมูลจากการสัมภาษณ์ผู้ที่เกี่ยวข้องเพิ่มเติม (ดร.นิพนธ์ นาชิน, 2567)

(4) วิเคราะห์ข้อมูลเปรียบเทียบสถานะปัจจุบันกับมาตรฐานหรือเป้าหมายที่ต้องการ และระบุช่องว่าง (Valdevit & Mayer, 2010)

(5) สรุปผลการวิเคราะห์ และจัดทำข้อเสนอแนะเพื่อการปรับปรุง (นาชิน, 2567)

การวิเคราะห์ช่องว่างสามารถนำไปใช้กับองค์กรที่จะเริ่มพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศให้เป็นไปตามมาตรฐานได้ ด้วยการประเมินสถานะความพร้อมขององค์กรในปัจจุบันในการที่จะปฏิบัติตามข้อกำหนดที่ระบุไว้ในมาตรฐาน ISO/IEC 27001 เพื่อประเมินทรัพยากรที่จำเป็นต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Valdevit & Mayer, 2010) โดยการวิเคราะห์ช่องว่างเพื่อพัฒนาระบบบริหาจัดการความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับมาตรฐาน ISO/IEC 27001 นั้นไม่ใช่เป็นการประเมินความเสี่ยง (Risk Assessment) แต่เป็นการพิจารณาใน 2 ประเด็นหลัก (The Department of Employment and Workplace Relations, Australian Government, 2022) คือ

(1) การระบุช่องว่างความสอดคล้องระหว่างการดำเนินงานขององค์กรกับข้อกำหนดหลัก (Main Requirements) ของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ โดยในข้อกำหนดที่ 4 ถึง 10 ซึ่งมีรายละเอียดตั้งแต่การกำหนดขอบเขตของระบบ การกำหนดบทบาทผู้นำ การประเมินและจัดการความเสี่ยง การจัดสรรทรัพยากรให้เพียงพอ การนำไปปฏิบัติ การประเมินประสิทธิภาพ และการปรับปรุงอย่างต่อเนื่อง

(2) การะบุช่องว่างเพื่อประเมินยืนยันว่าองค์กรมีการควบคุมความมั่นคงปลอดภัยแล้ว หรือต้องมีการดำเนินการเพิ่มเติมเพื่อจัดการความเสี่ยงตามข้อกำหนด 6.1.3 โดยอาจจะระบุยืนยันว่าดำเนินการแล้วหรือยังไม่ได้ดำเนินกาน หรืออาจจะระบุเป็นระดับของการประเมินว่ามีการดำเนินการอยู่ในระดับใด

การวิเคราะห์ช่องว่างเป็นเครื่องมือที่มีประสิทธิภาพในการระบุและจัดการกับช่องว่างระหว่างสถานะปัจจุบันและเป้าหมายขององค์กร ที่มุ่งมั่นจะพัฒนาระบบการจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 การดำเนินการวิเคราะห์ช่องว่างอย่างเป็นระบบช่วยให้องค์กรสามารถจัดลำดับความสำคัญในการปรับปรุงและพัฒนากระบวนงานได้อย่างมีประสิทธิภาพ นำไปสู่การเพิ่มระดับความมั่นคงปลอดภัยและความสอดคล้องกับมาตรฐาน ISO/IEC 27001 ในระยะยาวต่อไป

2.5. กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

2.5.1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

วัตถุประสงค์ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 คือเพื่อป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในประเทศและภายนอกประเทศ ที่อาจกระทบต่อการให้บริการแก่ประชาชน หรือส่งผลกระทบต่อความมั่นคง เศรษฐกิจ การทหาร และความความสงบเรียบร้อยภายในประเทศ เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที ซึ่งในพระราชบัญญัติได้กำหนดให้หน่วยงานของรัฐต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยในมาตรา 44 ของพระราชบัญญัติ กำหนดไว้ว่าให้แต่ละหน่วยต้องจัดทำประมวลผลแนวทางปฏิบัติและกรอบมาตรฐานด้านการนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งในประมวลผลแนวทางและกรอบมาตรฐานจะต้องประกอบด้วยแผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง และแผนการรับมือภัยคุกคามทางไซเบอร์เป็นอย่างน้อย และในมาตรา 45 ก็กำหนดให้หน่วยงานของรัฐต้องดำเนินการให้เป็นไปตามประมวลผลแนวทางปฏิบัติและกรอบมาตรฐานที่กำหนดไว้

ในมาตรา 60 ของพระราชบัญญัติฉบับนี้ได้กำหนดลักษณะของภัยคุกคามไซเบอร์ออกเป็น 3 ระดับ ได้แก่

(1) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง

(2) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลท าให้ระบบ

คอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหายจนไม่สามารถทำงานหรือให้บริการได้

(3) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะดังต่อไปนี้

(3.1) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรงโดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้างจนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

(3.2) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

2.5.2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีการประกาศฉบับแรก เมื่อปี 2550 และมีการปรับปรุงแก้ไขประกาศฉบับที่ 2 ออกมาเมื่อปี 2560 โดยมีวัตถุประสงค์เพื่อสร้างความตระหนักถึงความมั่นคงปลอดภัยสารสนเทศ มีการกำหนดฐานความผิดและบทลงโทษผู้ที่กระทำความผิดที่เกี่ยวกับข้อมูลและระบบคอมพิวเตอร์ หรือการไม่ปฏิบัติตามที่กฎหมายกำหนดไว้ รวมถึงมีการกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ ผู้ใช้บริการ และผู้ให้บริการ ซึ่งคำว่า “ผู้ให้บริการ” ในพระราชบัญญัติได้นิยามความหมายไว้ดังนี้

(1) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่นโดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

จากนิยามในพระราชบัญญัติแสดงให้เห็นว่าสำนักเทคโนโลยีดิจิทัลและสารสนเทศจึงอยู่ในบทบาทของผู้ให้บริการและมีหน้าที่ความรับผิดชอบที่ต้องปฏิบัติตามที่กฎหมายกำหนดไว้ ซึ่งหน้าที่ความรับผิดชอบและบทลงโทษที่เกี่ยวข้องกับผู้ให้บริการในพระบัญญัติฉบับนี้ มีดังนี้

(1) มาตรา 15 กำหนดว่าผู้ให้บริการที่จงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องรับโทษเช่นเดียวกับผู้กระทำความผิด ยกเว้นผู้ให้บริการสามารถพิสูจน์ได้ว่าได้ปฏิบัติตามประกาศของรัฐมนตรีที่กำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์ ซึ่งมาตรา 14 ได้กำหนดรูปแบบความผิดไว้ดังนี้

(1.1) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน

(1.2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(1.3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(1.4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(1.5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1.1) (1.2) (1.3) หรือ (1.4)

(2) มาตรา 18 หากมีการร้องขอจากพนักงานเจ้าหน้าที่ให้ดำเนินการตามพระราชบัญญัติ ต้องดำเนินการตามคำร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเจ็ดวันนับแต่วันที่ได้รับคำร้องขอ หรือภายในระยะเวลาที่พนักงานเจ้าหน้าที่กำหนด ซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ได้รับอนุญาตจากพนักงานเจ้าหน้าที่

(3) มาตรา 20 กรณีที่มีคำสั่งศาลให้ระงับการเผยแพร่หรือลบข้อมูลคอมพิวเตอร์ที่มีความผิดตามพระราชบัญญัติ หรือเป็นข้อมูลคอมพิวเตอร์ที่อาจจะกระทบความมั่นคงของประเทศ หรือเป็นข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา หรือกฎหมายอื่น ผู้ให้บริการมีหน้าที่ต้องปฏิบัติตามคำสั่งภายในระยะเวลาที่พนักงานเจ้าหน้าที่กำหนด

(4) มาตรา 26 กำหนดว่าผู้ให้บริการต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้ โดยต้องจัดเก็บรักษาข้อมูลผู้ใช้บริการเท่าที่จำเป็นที่สามารถระบุตัวตนของผู้ใช้บริการได้ ทั้งนี้หากผู้ให้บริการไม่ปฏิบัติตามจะต้องโดนปรับไม่เกิน 500,000 บาท

(5) มาตรา 27 กำหนดว่าหากไม่ปฏิบัติตามคำสั่งศาลหรือพนักงานเจ้าหน้าที่ตามมาตรา 18 และมาตรา 20 ต้องระวางโทษปรับไม่เกิน 200,000 บาท และปรับเป็นรายวันอีกไม่เกินวันละ 5,000 บาทจนกว่าจะปฏิบัติให้ถูกต้อง

2.6. บทความ/งานวิจัยที่เกี่ยวข้อง

รุ้งตะวัน ประสนิท, ศุภวัฒน์ แซ่วื้อ, นรินทร์ พนาวาส, และจิราภรณ์ ชมยิ้ม (2024) ได้ทำการวิจัยตรวจประเมินความสอดคล้องมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 และทำการตรวจสอบช่องโหว่ทางเทคนิคของระบบปฏิบัติการ และโปรแกรมแอปพลิเคชัน ด้วยเครื่องมือโปรแกรม OpenVAS (Open Vulnerability Assessment System) ผลการวิจัย พบว่า จากเกณฑ์ประเมินความสอดคล้องของมาตรการการรักษาความมั่นคงปลอดภัยสารสนเทศเทียบกับมาตรฐาน ISO/IEC 27001:2022 ที่กำหนดไว้ว่าต้องสอดคล้องกับข้อกำหนดไม่น้อยกว่า 80% นั้นพบว่า มาตรการการควบคุมของบริษัท A มีความสอดคล้องด้านองค์กร 16 % ด้านบุคลากร 88% ด้านกายภาพ 68% และด้านการควบคุมเทคโนโลยี 57% ซึ่งแสดงให้เห็นว่าองค์กรมีการควบคุมด้านบุคลากรที่ผ่านการประเมิน ส่วนอีก 3 ด้านที่เหลือควรมีการปรับปรุงมาตรการให้สอดคล้องกับข้อกำหนดของ ISO/IEC 27001:2022 ในส่วนการตรวจสอบช่องโหว่ทางเทคนิคของระบบปฏิบัติการ และโปรแกรมแอปพลิเคชันบนเครื่องแม่ข่าย จำนวน 4 เครื่อง พบช่องโหว่อยู่ระดับ Medium และ High ซึ่งอยู่ในระดับที่ไม่ปลอดภัย และมีความเสี่ยงต่อการถูกโจมตี องค์กรควรปรับปรุงแก้ไขระบบเครื่องแม่ข่าย และสร้างความตระหนักให้กับบุคลากรให้ตระหนักถึงความมั่นคงปลอดภัยสารสนเทศ

ชนกานต์ อาภรณ์พงษ์, และบัวเรียน สูงพล (2023) ได้ทำการวิจัยกรอบโครงร่างความมั่นคงปลอดภัยระบบสารสนเทศ (ISO27001:2013) : กรณีศึกษา สำนักงานคณะกรรมการหลักทรัพย์และตลาดหลักทรัพย์ ซึ่งมีวัตถุประสงค์เพื่อให้องค์กรในภาคตลาดทุนหรือตลาดหลักทรัพย์สามารถปฏิบัติ รักษา ปรับปรุง และพัฒนาระบบบริหารความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศอย่างต่อเนื่อง นอกจากนี้ ยังมุ่งหวังให้แนวปฏิบัติของสำนักงาน ก.ล.ต. สามารถเป็นแนวทางในการแนะนำองค์กรหรือหน่วยงานในภาคตลาดทุนในการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศตามมาตรฐานสากล โดยใช้ระเบียบวิธีวิจัยเชิงคุณภาพด้วยวิธีการวิเคราะห์เนื้อหา (Content Analysis) ของแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) เปรียบเทียบกับมาตฐาน ISO/IEC 27001:2013 เพื่อหาความแตกต่าง (Gap) ระหว่างระบบที่เป็นอยู่ในปัจจุบัน (As Is) กับมาตราฐานที่ต้องการจะเป็นในอนาคต (To Be) รวมทั้งมีการประเมินความพึงพอใจการเปรียบเทียบแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. กับมาตรฐาน ISO 27001:2013 จากบุคลากรที่ดำเนินการด้านความมั่นคงปลอดภัยในสำนักงาน ก.ล.ต. จำนวน 10 คน พบว่าอยู่ในระดับความพึงพอใจมาก มีค่าคะแนนเฉลี่ยอยู่ที่ 4.40 และมีค่าเบี่ยงเบนมาตรฐาน 0.457 ทั้งนี้ยังได้มีข้อเสนอแนะปรับปรุงเนื้อหาของแนวปฏิบัติใน

การจัดให้มีระบบเทคโนโลยีสารสนเทศเพิ่มเติมให้มีมาตรการควบคุมครอบคลุมทุกข้อกำหนดของมาตรฐาน ISO 27001:2013 เพื่อให้แนวปฏิบัติมีความสอดคล้องกับมาตราฐานได้ครบถ้วน

Omar A.Fonseca-Herrera, Alix E. Rojas และ Hector Flores (Fonseca-Herrera et al., 2021) ได้ศึกษาและพัฒนาแบบจำลอง (Model) ที่ช่วยในการประเมินสถานะด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรในปัจจุบัน เพื่อเตรียมความพร้อมในการนำระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 ไปใช้วางแผนการจัดการความมั่นปลอดภัยสารสนเทศขององค์กรอย่างต่อเนื่อง โดยแบบจำลองประกอบด้วย ระยะที่1 เป็นการวิเคราะห์องค์ประกอบความมั่นคงปลอดภัยขององค์กรในปัจจุบันเปรียบเทียบกับมาตรฐาน ISO/IEC 27001:2013 โดยใช้การสัมภาษณ์ แบบสอบถาม ทบทวนเอกสาร และสังเกตการณ์ ระยะที่ 2 เป็นการเตรียมความพร้อมด้วยการวิเคราะห์บริบทขององค์กร กำหนดปัจจัยภายในและภายนอก การกำหนดโครงสร้างองค์กร และการกำหนดทรัพยากรที่จำเป็นต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ระยะที่ 3 เป็นการจัดทำบัญชีทรัพย์สิน การระบุและประเมินความเสี่ยง การวางแผนจัดการความเสี่ยง และการกำหนดนโยบายควบคุมความมั่นคงปลอดภัยสารสนเทศ ซึ่งผู้วิจัยได้นำแบบจำลองนี้ไปใช้กับบริษัทหนึ่งในประเทศโคลอมเบียที่ทำธุรกิจเกี่ยวกับอุตสาหกรรมน้ำมันและไฮโดรคาร์บอน และพบว่าบริษัทมีการนำข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศไปใช้กับกระบวนการด้านเทคโนโลยีสารสนเทศ โดยไม่ได้ให้ความสำคัญกับกระบวนการอื่นของบริษัท มีข้อบกพร่องในด้านการจัดการเอกสารให้เป็นไปตามมาตรฐานที่กำหนด การประเมินและจัดการความเสี่ยง และการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศภายในบริษัท ทั้งนี้บทสรุปของการนำแบบจำลองนี้ไปใช้จะช่วยให้เข้าใจสถานะที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กรในปัจจุบัน และช่วยในการวางแผนกลยุทธในการขับเคลื่อนระบบบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กรให้รองรับมาตรฐาน ISO/IEC 27001

แววตาม เตชาทวีวรรณ (2020) ได้ศึกษาวิจัยเชิงคุณภาพแบบวิธีศึกษาเฉพาะกรณี เรื่อง “สภาพและปัญหาการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของห้องสมุดสถาบันอุดมศึกษาของรัฐ” โดยใช้เครื่องมือแบบสัมภาษณ์กึ่งโครงสร้าง และวิเคราะห์เนื้อหา (Content analysis) เกี่ยวกับสภาพ ปัญหา และแนวโน้มการดำเนินงานตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ของห้องสมุดสถาบันอุดมศึกษาของรัฐ จำนวน 7 แห่ง ซึ่งผลการศึกษาวิจัย พบว่ามีเพียงสถาบันอุดมศึกษาของรัฐบางแห่งที่มีการกำหนดนโยบายในการักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นลายลักษณ์อักษร แต่ห้องสมุดทุกแห่งก็มีการกำหนดข้อปฏิบัติในการรักษาความมั่นคงปลอดภัย

ด้านสารสนเทศของห้องสมุดเอง โดยกำหนดเป็นประกาศและข้อปฏิบัติสำหรับบุคลากรและผู้ใช้ห้องสมุด มีการกำหนดควบคุมและบริหารจัดการสิทธิในการเข้าถึงและใช้งานสารสนเทศ มีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต มีการกำหนดหน้าที่ความรับผิดชอบให้แก่บุคลากรที่ชัดเจน ยกเว้นตำแหน่งบรรณารักษ์และเจ้าหน้าที่ห้องสมุดที่ไม่ใช่ตำแหน่งที่เกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ที่ไม่พบการกำหนดหน้าที่ความรับผิดชอบในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของห้องสมุด และในส่วนการสำรองข้อมูลในระบบสารสนเทศของห้องสมุดมีทั้งแบบมือและแบบอัตโนมัติมากกว่า 1 วิธี นอกจากนี้ระบบสารสนเทศของห้องสมุดยังมีลักษณะเป็น Redundant ที่ระบบใดระบบหนึ่งเสียหายก็สามารถใช้อีกระบบแทนได้

ชุลีกร นวลสมศรี, และ ดร.สุทธิศักดิ์ จันทวงษ์โส (2017) ได้ทำการวิจัยเชิงสำรวจ เรื่อง “การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO 27001:2013 กรณีศึกษาขององค์กรด้านการบินแห่งหนึ่ง” ซึ่งมีวัตถุประสงค์เพื่อระบุและประเมินความเสี่ยง และนำเสนอแนวทางในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO 27001:2013 ขององค์กรด้านการบินแห่งหนึ่ง โดยดำเนินการวิจัยใช้แบบสอบถามเก็บรวบรวมข้อมูลจากพนักงานขององค์กร จำนวน 137 คน กำหนดตัวแปรต้นเป็น การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้ข้อกำหนด Annex A ของมาตรฐาน ISO 27001:2013 จำนวน 14 ด้าน และตัวแปรตาม เป็นระดับความเสี่ยงและแนวทางการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO 27001:2013 พบว่าองค์กรมีความเสี่ยงอยู่ในระดับสูง จำนวน 6 ด้าน ซึ่งอยู่ในเกณฑ์ที่องค์กรไม่สามารถยอมรับได้ ต้องมีการจัดการเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และมีความเสี่ยงอยู่ในระดับปานกลาง จำนวน 8 ด้าน ซึ่งจะต้องมีการควบคุมเพื่อไม่ให้ความเสี่ยงมีระดับสูงขึ้นจนอยู่ในเกณฑ์ที่ยอมรับไม่ได้ ทั้งนี้ยังได้นำเสนอแนวทางในการบริหารความเสี่ยงสำหรับนำไปกำหนดแผนบริหารความเสี่ยง และนำเสนอให้ผู้บริหารพิจารณานำไปใช้โดยมีกลไกติดตามผลการดำเนินงานเป็นระยะ

บทที่ 3. วิธีการดำเนินการวิเคราะห์

การวิเคราะห์ความพร้อมขององค์กรในการขอรับรองมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 กรณีศึกษาสำนักเทคโนโลยีดิจิทัลและสารสนเทศนี้ เป็นการวิเคราะห์เชิงปริมาณ ด้วยการวิเคราะห์ช่องว่าง (Gap Analysis) จากการศึกษาข้อมูลในเอกสาร และสอมถามผู้ที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ และทำการเปรียบเทียบว่าความสอดคล้องระหว่าง ข้อกำหนดในมาตรฐาน ISO/IEC 27001:2022 กับการดำเนินงานของสำนักเทคโนโลยีในปัจจุบัน โดยมีองค์ประกอบดังนี้

(1) ขั้นตอนการดำเนินงาน

(2) การเก็บรวบรวมข้อมูล

(3) เครื่องมือที่ใช้และวิธีการวิเคราะห์

3.1. ขั้นตอนการดำเนินงาน

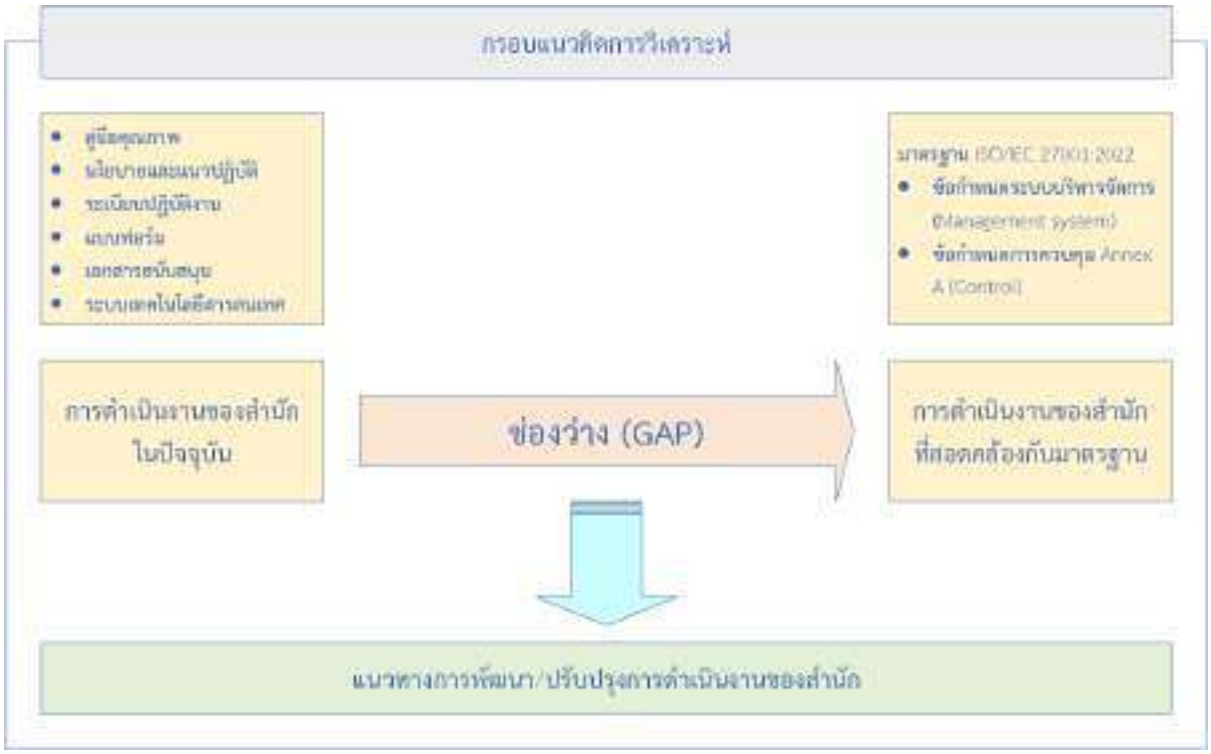
ในการวิเคราะห์ความพร้อมของสำนักเทคโนโลยีดิจิทัลและสารสนเทศเพื่อขอรับรองระบบมาตรฐานความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 นี้ มีกรอบแนวคิดในการวิเคราะห์ที่มุ่งเน้นการเปรียบเทียบสถานะการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัลในปัจจุบันกับเป้าหมายที่สำนักจะดำเนินงานให้สอดคล้องกับเป็นไปตามที่ข้อกำหนด เพื่อระบุช่องว่าง (Gap) ที่เกิดขึ้นและนำไปวิเคราะห์นำเสนอแนวทางในการพัฒนาหรือปรับปรุงการดำเนินงานของสำนักต่อไป โดยมีขั้นตอนการดำเนินงานวิเคราะห์ดังนี้

(1) ศึกษาข้อกำหนดในมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 และแนวทาง (Guidance) การควบคุมใน ISO/IEC 27002:2022

(2) ทำการรวบรวมข้อมูลและเอกสารที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

(3) วิเคราะห์เปรียบเทียบระหว่างข้อกำหนดของมาตรฐานเป้าหมายที่ต้องดำเนินการให้ครบถ้วนกับสถานะการดำเนินงานในปัจจุบันของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ ด้วยการศึกษาจากเอกสารที่รวบรวม และสอมถามเพิ่มเติมจากผู้ปฏิบัติงานที่เกี่ยวข้อง

(4) ประเมินผลการวิเคราะห์และจัดทำข้อเสนอแนะแนวทางปรับปรุงการดำเนินงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศให้มีความสอดคล้องกับข้อกำหนดของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022



ภาพที่ 3-1 กรอบแนวคิดการวิเคราะห์ความพร้อมในการขอรับรองมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 กรณีศึกษา สำนักเทคโนโลยีดิจิทัลและสารสนเทศ

3.2. การเก็บรวบรวมข้อมูล

ในการเก็บรวบรวมข้อมูลในงานวิเคราะห์นี้ได้มาจากการศึกษาข้อมูลและเอกสารภายในสำนักเทคโนโลยีดิจิทัลและสารสนเทศ และสัมภาษณ์เพื่อรวบรวมข้อมูลเพิ่มเติมจากผู้ปฏิบัติงานที่เกี่ยวข้องกับขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ โดยเอกสารระบบบริหารความมั่นคงปลอดภัยสารสนเทศของสำนักมีการจัดทำให้สอดคล้องกับมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013 และมาตรฐานระบบบริหารจัดการคุณภาพ ISO 9001:2015 เนื่องจากสำนักได้ขอรับรองมาตรฐานทั้งสองดังกล่าวร่วมกัน ซึ่งเอกสารที่จัดทำมีการควบคุมด้วยการจัดทำบัญชีเอกสารตามหมวดหมู่ ระบุส่วนงานที่รับผิดชอบเอกสาร และลำดับชั้นความลับของข้อมูล นอกจากนี้ยังมีข้อมูลที่ถูกจัดเก็บไว้ในระบบเทคโนโลยีสารสนเทศต่างๆที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศของสำนัก ซึ่งแหล่งข้อมูลที่รวบรวมมาใช้ในการวิเคราะห์ ประกอบด้วย

3.2.1. คู่มือคุณภาพ (Quality Manual : QM)

คู่มือคุณภาพของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ จัดทำขึ้นเพื่ออธิบายถึงขอบเขตการดำเนินงานเพื่อการขอรับรองมาตรฐานระบบบริหารคุณภาพ ISO 9001:2015 และระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013 โดยอธิบายถึงการบริหารจัดการที่ต้องดำเนินการ ตั้งแต่การทำความเข้าใจบริบทของสำนัก และความคาดหวังของผู้มีส่วนเกี่ยวข้อง กระบวนการในระบบบริหารจัดการ การวางแผนการปฏิบัติงาน การสนับสนุนกระบวนการ การติดตามเฝ้าระวัง ประเมินผล และการปรับปรุงการดำเนินงานอย่างต่อเนื่อง

ในส่วนขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศที่สำนักได้รับการรับรองมาตรฐาน ISO/IEC 27001:2013 คือ การให้บริการ Colocation และ Virtual Private Server สำหรับคณะ/สำนัก/ศูนย์ภายในสถาบัน

3.2.2. ระเบียบปฏิบัติงาน (Quality Procedure : QP)

เอกสารระเบียบปฏิบัติงานในหมวดหมู่นี้จัดทำขึ้นเพื่อใช้อธิบายรายละเอียดของกระบวนการปฏิบัติงาน โดยแต่ละระเบียบปฏิบัติงานจะระบุวัตถุประสงค์ ขอบเขต คำจำกัดความ หน้าที่ความรับผิดชอบ ขั้นตอนการปฏิบัติพร้อมผังการไหลของงาน แบบฟอร์มที่ใช้ประกอบ และเอกสารอ้างอิง ซึ่งแต่ละระเบียบปฏิบัติที่เกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ จะแบ่งตามส่วนงานภายในสำนักที่รับผิดชอบดังนี้

(1) ส่วนโครงสร้างพื้นฐานและความมั่นคง มีระเบียบปฏิบัติงานที่เกี่ยวข้อง ได้แก่ การให้บริการโครงสร้างพื้นฐาน งานบำรุงรักษา การควบคุมการเปลี่ยนแปลง (Change Management) และการจัดการเหตุขัดข้อง (Incident Management)

(2) ส่วนบริหารและพัฒนาองค์กร มีระเบียบปฏิบัติงานที่เกี่ยวข้อง ได้แก่ การควบคุมการดำเนินงานงานที่ไม่เป็นไปตามข้อกำหนดในระบบคุณภาพ การตรวจติดตามภายในของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ การจัดแผนการปฏิบัติงาน การติดตามและประเมินผลการปฏิบัติงาน และกระบวนการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลสารสนเทศ

(3) ส่วนธุรการ การเงิน และพัสดุ มีระเบียบปฏิบัติงานที่เกี่ยวข้อง ได้แก่ การปฏิบัติงานการรับส่ง-ส่งเอกสารผ่านระบบ e-doc การจัดทำแผนพัฒนาบุคลากรรายบุคคลประจำปี การควบคุมเอกสารของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ การจัดการกฎหมายและข้อกำหนดที่เกี่ยวข้อง การดูแลรักษาครุภัณฑ์ การจัดซื้อ/จัดจ้างของสำนัก การประเมินผู้ขายของสำนัก

3.2.3. แบบฟอร์ม (Form : FM)

การจัดทำแบบฟอร์มในการปฏิบัติงานมีวัตถุประสงค์ไว้สำหรับจัดเก็บข้อมูลรายละเอียดของการดำเนินงานเพื่อใช้เป็นหลักฐานอ้างอิงในการตรวจสอบย้อนหลังได้ ซึ่งบางขั้นตอนปฏิบัติงานก็มีการกำหนดไว้ว่าต้องใช้แบบฟอร์มใดในการใช้จัดเก็บข้อมูล โดยสำนักได้แบ่งหมวดหมู่ของแบบฟอร์มตามส่วนงานภายในสำนักที่รับผิดชอบดังนี้

(1) **ส่วนโครงสร้างพื้นฐานและความมั่นคง** มีแบบฟอร์มที่เกี่ยวข้อง ได้แก่ ทะเบียนรายการการบำรุงรักษาด้านโครงสร้างพื้นฐาน (Assets Register) แผน-ผลการบำรุงรักษาด้านโครงสร้างพื้นฐาน (Maintenance Schedule) ตารางการสำรองข้อมูลตามรายการอุปกรณ์หรือระบบ (Backup Register) แบบฟอร์มการขอใช้อินเทอร์เน็ตแบบชั่วคราว แบบฟอร์มการขออีเมลกลางสำหรับหน่วยงานหรือหลักสูตร แบบฟอร์มการขอรับบริการ Virtual Private Server/Domain แบบฟอร์มการขอบัญชีผู้ใช้งานสำหรับอาจารย์พิเศษ แบบฟอร์มการขอรับบริการ VPN แบบฟอร์มการขอรับฝากเครื่องแม่ข่าย Co-location และการขอเปลี่ยนแปลงระบบ (Change Request Form)

(2) **ส่วนบริหารและพัฒนาองค์การ** มีแบบฟอร์มที่เกี่ยวข้อง ได้แก่ แบบฟอร์มแผนปรับปรุงตามข้อมูล feedback ในแบบสำรวจของผู้รับบริการของสำนักเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ แบบฟอร์มการรายงานผลการดำเนินการตามแผนปรับปรุงตามข้อมูล feedback ในแบบสำรวจของผู้รับบริการของสำนักเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ Internal Audit Checklist แบบรับเรื่องร้องเรียนจากผู้รับบริการ NON-COMPLIANCE REPORT (NCR) รายงานการตรวจติดตามคุณภาพภายใน (Internal Audit Result Report) และ แบบฟอร์มการประเมินความเสี่ยงและโอกาสเกิด

(3) **ส่วนธุรการ การเงิน และพัสดุ** มีแบบฟอร์มที่เกี่ยวข้อง ได้แก่ แบบขออนุมัติเอกสาร (Document Approval Request : DAR) แบบฟอร์มแผนพัฒนาบุคลากรรายบุคคล แบบฟอร์มแบบติดตามและประเมินผลสัมฤทธิ์จากการพัฒนาตนเอง แบบฟอร์มการขออนุมัติเข้ารับการอบรม/สัมมนา/ประชุม ทั้งกรณีไม่ใช้งบประมาณ และกรณีไม่ใช้งบประมาณ แบบฟอร์มการยืม-คืนครุภัณฑ์ แบบฟอร์มการบันทึกติดตามและประสานงานกับผู้ขาย แบบฟอร์มการประเมินผู้ขายหลังการขาย แบบฟอร์มการขอซื้อวัสดุ/อุปกรณ์ แบบฟอร์มการจัดซื้อ/จัดจ้าง พร้อมแจ้งงบประมาณคงเหลือ แบบฟอร์มการประเมินคัดเลือกผู้ขาย แบบฟอร์มส่งซ่อมวัสดุ/ครุภัณฑ์ และรายงานการทำลายข้อมูล/สื่อบันทึกข้อมูล

3.2.4. แนวปฏิบัติ/นโยบายของส่วนงาน (Practice/Policy : PC)

เอกสารที่เกี่ยวข้องกับนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ ถูกจัดทำขึ้นเพื่อใช้เป็นกรอบแนวทางและมาตรการควบคุมการดำเนินงานให้เป็นเป็นไปตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศตามขอบเขตการขอรับรองมาตรฐาน ISO/IEC 27001:2013 ซึ่งประกอบด้วย แนวปฏิบัติเรื่องการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์(Log management) นโยบายการใช้งานอุปกรณ์พกพาและการทำงานจากระยะไกล (Mobile device and teleworking policy) นโยบายการควบคุมการเข้าถึง (Access Control Policy) แนวปฏิบัติในการควบคุมการเข้าถึงเครือข่าย (Network Access Control) นโยบายการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยต่อระบบสารสนเทศ แนวปฏิบัติการบริหารจัดการทรัพย์สิน (Asset Management Procedure) แนวปฏิบัติการบริหารจัดการใช้ทรัพยากร (Capacity Management) และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

3.2.5. เอกสารสนับสนุน (Supporting Document : SD)

เอกสารที่อยู่ในหมวดหมู่เอกสารสนับสนุน เป็นเอกสารที่ไม่สามารถจัดอยู่ในหมวดหมู่ใดๆที่กำหนดไว้ แต่เป็นเอกสารที่มีความจำเป็นที่ต้องกำหนดไว้ให้สอดคล้องกับข้อกำหนดในมาตรฐาน ISO/IEC 27001:2013 ได้แก่ Statement of Applicability (SOA) ซึ่งเป็นเอกสารที่จำเป็นต้องจัดทำขึ้นเพื่อบ่งบอกถึงมาตรการและเหตุผลในการดำเนินงานที่ครอบคลุมทั้งข้อกฎหมาย ทั้งทางกายภาพและทางเทคนิค เพื่อควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Stanik & Kiedrowicz, 2022) หรือเป็นเอกสารที่มีความสำคัญในการสนับสนุนระบบบริหารความมั่นคงปลอดภัยสารสนเทศของสำนัก ได้แก่ ข้อกำหนดและเงื่อนไขการให้บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Private Server) และ ข้อกำหนดและเงื่อนไขการให้บริการรับฝากเครื่องคอมพิวเตอร์แม่ข่าย (Colocation)

3.2.6. ระบบเทคโนโลยีสารสนเทศ (Information Technology System)

นอกจากข้อมูลที่อยู่ในรูปแบบของเอกสารกระดาษหรือไฟล์เอกสารแล้ว สำนักยังมีข้อมูลที่อยู่ในรูปแบบดิจิทัลและถูกจัดเก็บไว้ในระบบเทคโนโลยีสารสนเทศที่สำนักนำมาใช้เป็นเครื่องมือที่ช่วยในการบริหารจัดการระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ เช่น ระบบบริหารจัดการข้อมูลล็อก (Log management) ที่จัดเก็บข้อมูลล็อกให้เป็นตามพระราชบัญญัติว่าด้วยการการทำความผิดทางคอมพิวเตอร์ ระบบบริหารจัดการอุปกรณ์ Firewall ที่ช่วยในการควบคุมและจัดการสิทธิในการเข้าถึงเครือข่ายภายในสถาบัน และระบบกล้องวงจรปิด (CCTV) ที่สามารถตรวจสอบการเข้าออกห้องภายในศูนย์ข้อมูล (Data center) นอกจากนี้ส่วนงาน

โครงสร้างพื้นฐานและความมั่นคงปลอดภัยซึ่งเป็นส่วนงานสำคัญของขอบเขตระบบบริหารความมั่นคงปลอดภัยสารสนเทศยังบันทึกข้อมูลที่เกี่ยวข้องกับการดำเนินการไว้ใน SharePoint ของส่วนงานที่อยู่ในระบบ Microsoft 365 เช่น ข้อมูลบัญชีทรัพย์สิน (Asset) ข้อมูลประวัติการจัดการกับเหตุที่เกี่ยวข้องความมั่นคงปลอดภัยสารสนเทศ (Incident management)

3.3. เครื่องมือและวิธีการวิเคราะห์

การวิเคราะห์ช่องว่างระหว่างข้อกำหนดในมาตรฐาน ISO/IEC 27001:2022 กับการดำเนินงานในระบบบริหารความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัลและสารสนเทศนั้น ใช้เครื่องมือในการวิเคราะห์ข้อมูลที่ได้พัฒนาขึ้นเพื่อให้สอดคล้องกับแนวคิดของการวิเคราะห์ คือ แบบประเมินระดับการดำเนินงานดังรูปแบบนี้

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน

เกณฑ์ในการประเมินผลมีอยู่ 4 ระดับ ดังนี้

(1) C หมายถึง มีการดำเนินงานที่สอดคล้องกับข้อกำหนดครบถ้วน

(2) P หมายถึง มีการดำเนินงานที่สอดคล้องกับข้อกำหนดบางส่วน

(3) N หมายถึง ไม่มีการดำเนินงานที่สอดคล้องกับข้อกำหนด

(4) E หมายถึง สำนักขอยกเว้นไม่ขอรับการประเมินเพื่อขอรับรองมาตรฐาน

ในการวิเคราะห์ข้อมูลเพื่อประเมินระดับการดำเนินงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศนั้น ได้มาจากการศึกษาและพิจารณาเอกสารที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ ทั้งนโยบายและแนวปฏิบัติ ขั้นตอนปฏิบัติงาน บันทึกผลการดำเนินงาน และข้อมูลที่ได้จากการสัมภาษณ์บุคลากรภายในสำนักที่เกี่ยวข้อง มาเปรียบเทียบกับข้อกำหนดระบบบริหารจัดการ 23 ข้อกำหนด และข้อกำหนดการการควบคุม Annex A ทั้ง 93 ข้อกำหนด แล้วนำผลการประเมินมาคำนวณร้อยละของการดำเนินงานที่สอดคล้องกับข้อกำหนด แยกตามประเภทของข้อกำหนด และตามหมวดหมู่ของข้อกำหนดการควบคุม เพื่อระบุข้อกำหนดที่จำเป็นต้องปรับปรุงหรือแก้ไข

บทที่ 4. ผลการวิเคราะห์

การวิเคราะห์ความพร้อมขององค์กรในการขอรับรองมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 กรณีศึกษาสำนักเทคโนโลยีดิจิทัลและสารสนเทศนี้ เป็นการศึกษาความประเมินหาความแตกต่างหรือช่องว่าง (Gap) ของการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ กับข้อกำหนดในมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 โดยคาดว่าผลที่ได้จากการวิเคราะห์จะสามารถนำไปใช้ประโยชน์ในการประเมินความพร้อมของสำนักในการขอรับรองมาตรฐานดังกล่าว และนำไปใช้ในการวางแผนพัฒนาหรือปรับปรุงนโยบาย แนวปฏิบัติ กระบวนการ และขั้นตอนการปฏิบัติงานให้มีประสิทธิภาพมีความสอดคล้องกับข้อกำหนดในมาตรฐาน ISO/IEC 27001:2022 ครบถ้วนตามขอบเขตการขอรับรองมาตรฐาน โดยมีองค์ประกอบของผลการวิเคราะห์ดังนี้

(1) ผลการวิเคราะห์ข้อกำหนดการบริหารจัดการ

(2) ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านองค์กร

(3) ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านบุคคล

(4) ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านกายภาพ

(5) ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านเทคโนโลยี

4.1. ผลการวิเคราะห์ข้อกำหนดระบบบริหารจัดการ

ในข้อกำหนดระบบบริหารจัดการ (Management system requirements) ของมาตรฐาน ISO/IEC 27001:2022 ประกอบด้วย 7 หมวดหลัก จำนวน 23 ข้อ ซึ่งมีผลการวิเคราะห์ดังนี้

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
4	**บริบทขององค์กร (Context of the organization)**			
4.1	**ความเข้าใจองค์กรและบริบทขององค์กร (Understanding the organization and its context)** องค์กรต้องกำหนดประเด็นภายในและภายนอกที่เกี่ยวข้องกับวัตถุประสงค์ขององค์กร และส่งผลต่อความสามารถในการดำเนินงานเพื่อให้บรรลุผลลัพธ์ของระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามที่ต้องการ	สำนักมีการวิเคราะห์ประเด็นที่เป็นปัจจัยภายในและภายนอกด้วยการวิเคราะห์ SWOT (Strengths-Weaknesses-Opportunities-Threats) และกำหนดไว้ในแผนยุทธศาสตร์ของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ	- แผนยุทธศาสตร์ของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2567 - 2570	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
4.2	**ความเข้าใจในความต้องการที่จำเป็นและความคาดหวังของผู้ที่มีส่วนได้ส่วนเสีย (Understanding the needs and expectations of interested parties)** องค์กรต้องกำหนดผู้มีส่วนได้ส่วนเสีย และข้อกำหนดของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ข้อกำหนดอาจรวมถึงกฎหมาย กฎระเบียบ และพันธะสัญญาที่เกี่ยวข้อง	สำนักมีการกำหนดผู้มีส่วนได้ส่วนเสีย วิเคราะห์ความต้องการ/ความคาดหวังของผู้มีส่วนได้ส่วนเสียไว้ในแผนยุทธศาสตร์ของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ รวมถึงมีการระบุกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศของสำนัก	- แผนยุทธศาสตร์ของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2567 – 2570 - ไฟล์เอกสาร List of Legal	C
4.3	**การกำหนดขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Determining the scope of the information security management system)**	สำนักยังคงกำหนดขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศเพื่อเตรียมขอรับการรับรองมาตรฐาน ISO/IEC 27001:20022 เช่นเดียวกับการขอรับรองมาตรฐาน ISO/IEC	- คู่มือคุณภาพสำนักเทคโนโลยีดิจิทัลและสารสนเทศ	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	องค์กรต้องกำหนดขอบเขตและการประยุกต์ใช้ระบบบริหารความมั่นคงปลอดภัยสารสนเทศเพื่อระบุขอบเขตการดำเนินงาน โดยต้องพิจารณาประเด็นภายภายนอกและภายในที่ระบุไว้ในข้อที่ 4.1 และ 4.2 รวมถึงความสัมพันธ์ของกิจกรรมที่เชื่อมโยงกันทั้งกิจกรรมที่ดำเนินการโดยองค์กรเอง และที่ดำเนินการด้วยองค์กรอื่น ทั้งนี้ขอบเขตการดำเนินการต้องจัดทำเป็นลายลักษณ์อักษร	27001:2013 ซึ่งมีการระบุไว้ในคู่มือคุณภาพสำนักเทคโนโลยีดิจิทัลและสารสนเทศอยู่แล้ว		
4.4	**ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information security management system)** องค์กรต้องมีการกำหนด การนำไปปฏิบัติ การบำรุงรักษา และการปรับปรุงอย่างต่อเนื่องของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงกระบวนการที่จำเป็นและที่เชื่อมโยงกัน	สำนักมีการจัดทำคู่มือสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศเพื่อใช้เป็นแนวทางในการดำเนินงาน ที่สอดคล้องกับข้อกำหนดในมาตรฐาน ISO/IEC 27001:2013 และ ISO 9001:2015 แต่ยังไม่ได้มีการปรับปรุงให้สอดคล้องกับข้อกำหนดในมาตรฐาน ISO/IEC 27001:2022	- คู่มือคุณภาพสำนักเทคโนโลยีดิจิทัลและสารสนเทศ	P

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	โดยต้องมีความสอดคล้องกับข้อกำหนดในเอกสารมาตรฐานฉบับนี้			
5	**ความเป็นผู้นำ (Leadership)**			
5.1	**ความเป็นผู้นำและความมุ่งมั่น (Leadership and commitment)** ผู้บริหารระดับสูงต้องแสดงความเป็นผู้นำและความมุ่งมั่นในเรื่องระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศโดย: (1) ทำให้มั่นใจว่าองค์กรมีการกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ มีการบูรณาการข้อกำหนดของระบบกับกระบวนการขององค์กร มีการจัดสรรทรัพยากรที่จำเป็นให้พร้อมใช้งาน (2) มีการสื่อสารให้เห็นความสำคัญของระบบบริหารความมั่นคงปลอดภัยสารสนเทศและสนับสนุนให้บุคลากรมีส่วนรวมในการ	ผู้อำนวยการสำนักยังคงให้ความสำคัญกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง มีการปรับปรุงพิจารณาปรับปรุงนโยบาย มีการพิจารณาแผนการดำเนินงาน และมีการติดตามการทำงานเพื่อเตรียมการขอรับรองมาตรฐาน ISO/IEC 27001:2022	- นโยบายคุณภาพสำนักเทคโนโลยีดิจิทัลและสารสนเทศ - รายงานการประชุมทบทวนฝ่ายบริหาร (Management Review)	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ดำเนินงานของระบบ รวมถึงส่งเสริมให้เกิดการปรับปรุงอย่างต่อเนื่อง (3) สนับสนุนบทบาทการบริหารอื่นๆที่รับผิดชอบ ที่แสดงให้เห็นถึงความเป็นผู้นำ			
5.2	**นโยบาย (Policy)** ผู้บริหารระดับสูงต้องกำหนดนโยบายและวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษร และสื่อสารให้บุคลากรและผู้มีส่วนได้ส่วนเสียรับทราบอย่างเหมาะสม	ผู้อำนวยการสำนักยังคงให้มีการกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศไว้ในนโยบายคุณภาพของสำนักโดยปรับเปลี่ยนตัวชี้วัดให้มีความท้าท้ายเพิ่มขึ้นและมีการสื่อสารให้กับบุคลากรและผู้มีส่วนได้ส่วนเสียผ่านช่องทางเว็บไซต์ และอีเมลรับทราบ	- นโยบายคุณภาพสำนักเทคโนโลยีดิจิทัลและสารสนเทศ - การแจ้งนโยบายต่อบุคลากรผ่านทางอีเมล - เว็บไซต์สำนักเทคโนโลยีดิจิทัลและสารสนเทศ -	C
5.3	**บทบาท ความรับผิดชอบ และอำนาจหน้าที่ขององค์กร (Organizational roles, responsibilities and authorities)** ผู้บริหารระดับสูงต้องทำให้องค์กรมีการกำหนดความรับผิดชอบ อำนาจหน้าที่ ของบทบาทที่	สำนักมีการกำหนดโครงสร้างการบริหารจัดการภายในสำนักแบ่งออกเป็น 2 กอง กองบริหารเทคโนโลยีดิจิทัลที่รับผิดชอบในการจัดการด้านเทคโนโลยี และกองบริหารงานสำนักที่รับผิดชอบในการสนับสนุนการจัดการของสำนัก และมีการ	- โครงสร้างสำนักและอัตรากำลังของสำนัก - คำสั่งแต่งตั้งผู้ทำหน้าที่รับผิดชอบในการดำเนินกิจกรรมตามระบบบริหารคุณภาพมาตรฐาน ISO	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และมีการสื่อสารภายในองค์กร โดยต้องมีการมอบหมายความรับผิดชอบและอำนาจหน้าที่ในการดำเนินการให้เป็นไปตามข้อกำหนดของมาตรฐานและมีการรายงานผลการดำเนินงานให้ผู้บริหารระดับสูง	มอบหมายผู้ที่เกี่ยวข้องรับผิดชอบดำเนินการตามขอบเขตของระบบบริหารจัดการ และให้มีการรายงานผลการดำเนินงานตามแผนงานตามรอบระยะเวลาที่กำหนด		
6	**การวางแผน (Planning)**			
6.1	**การดำเนินงานเพื่อจัดการกับความเสี่ยงและโอกาส (Actions to address risks and opportunities)** องค์กรต้องมีการดำเนินการดังนี้ (1) พิจารณาประเด็นจากข้อกำหนด 4.1 และ 4.2 เพื่อความเสี่ยงและโอกาสของสำนัก รวมถึงต้องวางแผนเพื่อจัดการความเสี่ยงและโอกาส	สำนักมีการวิเคราะห์ความเสี่ยงและโอกาสของสำนักและจัดทำแผนปฏิบัติงานเพื่อจัดการความเสี่ยงและโอกาส มีการจัดทำระเบียบปฏิบัติงานสำหรับเป็นแนวทางในการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment) และกำหนดมาตรการควบคุมเพื่อจัดการความเสี่ยง (Risk treatment) รวมถึงจัดทำเอกสาร Statement of Applicability (SOA) แต่	- ตารางวิเคราะห์ความเสี่ยงและโอกาส - แผนปฏิบัติงานประจำปีของสำนัก - ระเบียบปฏิบัติงานการจัดการความเสี่ยงด้านสารสนเทศ - Statement of Applicability (SOA)	P

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	(2) อประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีการกำหนดเกณฑ์การประเมินและการยอมรับความเสี่ยง มีการระบุความเสี่ยง เจ้าของความเสี่ยง วิเคราะห์โอกาสและผลกระทบที่อาจเกิดขึ้น และประเมินเปรียบเทียบกับเกณฑ์ที่กำหนด (3) กำหนดกระบวนการจัดการความเสี่ยงโดยการจัดทำ Statement of Applicability (SOA) เพื่อเปรียบเทียบมาตรการควบคุมของสำนักกับข้อกำหนดการควบคุม Annex A และมีการกำหนดแผนจัดการความเสี่ยงที่ได้รับการอนุมัติจากเจ้าของความเสี่ยง ทั้งนี้ต้องจัดเก็บเอกสารข้อมูลที่เกี่ยวข้องกับการจัดการความเสี่ยง	เนื่องจาก ISO/IEC 27001:2022 มีการเพิ่มและปรับเปลี่ยนข้อกำหนด Annex A ทำให้ Statement of Applicability ที่มีอยู่ของสำนักไม่สอดคล้องกับข้อกำหนดการควบคุม Annex A ในมาตรฐานใหม่		

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
6.2	**วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและการวางแผนดำเนินการ (Information security objectives and planning to achieve them)** องค์กรต้องกำหนดวัตถุประสงค์และตัวชี้วัดด้านความมั่นคงปลอดภัยสารสนเทศ และวางแผนการดำเนินงานเพื่อให้บรรลุวัตถุประสงค์โดยมีการกำหนดผู้รับผิดชอบ ระยะเวลา และวิธีการติดตามประเมินผล	สำนักมีการกำหนดวัตถุประสงค์และตัวชี้วัดเพื่อใช้ในการประเมินผลการบรรลุด้านความมั่นคงปลอดภัยสารสนเทศดังนี้ (1) จำนวนปัญหาด้านความมั่นคงปลอดภัยสารสนเทศในการให้บริการ Colocation และ VPS ที่ได้รับการพิจารณาดำเนินการ ชี้แจง หรือแก้ไข ร้อยละ 100 (2) ระยะเวลาในการให้บริการได้อย่างต่อเนื่องของบริการ Colocation และ VPS ตามข้อตกลงการให้บริการ ไม่น้อยกว่าร้อยละ 97 โดยสำนักมีการจัดทำแผนปฏิบัติงานประจำปีเพื่อใช้ติดตามผลการดำเนินงานทุก 6 เดือน	- นโยบายคุณภาพสำนักเทคโนโลยีดิจิทัลและสารสนเทศ - แผนปฏิบัติงานประจำปีของสำนัก	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
6.3	**การวางแผนในการเปลี่ยนแปลง (Planning of changes)** องค์กรต้องมีการกำหนดความจำเป็นและแผนการดำเนินงานในการเปลี่ยนแปลงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	ข้อกำหนดนี้เป็นข้อกำหนดใหม่ของมาตรฐาน ISO/IEC 27001:2022 แต่เนื่องจากสำนักมีกำหนดเรื่องนี้ไว้ในคู่มือคุณภาพที่สอดคล้องตามมาตรฐาน ISO 9001:2015 ของสำนักไว้ และสำนักก็มีการจัดทำแผนงานการเปลี่ยนแปลงระบบให้รองรับมาตรฐาน ISO/IEC 27001:2022 ไว้	- แผนดำเนินโครงการรับรองมาตรฐานสากล ประจำปีงบประมาณ พ.ศ. 2568	C
7	**การสนับสนุน (Support)**			
7.1	**ด้านทรัพยากร (Resources)** องค์กรต้องกำหนดทรัพยากรที่จำเป็นในการดำเนินงานและมีการบำรุงรักษาอย่างต่อเนื่อง	สำนักมีการกำหนดระเบียบปฏิบัติงานในการบำรุงรักษาทรัพยากรระบบโครงสร้างพื้นฐานที่เกี่ยวข้องกับการให้บริการ Colocation และ Virtual Private Server และมีการจัดจ้างผู้ให้บริการจากภายนอกที่เชี่ยวชาญเฉพาะทางมาทำการบำรุงรักษาระบบและอุปกรณ์หลักที่สำคัญ เช่น ระบบไฟฟ้าสำรอง ระบบปรับอากาศ	- ระเบียบปฏิบัติงานบำรุงรักษาของส่วนโครงสร้างพื้นฐานและความมั่นคงปลอดภัย - รายงานผลการบำรุงรักษาของส่วนโครงสร้างพื้นฐานและความมั่นคงปลอดภัย	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
		อุปกรณ์เครือข่ายหลัก และอุปกรณ์ Firewall โดยมีการติดตามผลการดำเนินงาน		
7.2	**ด้านสมรรถนะ (Competence)** องค์กรต้องกำหนดสมรรถนะที่จำเป็นสำหรับบุคลากร ทำให้บุคลากรได้รับการอบรม หรือมีประสบการณ์ที่เหมาะสม และมีการติดตามประเมินผลการดำเนินงาน ทั้งนี้จะต้องเก็บข้อมูลเป็นลายลักษณ์อักษรเพื่อเป็นหลักฐาน	สำนักมีการจัดทำแผนพัฒนาบุคลากรของสำนัก มีการจัดอบรมทางด้านเทคนิคให้กับบุคลากรที่รับผิดชอบดูแลระบบโครงสร้างพื้นฐาน เช่น อุปกรณ์เครือข่ายหลัก Core Switch และอุปกรณ์ SAN Storage รวมถึงมีการรายงานติดตามประเมินผลการพัฒนาบุคลากร	- แผนพัฒนาบุคลากรประจำปี - แบบติดตามผลการพัฒนาตนเอง	C
7.3	**ด้านการสร้างความตระหนัก (Awareness)** บุคลากรขององค์กรต้องมีความตระหนักถึง (1) นโยบายความมั่นคงปลอดภัยสารสนเทศ (2) การมีส่วนรวมของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (3) ผลกระทบของการไม่ปฏิบัติตามข้อกำหนด	สำนักมีการจัดทำแผนดำเนินงานโครงการรับรองมาตรฐานสากล ISO และแผนปฏิบัติงานที่เกี่ยวข้องระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ประจำปี ซึ่งมีการแจ้งให้บุคลากรรับทราบเพื่อสร้างความตระหนัก และปฏิบัติตามแผนงานที่กำหนด	- รายงานการประชุมบุคลากรของสำนัก - แผนปฏิบัติงานประจำปีของสำนัก - แผนการดำเนินงานโครงการขอรับรองมาตรฐานสากลประจำปีของสำนัก	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
7.4	**ด้านการสื่อสาร (Communication)** องค์กรต้องกำหนดความจำเป็นในการสื่อสารภายในและภายนอก ที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ รวมถึงสิ่งจะที่สื่อสาร เวลาที่จะสื่อสาร บุคคลที่จะสื่อสาร และวิธีการสื่อสาร	สำนักมีการกำหนดเรื่องที่จะสื่อสาร ช่องทางการสื่อสาร ช่วงเวลาการสื่อสาร ไว้ในแผนยุทธศาสตร์ของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ ซึ่งจะครอบคลุมทั้งบุคลากรภายในสำนัก และผู้มีส่วนได้ส่วนเสีย	- แผนยุทธศาสตร์ของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2567 – 2570 - รายงานประชุมบุคลากรของสำนัก - เว็บไซต์สำนัก	C
7.5	**ข้อมูลสารสนเทศที่เป็นลายลักษณ์อักษร (Documented information)** ข้อมูลและเอกสารที่เป็นลายลักษณ์อักษรของระบบบริหารความมั่นคงปลอดภัยสารสนเทศต้องมีการระบุและอธิบาย ต้องกำหนดรูปแบบและการจัดเก็บ ต้องมีการทบทวนและอนุมัติ ต้องมีการควบคุมการแจกจ่าย การเข้าถึง การเปลี่ยนแปลง การเก็บรักษา และการทำลาย	สำนักมีกระบวนการจัดการด้านเอกสารโดยกำหนดเป็นระเบียบปฏิบัติงาน ซึ่งมีขั้นตอนการควบคุมเอกสารที่สอดคล้องกับข้อกำหนด และเอกสารที่ควบคุมนั้นมีการจัดทำประวัติการแก้ไขและได้รับพิจารณาอนุมัติโดยผู้บริหารของสำนักในแต่ละครั้งที่แก้ไข	- ระเบียบปฏิบัติงานการควบคุมเอกสารของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ - เอกสารควบคุมทั้งหมดของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
8	**การปฏิบัติงาน (Operation)**			
8.1	**การวางแผนและการควบคุมการปฏิบัติงาน (Operational planning and control)** องค์กรต้องวางแผนดำเนินการ และควบคุมกระบวนการให้เป็นไปตามข้อกำหนด โดยต้องกำหนดเกณฑ์เพื่อใช้ในการควบคุม มีการจัดทำเป็นเอกสารข้อมูล	สำนักมีการจัดทำแนวปฏิบัติ และขั้นตอนการปฏิบัติงานของกระบวนการทำงานเป็นลายลักษณ์อักษร เพื่อให้ควบคุมบุคลากรในสำนักได้ปฏิบัติตาม นอกจากนี้ยังสำนักยังมีการจัดทำแผนปฏิบัติงานประจำปี และมีติดตามผลการปฏิบัติงานทุก 6 เดือน	- เอกสารระเบียบปฏิบัติงานของสำนัก - แผนปฏิบัติงานประจำปีของสำนัก	C
8.2	**การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment)** องค์กรต้องดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามที่กำหนดไว้	สำนักมีการวิเคราะห์และประเมินความเสี่ยงด้านสารสนเทศในรูปแบบ Asset based เปรียบเทียบกับเกณฑ์ที่กำหนดไว้และจัดทำเป็นรายงานผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศประจำปี	- ระเบียบปฏิบัติงานการจัดการความเสี่ยงด้านสารสนเทศ - รายงานผลการประเมินความเสี่ยงและแผนการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลสารสนเทศประจำปี	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น โดยคำนึงถึงเกณฑ์ที่กำหนดในข้อกำหนด 6.1 ทั้งนี้จะต้องจัดเก็บเอกสารข้อมูลของผลลัพธ์การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ			
8.3	**การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk treatment)** องค์กรต้องดำเนินการตามแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ต้องจัดเก็บรักษาเอกสารข้อมูลของผลลัพธ์จากการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ	สำนักได้นำผลการประเมินความเสี่ยงด้านสารสนเทศมาจัดทำมาตรการควบคุมความเสี่ยงและจัดทำแผนการจัดการความเสี่ยงปีละครั้ง โดยมีการรายงานผลการดำเนินงานในการประชุมทบทวนฝ่ายบริหาร	- รายงานผลการประเมินความเสี่ยงและแผนการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลสารสนเทศประจำปี - รายงานการประชุมทบทวนฝ่ายบริหาร (Management Review)	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
9	**การประเมินประสิทธิภาพ (Performance evaluation)**			
9.1	**การเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมินผล (Monitoring, measurement, analysis and evaluation)** องค์กรต้องกำหนดตัวชี้วัด วิธีการ ช่วงเวลา ผู้รับผิดชอบ ในการเฝ้าติดตาม วิเคราะห์ ประเมินผลของประสิทธิภาพการบริหารความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ต้องจัดเก็บข้อมูลสารสนเทศเป็นลายลักษณ์อักษร	สำนักมีการกำหนดกระบวนการติดตามประเมินผลการปฏิบัติงานไว้ในระเบียบปฏิบัติการติดตามและประเมินผล โดยมีการติดตามรายงานผลการปฏิบัติงานอย่างน้อยปีละ 2 ครั้ง และนำเข้าที่ประชุมการทบทวนฝ่ายบริหารของสำนักเพื่อวิเคราะห์และประเมินผลประสิทธิภาพการดำเนินงาน	- ระเบียบปฏิบัติงานการติดตามและประเมินผลการปฏิบัติงาน - รายงานการประชุมทบทวนฝ่ายบริหาร (Management Review)	C
9.2	**การตรวจประเมินภายใน (Internal audit)** องค์กรต้องมีการวางแผนกำหนดการตรวจประเมิน และทำการประเมินภายในตามรอบระยะเวลาที่กำหนด	สำนักกำหนดกระบวนการตรวจประเมินภายในเป็นระเบียบปฏิบัติงานเพื่อบุคลากรในสำนักปฏิบัติตาม และดำเนินการตรวจประเมินภายในสำนักปีละ 1 ครั้ง ซึ่งสำนักการวางแผนเตรียม	- ระเบียบปฏิบัติงานการตรวจติดตามภายในของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ	P

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
		ดำเนินการตรวจติดตามภายในตามมาตรฐาน ISO/IEC 27001:2022 และมีการจัดทำ Requirement matrix แล้ว แต่ยังไม่ได้รับการปรับปรุงให้เป็นปัจจุบัน	- กำหนดการตรวจติดตามภายใน (Internal Audit Schedule) - Requirement matrix	
9.3	**การทบทวนฝ่ายบริหาร (Management review)** ผู้บริหารต้องทำการทบทวนการดำเนินงานของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ โดยพิจารณาถึง (1) สถานะของการดำเนินงานครั้งที่ผ่านมา (2) การเปลี่ยนแปลงของประเด็นภายนอกและภายในที่เกี่ยวข้อง (3) การเปลี่ยนแปลงความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย (4) ผลของประสิทธิภาพในการดำเนินงาน รวมถึง ความไม่สอดคล้องกับข้อกำหนด	สำนักกำหนดให้มีการประชุมการทบทวนฝ่ายบริหารอย่างน้อยปีละ 2 ครั้ง และในการประชุมครั้งล่าสุดมีการกำหนดประเด็นที่จะพิจารณาในการประชุมครอบคลุมทุกข้อกำหนด รวมถึงประเด็นการเปลี่ยนแปลงความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสียที่เป็นประเด็นใหม่ของมาตรฐานฉบับปี 2022 ที่เพิ่มเติมจากฉบับปี 2013	- ระเบียบปฏิบัติงานการประเมินผลการปฏิบัติงาน - รายงานการประชุมทบทวนฝ่ายบริหาร (Management Review)	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ผลลัพธ์ของการติดตามเฝ้าระวัง ผลลัพธ์ของการตรวจประเมิน (5) ผลสะท้อนกลับ (Feedback) จากผู้มีส่วนได้ส่วนเสีย (6) ผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง (7) โอกาสในการปรับปรุงและพัฒนาอย่างต่อเนื่อง			
10	**การปรับปรุง (Improvement)**			
10.1	**การปรับปรุงอย่างต่อเนื่อง (Continual improvement)** องค์ต้องนำผลการประเมินมาปรับปรุงประสิทธิการดำเนินงานขององค์กรอย่างต่อเนื่อง	สำนักมีการนำผลการประเมินประสิทธิภาพ และผลประเมินความเสี่ยงและโอกาสมาวิเคราะห์และจัดทำแผนปฏิบัติงานอย่างต่อเนื่องทุกปี นอกจากนี้ยังนำผลการตรวจประเมินภายในและภายนอกมาจัดทำแนวทางการปรับปรุง โดยกำหนดผู้รับผิดชอบ และระยะเวลาแล้วเสร็จด้วย	- รายงานการประชุมทบทวนฝ่ายบริหาร (Management Review)	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
10.2	**ความไม่สอดคล้องและการดำเนินการแก้ไข (Nonconformity and corrective action)** องค์กรต้องมีการจัดการสิ่งที่ไม่สอดคล้องกับข้อกำหนด โดยวิเคราะห์สาเหตุ ทำการแก้ไขและดำเนินการทบทวนและปรับปรุงเพื่อป้องกันไม่ให้เกิดซ้ำ	สำนักจัดทำกระบวนการควบคุมการดำเนินงานที่ไม่เป็นไปตามข้อกำหนดของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ โดยจะนำผลความไม่สอดคล้องจากข้อร้องเรียน การตรวจติดตามภายใน และการตรวจประเมินจากภายนอกมาดำเนินการหาสาเหตุ ดำเนินการแก้ไข และหาวิธีการป้องกันการเกิดซ้ำ	- ระเบียบปฏิบัติงานการควบคุมการดำเนินงานที่ไม่เป็นไปตามข้อกำหนดในระบบคุณภาพ - รายงานการดำเนินงานที่ไม่เป็นไปตามข้อกำหนดในระบบคุณภาพ (Non-Compliance Report : NCR)	C

ตารางที่ 4-1 ผลการวิเคราะห์ข้อกำหนดระบบบริหารจัดการ

ผลการวิเคราะห์ข้อกำหนดระบบบริหารจัดการ (Management system requirements) จำนวน 23 ข้อ พบว่าระดับผลประเมินความสอดคล้องของการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของสำนักเมื่อเทียบกับข้อกำหนดในมาตรฐาน ISO/IEC 27001:2022 อยู่ในระดับดังนี้

(1) มีการดำเนินงานที่สอดคล้องกับข้อกำหนดครบถ้วน (C) จำนวน 21 ข้อ (คิดเป็นร้อยละ 91.3)

(2) มีการดำเนินงานที่สอดคล้องกับข้อกำหนดบางส่วน (P) จำนวน 2 ข้อ (คิดเป็นร้อยละ 8.7)

จากผลการวิเคราะห์พบว่าการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ มีความครอบคลุมข้อกำหนดหลักของมาตรฐาน ISO/IEC 27001:2022 แต่ยังมีบางข้อกำหนดที่การดำเนินงานของสำนักยังไม่สอดคล้องกับข้อกำหนดหลักของมาตรฐาน ISO/IEC 27001:2022 ครบถ้วน ได้แก่

(1) ข้อกำหนด 4.4 ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information security management system) ซึ่งพบว่าสำนักยังไม่ได้มีการทบทวนและปรับปรุงคู่มือสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับมาตรฐาน

(2) ข้อกำหนด 6.1 การดำเนินงานเพื่อจัดการกับความเสี่ยงและโอกาส (Actions to address risks and opportunities) ซึ่งพบว่าสำนักยังไม่ได้มีการทบทวนและปรับปรุงเอกสาร Statement of Applicability (SOA) ตามข้อกำหนดการควบคุม Annex A ในมาตรฐาน ISO/IEC 27001:2022

(3) ข้อกำหนด 9.2 การตรวจประเมินภายใน (Internal audit) ซึ่งพบว่าสำนักยังไม่ได้มีการทบทวนและปรับปรุง Requirement matrix เพื่อใช้เป็นแนวทางในการตรวจประเมินภายใน

4.2. ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านองค์กร

ในข้อกำหนดการควบคุม Annex A ด้านองค์กร (Organization controls) ของมาตรฐาน ISO/IEC 27001:2022 ประกอบด้วยข้อกำหนด 37 ข้อ มีผลการวิเคราะห์ดังนี้

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.5.1	**นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Policies for information security)** นโยบายความมั่นคงปลอดภัยสารสนเทศและที่เกี่ยวข้องต้องได้รับการกำหนดและอนุมัติโดยผู้บริหาร มีการสื่อสารให้กับบุคคลากรและผู้มีส่วนได้ส่วนเสียรับทราบ รวมถึงต้องมีการทบทวนเป็นระยะหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ	สำนักมีการกำหนดนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งสอดคล้องกับมาตรฐาน ISO/IEC 27001:2013 และมีการพิจารณาทบทวนโดยผู้บริหารสำนัก ปีละ 1 ครั้ง ทั้งนี้พบว่านโยบายและแนวปฏิบัติยังไม่ครอบคลุมประเด็นที่กำหนดไว้ข้อกำหนดการควบคุมใหม่ในมาตรฐาน ISO/IEC 27001:2022 เช่น นโยบายการใช้คลาวด์	- เอกสารแนวปฏิบัติ/นโยบายของส่วนงาน - รายงานการประชุมทบทวนฝ่ายบริหาร (Management Review)	P
A.5.2	**บทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)**	สำนักมีการกำหนดโครงสร้างขององค์กรพร้อมหน้าที่และความรับผิดชอบของแต่ละส่วนงาน และกำหนดอัตรากำลังและ Job Description ของแต่ละตำแหน่ง นอกจากนี้ยังกำหนดตำแหน่ง	- โครงสร้างองค์กรและอัตรากำลังของสำนัก - Job Description ของบุคลากร	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	บทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศต้องถูกกำหนดและมอบหมายตามความเหมาะสมขององค์กร	และความรับผิดชอบในการดำเนินการกิจกรรมตามระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เช่น ผู้แทนฝ่ายบริหาร (Quality Management Representative) ผู้ควบคุมเอกสาร (Documents Control) และคณะกรรมการตรวจติดตามภายใน (Internal Audit)	- คำสั่งแต่งตั้งผู้ทำหน้าที่รับผิดชอบในการดำเนินกิจกรรมตามระบบบริหารคุณภาพมาตรฐาน ISO - คำสั่งแต่งตั้งหัวหน้าทีมการตรวจติดตามภายใน และคณะกรรมการตรวจติดตามระบบบริหารคุณภาพภายใน	
A.5.3	**การแบ่งแยกหน้าที่ (Segregation of duties)** หน้าที่ความรับผิดชอบที่ขัดกันหรือทับซ้อนกันจนอาจก่อให้เกิดความผิดพลาดต้องแยกออกจากกันชัดเจน	โครงสร้างองค์กรของสำนักมีการแบ่งเป็น 2 กองรวม 5 ส่วนงาน ซึ่งแต่ละส่วนที่มีการกำหนดหน้าที่ความรับผิดชอบแตกต่างกัน และมีการกำหนดสายบังคับบัญชาแยกออกจากกันชัดเจน	- โครงสร้างองค์กรและอัตรากำลังของสำนัก	C
A.5.4	**หน้าที่ความรับผิดชอบของฝ่ายบริหาร (Management responsibilities)** ผู้บริหารต้องกำหนดให้บุคลากรทุกคนในองค์กรปฏิบัติตามนโยบายความมั่นคงปลอดภัยสาร	ผู้บริหารของสำนักมีการสื่อสารให้บุคลากรในสำนักรับทราบนโยบาย แนวปฏิบัติ และแผนปฏิบัติงานที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศที่มีการกำหนดผู้รับผิดชอบ	- เอกสารควบคุมภายใน นโยบาย/แนวปฏิบัติของส่วนงาน ระเบียบการปฏิบัติงาน - รายงานการประชุมทบทวนฝ่ายบริหาร (Management Review)	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	นโยบายเฉพาะทางที่เกี่ยวข้อง และกระบวนการดำเนินงานขององค์กรที่กำหนดขึ้น	และมีการติดตามผลการดำเนินงานตามรอบระยะเวลาที่กำหนด	- รายงานการประชุมบุคลากร	
A.5.5	**การติดต่อกับหน่วยงานกำกับดูแล (Contact with authorities)** องค์กรต้องจัดทำข้อมูลและปรับปรุงข้อมูลสำหรับใช้ติดต่อกับหน่วยงานที่กำกับดูแลองค์กร	สำนักมีการจัดเก็บข้อมูลช่องทางการติดต่อกับหน่วยงานของรัฐที่มีอำนาจในการกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศไว้ในทะเบียนข้อมูลผู้ติดต่อ (Contact Information)	- Contact Information	C
A.5.6	**การติดต่อกับกลุ่มพิเศษที่มีความสนใจเฉพาะทาง (Contact with special interest groups)** องค์กรต้องจัดทำข้อมูลและปรับปรุงข้อมูลสำหรับใช้ติดต่อกับกลุ่มพิเศษทีมีความสนใจเรื่องเดียวกัน หรือกลุ่มสมาคมที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัย	สำนักมีการจัดเก็บข้อมูลช่องทางการติดต่อกับผู้ให้บริการภายนอกหรือผู้ที่มีเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศไว้ในทะเบียนข้อมูลผู้ติดต่อ (Contact Information)	- Contact Information	C
A.5.7	**ข่าวกรองภัยคุกคามด้านความมั่นคงปลอดภัย (Threat intelligence)**	สำนักมีระบบ Threat Prevention ในอุปกรณ์ Firewall ที่มีการ Update ข้อมูลวิเคราะห์ข้อมูล	- ระบบ Threat Prevention ในอุปกรณ์ Firewall ของสถาบัน	P

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ต้องมีการเก็บรวบรวบข้อมูลสารสนเทศที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ และนำไปวิเคราะห์เพื่อจัดทำเป็นข่าวกรองด้านภัยคุกคาม	การจราจร (Traffic) ของระบบเครือข่ายเพื่อตรวจหาและป้องกันการโจมตีทางระบบเครือข่าย แต่ไม่ได้มีการติดตาม รวบรวมและวิเคราะห์ข้อมูลที่มาจากข่าวสารจากแหล่งอื่น เช่น ข้อมูลแจ้งเตือนภัยคุกคามจากหน่วยงานหรือองค์กรที่เกี่ยวข้อง		
A.5.8	**ความมั่นคงปลอดภัยสารสนเทศในการบริหารโครงการ (Information security in project management)** ต้องมีการบูรณาการด้านความมั่นคงปลอดภัยเข้าไปในการบริหารจัดการโครงการขององค์กร	โครงการปรับปรุง/พัฒนาที่เกี่ยวข้องและมีผลกระทบตามขอบเขตการขอรับรองมาตรฐาน ISO/IEC 27001 จะมีการประเมินความเสี่ยงและพิจารณาแนวทางในการจัดการความเสี่ยงก่อนเริ่มดำเนินการ	- แผนการดำเนินงานโครงการระบบการให้บริการการศึกษาแบบเปิด (Open System for Lifelong Learning) รองรับการเรียนรู้ตลอดชีวิตเพื่อการพัฒนาที่ยั่งยืน ระยะที่ 2	C
A.5.9	**บัญชีของข้อมูลและทรัพย์สินที่เกี่ยวข้อง (Inventory of information and other associated assets)**	สำนักมีการจัดทำทะเบียนทรัพย์สิน (Asset) พร้อมระบุเจ้าของทรัพย์สิน โดยแบ่งทรัพย์สินตามหมวด (Category) และประเภท (Type)	- ทะเบียนทรัพย์สิน (Asset)	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ดำเนินการจัดทำและปรับปรุงรายการข้อมูลสารสนเทศและทรัพย์สินที่เกี่ยวข้อง รวมถึงต้องระบุความเป็นเจ้าของข้อมูลสารสนเทศและทรัพย์สินอย่างชัดเจน			
A.5.10	**การใช้สารนเทศและทรัพย์สินที่ยอมรับได้ (Acceptable use of information and other associated assets)** มีการกำหนดกฎเกณฑ์การใช้และกระบวนการจัดการสารสนเทศและทรัพย์สินที่เกี่ยวข้องที่ยอมรับได้เป็นลายลักษณ์อักษร และมีการนำไปปฏิบัติ	สำนักมีขั้นตอนปฏิบัติในการดูแลรักษาทรัพย์สินที่เป็นครุภัณฑ์ และมีแนวปฏิบัติในการจัดการในการทำบัญชีทรัพย์สิน แต่ยังขาดการกฎระเบียบหรือแนวปฏิบัติในการใช้สารสนเทศที่ชัดเจน	- ระเบียบปฏิบัติงานการดูแลรักษาครุภัณฑ์ - แนวปฏิบัติการบริหารจัดการทรัพย์สิน (Asset Management)	P
A.5.11	**การคืนทรัพย์สิน (Return of assets)** บุคลากรและผู้ที่เกี่ยวข้องจากหน่วยงานภายนอกต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนเองถือ	สำนักมีการกำหนดให้บุคลากรภายในสำนักทำการคืนทรัพย์สินเมื่อเกษียณหรือลาออก และลงนามส่งคืนในแบบฟอร์มการยืม-คืนวัสดุ/ครุภัณฑ์	- ระเบียบปฏิบัติงานการดูแลรักษาครุภัณฑ์	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ครอง เป็นไปตามการเปลี่ยนแปลงหรือการสิ้นสุดของสัญญาหรือข้อตกลงที่ทำร่วมกัน			
A.5.12	**การจัดหมวดหมู่สารสนเทศ (Classification of information)** ต้องมีการจัดหมวดหมู่สารสนเทศให้เป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยคำนึงถึงในเรื่องการรักษาความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้งาน รวมถึงข้อกำหนดของผู้มีส่วนเกี่ยวข้องภายนอกองค์กรด้วย	สำนักมีการจัดแบ่งหมวดหมู่ของเอกสาร และกำหนดระดับชั้นความลับข้อมูล ระบุไว้ในระเบียบงาน และมีการกำหนดระดับชั้นของสารสนเทศที่เกี่ยวกับระบบโครงสร้างพื้นฐานไว้ในทะเบียนทรัพยสิน (Asset) ของส่วนงานโครงสร้างพื้นฐานและความมั่นคงปลอดภัยสารสนเทศ	- ระเบียบปฏิบัติงานการควบคุมเอกสารของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ - ทะเบียนทรัพย์สิน (Asset)	C
A.5.13	**การติดป้ายบ่งชี้สารสนเทศ (Labeling of information)** ต้องมีการกำหนดขั้นตอนการปฏิบัติงานในการระบุข้อมูลสารสนเทศ และนำไปปฏิบัติให้	สำนักมีการกำหนดรหัสเอกสารเพื่อแบ่งแยกหมวดหมู่เอกสาร รวมทั้งมีการแบ่งพื้นที่เพื่อจัดเก็บเอกสารแยกตามหมวดหมู่ด้วย ในส่วนสารสนเทศที่เกี่ยวกับระบบโครงสร้างพื้นฐานมี	- ระเบียบปฏิบัติงานการควบคุมเอกสารของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ - ทะเบียนทรัพย์สิน (Asset)	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	สอดคล้องกับการจัดหมวดหมู่สารสนเทศที่กำหนดไว้	การระบุระดับชั้นของข้อมูล และแหล่งจัดเก็บไว้ในทะเบียนทรัพย์สิน (Asset)		
A.5.14	**การถ่ายโอนข้อมูล (Information transfer)** ต้องมีการกำหนดกฎระเบียบ ขั้นตอนปฏิบัติงาน หรือข้อตกลงสำหรับการถ่ายโอนข้อมูลสำหรับเครื่องมือหรืออุปกรณ์ในการถ่ายโอนข้อมูลทุกระเภท รวมทั้งการถ่ายโอนภายในองค์กร และระหว่างองค์กรกับหน่วยงานภายนอก	สำนักมีการกำหนดความรับผิดชอบในการถ่ายโอนข้อมูลในข้อตกลงและเงื่อนไขการให้บริการของสำนัก แต่ไม่ได้มีการกำหนดเป็นกฎระเบียบหรือแนวปฏิบัติในการถ่ายโอนข้อมูลสารสนเทศระหว่างภายในองค์กรที่ชัดเจน	- ข้อกำหนดและเงื่อนไขการให้บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Private Server)	P
A.5.15	**การควบคุมการเข้าถึง (Access control)** ต้องมีการกำหนดกฎระเบียบในการเข้าถึงข้อมูลสารสนเทศและการทรัพย์สินที่เกี่ยวข้อง ทั้งทางกายภาพและที่ไม่ใช่กายภาพ และนำไปปฏิบัติโดยให้สอดคล้องกับบริบทขององค์กรและข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ	สำนักมีการกำหนดนโยบายการควบคุมการเข้าถึง (Access control) ในขอบเขตระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ไว้ในแนวปฏิบัติ/นโยบายของส่วนงาน ที่มีรวมทั้งการเข้าถึงข้อมูลในระบบ/อุปกรณ์ การเข้าถึงเครือข่าย การเข้าถึงทางกายภาพ	- นโยบายการควบคุมการเข้าถึง (Access Control) - แนวปฏิบัติในการควบคุมการเข้าถึงเครือข่าย (Network Access Control)	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
			- แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	
A.5.16	**การจัดการข้อมูลระบุตัวตน (Identity management)** ต้องมีการจัดการข้อมูลที่ใช้ระบุตัวตน (Identity) ตลอดอายุของข้อมูล	สำนักมีกระบวนการในจัดการบัญชีผู้ใช้งานระบบตั้งแต่การลงทะเบียนเพื่อขอบัญชีผู้ใช้งานผ่านกระบวนการขอใช้บริการโครงสร้างพื้นฐาน การทบทวนบัญชีผู้ใช้งานปีละครั้ง จนถึงการยกเลิกบัญชีผู้ใช้งานเมื่อสิ้นสุดระยะเวลาการใช้งานหรือเมื่อมีการแจ้งความจำนงในการยกเลิก	- นโยบายการควบคุมการเข้าถึง (Access Control) - ระเบียบปฏิบัติงานการให้บริการงานโครงสร้างพื้นฐาน	C
A.5.17	**ข้อมูลที่ใช้ในการพิสูจน์ยืนยันตัวตน (Authentication information)** การจัดสรรและการจัดการข้อมูลที่ใช้ในการยืนยันพิสูจน์ตัวตน (Authentication) ต้องมีกระบวนการบริหารจัดการควบคุม ซึ่งรวมถึงการ	สำนักกำหนดแนวปฏิบัติการจัดการรหัสผ่าน (Password Management) ไว้ในนโยบายการควบคุมการเข้าถึง และมีการกำหนดรหัสผ่านของผู้ใช้งานตามแนวปฏิบัติที่กำหนด โดยจะส่งมอบรหัสผ่านพร้อมคำแนะนำให้กับผู้ใช้งานทางอีเมลเท่านั้น	- นโยบายการควบคุมการเข้าถึง (Access Control)	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ให้คำแนะนำแก่บุคลากรเกี่ยวกับการจัดการกับข้อมูลพิสูจน์ยืนยันตัวตนที่เหมาะสม			
A.5.18	**สิทธิการเข้าถึง (Access rights)** ต้องมีการกำหนด การทบทวน การปรับปรุงสิทธิการเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องให้เป็นไปตามนโยบายและกฎเกณฑ์ที่เกี่ยวข้องกับการควบคุมการเข้าถึงขององค์กร	สำนักมีการกำหนดเรื่องการจัดการสิทธิไว้ในนโยบายการควบคุมการเข้าถึง (Access Control Policy) และมีการจัดทำ Access Rights Matrix สำหรับกำหนดผู้ที่มีสิทธิและสิทธิที่ได้รับในการเข้าถึงระบบ โดยมีการทบทวนสิทธิเพื่อปรับปรุง Access Rights Matrix อย่างน้อยปีละ 2 ครั้ง	- นโยบายการควบคุมการเข้าถึง (Access Control) - ตาราง Access Rights Matrix	C
A.5.19	**ความมั่นคงปลอดภัยสารสนเทศกับผู้ให้บริการภายนอก (Information security in supplier relationships)** ต้องมีการกำหนดกระบวนการและขั้นตอนปฏิบัติในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการใช้ผลิตภัณฑ์หรือบริการของผู้ให้บริการภายนอก	สำนักมีขั้นตอนปฏิบัติงานจัดซื้อจัดจ้างตามระเบียบจัดซื้อจัดจ้างของสถาบัน ตั้งแต่การจัดทำ TOR การประกาศเพื่อให้ยื่นข้อเสนอ การพิจารณาจัดซื้อ/จัดจ้าง และการตรวจรับ และกำหนดให้มีการประเมินด้านความมั่นคงปลอดภัยสารสนเทศในการดำเนินงานของผู้ขาย/ผู้ให้บริการภายนอก	- ระเบียบปฏิบัติงานการจัดซื้อ/จัดจ้างของสำนัก - ระเบียบปฏิบัติงานการประเมินผู้ขายของสำนัก	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.5.20	**การระบุเรื่องความมั่นคงปลอดภัยสารสนเทศในข้อตกลงกับผู้ให้บริการภายนอก (Addressing information security within supplier agreements)** ข้อกำหนดความมั่นคงปลอดภัยสารสนที่เกี่ยวข้องต้องมีการกำหนดและตกลงกับผู้ให้บริการภายนอกแต่ละราย โดยเป็นไปตามประเภทและความสัมพันธ์กับผู้ให้บริการภายนอก	สำนักกำหนดให้ระบุเงื่อนไขการรักษาข้อมูลที่เป็นความลับ หรือเงื่อนไขการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศลงในรายละเอียดและคุณสมบัติของงานจัดซื้อจัดจ้างที่ต้องเข้าถึงข้อมูล	- ระเบียบปฏิบัติงานการจัดซื้อ/จัดจ้างของสำนัก - TOR โครงการระบบการให้บริการการศึกษาแบบเปิด (Open System for Lifelong Learning) รองรับการเรียนรู้ตลอดชีวิตเพื่อการพัฒนาที่ยั่งยืน พร้อมค่าติดตั้ง ระยะที่ 2	C
A.5.21	**การจัดการความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่อุปทานด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) จากภายนอก (Managing information security in the information and communication technology (ICT) supply chain)**	สำนักมีขั้นตอนปฏิบัติงานจัดซื้อจัดจ้างตามระเบียบปฏิบัติงานจัดซื้อจัดจ้างของสำนัก โดยมีการกำหนดมาตรฐานด้านความมั่นคงปลอดภัยของผลิตภัณฑ์ ที่จัดหา เช่น มาตรฐาน CE (Conformance European) หรือมาตรฐาน UL (Underwriters Laboratories) ไว้ในข้อกำหนดและขอบเขตการดำเนินงาน (TOR)	- TOR โครงการระบบการให้บริการการศึกษาแบบเปิด (Open System for Lifelong Learning) รองรับการเรียนรู้ตลอดชีวิตเพื่อการพัฒนาที่ยั่งยืน พร้อมค่าติดตั้ง ระยะที่ 2	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ต้องมีการกำหนดกระบวนการ ขั้นตอนปฏิบัติ และการนำไปปฏิบัติในการจัดการความเสี่ยงที่เกี่ยวข้องกับห่วงโซ่การให้บริการและผลิตภัณฑ์ด้าน ICT			
A.5.22	**การติดตามและทบทวนการให้บริการของผู้ให้บริการภายนอก (Monitoring, review and change management of supplier services)** องค์กรต้องมีการติดตาม ทบทวน ประเมินผล และบริหารการเปลี่ยนแปลงในการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศและการส่งมอบงานของผู้ให้บริการภายนอก	สถาบันมีระเบียบและขั้นตอนที่เกี่ยวกับการจัดซื้อจัดจ้างบริการภายนอก โดยจะแต่งตั้งคณะกรรมการตรวจรับเพื่อติดตาม และตรวจสอบผลลัพธ์การดำเนินงานให้เป็นตามระเบียบ และ TOR ที่กำหนด นอกจากนี้ยังมีการประเมินผู้ขายหรือผู้ให้บริการหลังการตรวจรับในแต่ละงวดที่ส่งมอบ	- ระเบียบปฏิบัติงานจัดซื้อ/จัดจ้างของสำนัก - ระเบียบปฏิบัติงานการประเมินผู้ขายของสำนัก - ตัวอย่างผลการประเมินในแบบฟอร์มการประเมินผู้ขายหลังการขาย	C
A.5.23	**ความมั่นคงปลอดภัยในการใช้บริการคลาวด์ (Information security for use of cloud services)**	สำนักมีกระบวนการงานจัดซื้อ/จัดจ้างซึ่งเป็นไปตามระเบียบของสถาบันสำหรับใช้ในการจัดหาการให้บริการคลาวด์ แต่ยังไม่ได้กำหนดกระบวนการหรือแนวทางการใช้ การบริหาร	- ระเบียบปฏิบัติงานจัดซื้อ/จัดจ้างของสำนัก	P

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ต้องกำหนดกระบวนการสำหรับการจัดหา การใช้บริการ และการบริหารจัดการ และการสิ้นสุดการให้บริการคลาวด์ ให้เป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ	จัดการ และการสิ้นสุดการใช้บริการคลาวด์ที่ชัดเจน		
A.5.24	**การวางแผนและเตรียมการเพื่อจัดการกับเหตุด้านความมั่นคงปลอดภัยสารสนเทศ (Information security incident management planning and preparation)** องค์กรต้องมีการวางแผนและเตรียมการสำหรับการบริหารจัดการเหตุด้านความมั่นคงปลอดภัยสารสนเทศ โดยต้องกำหนดและสื่อสารกระบวนการ บทบาท และหน้าที่ความรับผิดชอบสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ	สำนักจัดทำนโยบายการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยต่อระบบสารสนเทศ และกำหนดขั้นตอนการปฏิบัติงานการจัดการเหตุขัดข้อง (Incident Management) โดยมีการบันทึกจัดเก็บข้อมูลตามขั้นตอนที่กำหนด	- นโยบายการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยต่อระบบสารสนเทศ - ระเบียบปฏิบัติงานการจัดการเหตุขัดข้อง (Incident Management) - บันทึกข้อมูล Event-Incident Log	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.5.25	**การประเมินและตัดสินใจเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัย (Assessment and decision on information security events)** องค์กรต้องประเมินเหตุการณ์ (Event) ด้านความมั่นคงปลอดภัยสารสนเทศ และมีการตัดสินใจหากเป็นเหตุ (Incident) ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ	สำนักกำหนดให้ผู้ดูแลระบบประเมินความเสี่ยงโดยตรวจสอบและพิจารณาระดับผลกระทบจากเหตุการณ์ และแจ้งให้ผู้เกี่ยวข้องรับทราบ ทั้งนี้การตัดสินใจเป็นไประดับผลกระทบที่กำหนดไว้	- นโยบายการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยต่อระบบสารสนเทศ - ระเบียบปฏิบัติงานการจัดการเหตุขัดข้อง (Incident Management) - บันทึกข้อมูล Event-Incident Log	C
A.5.26	**การตอบสนองรับมือต่อเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)** เหตุด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการรับมือที่เป็นไปตามกระบวนการที่กำหนดไว้เป็นลายลักษณ์อักษร	สำนักกำหนดขั้นตอนการปฏิบัติงานรับมือกับเหตุการด้านความมั่นคงปลอดภัยต่อระบบสารสนเทศและการทำงานที่บกพร่องของระบบสารสนเทศไว้ และมีกการดำเนินงานตรวจสอบและดำเนินการแก้ไขเหตุขัดข้องตามระดับผลกระทบที่กำหนดไว้ขั้นตอนปฏิบัติการจัดการเหตุขัดข้อง (Incident Management)	- นโยบายการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยต่อระบบสารสนเทศ - ระเบียบปฏิบัติงานการจัดการเหตุขัดข้อง (Incident Management) - บันทึกข้อมูล Event-Incident Log	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.5.27	**การเรียนรู้จากเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from Information Security Incidents)** บทเรียนที่ได้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศต้องถูกนำมาใช้เพื่อเสริมสร้างและปรับปรุงมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ	สำนักกำหนดนโยบายในการเรียนรู้จากเหตุละเมิดด้านความมั่นคงปลอดภัย โดยจะบันทึกเหตุและวิธีการแก้ไข เพื่อใช้ทบทวนและพิจารณาแนวทางป้องกันหรือจัดการความเสี่ยงที่อาจเกิดขึ้นอีก	- นโยบายการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยต่อระบบสารสนเทศ - บันทึกข้อมูล Event-Incident Log	C
A.5.28	**การเก็บรวบรวมหลักฐาน (Collection of evidence)** องค์กรต้องมีการกำหนดและนำไปปฏิบัติสำหรับขั้นตอนปฏิบัติเพื่อระบุรวบรวม ค้นหาเพื่อให้ได้มา และเก็บรักษาหลักฐานของเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ	ผู้ปฏิบัติงานจัดเก็บข้อมูลเหตุการณ์ ช่วงเวลาที่เกิดเหตุหรือพบเหตุ ผู้รับผิดชอบ และการดำเนินการแก้ไข พร้อมหลักฐานการเกิดเหตุขัดข้อง (Incident)	- บันทึกข้อมูล Event-Incident Log	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.5.29	**ความมั่นคงปลอดภัยในช่วงการหยุดชะงัก (Information security during disruption)** องค์กรต้องวางแผนวิธีการรักษาความมั่นคงปลอดภัยสารสนเทศให้อยู่ในระดับที่เหมาะสมระหว่างที่เกิดการหยุดชะงักของระบบ	สำนักใช้แผนบริหารความต่อเนื่องของสถาบันเป็นกรอบในการดำเนินงานเมื่อเกิดเหตุที่ทำให้ระบบหยุดชะงัก ซึ่งมีการดำเนินงานตามแผนที่กำหนดไว้	- แผนบริหารความต่อเนื่อง สถาบันบัณฑิตพัฒนบริหารศาสตร์	C
A.5.30	**ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)** ต้องวางแผน นำไปปฏิบัติ รักษา และทดสอบความพร้อมด้าน ICT ตามวัตถุประสงค์การบริหารความต่อเนื่องทางธุรกิจและข้อกำหนดความต่อเนื่องด้าน ICT	สำนักใช้แผนบริหารความต่อเนื่องของสถาบันเป็นกรอบในการดำเนินงาน ซึ่งมีการวิเคราะห์ผลกระทบและกำหนดการเตรียมความพร้อมด้านเทคโนโลยีสารสนเทศไว้ในแผนบริหารความต่อเนื่อง	- แผนบริหารความต่อเนื่อง สถาบันบัณฑิตพัฒนบริหารศาสตร์ - รายงานผลการดำเนินงานตามแผนบริหารความต่อเนื่องของสถาบัน	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.5.31	**ข้อกำหนดทางกฎหมาย ข้อบังคับ ระเบียบและสัญญา (Legal, statutory, regulatory and contractual requirements)** องค์กรต้องระบุข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และพันธสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ รวมถึงวิธีการขององค์กรที่เป็นตามข้อกำหนดดังกล่าว โดยจัดทำเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบัน	สำนักมีขั้นตอนการปฏิบัติงานการจัดการกฎหมายและข้อกำหนดที่เกี่ยวข้อง โดยมีการระบุกฎหมาย ระเบียบข้อบังคับ ที่เกี่ยวข้องการระบบริหารความมั่นคงปลอดภัยสารสนเทศของสำนัก พร้อมระเบียบปฏิบัติงานที่เกี่ยวข้อง โดยมีการทบทวนอย่างน้อยปีละ 1 ครั้งหรือมีการเปลี่ยนที่สำคัญ	- ระเบียบปฏิบัติงานการจัดการกฎหมายและข้อกำหนดที่เกี่ยวข้อง - List of legal	C
A.5.32	**สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)** องค์กรต้องมีขั้นตอนการปฏิบัติงานที่เหมาะสมเพื่อป้องกันสิทธิในทรัพย์สินทางปัญญา	สำนักมีขั้นตอนการปฏิบัติงานในการจัดการและประเมินความสอดคล้องกับข้อกำหนดกฎหมาย ซึ่งรวมถึงพระราชบัญญัติลิขสิทธิ์ รวมถึงสำนักยังมีจัดหาและใช้ซอฟต์แวร์สำหรับใช้ในการปฏิบัติงานที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	- ระเบียบปฏิบัติงานการจัดการกฎหมายและข้อกำหนดที่เกี่ยวข้อง - ประกาศประกวดราคาซื้อโครงการจัดหาซอฟต์แวร์ลิขสิทธิ์พื้นฐานสำหรับสถาบันการศึกษา	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.5.33	**การป้องกันข้อมูลที่บันทึก (Protection of records)** ต้องมีการป้องกันข้อมูลที่บันทึกไว้จากการสูญหาย การถูกทำลาย การถูกปลอมแปลง การเข้าถึง และการเผยแพร่ โดยไม่ได้รับอนุญาต	สำนักกำหนดระดับชั้นข้อมูล วิธีการจัดเก็บ และระยะเวลาในการจัดเก็บ ซึ่งมีการกำหนดการเข้าถึงข้อมูลในระบบตามสิทธิและบทบาทของผู้เกี่ยวข้อง เช่น มีการกำหนดสิทธิเข้าไปดูหรือแก้ไขข้อมูลใน Microsoft 365 มีการกำหนดสิทธิในการเข้าถึงระบบเพื่อดูข้อมูลล็อก (Log) ในระบบ	- ระเบียบปฏิบัติการควบคุมเอกสารของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ - ทะเบียนทรัพย์สิน (Asset) - ตาราง Access Rights Matrix - กำหนดสิทธิการเข้าถึงใน Microsoft 365	C
A.5.34	**ความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information - PII)** องค์กรต้องระบุและปฏิบัติตามข้อกำหนดเกี่ยวกับการรักษาความเป็นส่วนตัวและการ	สำนักมีการดำเนินงานภายใต้นโยบายคุ้มครองข้อมูลส่วนบุคคลของสถาบัน และได้มีการแจ้งการรักษาข้อมูลของผู้รับบริการไว้ในข้อตกลงในการให้บริการ Colocation และ VPS	- นโยบายคุ้มครองข้อมูลส่วนบุคคล สถาบันบัณฑิตพัฒนบริหารศาสตร์ - ข้อกำหนดและเงื่อนไขการให้บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Private Server) - ข้อกำหนดและเงื่อนไขการให้บริการรับฝากเครื่องคอมพิวเตอร์แม่ข่าย (Colocation)	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ปกป้องข้อมูลส่วนบุคคลตามกฎหมาย ข้อบังคับ และข้อกำหนดในสัญญาที่เกี่ยวข้อง			
A.5.35	**การทบทวนความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Independent review of information security)** ต้องมีการทบทวนการบริหารจัดการและการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรอย่างเป็นอิสระตามรอบระยะเวลาที่กำหนดหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ	สถาบันมีการขอรับการประเมินและได้รับการรับรองการดำเนินงานที่สอดคล้องกับมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 จากผู้ตรวจภายนอกอย่างต่อเนื่องทุกปี	- Assessment Report ประจำปี	C
A.5.36	**การปฏิบัติตามนโยบาย กฎเกณฑ์ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ (Compliance with policies, rules and standards for information security)**	สำนักมีการกำหนดให้มีการประเมินเพื่อพิจารณาทบทวนความสอดคล้องของการปฏิบัติงานให้เป็นไปตามกฎหมายและข้อกำหนดที่เกี่ยวข้องอย่างน้อยปี ละ 1 ครั้ง	- ระเบียบปฏิบัติงานการจัดการกฎหมายและข้อกำหนดที่เกี่ยวข้อง	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ต้องมีการทบทวนการปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร อย่างสม่ำเสมอ			
A.5.37	**ขั้นตอนปฏิบัติงานที่เป็นเอกสาร (Documented operating procedures)** ขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับงานประมวลผลข้อมูลต้องมีการจัดทำเป็นลายลักษณ์อักษร และจัดเตรียมพร้อมไว้สำหรับบุคลากรเมื่อต้องการใช้งาน	สำนักมีการจัดทำขั้นตอนการปฏิบัติงานเป็นลายลักษณ์อักษร และเผยแพร่ไว้ใน Microsoft 365 ที่ผู้ปฏิบัติงานสามารถเข้าถึงได้ตลอดเวลา	- เอกสารระเบียบปฏิบัติงานของสำนัก - การจัดเก็บเอกสารใน Microsoft 365	C

ตารางที่ 4-2 ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านองค์กร

ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านองค์กร (Organizational controls) จำนวน 37 ข้อ พบว่าระดับผลประเมินความสอดคล้องของการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของสำนักเมื่อเทียบกับข้อกำหนดการควบคุม Annex A ในมาตรฐาน ISO/IEC 27001:2022 อยู่ในระดับดังนี้

(1) มีการดำเนินงานที่สอดคล้องกับข้อกำหนดครบถ้วน (C) จำนวน 32 ข้อ (คิดเป็นร้อยละ 86.5)

(2) มีการดำเนินงานที่สอดคล้องกับข้อกำหนดบางส่วน (P) จำนวน 5 ข้อ (คิดเป็นร้อยละ 13.5)

จากผลการวิเคราะห์พบว่าสำนักมีการดำเนินงานเพื่อควบคุมความมั่นคงปลอดภัยสารสนเทศครอบคลุมทุกข้อกำหนดการควบคุมด้านองค์กร แต่มีบางข้อกำหนดที่การดำเนินงานยังไม่สอดคล้องกับข้อกำหนดการควบคุมด้านองค์กรใน Annex A ของมาตรฐาน ISO/IEC 27001:2022 ครบถ้วน ได้แก่

(1) ข้อกำหนด A.5.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Policies for information security) ซึ่งสำนักยังไม่ได้มีการทบทวนปรับปรุงนโยบายเฉพาะด้านที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ เช่น นโยบายที่เกี่ยวข้องกับการใช้บริการคลาวด์ นโยบายที่เกี่ยวข้องการใช้ข้อมูลสารสนเทศ

(2) ข้อกำหนด A.5.7 ข่าวกรองภัยคุกคามด้านความมั่นคงปลอดภัย (Threat intelligence) ซึ่งไม่พบว่าสำนักมีการรวบรวม วิเคราะห์ และจัดทำเป็นรายงานข่าวกรองภัยคุกคามอย่างเป็นระบบ

(3) ข้อกำหนด A.5.10 การใช้สารนเทศและทรัพย์สินที่ยอมรับได้ (Acceptable use of information and other associated assets) ซึ่งไม่พบว่าสำนักมีการกำหนดกฎ ระเบียบหรือแนวปฏิบัติในการใช้ข้อมูลสารสนเทศเป็นลายลักษณ์อักษรอย่างชัดเจน

(4) ข้อกำหนด A.5.14 การถ่ายโอนข้อมูล (Information transfer) ซึ่งไม่พบว่าสำนักมีการกำหนดกฎ ระเบียบ หรือแนวปฏิบัติในการถ่ายโอนข้อมูลระหว่างภายในองค์กร

(5) ข้อกำหนด A.5.23 ความมั่นคงปลอดภัยในการใช้บริการคลาวด์ (Information security for use of cloud services) ซึ่งยังไม่พบว่าสำนักมีการกำหนดกระบวนการหรือแนวทางการจัดการที่เกี่ยวข้องกับการใช้บริการคลาวด์

4.3. ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านบุคคล

ในข้อกำหนดการควบคุม Annex A ด้านบุคคล (People controls) ของมาตรฐาน ISO/IEC 27001:2022 ประกอบด้วยข้อกำหนด 8 ข้อ มีผลการวิเคราะห์ดังนี้

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.6.1	**การคัดเลือกบุคลากร (Screening)** การตรวจสอบประวัติความเป็นมาของผู้สมัครงานทั้งหมดเพื่อเป็นพนักงานต้องดำเนินการก่อนเข้ามาปฏิบัติงานและดำเนินการอย่างต่อเนื่องโดยให้สอดคล้องตามกฎหมาย ระเบียบข้อบังคับ และจริยธรรมที่เกี่ยวข้องและเหมาะสมต่อข้อกำหนดขององค์กร ระดับชั้นความลับข้อมูลที่จะเข้าถึง และความเสี่ยงที่เกี่ยวข้อง	การคัดเลือกบุคลากรของสำนักเป็นไปตามกระบวนการคัดเลือกของสถาบัน ซึ่งสำนักจะเป็นผู้กำหนดคุณสมบัติของผู้ที่ผ่านการคัดเลือก โดยสถาบันจะทำการตรวจสอบประวัติของผู้ที่ผ่านการคัดเลือก เช่นประวัติอาชญากรรม ก่อนที่จะเริ่มปฏิบัติงาน	- ข้อบังคับว่าด้วยการบริหารงานบุคคลของพนักงานสถาบัน พ.ศ. 2563 - ประกาศรับสมัครงานของสถาบัน	C
A.6.2	**ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)**	การทำสัญญาการปฏิบัติงานกับบุคลากรของสำนักเป็นตามกระบวนการของสถาบัน ซึ่งแบบของสัญญาการปฏิบัติงานเป็นไปตามที่คณะกรรมการ	- ข้อบังคับว่าด้วยการบริหารงานบุคคลของพนักงานสถาบัน พ.ศ. 2563 - สัญญาจ้างบุคลากรของสถาบัน	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ข้อตกลงในสัญญาจ้างงานต้องระบุถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรและขององค์กร	บริหารงานบุคคลของสถาบันกำหนด ซึ่งกำหนดว่าต้องปฏิบัติตามกฎหมาย ระเบียบข้อบังคับของสถาบัน ซึ่งครอบคลุมถึงความรับผิดชอบในการปปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของสถาบัน		
A.6.3	**การสร้างความตระหนัก การให้ความรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information security awareness, education, and training)** บุคลากรขององค์กรและผู้ที่เกี่ยวข้องจากภายนอกต้องได้รับการสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม รวมถึงการให้ความรู้เกี่ยวกับนโยบายความมั่นคงปลอดภัยสารสนเทศ	สำนักจัดทำแผนสร้างความตระหนัก (Awareness) สำหรับบุคลารของสำนัก โดยมีการชี้แจงแผนงานและจัดอบรมที่เกี่ยวกับข้อกำหนด ISO 27001:2022 ให้บุคลากรของสำนัก นอกจากนี้ยังมีการส่งเสริมให้เกิดการเรียนรู้เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศด้วยการเข้าอบรม การเรียนรู้ด้วยตนเอง ซึ่งจะมีการจัดทำแผนพัฒนารายบุคคลและรายงานผลการพัฒนาของแต่ละบุคคลด้วย	- แผนสร้างความตระหนัก (Awareness) สำหรับบุคลากรสสำนักเทคโนโลยีดิจิทัลและสารสนเทศ และผู้รับบริการ - แผนพัฒนารายบุคคลประจำปี - แบบติดตามการพัฒนาตนเอง	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	นโยบายเฉพาะทาง และขั้นตอนการปฏิบัติที่เป็นปัจจุบัน ซึ่งเกี่ยวข้องกับงานในหน้าที่ที่ต้องปฏิบัติ			
A.6.4	**กระบวนการทางวินัย (Disciplinary process)** ต้องกำหนดกระบวนการทางวินัยอย่างเป็นทางการ และสื่อสารให้บุคลากรรับทราบ เพื่อดำเนินการกับบุคลากรและผู้เกี่ยวข้องจากภายนอกที่มีการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ	สถาบันมีกระบวนการในการจัดการกับบุคลากรของสำนักที่กระทำผิดต่อกฎระเบียบและนโยบายของสถาบัน	- ข้อบังคับว่าด้วยการบริหารงานบุคคลของพนักงานสถาบัน พ.ศ. 2563 - ข้อบังคับสถาบันว่าด้วยการสอบสวนทางวินัย การลงโทษ การสั่งพักราชการ การสั่งให้ออกจากราชการไว้ก่อน พ.ศ. 2552	C
A.6.5	**ความรับผิดชอบภายหลังการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Responsibilities after termination or change of employment)**	ความรับผิดชอบภายหลังการลาออกหรือพ้นสภาพการเป็นบุคลากรของสำนักเป็นไปตามข้อบังคับฯว่าด้วยการลาออกจากราชการของสถาบัน	- ข้อบังคับสถาบันฯว่าด้วยการลาออกจากราชการ พ.ศ. 2552	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ต้องกำหนด บังคับใช้ และสื่อสารความรับผิดชอบและหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศที่ยังคงมีผลบังคับใช้หลังการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงานให้แก่บุคลากรและผู้ที่เกี่ยวข้อง			
A.6.6	**ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยข้อมูล (Confidentiality or non-disclosure agreements)** ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยข้อมูลที่สะท้อนความต้องการในการปกป้องข้อมูลสารสนเทศ ต้องมีการระบุ จัดทำเป็นเอกสาร ทบทวนอย่างสม่ำเสมอ โดยให้บุคลากรและผู้มีส่วนได้ส่วนเสียลงนามในข้อตกลงดังกล่าว	ในข้อตกลงสัญญาการปฏิบัติงานกำหนดว่าบุคลากรต้องปฏิบัติตามกฎระเบียบของสถาบัน และกฎระเบียบทางราชการ ซึ่งรวบถึงการรักษาความลับของข้อมูล	- สัญญาจ้างบุคลากรของสถาบัน	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.6.7	**การปฏิบัติงานจากระยะไกล (Remote working)** ต้องมีมาตรการรักษาความมั่นคงปลอดภัยเมื่อบุคลากรรีโมท (Remote) เข้าทำงานจากภายนอกองค์กร และนำไปปฏิบัติ เพื่อปกป้องสารสนเทศที่มีการเข้าถึง ประมวลผล หรือจัดเก็บจากสถานที่นอกองค์กร	สำนักกำหนดแนวปฏิบัติงานจากภายนอกสถาบัน (Teleworking) และกำหนดให้ผู้รับบริการที่ต้องการ Remote มาที่เครื่องคอมพิวเตอร์แม่ข่ายจะต้องทำผ่านระบบ Virtual Private Network (VPN) ของสถาบันได้เฉพาะเครื่องที่ขอรับบริการเท่านั้น	- นโยบายการใช้งานอุปกรณ์พกพาและการทำงานจากระยะไกล (Mobile device and teleworking policy) - แบบฟอร์มการขอรับบริการ VPN	C
A.6.8	**การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting)** องค์กรต้องจัดให้มีกลไกสำหรับบุคลากรในการรายงานเหตุการณ์ด้านความมั่นคง	สำนักมีช่องทางการสื่อสารภายในสำนักทั้งไลน์ และอีเมล ที่บุคลากรของสำนักสามารถแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศได้ทันที และมีนโยบายและขั้นตอนในการจัดการกับเหตุการณ์ที่เกิดขึ้น	- นโยบายการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยต่อระบบสารสนเทศ - Email แจ้งการตรวจพบการโจมตีเว็บไซต์	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ปลอดภัยสารสนเทศที่พบเห็นหรือสงสัย ผ่านช่องทางที่เหมาะสมอย่างทันท่วงที			

ตารางที่ 4-3 ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านบุคคล

ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านบุคคล (People controls) จำนวน 8 ข้อ พบว่าระดับผลประเมินความสอดคล้องของการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของสำนัก เมื่อเทียบกับข้อกำหนดการควบคุม Annex A ในมาตรฐาน ISO/IEC 27001:2022 อยู่ในระดับ มีการดำเนินงานที่สอดคล้องกับข้อกำหนดครบถ้วน (C) จำนวนครบทั้ง 8 ข้อ (คิดเป็นร้อยละ 100)

จากการวิเคราะห์พบว่าสำนักมีการดำเนินงานเพื่อควบคุมความมั่นคงปลอดภัยสารสนเทศครอบคลุมทุกข้อกำหนดการควบคุมด้านบุคคล และมีการดำเนินงานที่สอดคล้องกับข้อกำหนดการควบคุมด้านบุคคลใน Annex A ของมาตรฐาน ISO/IEC 27001:2022 ครบถ้วนทุกข้อ

4.4. ผลวิเคราะห์ข้อกำหนดการควบคุมด้านกายภาพ

ในข้อกำหนดการควบคุม Annex A ด้านกายภาพ (Physical controls) ของมาตรฐาน ISO/IEC 27001:2022 ประกอบด้วยข้อกำหนด 14 ข้อ มีผลการวิเคราะห์ดังนี้

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.7.1	**ขอบเขตทางกายภาพที่มีความมั่นคงปลอดภัย (Physical Security Perimeter)** ต้องกำหนดและใช้ขอบเขตพื้นที่ความมั่นคงปลอดภัย เพื่อปกป้องพื้นที่ที่มีข้อมูลสารสนเทศและทรัพย์สินที่เกี่ยวข้อง	สำนักมีศูนย์ข้อมูล (Data Center) สำหรับจัดเก็บอุปกรณ์ระบบคอมพิวเตอร์และระบบเครือข่าย ที่มีการออกแบบและก่อสร้างให้มีความมั่นคงแข็งแรง มีการกั้นห้องแบ่งตามโซน Server และโซน Network มีประตูที่ควบคุมการเข้าห้องด้วยลายนิ้วมือ	- แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม - การสำรวจพื้นที่ภายในศูนย์ข้อมูล	C
A.7.2	**การเข้าออกทางกายภาพ (Physical entry)** พื้นที่ความมั่นคงปลอดภัยต้องมีการป้องกัน ด้วยการควบคุมทางเข้าออกและจุดที่เข้าถึงอย่างเหมาะสม	สำนักกำหนดมาตรการควบคุมการเข้าออกพื้นที่ของศูนย์ข้อมูล และติดตั้งระบบสแกนลายนิ้วมือ (Fingerprint) สำหรับควบคุมการเปิดประตูทางเข้าพื้นที่ในแต่ละโซนภายใน Data Center	- แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม - อุปกรณ์สแกนลายนิ้วมือและระบบควบคุมประตูเข้าออก	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.7.3	**การรักษาความปลอดภัยส่วนสำนักงาน ห้อง และสิ่งอำนวยความสะดวก (Securing offices, rooms and facilities)** การรักษาความปลอดภัยทางกายภาพสำหรับสำนักงาน ห้อง และสิ่งอำนวยความสะดวก ต้องมีการออกแบบ และนำไปปฏิบัติ	สำนักแบ่งพื้นที่ของส่วนสำนักงาน เช่น พื้นที่ทำงานของบุคลากร ห้องสำหรับรับส่งอุปกรณ์ และห้องเก็บของชัดเจน มีมาตรการควบคุมการเข้าออกพื้นที่ภายในสำนักงานของสำนัก และมีการการป้องกันการเข้าออกบุคคลภายนอกด้วยระบบสแกนลายนิ้วมือ (Fingerprint)	- แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม - อุปกรณ์สแกนลายนิ้วมือและระบบควบคุมประตูเข้าออก	C
A.7.4	**การเฝ้าระวังความมั่นคงปลอดภัยทางกายภาพ (Physical security monitoring)** สถานที่ภายในองค์กรต้องได้มีการติดตามเฝ้าระวังการเข้าถึงพื้นที่ทางกายภาพโดยไม่ได้รับอนุญาต	สำนักมีการติดตั้งกล้องวงจรปิด (CCTV) ในพื้นที่ศูนย์ข้อมูลของสำนัก และบริเวณทางเข้าสำนักงานสำหรับตรวจสอบการเข้าพื้นที่ของสำนัก แต่ยังไม่ได้มีกระบวนการในการแจ้งเตือน หรือมีการติดตามตรวจสอบอย่างต่อเนื่องที่ชัดเจน	- ระบบกล้องวงจรปิด (CCTV)	P

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.7.5	**การป้องกันภัยคุกคามทางกายภาพและสภาพแวดล้อม (Protecting against physical and environmental threats)** ต้องมีการออกแบบการป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อม เช่น ภัยธรรมชาติและภัยคุกคามทางกายภาพต่อโครงสร้างพื้นฐาน ที่เกิดขึ้นโดยตั้งใจและไม่ตั้งใจ และนำไปปฏิบัติ	ศูนย์ข้อมูล (Data Center) ของสำนักมีการออกแบบติดตั้งระบบไฟฟ้าสำรองจำนวน 2 ชุด มีระบบตรวจจับและแจ้งเตือนน้ำรั่ว (Water leakage) ระบบตรวจจับและแจ้งเตือนเมื่อพบควันหรือความร้อนเพื่อป้องกันเกิดเหตุเกิดอัคคีภัยที่รุนแรง และมีระบบดับเพลิงด้วยสารเคมีเฉพาะทางเพื่อระงับเหตุอัคคีภัย	- อุปกรณ์ที่ติดตั้งภายในพื้นที่ศูนย์ข้อมูล (Data center)	C
A.7.6	**การปฏิบัติงานในพื้นที่ความมั่นคงปลอดภัย (Working in secure areas)** ต้องมีการออกแบบมาตรการรักษาความปลอดภัยสำหรับการทำงานในพื้นที่ความมั่นคงปลอดภัย และนำไปปฏิบัติ	สำนักมีแนวปฏิบัติสำหรับปฏิบัติงานในพื้นที่ Data Center และมีการควบคุมการเข้าออกพื้นที่ Data Center โดยบุคคลภายนอกจะต้องได้อนุญาตและทำการแลกบัตรประชาชนก่อนเข้าพื้นที่	- แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม - บันทึกข้อมูลการเข้าออกพื้นที่ในศูนย์ข้อมูล	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.7.7	**โต๊ะทำงานและหน้าจอคอมพิวเตอร์ที่สะอาดเรียบร้อย (Clear desk and clear screen)** ต้องมีการกำหนดกฎเกณฑ์ทำให้โต๊ะทำงานต้องเรียบร้อย ปราศจากเอกสารและสื่อบันทึกข้อมูลแบบถอดได้บนโต๊ะ และกฎเกณฑ์การทำให้หน้าจอต้องเรียบร้อยปราศจากเครื่องมือที่ใช้ในการประมวลผลสารสนเทศ และมีการบังคับใช้อย่างเหมาะสม	สำนักมีแนวปฏิบัติในการจัดเก็บโต๊ะทำงานและจัดการหน้าจอให้เรียบร้อยไม่เก็บข้อมูลที่เป็นความลับไว้บนโต๊ะทำงานหรือบนหน้า Desktop บนเครื่องคอมพิวเตอร์	- แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม - การสำรวจพื้นที่ภายในศูนย์ข้อมูล	C
A.7.8	**การจัดวางและป้องกันอุปกรณ์ (Equipment siting and protection)** เครื่องมืออุปกรณ์ต้องมีการจัดวางอยู่ในที่ที่ปลอดภัยและมีการป้องกัน	สำนักมีแนวปฏิบัติในการจัดวางและป้องกันอุปกรณ์ โดยมีการติดตั้งอุปกรณ์ภายใน Data Center ให้อยู่ภายในตู้ Rack ที่มีประตูปิดเรียบร้อย	- แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม - การสำรวจพื้นที่ภายในศูนย์ข้อมูล	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.7.9	**ความมั่นคงปลอดภัยของทรัพย์สินที่มีการใช้งานนอกสถานที่ (Security of assets off-premises)** ทรัพย์สินที่อยู่นอกสถานที่ต้องมีมาตรการในการป้องกัน	สำนักมีแนวปฏิบัติและขั้นตอนในนำทรัพย์สินไปใช้ภายนอกสถาบัน	- แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม - ระเบียบปฏิบัติงานการดูแลรักษาครุภัณฑ์	C
A.7.10	**สื่อบันทึกข้อมูล (Storage media)** ต้องมีการจัดการสื่อบันทึกข้อมูลอย่างปลอดภัย ตั้งแต่การจัดหา การใช้งาน การขนส่ง และการกำจัด โดยให้เป็นไปตามข้อกำหนดระดับชั้นและการจัดการข้อมูลขององค์กร	สำนักมีข้อปฏิบัติในการทำลายข้อมูลและสื่อบันทึกข้อมูลก่อนที่จะจำหน่ายหรือส่งต่อให้หน่วยงานอื่น โดยมีการบันทึกรายงานการทำลายข้อมูลไว้ตรวจสอบ	- ระเบียบปฏิบัติงานการดูแลรักษาครุภัณฑ์	C
A.7.11	**ระบบสาธารณูปโภคที่สนับสนุน (Supporting utilities)** ระบบหรืออุปกรณ์ประมวลผลข้อมูลต้องได้รับการปกป้องความเสียหายจาก	ระบบไฟฟ้าภายในอาคารที่ดูแลโดยกองบริหารงานกลาง ซึ่งมีเครื่องกำหนดไฟฟ้าสำรองและมีการจ่ายให้กับ Data Center ของสำนักเมื่อเกิดเหตุระบบไฟฟ้าขัดข้อง ซึ่งกองบริหารกลางมีการบำรุงรักษา	- หนังสือขอความอนุเคราะห์ตรวจสอบการสำรองน้ำมันเชื้อเพลิงของเครื่องกำเนิดไฟฟ้า	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	กระแสไฟฟ้าดับและการหยุดชะงักอื่นๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบสาธารณูปโภคสนับสนุน	ระบบไฟฟ้าเป็นประจำอย่างน้อยปีละครั้ง ทั้งนี้สำนักได้ทำหนังสือเพื่อขอให้กองบริหารงานกลางทบทวนการสำรองน้ำมันเชื้อเพลิงด้วย นอกจากนี้สำนักยังมีระบบไฟฟ้าสำรองเพื่อป้องกันไม่ให้อุปกรณ์เสียหายจากกระแสไฟฟ้าดับ	- หนังสือเวียนแจ้งการปิดบำรุงรักษาระบบไฟฟ้าของอาคาร - ระบบไฟฟ้าสำรอง	
A.7.12	**ความปลอดภัยของสายสัญญาณ (Cabling security)** สายสัญญาณในการส่งกระแสไฟฟ้า หรือข้อมูลสารสนเทศต้องได้รับการป้องกันจากการดักจับ การรบกวน หรือการทำให้เสียหาย	สำนักมีแนวปฏิบัติในการเดินสายสัญญาณภายใน Data Center โดยสายสัญญาณภายในที่เดินจะถูกจัดเก็บไว้ภายในท่อหรือรางเดินสายสัญญาณ และแยกประเภทสายสัญญา	- แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม - การสำรวจพื้นที่ภายในศูนย์ข้อมูล	C
A.7.13	**การบำรุงรักษาอุปกรณ์ (Equipment maintenance)** ต้องมีการบำรุงรักษาอุปกรณ์อย่างถูกต้องเพื่อให้มั่นใจในความพร้อมใช้งาน ความ	สำนักจัดทำระเบียบปฏิบัติงานงานบำรุงรักษาในการบำรุงรักษาอุปกรณ์ระบบโครงสร้างพื้นฐาน โดยมีการจัดจ้างผู้ให้บริการภายนอกที่เชี่ยวชาญมาบำรุงรักษาอุปกรณ์หลัก และมีการบำรุงรักษาเชิง	- ระเบียบปฏิบัติงานบำรุงรักษา - รายงานการบำรุงรักษาของส่วนโครงสร้างพื้นฐานและความมั่นคงปลอดภัย	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ถูกต้องสมบูรณ์ และการรักษาความลับของสารสนเทศ	ป้องกัน (Preventive Maintenance) ตามรอบระยะเวลาที่กำหนด		
A.7.14	**การกำจัดหรือนำอุปกรณ์มาใช้อย่างปลอดภัย (Secure disposal or re-use of equipment)** ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลก่อนการกำจัดหรือนำกลับมาใช้ใหม่ เพื่อให้มั่นใจว่าข้อมูลที่สำคัญหรืออ่อนไหวและซอฟต์แวร์ที่มีลิขสิทธิ์ได้ถูกลบออกหรือเขียนทับอย่างปลอดภัย	สำนักมีแนวปฏิบัติในการกำจัดอุปกรณ์หรือนำมาใช้ซ้ำ โดยจะต้องมีการทำลายข้อมูลและซอฟต์แวร์ที่ติดตั้งไว้ในอุปกรณ์ตามขั้นตอนปฏิบัติการดูแลรักษาครุภัณฑ์ก่อนนำไปใช้งาน	- แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม - ระเบียบปฏิบัติงานการดูแลรักษาครุภัณฑ์	C

ตารางที่ 4-4 ผลวิเคราะห์ข้อกำหนดการควบคุมด้านกายภาพ

ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านกายภาพ (Physical controls) จำนวน 14 ข้อ พบว่าระดับผลประเมินความสอดคล้องของการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของสำนักเมื่อเทียบกับข้อกำหนดการควบคุม Annex A ในมาตรฐาน ISO/IEC 27001:2022 อยู่ในระดับดังนี้

(1) มีการดำเนินงานที่สอดคล้องกับข้อกำหนดครบถ้วน (C) จำนวน 13 ข้อ (คิดเป็นร้อยละ 92.9)

(2) มีการดำเนินงานที่สอดคล้องกับข้อกำหนดบางส่วน (P) จำนวน 1 ข้อ (คิดเป็นร้อยละ 8.1)

จากผลการวิเคราะห์พบว่าสำนักมีการดำเนินงานเพื่อควบคุมความมั่นคงปลอดภัยสารสนเทศครอบคลุมทุกข้อกำหนดการควบคุมด้านกายภาพ แต่มีบางข้อกำหนดที่การดำเนินงานยังไม่สอดคล้องกับข้อกำหนดการควบคุมด้านกายภาพใน Annex A ของมาตรฐาน ISO/IEC 27001:2022 ครบถ้วน ได้แก่ ข้อกำหนด A.7.4 การเฝ้าระวังความมั่นคงปลอดภัยทางกายภาพ (Physical security monitoring) ซึ่งไม่พบว่าสำนักมีกระบวนการในการแจ้งเตือนหรือตรวจสอบเฝ้าระวังอย่างต่อเนื่องที่ชัดเจน

4.5. ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านเทคโนโลยี

ในข้อกำหนดการควบคุม Annex A ด้านเทคโนโลยี (Technological controls) ของมาตรฐาน ISO/IEC 27001:2022 ประกอบด้วยข้อกำหนด 34 ข้อ มีผลการวิเคราะห์ดังนี้

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.8.1	**อุปกรณ์ปลายทางของผู้ใช้งาน (User endpoint devices)** อุปกรณ์ปลายทางของผู้ที่สามารถเข้าถึงหรือประมวลผลสารสนเทศ ต้องมีมาตรการในการควบคุมและป้องกัน	สำนักได้กำหนดแนวปฏิบัติในการใช้งานอุปกรณ์ประเภทพกพาไว้ในนโยบายการใช้งานอุปกรณ์พกพาและการทำงานจากระยะไกล (Mobile device and teleworking policy) และการป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended user equipment) ไว้ในแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม	- นโยบายการใช้งานอุปกรณ์พกพาและการทำงานจากระยะไกล - แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	C
A.8.2	**สิทธิ์การเข้าถึงแบบพิเศษ (Privileged access rights)** ต้องมีการจำกัดและบริหารจัดการสิทธิ์การเข้าถึงและใช้ข้อมูลแบบพิเศษ	สำนักกำหนดแนวปฏิบัติการจัดการสิทธิระดับ Admin ไว้ในนโยบายการควบคุมการเข้าถึง และจัดทำ Access Rights Matrix ในการระบุสิทธิในการเข้าถึงระดับ Admin ของผู้ดูแลระบบแต่ละคน	- นโยบายการควบคุมการเข้าถึง (Access Control Policy) - Access Rights Matrix	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.8.3	**การจำกัดการเข้าถึงข้อมูล (Information access restriction)** ต้องมีการจำกัดสิทธิในการเข้าถึงสารสนเทศและสินทรัพย์ที่เกี่ยวข้องอื่นๆ เป็นไปตามนโยบายเฉพาะทางที่ควบคุมการเข้าถึงที่กำหนดไว้	สำนักกำหนดคำนิยามระดับชั้นความลับของข้อมูลไว้ในระเบียบปฏิบัติการควบคุมเอกสารของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ โดยกำหนดระดับชั้นให้กับเอกสารส่วนสนับสนุนไว้ในในระเบียบปฏิบัติการควบคุมเอกสารของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ และกำหนดระดับชั้นให้กับข้อมูลของระบบโครงสร้างพื้นฐานไว้ในบัญชีทะเบียนทรัพย์สิน (Asset)	- ระเบียบปฏิบัติงานการควบคุมเอกสารของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ - ทะเบียนทรัพย์สิน (Asset)	C
A.8.4	**การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Source code access control)** ต้องมีการบริหารจัดการควบคุมการเข้าถึงเพื่ออ่านและเขียนซอร์สโค้ด เครื่องมือที่ใช้ในการพัฒนาระบบ และไลบรารีซอฟต์แวร์อย่างเหมาะสม	สำนักขอยกเว้นไม่ดำเนินการตามมาตรการควบคุม เนื่องจากโปรแกรมที่ใช้งานเป็นซอฟต์แวร์สำเร็จรูปที่ถูกลิขสิทธิ์ ไม่ได้มีการพัฒนาโปรแกรมหรือระบบใช้งานเองจึงไม่มีซอร์สโค้ดของโปรแกรม		E

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.8.5	**การพิสูจน์ตัวตนที่ปลอดภัย (Secure authentication)** ต้องมีการนำเทคโนโลยีและขั้นตอนปฏิบัติในการพิสูจน์ยืนยันตัวตนที่มีความมั่นคงปลอดภัยไปปฏิบัติใช้ ให้สอดคล้องกับการจำกัดสิทธิการเข้าถึงข้อมูลและนโยบายควบคุมการเข้าถึง	การเข้าถึงระบบจะมีการป้องกันด้วยรหัสผ่านที่ต้องกำหนดให้มีความยากตาม Password Policy ที่กำหนดไว้ และมีการใช้ Multi Factor Authentication (MFA) ในการเข้าสู่ระบบ Microsoft 365 ส่วนการเข้าถึงพื้นที่ภายในศูนย์ข้อมูล (Data Center) จะใช้เทคโนโลยี Biometric ด้วยการสแกนลายนิ้วมือ	- นโยบายการควบคุมการเข้าถึง (Access Control Policy) - ระบบ Microsoft 365 - อุปกรณ์สแกนลายนิ้วมือและระบบควบคุมประตูเข้าออก	C
A.8.6	**การบริหารจัดการขีดความสามารถของระบบ (Capacity management)** ต้องมีการตรวจสอบ เฝ้าระวัง ติดตามการใช้ทรัพยากร และปรับปรุงให้สอดคล้องกับความต้องการใช้ทรัพยากรในปัจจุบันและรองรับในอนาคต	สำนักมีแนวปฏิบัติการบริหารจัดการใช้ทรัพยากร (Capacity Management) โดยมีการกำหนดระบบและอุปกรณ์ที่ต้องมีการวัดเฝ้าระวัง พร้อมค่าที่ต้องเฝ้าระวัง ซึ่งสามารถตรวจสอบผ่านระบบได้	- แนวปฏิบัติการบริหารจัดการใช้ทรัพยากร (Capacity Management) - การตั้งค่าแจ้งเตือนบนระบบที่ใช้ในการเฝ้าระวัง (Monitoring)	C
A.8.7	**การป้องกันการโจมตีจากมัลแวร์ (Protection against malware)**	อุปกรณ์ Firewall ของสำนักมีระบบ URL Filtering ที่ตรวจสอบเว็บไซต์ที่เสี่ยงต่อการถูกโจมตีจากมัลแวร์	- ระบบ Firewall - ซอฟต์แวร์ Antivirus	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ต้องมีมาตรการป้องกันมัลแวร์และสร้างความตระหนักในการป้องกันให้กับผู้ใช้งานอย่างเหมาะสม	รวมถึงมีการติดตั้ง Antivirus บนเครื่องคอมพิวเตอร์ที่ใช้งาน ซึ่งมีการปรับปรุง Signature ให้ทันสมัยตลอด		
A.8.8	**การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)** ต้องมีการติดตามรวบรวมข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบสารสนเทศที่ใช้งาน ต้องมีการประเมินและมีมาตรการดำเนินการกับช่องโหว่ดังกล่าวอย่างเหมาะสม	สำนักเข้าร่วมโครงการ Proactive Cyber Watch ของสำนักคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ซึ่งจะช่วยตรวจสอบช่องโหว่ของระบบที่อยู่ภายใต้โดเมน nida.ac.th และมีการใช้ซอฟต์แวร์ตรวจสอบช่องโหว่ของอุปกรณ์เครือข่าย แต่ยังไม่มีการประเมินและมีมาตรการดำเนินการกับช่องโหว่ที่พบอย่างชัดเจน	- รายงานสรุปโครงการระบบตรวจจับพฤติกรรมและวิเคราะห์ข้อมูลอาชญากรรมทางไซเบอร์เชิงรุกสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานภาครัฐ (Proactive Cyber Watch) - ซอฟต์แวร์ตรวจประเมินช่องโหว่ (Vulnerability Assessment)	P
A.8.9	**การบริหารจัดการการตั้งค่าระบบ (Configuration Management)** ข้อมูลการตั้งค่า (Configuration) ที่รวมถึงการตั้งค่าที่เกี่ยวกับความมั่นคง	สำนักมีการสำรองข้อมูล Configuration ของอุปกรณ์ มีการใช้ระบบบริหารจัดการเครือข่ายเพื่อบันทึกข้อมูล Configuration ของอุปกรณ์เครือข่าย แต่ยังไม่ได้มีการจัดการกับ Configuration ในส่วน	- ระบบบริหารจัดการเครือข่าย (Network Management System)	P

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ปลอดภัย ฮาร์ดแวร์ ซอฟต์แวร์ บริการและเครือข่าย ต้องมีการจัดทำเป็นเอกสารนำไปปฏิบัติ และมีการทบทวน	ของระบบคอมพิวเตอร์ รวมถึงยังไม่มีแนวทางการจัดการกับข้อมูลและการทบทวนข้อมูลที่ชัดเจน		
A.8.10	**การลบข้อมูล (Information deletion)** ข้อมูลที่จัดเก็บในระบบสารสนเทศ อุปกรณ์ หรือสื่อจัดเก็บอื่นๆ จะต้องถูกลบทำลายเมื่อไม่มีความจำเป็นต้องใช้อีกต่อไป	สำนักมีการจัดการกับข้อมูลในเอกสารตามระเบียบและแนวทางของสถาบัน แต่ยังไม่มีการจัดการกับข้อมูลในระบบสารสนเทศอย่างเป็นระบบที่ชัดเจน	- การกำหนดประเภท และอายุการเก็บเอกสาร สถาบันบัณฑิตพัฒนบริหารศาสตร์	P
A.8.11	**การปกปิดข้อมูล (Data masking)** ต้องมีการปกปิดข้อมูลไม่ให้มองเห็นหรือนำไปใช้ต่อได้ ตามนโยบายควบคุมการเข้าถึงและนโยบายที่เกี่ยวข้อง และข้อกำหนดทางธุรกิจ โดยคำนึงถึงกฎหมายที่เกี่ยวข้องประกอบด้วย	สำนักกำหนดให้รหัสผ่านที่ผู้ใช้งานกรอกในระบบจะต้องถูกปิดบังไว้ไม่ให้รู้ แต่ในด้านข้อมูลส่วนบุคคล สถาบันมีคู่มือการปฏิบัติงานตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลใช้เป็นแนวทางในการจัดการ	- คู่มือการปฏิบัติงานของบุคลากรในส่วนของการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล - หน้าจอ Login เข้าระบบ VPN	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.8.12	**การป้องกันการรั่วไหลของข้อมูล (Data Leakage Prevention)** ต้องมีการนำมาตรการป้องกันการรั่วไหลของข้อมูลมาใช้กับระบบ เครือข่าย และอุปกรณ์อื่นๆ ที่ใช้ในการประมวลผล จัดเก็บ หรือรับส่งข้อมูลที่มีความสำคัญหรืออ่อนไหว	สำนักยังไม่มีมาตรการดำเนินงานตามข้อกำหนดการควบคุม		N
A.8.13	**การสำรองข้อมูล (Information backup)** สำเนาข้อมูล ซอฟต์แวร์ และระบบที่สำรองไว้ จะต้องมีการดูแลรักษาและทดสอบเป็นประจำตามนโยบายการสำรองข้อมูลที่กำหนดไว้	สำนักกำหนดขั้นตอนการสำรองข้อมูลไว้ในขั้นตอนการปฏิบัติงานบำรุงรักษา โดยมีการกำหนดระยะเวลาการจัดเก็บและความถี่ในการสำรองข้อมูล	- ระเบียบปฏิบัติงานงานบำรุงรักษาระบบโครงสร้างพื้นฐาน - ระบบสำรองข้อมูล (Backup)	C
A.8.14	**การทำงานแบบทดแทนกันได้ของอุปกรณ์ที่ช่วยสนับสนุนการประมวผล**	อุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของระบบโครงสร้างพื้นฐานจะออกแบบให้อุปกรณ์	- อุปกรณ์ Core Switch	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	สารสนเทศ (Redundancy of information processing facilities) อุปกรณ์ที่ช่วยสนับสนุนการประมวลผลสารสนเทศต้องมีการทำงานแบบทดแทนกันได้ (Redundancy) ที่เพียงพอต่อความพร้อมในการใช้งานอย่างต่อเนื่อง	ภายในมีการทำงานแบบ Redundant เพื่อป้องกันเมื่อชุดใดชุดหนึ่งล่ม เช่น มี Power Supply จำนวน 2 ชุด มีอุปกรณ์จัดเก็บข้อมูล (Disk) จำนวน 2 ชุด ที่ทำงานแบบ Redundant	- เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ VPS	
A.8.15	**การบันทึกข้อมูลล็อก (Logging)** ต้องมีการจัดทำระบบให้มีการจัดเก็บและป้องกันข้อมูลล็อกที่บันทึกกิจกรรม ข้อยกเว้น ข้อผิดพลาด และเหตุการณ์อื่นๆ ที่เกี่ยวข้อง จัดเก็บ และสามารถนำข้อมูลไปวิเคราะห์ได้	สำนักมีระบบจัดเก็บข้อมูลล็อกและมีการจัดการเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์	- ระบบ Log Management	C
A.8.16	**กิจกรรมการเฝ้าระวังการทำงานของระบบและอุปกรณ์ (Monitoring activities)**	สำนักมีระบบตรวจสอบเฝ้าระวังการทำงานของระบบและอุปกรณ์หลัก พร้อมกับตั้งค่าการแจ้งเตือนผู้ดูแลระบบเมื่อมีการทำงานที่ผิดปกติ	- ระบบ Network Monitor	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ต้องมีการเฝ้าระวังความผิดปกติของเครือข่าย ระบบ และแอปพลิเคชัน และต้องดำเนินการประเมินความเป็นไปได้ของเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้น			
A.8.17	**การเทียบเวลา (Clock synchronization)** นาฬิกาของระบบประมวลผลข้อมูลสารสนเทศที่องค์กรใช้งานต้องมีการตั้งค่าให้เที่ยงตรงโดยการเทียบเวลากับแหล่งเทียบเวลาที่ได้รับการรับรอง	สำนักมีระบบ Time Server ที่มีการเทียบเวลาสากล และจะทำการตั้งค่าอุปกรณ์ระบบต่างๆจะทำการเชื่อมต่อกับ Time Server เพื่อทำการเทียบเวลา	- ระบบ Time Sever	C
A.8.18	**การใช้โปรแกรมอรรถประโยชน์ที่มีสิทธิในระดับพิเศษ (Use of privileged utility programs)**	สำนักมีการกำหนดสิทธิระดับ Admin ในการเข้าถึงอุปกรณ์ให้กับผู้ดูแลระบบที่เกี่ยวข้องเพื่อติดตั้งโปรแกรมประเภทเท่าที่จำเป็นต่อการใช้งานเท่านั้น	- นโยบายการควบคุมการเข้าถึง - ทะเบียนทรัพย์สิน (Asset)	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ต้องมีการจำกัดและควบคุมการใช้โปรแกรมอรรถประโยชน์ (Utility) ที่สามารถควบคุมแอปพลิเคชันและระบบอย่างเข้มงวด	และมีการกำหนดรายชื่อซอฟต์แวร์ที่สามารถติดตั้งใช้งานได้ไว้ในทะเบียนทรัพย์สิน (Asset)		
A.8.19	**การติดตั้งซอฟต์แวร์ระบบปฏิบัติการ (Installation of software on operational systems** ต้องดำเนินการตามขั้นตอนปฏิบัติงานและมาตรการในการจัดการการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการอย่างปลอดภัย	สำนักมีการติดตั้งซอฟต์แวร์ตามคู่มือหรือคำแนะนำจากเจ้าของผลิตภัณฑ์ และมีการอัปเดตซอฟต์แวร์ตามความจำเป็น	- คู่มือการติดตั้งและใช้งานซอฟต์แวร์	C
A.8.20	**ความมั่นคงปลอดภัยของเครือข่าย (Networks security)** เครือข่ายและอุปกรณ์เครือข่ายต้องมีการรักษาความมั่นคงปลอดภัย ได้รับการ	สถาบันมีการออกแบบผังการเชื่อมต่อเครือข่ายของสถาบัน มีอุปกรณ์ระบบ Firewall ในการควบคุมการเข้าถึงเครือข่ายของสถาบัน มีการนำระบบ	- ผังเครือข่ายสถาบัน - ระบบ Firewall - ระบบ Virtual Private Network (VPN)	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	บริหารจัดการ และมีการควบคุมเพื่อป้องกันข้อมูลทั้งในระบบและแอปพลิเคชัน	Virtual Private Network มาใช้กับระบบที่มีการจำกัดการเข้าถึงจากเครือข่ายภายนอก		
A.8.21	**ความมั่นคงปลอดภัยของบริการเครือข่าย (Security of network services)** ต้องมีการกำหนดกลไกความปลอดภัย ระดับการให้บริการ และข้อกำหนดการให้บริการของบริการเครือข่าย โดยต้องนำไปปฏิบัติและติดตามเฝ้าระวัง	สถาบันใช้บริการเครือข่ายอินเทอร์เน็ตจากผู้ให้บริการที่ได้รับมาตรฐาน ISO/IEC 27001 และมีการกำหนดระดับการให้บริการ (SLA) ที่ชัดเจน โดยสำนักมีการตรวจรับการให้บริการตามงวดงานที่มีการตกลงกับผู้ให้บริการ	- ข้อมูลของผู้ให้บริการอินเทอร์เน็ต - เอกสารตรวจรับการให้บริการอินเทอร์เน็ต	C
A.8.22	**การแบ่งแยกเครือข่าย (Segregation in networks)** ในเครือข่ายขององค์กรต้องมีการแบ่งแยกกลุ่มของการให้บริการสารสนเทศ กลุ่ม	สถาบันมีการใช้ระบบ Firewall หลักของสถาบันในการแบ่งโซนเครือข่ายทั้งแบบ Wired LAN และ Wireless LAN รวมถึงมีการแยกโซนของระบบที่ให้บริการเทคโนโลยีสารสนเทศออกจากโซนของผู้ใช้งาน	- ผังเครือข่ายสถาบัน - ระบบ Firewall	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ของผู้ใช้งาน และกลุ่มของระบบสารสนเทศออกจากกัน			
A.8.23	**การคัดกรองเว็บ (Web filtering)** การเข้าถึงและเปิดเว็บไซต์ภายนอกจะต้องได้รับการบริหารจัดการเพื่อลดการเข้าถึงเนื้อหาที่เป็นอันตราย	สำนักมีระบบ URL Filtering ในอุปกรณ์ Firewall และระบบ Antivirus ที่ช่วยตรวจสอบและป้องกันการเข้าถึงเว็บไซต์ที่ไม่ปลอดภัย	- ระบบ Firewall	C
A.8.24	**การใช้การเข้ารหัสข้อมูล (Use of cryptography)** ต้องมีการกำหนดกฎระเบียบสำหรับการใช้งานการเข้ารหัสข้อมูลอย่างมีประสิทธิภาพ รวมถึงการจัดการกับกุญแจที่ใช้ในการเข้ารหัสข้อมูล โดยนำไปปฏิบัติ	สำนักมีการเข้ารหัส (Encryption) ในข้อมูล VPS ที่ทำการสำรองไว้ แต่ยังไม่มีกฎระเบียบ หรือแนวปฏิบัติการจัดการเข้ารหัสข้อมูลกับกุญแจที่ใช้ในการเข้ารหัสข้อมูล	- ระบบสำรองข้อมูล (Backup)	P
A.8.25	**วงจรการพัฒนาที่ปลอดภัย (Secure development life cycle)**	สำนักขอยกเว้นไม่ดำเนินการตามมาตรการควบคุม เนื่องจากขอบเขตการขอรับรองไม่มีการพัฒนาระบบ		E

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ต้องกำหนดกฎระเบียบสำหรับการพัฒนาซอฟต์แวร์และระบบที่มีความปลอดภัยและนำไปปฏิบัติ			
A.8.26	**ข้อกำหนดความปลอดภัยของแอปพลิเคชัน (Application security requirements)** ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศของแอปพลิเคชัน จะต้องถูกกำหนด และได้รับการอนุมัติเมื่อมีการพัฒนาหรือจัดหาแอปพลิเคชัน	สำนักขอยกเว้นไม่ดำเนินการตามมาตรการควบคุม เนื่องจากขอบเขตการขอรับรองไม่มีการพัฒนาระบบ		E
A.8.27	**หลักการสถาปัตยกรรมระบบและวิศวกรรมที่ปลอดภัย (Secure system architecture and engineering principles)**	ข้อกำหนดการดำเนินงานโครงการของสำนักที่เกี่ยวกับระบบโครงสร้างพื้นฐาน จะกำหนดให้ต้องมีการจัดทำแผนภาพสถาปัตยกรรมของระบบมาให้พิจารณาก่อนดำเนินการ	- TOR โครงการระบบการให้บริการการศึกษาแบบเปิด (Open System for Lifelong Learning) รองรับการเรียนรู้ตลอดชีวิตเพื่อการพัฒนาที่ยั่งยืน พร้อมค่าติดตั้ง ระยะที่ 2	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	หลักการสำหรับการออกแบบระบบที่ปลอดภัยจะต้องถูกกำหนด จัดทำเป็นเอกสาร ปรับปรุง และนำไปใช้กับกิจกรรมการพัฒนาระบบสารสนเทศ			
A.8.28	**การเขียนโปรแกรมให้มีความปลอดภัย (Secure Coding)** หลักการเขียนโปรแกรมให้มีความมั่นคงปลอดภัยจะต้องถูกนำไปใช้ในการพัฒนาซอฟต์แวร์	สำนักขอยกเว้นไม่ดำเนินการตามมาตรการควบคุม เนื่องจากขอบเขตการขอรับรองไม่มีการพัฒนาระบบ		E
A.8.29	**การทดสอบความปลอดภัยในการพัฒนาและการยอมรับ (Security testing in development and acceptance)** ต้องกำหนดกระบวนการทดสอบด้านความมั่นคงปลอดภัยและมีการนำไปใช้ตลอดการพัฒนาทั้งวงจร	สำนักขอยกเว้นไม่ดำเนินการตามมาตรการควบคุม เนื่องจากขอบเขตการขอรับรองไม่มีการพัฒนาระบบ		E

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
A.8.30	**การพัฒนาโดยผู้ให้บริการภายนอก (Outsourced development)** องค์กรต้องกำกับดูแล ติดตามเฝ้าระวัง และทบทวนกิจกรรมในการพัฒนาระบบโดยผู้ให้บริการภายนอก	สำนักขอยกเว้นไม่ดำเนินการตามมาตรการควบคุม เนื่องจากขอบเขตการขอรับรองไม่มีการพัฒนาระบบ		E
A.8.31	**การแยกสภาพแวดล้อมการพัฒนา ทดสอบ และใช้งานจริง (Separation of development, testing and operational environments)** สภาพแวดล้อมสำหรับใช้ในการพัฒนา การทดสอบ และการใช้งานจริง ต้องมีการแยกจากกันและมีการรักษาความมั่นคงปลอดภัย	สำนักไม่สามารถแยกสภาพแวดล้อมของทรัพยากรระบบโครงสร้างพื้นฐานเพื่อใช้ในการทดสอบได้ แต่สำนักมีการยอมรับความเสี่ยงที่อาจจะเกิดข้อผิดพลาดในระหว่างการทดสอบระบบโดยผู้บริหารสำนัก	- รายงานผลการประเมินความเสี่ยงและแผนการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลสารสนเทศ ประจำปี	C
A.8.32	**การบริหารจัดการการเปลี่ยนแปลง (Change management)**	สำนักมีขั้นตอนการบริหารจัดการการเปลี่ยนแปลง (Change Management) และมีการดำเนินงานเมื่อ	- ระเบียบปฏิบัติงานการควบคุมการเปลี่ยนแปลง (Change Management)	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	การเปลี่ยนแปลงที่มีผลต่ออุปกรณ์หรือระบบประมวลผลข้อมูลและระบบสารสนเทศจะต้องปฏิบัติตามขั้นตอนการบริหารจัดการการเปลี่ยนแปลง	มีการปรับเปลี่ยนในส่วนที่มีผลกระทบต่อการให้บริการของสำนัก	- บันทึกข้อมูล Event-Incident Log	
A.8.33	**ข้อมูลทดสอบ (Test information)** ข้อมูลสำหรับใช้ในการทดสอบจะต้องมีการคัดเลือก มีการป้องกัน และมีการบริหารจัดการอย่างเหมาะสม	สำนักขอยกเว้นไม่ดำเนินการตามมาตรการควบคุม เนื่องจากขอบเขตการขอรับรองไม่มีการพัฒนาระบบ		E
A.8.34	**การป้องกันระบบสารสนเทศในช่วงที่มีการทดสอบระบบโดยผู้ตรวจประเมิน (Protection of information systems during audit testing)** ต้องมีการวางแผนการทดสอบระบบโดยผู้ตรวจประเมินและกิจกรรมการตรวจประเมินอื่นๆ ที่เกี่ยวข้องกับการประเมิน	สำนักทำข้อตกลงเรื่องการปฏิบัติตามระเบียบของสถาบันและเรื่องความเป็นส่วนตัวของข้อมูลกับผู้ตรวจประเมินจากภายนอก	ข้อตกลงและเงื่อนไขการให้บริการของผู้ตรวจประเมิน	C

ลำดับ	ข้อกำหนด	การดำเนินงานของสำนัก	หลักฐานอ้างอิง	ผลประเมิน
	ระบบให้บริการ และต้องมีข้อตกลงกันระหว่างผู้ดำเนินการทดสอบและฝ่ายบริหารอย่างเหมาะสม			

ตารางที่ 4-5 ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านเทคโนโลยี

ในผลการวิเคราะห์ข้อกำหนดการควบคุมด้านเทคโนโลยี จำนวน 34 ข้อ นั้น พบว่า สำนักขอยกเว้นไม่ขอรับการประเมินเพื่อรับรองมาตรฐาน จำนวน 7 ข้อ และข้อกำหนดที่มีการประเมินอีกจำนวน 27 ข้อ ซึ่งระดับผลประเมินความสอดคล้องของการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของสำนักเมื่อเทียบกับข้อกำหนดการควบคุม Annex A ในมาตรฐาน ISO/IEC 27001:2022 อยู่ในระดับดังนี้

(1) มีการดำเนินงานที่สอดคล้องกับข้อกำหนดครบถ้วน (C) จำนวน 22 ข้อ (คิดเป็นร้อยละ 81.5 เทียบข้อกำหนดที่มีการประเมิน)
(2) มีการดำเนินงานที่สอดคล้องกับข้อกำหนดบางส่วน (P) จำนวน 4 ข้อ (คิดเป็นร้อยละ 14.8 เทียบกับข้อกำหนดที่มีการประเมิน)
(3) ไม่มีการดำเนินงานที่สอดคล้องกับข้อกำหนด (N) จำนวน 1 ข้อ (คิดเป็นร้อยละ 3.7 เทียบกับข้อกำหนดที่มีการประเมิน)

จากผลการวิเคราะห์พบว่าการบริหารจัดการด้านความมั่นคงปลอดภัยของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ ยังไม่ครอบคลุมข้อกำหนดการควบคุมด้านเทคโนโลยีในข้อกำหนด Annex A ทุกข้อ โดยยังไม่พบการดำเนินงานในข้อกำหนด A.8.12 การป้องกันการรั่วไหลของข้อมูล (Data Leakage Prevention) ซึ่งไม่พบการดำเนินงานใดๆที่สอดคล้องกับข้อกำหนด ส่วนผลการดำเนินงานที่สอดคล้องกับข้อกำหนดการควบคุมเทคโนโลยีบางส่วนนั้น ซึ่งประกอบด้วย

(1) ข้อกำหนด A.8.8 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities) ซึ่งพบว่าการประเมินและการจัดการกับช่องโหว่ยังไม่มีมาตรการที่เป็นระบบอย่างชัดเจน
(2) ข้อกำหนด A.8.9 การบริหารจัดการการตั้งค่าระบบ (Configuration Management) ซึ่งพบว่าการจัดการกับข้อมูลการตั้งค่ายังไม่เป็นระบบและไม่มีการทบทวนข้อมูลเป็นประจำ
(3) ข้อกำหนด A.8.10 การลบข้อมูล (Information deletion) ซึ่งพบว่ามีการจัดการกับข้อมูลที่ยังไม่ครอบคลุมถึงข้อมูลในระบบสารสนเทศ
(4) ข้อกำหนด A.8.24 การใช้การเข้ารหัสข้อมูล (Use of cryptography) ซึ่งพบว่ายังไม่มีการกำหนดกฎระเบียบ หรือแนวปฏิบัติในการจัดการเข้ารหัสข้อมูลและการจัดการกุญแจที่ใช้ในการเข้ารหัส

ส่วนข้อกำหนดการควบคุมด้านเทคโนโลยีในข้อกำหนด Annex A ที่สำนักเทคโนโลยีดิจิทัลและสารสนเทศไม่ขอรับการประเมิน ประกอบด้วย

(1) ข้อกำหนด 8.4 การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Source code access control)

(2) ข้อกำหนด 8.25 วงจรการพัฒนาที่ปลอดภัย (Secure development life cycle)

(3) ข้อกำหนด 8.26 ข้อกำหนดความปลอดภัยของแอปพลิเคชัน (Application security requirements)

(4) ข้อกำหนด 8.28 การเขียนโปรแกรมให้มีความปลอดภัย (Secure Coding)

(5) ข้อกำหนด 8.29 การทดสอบความปลอดภัยในการพัฒนาและการยอมรับ (Security testing in development and acceptance)

(6) ข้อกำหนด 8.30 การพัฒนาโดยผู้ให้บริการภายนอก (Outsourced development)

(7) ข้อกำหนด 8.33 ข้อมูลทดสอบ (Test information)

บทที่ 5. สรุปผลและข้อเสนอแนะ

การวิเคราะห์ความพร้อมขององค์กรในการขอรับรองมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 กรณีศึกษาสำนักเทคโนโลยีดิจิทัลและสารสนเทศ มีวัตถุประสงค์ในการวิเคราะห์ดังนี้

(1) เพื่อศึกษาระบบบริหารความมั่นคงปลอดภัยสารสนเทศและมาตรการควบคุม (Control) ของมาตรฐาน ISO/IEC 27001:2022

(2) เพื่อประเมินความสอดคล้องและวิเคราะห์ช่องว่าง (Gap Analysis) ระหว่างข้อกำหนดของมาตรฐาน ISO/IEC 27001:2022 กับการดำเนินงานในการบริหารความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

(3) นำเสนอแนวทางในการปรับปรุงการดำเนินงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศให้สอดคล้องกับมาตรฐาน ISO/IEC 27001:2022

โดยผู้ศึกษาได้ใช้วิธีการเก็บรวบรวมข้อมูลจากเอกสารสารสนเทศที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศของสำนัก ทั้งเอกสารภายในสำนัก และเอกสารภายนอกสำนัก รวมถึงทำการสอบถามเพิ่มเติมจากบุคลากรของสำนักที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศของสำนัก

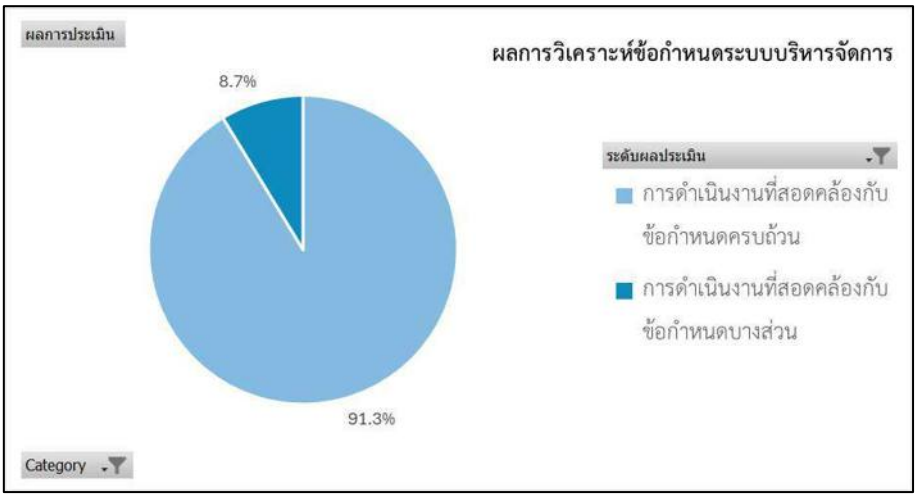
5.1. สรุปผลการวิเคราะห์

ในงานวิเคราะห์นี้ ผู้ศึกษาได้แยกการวิเคราะห์ช่องว่าง (Gap analysis) ความสอดคล้องระหว่างการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศกับข้อกำหนดในมาตรฐาน ISO/IEC 27001:2022 ออกเป็น 5 กลุ่มข้อกำหนด ประกอบด้วย กลุ่มข้อกำหนดระบบบริหารจัดการ กลุ่มข้อกำหนดการควบคุมด้านองค์กร กลุ่มข้อกำหนดการควบคุมด้านบุคคล กลุ่มข้อกำหนดการควบคุมด้านกายภาพ และกลุ่มข้อกำหนดการควบคุมด้านเทคโนโลยี ซึ่งได้ผลสรุปการวิเคราะห์ดังนี้

5.1.1. สรุปผลการวิเคราะห์ข้อกำหนดระบบบริหารจัดการ

ในกลุ่มข้อกำหนดระบบบริหารจัดการ (Management system) เป็นการวิเคราะห์ช่องว่าง (Gap analysis) ความสอดคล้องของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ กับข้อกำหนดระบบบริหารจัดการในมาตรฐาน ISO/IEC 27001:2022 ซึ่งพบว่าสำนักเทคโนโลยีสารสนเทศมีการดำเนินงานตามข้อกำหนดการบริหารจัดการหรือข้อกำหนดหลักของมาตรฐาน ISO/IEC 27001:2022 ครบทุกข้อกำหนด 23 ข้อ โดยมีการดำเนินงานที่สอดคล้องกับข้อกำหนดครบถ้วน

จำนวน 21 ข้อ คิดเป็นร้อยละ 91.3 และมีการดำเนินงานที่สอดคล้องกับข้อกำหนดบางส่วนจำนวน 2 ข้อ คิดเป็นร้อยละ 8.7



ภาพที่ 5-1 ผลการวิเคราะห์ข้อกำหนดระบบบริหารจัดการ

ซึ่งพบว่าการบริหารจัดการของสำนักยังขาดการดำเนินงานที่อาจทำให้สำนักไม่ผ่านการรับรองมาตรฐาน ISO/IEC 27001:2022 ดังนี้

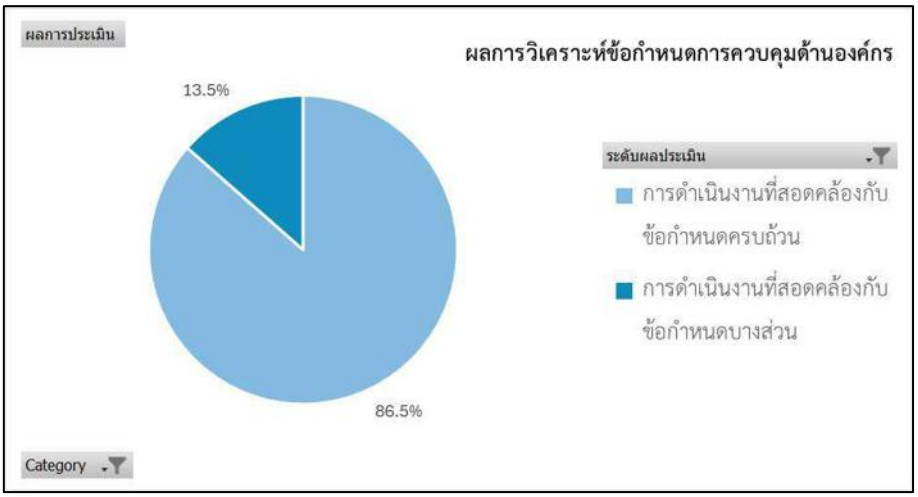
(1) สำนักยังไม่ได้มีการทบทวนและปรับปรุงข้อกำหนดในการดำเนินงานของระบบบริหารความปลอดภัยสารสนเทศที่อยู่ในคู่มือคุณภาพของสำนักเทคโนโลยีดิจิทัลและสารสนเทศให้สอดคล้องกับข้อกำหนด

(2) สำนักยังไม่ได้มีการทบทวนและปรับปรุงเอกสาร Statement of Applicability (SOA) ให้เป็นตามข้อกำหนดการควบคุม Annex A ของมาตรฐาน ISO/IEC 27001:2022 เพื่อแสดงให้เห็นถึงมาตรการในการจัดการเพื่อควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของสำนักในแต่ละด้าน

5.1.2. สรุปผลการวิเคราะห์ข้อกำหนดการควบคุมด้านองค์กร

ในกลุ่มข้อกำหนดการการควบคุมด้านองค์กร เป็นการวิเคราะห์ช่องว่าง (Gap analysis) ความสอดคล้องระหว่างการดำเนินงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ กับข้อกำหนดการควบคุมด้านองค์กร (Organizational control) ใน Annex A ของมาตรฐาน ISO/IEC 27001:2022 ซึ่งพบว่าสำนักเทคโนโลยีสารสนเทศมีการดำเนินงานตามข้อกำหนดครบทุกข้อกำหนด 37 ข้อ โดยมีการดำเนินงานที่

สอดคล้องกับข้อกำหนดครบถ้วนจำนวน 32 ข้อ คิดเป็นร้อยละ 86.5 และมีการดำเนินงานที่สอดคล้องกับข้อกำหนดบางส่วนจำนวน 5 ข้อ คิดเป็นร้อยละ 13.5



ภาพที่ 5-2 ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านองค์กร

ซึ่งการตรวจประเมินพบว่าสำนักยังขาดการดำเนินงานที่อาจทำให้สำนักไม่ผ่านการรับรองมาตรฐาน ISO/IEC 27001:2022 ดังนี้

(1) สำนักยังไม่มีการทบทวนและปรับปรุงนโยบายเฉพาะด้านที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ให้สอดคล้องกับข้อกำหนดของมาตรฐาน

(2) สำนักยังไม่มีขั้นตอนในการรวบรวม วิเคราะห์ และจัดทำรายงานข่าวกรองภัยข้อมูลภัยคุกคามอย่างเป็นระบบ

(3) สำนักยังไม่ได้กำหนดกฎระเบียบหรือแนวปฏิบัติในการใช้ข้อมูลสารสนเทศที่เป็นลายลักษณ์อักษรอย่างชัดเจน

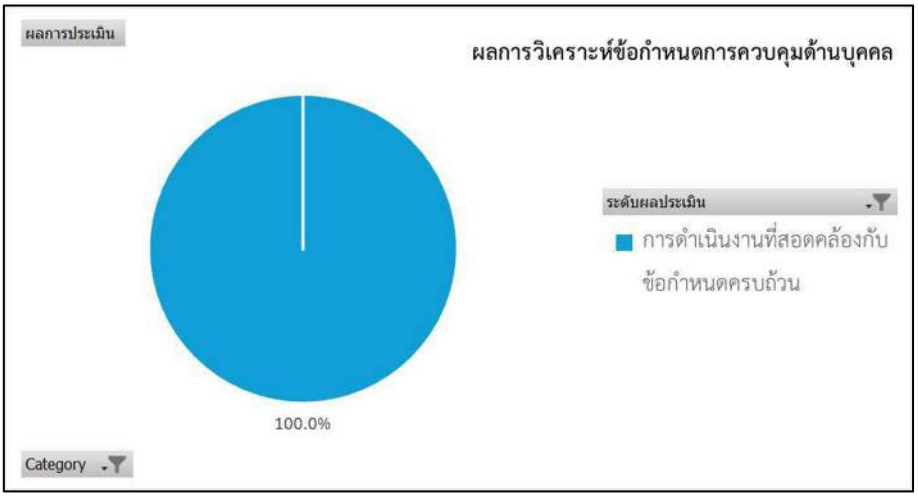
(4) สำนักยังไม่ได้กำหนดกฎระเบียบหรือแนวปฏิบัติในการถ่ายโอนข้อมูลภายในองค์กร

(5) สำนักยังไม่มีกระบวนการหรือแนวทางในการจัดการที่เกี่ยวข้องกับการใช้บริการคลาวด์ อย่างชัดเจน

5.1.3. สรุปผลการวิเคราะห์ข้อกำหนดการควบคุมด้านบุคคล

ในกลุ่มข้อกำหนดการการควบคุมด้านบุคคล เป็นการวิเคราะห์ช่องว่าง (Gap analysis) ความสอดคล้องระหว่างการดำเนินงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ กับข้อกำหนดการควบคุมด้านบุคคล (People control) ใน Annex A ของมาตรฐาน ISO/IEC 27001:2022 ซึ่งพบว่าสำนักเทคโนโลยี

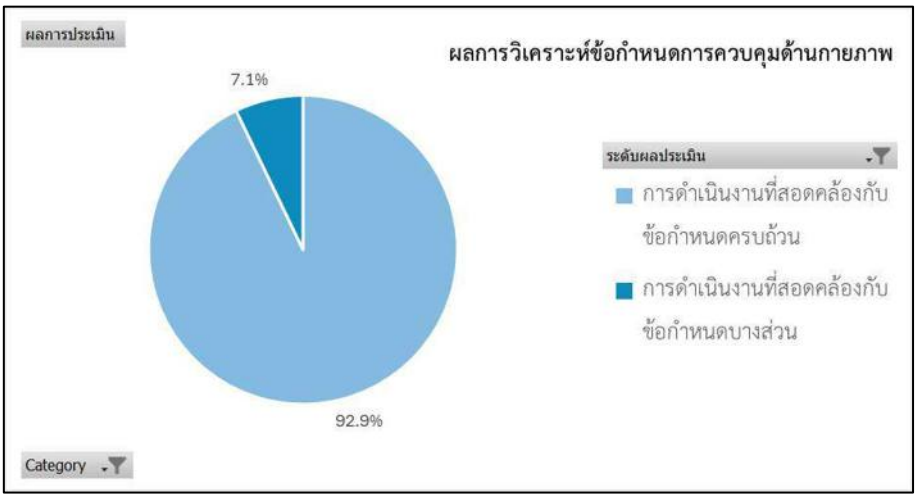
สารสนเทศมีการดำเนินงานตามข้อกำหนดครบทุกข้อกำหนด 8 ข้อ โดยมีการดำเนินงานที่สอดคล้องกับข้อกำหนดครบถ้วนทุกข้อ คิดเป็นร้อยละ 100



ภาพที่ 5-3 ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านบุคคล

5.1.4. สรุปผลการวิเคราะห์ข้อกำหนดการควบคุมด้านกายภาพ

ในกลุ่มข้อกำหนดการการควบคุมด้านองค์กร เป็นการวิเคราะห์ช่องว่าง (Gap analysis) ความสอดคล้องระหว่างการดำเนินงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ กับข้อกำหนดการควบคุมด้านกายภาพ (Physical control) ใน Annex A ของมาตรฐาน ISO/IEC 27001:2022 ซึ่งพบว่าสำนักเทคโนโลยีสารสนเทศมีการดำเนินงานตามข้อกำหนดครบทุกข้อกำหนด 14 ข้อ โดยมีการดำเนินงานที่สอดคล้องกับข้อกำหนดครบถ้วนจำนวน 13 ข้อ คิดเป็นร้อยละ 92.9 และมีการดำเนินงานที่สอดคล้องกับข้อกำหนดบางส่วนจำนวน 1 ข้อ คิดเป็นร้อยละ 7.1

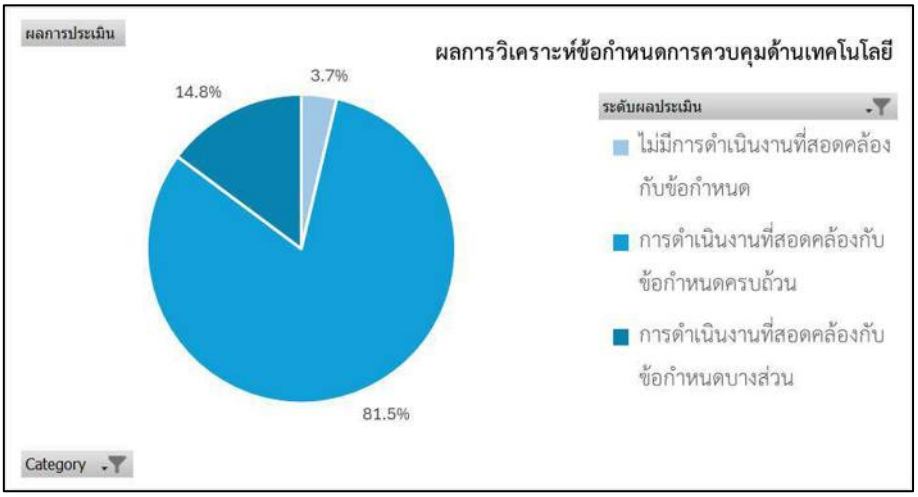


ภาพที่ 5-4 ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านกายภาพ

ซึ่งการตรวจประเมินพบว่าสำนักยังขาดการดำเนินงานที่อาจทำให้สำนักไม่ผ่านการรับรองมาตรฐาน ISO/IEC 27001:2022 คือ สำนักยังไม่มีกระบวนการจัดการในตรวจสอบเฝ้าระวังต่อเนื่องหรือแจ้งเตือนเมื่อเกิดการบุกรุกพื้นที่ทางกายภาพโดยไม่ได้รับอนุญาต

5.1.5. สรุปผลการวิเคราะห์ข้อกำหนดการควบคุมด้านเทคโนโลยี

ในกลุ่มข้อกำหนดการการควบคุมด้านเทคโนโลยี เป็นการวิเคราะห์ช่องว่าง (Gap analysis) ความสอดคล้องระหว่างการดำเนินงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ กับข้อกำหนดการควบคุมด้านเทคโนโลยี (Technological control) ใน Annex A ของมาตรฐาน ISO/IEC 27001:2022 ซึ่งพบว่าสำนักเทคโนโลยีสารสนเทศมีการดำเนินงานตามข้อกำหนดจำนวน 27 ข้อ และขอยกเว้นไม่ขอรับการประเมินจำนวน 7 ข้อ โดยข้อกำหนดที่ขอรับการประเมินจำนวน 27 ข้อ พบว่ามีการดำเนินงานที่สอดคล้องกับข้อกำหนดครบถ้วนจำนวน 22 ข้อ คิดเป็นร้อยละ 81.5 มีการดำเนินงานที่สอดคล้องกับข้อกำหนดบางส่วนจำนวน 4 ข้อ คิดเป็นร้อยละ 14.8 และยังไม่มีการดำเนินงานที่สอดคล้องกับข้อกำหนด จำนวน 1 ข้อ คิดเป็นร้อยละ 3.7



ภาพที่ 5-5 ผลการวิเคราะห์ข้อกำหนดการควบคุมด้านเทคโนโลยี

ซึ่งการตรวจประเมินพบว่าสำนักยังขาดการดำเนินงานที่อาจทำให้สำนักไม่ผ่านการรับรองมาตรฐาน ISO/IEC 27001:2022 ดังนี้

(1) สำนักยังไม่มีการดำเนินการประเมินช่องโหว่และมาตรการดำเนินการเพื่อจัดการกับช่องโหว่ที่ตรวจพบอย่างเป็นระบบ

(2) สำนักยังไม่มีขั้นตอนในการจัดการกับข้อมูลการตั้งค่า (Configuration) เช่นการสร้าง การเปลี่ยนแปลง จัดเก็บเป็นเอกสารสารสนเทศ และมีการทบทวนเป็นประจำ

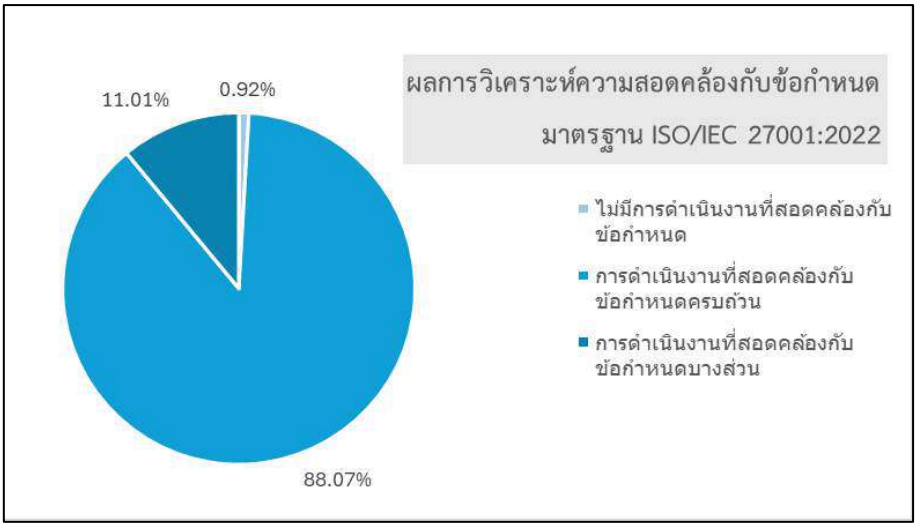
(3) สำนักมีขั้นตอนปฏิบัติในการจัดการลบข้อมูลที่อยู่อุปกรณ์จัดเก็บข้อมูล แต่ยังไม่ครอบคลุมการจัดการข้อมูลที่อยู่ในระบบสารสนเทศ

(4) สำนักยังไม่มีกฎระเบียบหรือแนวปฏิบัติในการจัดการเข้ารหัสข้อมูล (Cryptography) และกุญแจที่ใช้ในการเข้ารหัส

จากผลการประเมินความสอดคล้องของการดำเนินงานที่เป็นไปตามข้อกำหนดมาตรฐาน ISO/IEC 27001:2022 ทั้ง 5 กลุ่มนั้น พบว่าสำนักมีการดำเนินงานที่สอดคล้องกับข้อกำหนดในกลุ่มข้อกำหนดการควบคุมด้านบุคคลอยู่ในระดับสูงสุด คือ มีการดำเนินงานที่สอดคล้องกับข้อกำหนดครบถ้วนทุกข้อกำหนด คิดเป็นร้อยละ และกลุ่มข้อกำหนดการควบคุมด้านเทคโนโลยีสำนักมีการดำเนินที่สอดคล้องกับข้อกำหนดครบถ้วน อยู่ในระดับต่ำสุด คือ ร้อยละ 81.5

ภาพที่ 5-6 ผลการเปรียบเทียบความสอดคล้องกับข้อกำหนดมาตรฐาน IsO/IEC 27001:2022

ทั้งนี้ผลการประเมินในภาพรวมทุกข้อกำหนดที่มีการประเมินจำนวน 109 ข้อ จากจำนวนทั้งหมด 116 ข้อ แล้ว สำนักเทคโนโลยีมีการดำเนินงานที่สอดคล้องกับข้อกำหนดของมาตรฐาน จำนวน 96 ข้อ คิดเป็นร้อยละ 88.07 จากข้อกำหนดที่มีการประเมิน มีการดำเนินงานที่สอดคล้องกับข้อกำหนดบางส่วนจำนวน 12 ข้อ คิดเป็นร้อยละ 11.01 จากข้อกำหนดที่มีการประเมิน และไม่มีการดำเนินงานที่สอดคล้องกับข้อกำหนดจำนวน 1 ข้อ คิดเป็นร้อยละ 0.92 จากข้อกำหนดที่มีการประเมิน



ภาพที่ 5-7 ผลการวิเคราะห์ความสอดคล้องกับข้อกำหนดมาตรฐาน IsO/IEC 27001:2022

5.2. อภิปรายผลการวิเคราะห์

จากผลการศึกษาวิเคราะห์ความพร้อมของสำนักเทคโนโลยีดิจิทัลและสารสนเทศในการขอรับรองมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 นั้น แสดงให้เห็นว่าสำนักมีความพร้อมในการขอรับรองมาตรฐานในระดับสูง ด้วยระดับผลการประเมินที่สำนักมีการดำเนินการที่สอดคล้องกับข้อกำหนดครบถ้วนถึงร้อยละ 88.07 ส่วนหนึ่งเป็นเพราะสำนักมีการดำเนินงานที่เป็นระบบ และได้รับการรับรองมาตรฐานระบบบริหารคุณภาพ ISO 9001:2015 และระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013 อยู่แล้ว ทำให้การดำเนินงานของสำนักโดยส่วนใหญ่จึงสอดคล้องกับข้อกำหนด ซึ่งจากการวิเคราะห์แสดงให้เห็นว่าสภาพปัจจุบันของสำนักมีดังนี้

5.2.1. ด้านบุคลากร (Man)

จากผลการวิเคราะห์ข้อมูลในข้อกำหนดการควบคุมด้านบุคคลที่มีความสอดคล้องอยู่ในระดับร้อยละ 100 แสดงให้เห็นว่าสำนักมีการจัดการทรัพยากรบุคคลาภายในอยู่ระดับดี ส่วนหนึ่งเป็นเพราะสำนักอยู่ภายใต้สถาบันบัณฑิตพัฒนบริหารศาสตร์ซึ่งหน่วยงานภาครัฐ ซึ่งมีการดำเนินงานด้านบุคคลที่สอดคล้องกับกฎหมายและกฎระเบียบซึ่งครอบคลุมเรื่องความมั่นคงปลอดภัยสารสนเทศแล้ว และสำนักก็มีการเปิดโอกาสให้บุคลากรภายในสำนักได้รับการพัฒนา และฝึกอบรมที่เกี่ยวกับความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ แต่จากการวิเคราะห์พบว่าบุคลากรอาจจะขาดความเข้าใจถึงข้อกำหนดระบบบริหารความมั่นคงปลอดภัยสารสนเทศของมาตรฐาน ISO 27001:2022 ทำให้บางข้อกำหนดจึงยังไม่มีการดำเนินงาน หรือมีการดำเนินงานแต่ไม่สอดคล้องกับข้อกำหนด เช่น การที่ไม่ได้ดำเนินการประเมินและมีมาตรการในการจัดการช่องโหว่ ทั้งที่มีการใช้

เครื่องมือในการตรวจสอบช่องโหว่แล้ว ซึ่งส่วนนี้แสดงว่าถึงแม้สำนักจะมีการดำเนินงานด้านบุคคลที่สอดคล้องกับข้อกำหนดแล้ว อย่างเช่น มีการจัดอบรมข้อกำหนด ISO 27001:2022 ให้กับบุคลากรของสำนัก แต่ก็อาจจะไม่เพียงพอที่จะสร้างความเข้าใจและความตระหนักของระบบบริหารความมั่นคงปลอดภัยสารสนเทศภายในสำนัก

5.2.2. ด้านเครื่องมือ (Machine)

จากผลการวิเคราะห์ข้อกำหนดด้านกายภาพซึ่งมีผลการประเมินอยู่ในระดับร้อยละ 92.9 แสดงให้เห็นว่าสำนักมีเครื่องมือที่ช่วยในการควบคุมและจัดการกับพื้นที่ที่มีความจำเป็นในการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างศูนย์ข้อมูล (Data center) ซึ่งมีการควบคุมการเข้าถึงพื้นที่ มีระบบไฟฟ้าสำรองเพื่อรองรับกรณีไฟฟ้าดับกระทันหัน และระบบดับเพลงและระบบตรวจจับเหตุอัคคีภัย ในส่วนข้อกำหนดการควบคุมด้านเทคโนโลยีส่วนใหญ่ก็มีความสอดคล้องซึ่งจากการวิเคราะห์พบว่าสำนักมีอุปกรณ์และระบบเทคโนโลยีสารสนเทศที่รองรับการจัดการด้านความมั่นคงปลอดภัยตามข้อกำหนดในมาตรฐาน ISO/IEC 27001:2013 อยู่แล้วเป็นส่วนใหญ่ เนื่องจากสำนักก็มีการจัดหาเครื่องมือทั้งฮารด์แวร์ และซอฟต์แวร์ที่จำเป็นต่อการปฏิบัติงานและการรักษาความมั่นคงปลอดภัยสารสนเทศ แต่เนื่องจากมาตรฐาน ISO/IEC 27001:2022 มีข้อกำหนดใหม่ซึ่งพบว่าจำเป็นต้องมีการใช้เครื่องมือเทคโนโลยีเพิ่มเติมในการจัดการ เช่น ข้อกำหนดการป้องกันข้อมูลรั่วไหล ที่สำนักยังไม่มีการดำเนินการใดๆที่สอดคล้องกับข้อกำหนด ซึ่งอาจจำเป็นต้องจัดหาทรัพยากรหรือเครื่องมือมาช่วยในการจัดการ

5.2.3. ด้านทรัพยากร (Material)

สำนักมีการกำหนดแนวปฏิบัติในการจัดการทรัพยากร (Capacity management) เพื่อแนวทางในการตรวจสอบการใช้งานทรัพยากรของระบบโครงสร้างพื้นฐานที่สนับสนุนการให้บริการ Colocation และ VPS ซึ่งจะช่วยให้สำนักได้ประเมินความพอเพียงของทรัพยากรที่จะรองรับการให้บริการ และช่วยเป็นข้อมูลสนับสนุนในการจัดหาเพิ่มเติมในอนาคต แต่ก็พบว่าสำนักมีการยอมรับความเสี่ยงในข้อกำหนดการแยกสภาพแวดล้มการพัฒนา การทดสอบ และการใช้งาน ซึ่งแสดงให้เห็นว่าสำนักมีข้อจำกัดในการจัดสรรทรัพยากรระบบโครงสร้างพื้นฐานที่ไม่เพียงพอที่จะรองรับการแยกสภาพแวดล้อมออกจากกัน ส่วนทรัพยากรที่อยู่ในรูปแบบข้อมูลสารสนเทศที่ช่วยสนับสนุนการดำเนินงาน พบว่าสำนักมีการจัดการอย่างเป็นระบบ ไม่ว่าจะเป็นการจัดทำและควบคุมเอกสารที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เช่น นโยบาย แนวปฏิบัติ ขั้นตอนการปฏิบัติงาน ไว้พร้อมรองรับที่บุคลากรของสำนักสามารถนำไปใช้ได้ตลอดเวลา แต่ก็พบว่าข้อมูลสารสนเทศบางอย่างเช่น กฎหมาย และระเบียบข้อบังคับ มีการทบทวนและปรับปรุงปีละ 1 ครั้ง

ซึ่งอาจจะทำให้ข้อมูลไม่ทันสมัยและเป็นปัจจุบัน และสำนักอาจจะไม่ได้มีการดำเนินการเพื่อรองรับการเปลี่ยนแปลงได้ทันกาล

5.2.4. ด้านกระบวนการ (Method)

สำนักมีกำหนดขั้นตอนการปฏิบัติงานเพื่อเป็นแนวทางในการดำเนินงานด้านต่างๆ มีกระบวนการทำงานเป็นระบบ ซึ่งสอดคล้องกับข้อกำหนดระบบบริหารจัดการของมาตรฐาน ISO/IEC 27001:2022 ซึ่งมีการกำหนดกระบวนการตั้งแต่การวางแผน การปฏิบัติงาน การประเมินผล และการปรับปรุงอย่างต่อเนื่องตามหลักการ PDCA ซึ่งเป็นสิ่งที่น่าจะทำให้สำนักมีความพร้อมในการขอรับรองมาตรฐาน แต่เมื่อวิเคราะห์ในข้อกำหนดการควบคุมที่สำนักดำเนินการสอดคล้องกับข้อกำหนดบางส่วนนั้น อย่างข้อกำหนดการควบคุมด้านเทคโนโลยีที่มีระดับประเมินต่ำสุด เช่น สำนักไม่ได้มีขั้นตอนการจัดการกับข้อมูลการตั้งค่า (Configuration) ถึงแม้จะเป็นข้อกำหนดเกี่ยวกับเทคโนโลยีก็พบว่าสิ่งที่ทำให้การดำเนินงานไม่สอดคล้องนั้น ส่วนใหญ่เป็นเพราะการขาดกระบวนการหรือวิธีการดำเนินงานที่เป็นระบบ ไม่มีการกำหนดแนวทางการจัดการที่ชัดเจน ซึ่งสำนักอาจจะต้องมีการศึกษาข้อกำหนดอย่างละเอียดเพื่อนำมาพัฒนาหรือปรับปรุงกระบวนการที่มีอยู่ให้สอดคล้องกับข้อกำหนดของมาตรฐาน

5.3. ข้อเสนอแนะ

จากการวิเคราะห์ความพร้อมของสำนักเทคโนโลยีดิจิทัลและสารสนเทศในการขอรับรองมาตรฐาน ISO/IEC 27001:2022 นั้นมีข้อเสนอแนะดังนี้

5.3.1. ข้อเสนอแนะเชิงนโยบาย

(1) มีการกำหนดคณะทำงานและมอบหมายให้มีการการทบทวนนโยบายและแนวปฏิบัติให้มีความสอดคล้องกับข้อกำหนดและกฎหมาย โดยอาจจะศึกษาจากแนวทางจากหน่วยงานกำกับด้านความมั่นคงปลอดภัยสารสนเทศอย่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ หรืออาจจะศึกษาจากกรอบแนวทางการักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล เพื่อมาใช้ประกอบการพิจารณาในการจัดทำ

(2) มีการวิเคราะห์และจัดสรรอัตรากำลังของบุคลากรเพิ่มเติมเพื่อรองรับการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศที่มีความสำคัญเพิ่มขึ้น อันเนื่องจากมีรูปแบบภัยคุกคามต่างๆที่มากขึ้นซึ่งอาจจะทำให้ทรัพยากรบุคคลของสำนักไม่เพียงพอที่จะรับมือหรือดำเนินการป้องกันได้

(3) มีการวางแผนการจัดสรรและจัดหาทรัพยากรและเครื่องมือเทคโนโลยีสารสนเทศเพื่อรองรับข้อกำหนดและภัยคุกคามต่างๆที่เพิ่มขึ้น โดยวิเคราะห์ทรัพยากรที่มีอยู่และวางแผนการระยะสั้น ระยะยาวต่อไป

5.3.2. ข้อเสนอแนะเชิงปฏิบัติงาน

(1) นอกเหนือจากที่สำนักเทคโนโลยีดิจิทัลและสารสนเทศจัดอบรมข้อกำหนด ISO ให้กับบุคลากรในสำนักแล้ว ผู้ปฏิบัติงานควรมีศึกษาข้อกำหนดของมาตรฐาน ISO/IEC 27001:2022 และแนวทางการควบคุมจากมาตรฐาน ISO/IEC 27002:2022 ด้วยตนเองเพิ่มเติม เพื่อสร้างความเข้าใจในข้อกำหนด และตระหนักถึงระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

(2) ควรมีการทบทวนและปรับปรุงหรือพัฒนากระบวนการเพื่อให้รองรับในการดำเนินงานให้สอดคล้องกับข้อกำหนดในมาตรฐานที่เปลี่ยนไป โดยมอบหมายให้ส่วนงานที่เกี่ยวข้องรับผิดชอบในการทบทวน

(3) นอกเหนือจากแผนปฏิบัติงานประจำปีของสำนักแล้ว การปฏิบัติงานภายในส่วนงานควรมีการมอบหมายถ่ายทอดงานให้สอดคล้องกับแผนปฏิบัติงานของสำนัก และมีการติดตามเป็นระยะเพื่อตรวจสอบการปฏิบัติการให้เป็นไปตามข้อกำหนดการดำเนินงาน

5.3.3. ข้อเสนอแนะสำหรับการวิเคราะห์ในอนาคต

(1) ควรขยายขอบเขตการวิเคราะห์ความพร้อมขององค์กรเพิ่มเติม เช่น วิเคราะห์กระบวนการจัดการความเสี่ยงตามมาตรฐาน ISO/IEC 27005

(2) ควรศึกษาวิเคราะห์ผลสัมฤทธิ์ของการนำมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 มาใช้กับองค์กร โดยเปรียบเทียบผลการดำเนินงานที่เปลี่ยนแปลง

(3) ควรศึกษาเปรียบเทียบระบบบริหารความมั่นคงปลอดภัยสารสนเทศของสำนัก กับหน่วยงานภายนอกที่ได้รับการรับรองมาตรฐาน ISO/IEC 27001

บรรณานุกรม

Achmadi, D., Suryanto, Y., & Ramli, K. (2018). On Devloping Information Security Management System (ISMS) Framework for ISO 27001-based Data Center. *International Workshop on Big Data and Information Security (IWBIS)*, 149-157.

AIS. (n.d.). *Data Center มาตรฐานระดับโลก เพิ่มความปลอดภัยให้บริษัท Startup Thailand*. Retrieved 2025, from AIS: https://www.ais.th/thestartup/solution-data-center.html

Almurayh, A. (2010). *VPS Virtual Private Server.* Retrieved from https://www.ssra2022.org/-cs526/studentproj/projS2010/aalmuray/doc/Almurayh_VPS.pdf

BALEN, J., VAJAK, D., & SALAH, K. (2020). Comparative Performance Evaluation of Popular Virtual Private Servers. *Journal of Internet Technology, 21*(2). Retrieved from https://jit.ndhu.edu.tw/article/view/2256/2269

Einstein, B. (2024, December 10). *How Gap Analysis Can Drive Strategic Change in Your Organization*. Retrieved from Harvard Business School Online: https://online.hbs.edu/blog/post/gap-analysis

Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021, June). A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. *IAENG International Journal of Computer Science, 48*(2).

Hanna, K. T., & Sales, F. (2021, October). *What is gap analysis and how does it work?* Retrieved 2025, from TechTarget: https://www.techtarget.com/searchcio/definition/gap-analysis

ISO/IEC. (2022). *มาตรฐาน ISO/IEC 27001:2022.* (ดร.บรรจง หะรังษี, Trans.) Retrieved from https://www.tnetsecurity.com/download/%E0%B8%A1%E0%B8%B2%E0%B8%95%E0%B8%A3%E0%B8%90%E0%B8%B2%E0%B8%99-iso-iec-270012022-%E0%B8%89%E0%B8%9A%E0%B8%B1%E0%B8%9A%E0%B8%A0%E0%B8%B2%E0%B8%A9%E0%B8%B2%E0%B9%84%E0%B8%97%E0%B8%A2/

Mataracioglu, T. (2017, July 16). *Proposal for the Next Version of the ISO/IEC 27001 Standard*. Retrieved from ISACA: https://www.isaca.org/resources/isaca-

journal/issues/2017/volume-4/proposal-for-the-next-version-of-the-isoiec-27001-standard

Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021, October). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers & Security, 109*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404821002078

Panawas, N. (2024). การตรวจประเมินความสอดคล้องมาตรการรักษาความมั่นคง ปลอดภัยสารสนเทศ เทียบกับมาตรฐาน ISO/IEC 27001:2022 และการตรวจสอบช่องโหว่ทางเทคนิคของระบบปฏิบัติการบริษัท A. *วารสารนวัตกรรมวิทยาศาสตร์เพื่อการพัฒนาอย่างยั่งยืน, 5*(1), 1-11. Retrieved from https://ph01.tci-thaijo.org/index.php/JSISD/article/view/255575

PCMag. (n.d.). *Definition of colocation*. Retrieved from PCMag: https://www.pcmag.com/encyclopedia/term/colocation

Seymour Goodman, Detmar W. Straub, และ Richard Baskerville. (2008). *Information Security : Policy, Processes, and Practices. Routledge.*

Stanik, J., & Kiedrowicz, M. (2022). STATEMENT OF APPLICABILITY AS A KEY ELEMENT OF THE GIS CERTIFICATION PROCESS IN THE LIGHT OF CYBERSECURITY STANDARDS. *GIS Odyssey Journal, 2*(2), 79-92. https://doi.org/https://doi.org/10.57599/gisoj.2022.2.2.79

The Department of Employment and Workplace Relations, Australian Government. (2022, May). *Gap analysis versus risk assessment.* Retrieved from The Department of Employment and Workplace Relations, Australian Government: https://www.dewr.gov.au/download/13644/gap-analysis-versus-risk-assessment/27360/document/pdf

The National Institute of Standards and Technology. (2020, December). *Data Integrity*. Retrieved from The National Institute of Standards and Technology: https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html

True IDC. (2018). *True IDC ผ่านการรับรองจาก Uptime Institute ถึง 2 ด้าน แห่งเดียวในประเทศไทย*. Retrieved 2025, from https://www.trueidc.com/en/news-detail/52/TrueIDC-%E0%B8%9C%E0%B9%88%E0%B8%B2%E0%B8%99%E0%B8%81%

E0%B8%B2%E0%B8%A3%E0%B8%A3%E0%B8%B1%E0%B8%9A%E0%B8%A3%E0%B8%AD%E0%B8%87%E0%B8%88%E0%B8%B2%E0%B8%81-Uptime-Institute-%E0%B8%96%E0%B8%B6%E0%B8%87-2-%E0%B8%94%E0%

Valdevit, T., & Mayer, N. (2010). A Gap Analysis Tool for SMEs Targeting ISO/IEC 27001 Compliance. *International Conference on Enterprise Information Systems*.

แววตา เตชาทวีวรรณ. (2020). สภาพและปัญหาการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของห้องสมุดสถาบันอุดมศึกษาของรัฐ. *วารสารวิจัย สมาคมห้องสมุดแห่งประเทศไทย, 13*(2), 96-112.

กิตติพงษ์ เกียรตินิยมรุ่. (ม.ป.ป.). *ความเป็นมา ISO/IEC 27001*. เข้าถึงได้จาก สถาบันมาตรฐานอังกฤษ: https://www.bsigroup.com/th-TH/ISOIEC-27001-Information-Security/article-27001/Established-27001/

ชุลีกร นวลสมศรี, และ ดร.สุทธิศักดิ์ จันทวงษ์โส. (2017). การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO 27001:2013 กรณีศึกษาขององค์กรด้านการบินแห่งหนึ่ง. *วารสารวิจัย มข. (ฉบับบัณฑิตศึกษา), 17*(4).

ดร.นิพนธ์ นาชิน. (พฤษภาคม 2567). *Gap Analysis vs. Internal Audit: เข้าใจความแตกต่าง เพื่อพัฒนากระบวนการองค์กร*. เข้าถึงได้จาก ALPHASEC: https://www.alphasec.co.th/post/gap-analysis-vs-internal-audit-%E0%B9%80%E0%B8%82%E0%B9%89%E0%B8%B2%E0%B9%83%E0%B8%88%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B9%81%E0%B8%95%E0%B8%81%E0%B8%95%E0%B9%88%E0%B8%B2%E0%B8%87-%E0%B9%80%E0%B8%9E%E0%B8%B7%E0%B9%88%E

มหาวิทยาลัยมหิดล. (2025). *มหาวิทยาลัยมหิดล ได้รับรองมาตรฐาน ISO/IEC 27001:2022 ด้านระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ*. Retrieved 2025, from https://mahidol.ac.th/th/2025/iso-iec-270012022/

สมศิริ พันธุ์ศักดิ์ศิริ, และ เสาวนีย์ สมันต์ตรีพร. (2023). ประสิทธิผลของการจัดการความปลอดภัยระบบสารสนเทศโรงพยาบาลสระบุรี. *วารสารสหวิทยาการมนุษยศาสตร์และสังคมศาสตร์, 6*(2), 1046–1066. เข้าถึงได้จาก https://so04.tci-thaijo.org/index.php/jmhs1_s/article/view/264039

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.). (2568). *สถิติภัยคุกคามทางไซเบอร์ แยกตามภารกิจหรือบริการของหน่วยงานที่ถูกโจมตี ปี พ.ศ. 2567*. เข้าถึงได้จาก ระบบบัญชี

ข้อมูล GD Catalog: https://ncsa.gdcatalog.go.th/dataset/ncsa_04_01/resource/e48826cd-a83d-4a8e-ae97-071d7f5c69df

สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา. (ม.ป.ป.). *การให้บริการ DATA CENTER & DISASTER RECOVERY CENTER*. เรียกใช้เมื่อ 2568 จาก สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา: https://www.uni.net.th/index.php/data-center/

ภาคผนวก

(1) **คำแถลงนโยบายคุณภาพ สำนักเทคโนโลยีดิจิทัลและสารสนเทศ**

(2) **ข้อกำหนดและเงื่อนไขการให้บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Private Server)**

ข้อกำหนดและเงื่อนไขการให้บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Private Server)
สำนักเทคโนโลยีดิจิทัลและสารสนเทศ สถาบันบัณฑิตพัฒนบริหารศาสตร์

การให้บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Private Server) คือ บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน เพื่อติดตั้งใช้งานกับระบบสารสนเทศของหน่วยงานต่าง ๆ ภายในสถาบัน โดยการบริหารจัดการและข้อมูลภายในเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Private Server) จะเป็นสิทธิ์ของหน่วยงาน

ผู้ให้บริการ หมายถึง สำนักเทคโนโลยีดิจิทัลและสารสนเทศ
ผู้ขอรับบริการ หมายถึง หน่วยงานต่าง ๆ ภายในสถาบัน

1. ขอบเขตการให้บริการ

1.1. ผู้ให้บริการจะจัดเตรียมเครื่องคอมพิวเตอร์แม่ข่ายเสมือน สำหรับให้บริการตามรูปแบบที่ผู้ขอรับบริการร้องขอ โดยผู้ให้บริการจะทำการจัดสรรทรัพยากรให้ผู้ขอรับบริการ ตามความเหมาะสม หากผู้ขอรับบริการต้องการให้จัดสรรทรัพยากรเพิ่ม ผู้ให้บริการจะพิจารณาเปลี่ยนแปลงการให้บริการหรือจัดสรรทรัพยากรตามความเหมาะสม

1.2. ผู้ให้บริการจะดำเนินการสร้างเครื่องคอมพิวเตอร์แม่ข่ายเสมือนที่มีระบบปฏิบัติการ ภายในระยะเวลา 3 วันทำการ หลังจากได้รับแบบฟอร์มขอใช้บริการ ผ่านระบบสารบรรณอิเล็กทรอนิกส์ โดยผู้ขอรับบริการจะเป็นผู้ตั้งค่าอื่น ๆ ของระบบปฏิบัติการ กรณีที่ผู้ขอรับบริการ มีความจำเป็นต้องใช้ซอฟต์แวร์อื่นนอกเหนือจากที่ผู้ให้บริการจัดเตรียมให้ ผู้ขอรับบริการต้องเป็นผู้จัดหาและดำเนินการติดตั้ง รวมถึงรับผิดชอบค่าลิขสิทธิ์ที่เกิดขึ้น

1.3. ผู้ให้บริการจะส่งมอบชื่อบัญชีและรหัสผ่านของเครื่องแม่ข่ายเสมือนสำหรับผู้ดูแลระบบเครื่องแม่ข่ายเสมือน โดยส่งผ่านทางจดหมายอิเล็กทรอนิกส์ที่กรอกไว้ในแบบฟอร์มขอรับบริการ ทั้งนี้ เมื่อผู้ขอรับบริการได้รับชื่อบัญชีและรหัสผ่านแล้ว จะต้องทำการเปลี่ยนรหัสผ่านใหม่ทันทีเพื่อความปลอดภัย หากเครื่องแม่ข่ายคอมพิวเตอร์เสมือนนั้นถูกโจมตีอันเนื่องมาจากรหัสผ่านเริ่มต้น ผู้ให้บริการจะไม่รับผิดชอบต่อความเสียหายดังกล่าว

1.4. ผู้ให้บริการจะทำการสำรองข้อมูล (Backup) ของผู้ขอรับบริการ และทำการบันทึกข้อมูลของระบบเครื่องแม่ข่ายเสมือนทั้งหมดทุกวัน โดยทำการเก็บสำรองข้อมูลไว้เป็นรายวัน จำนวน 7 วัน

2. ระยะเวลาในการกู้คืนข้อมูล

2.1. ระยะเวลาที่ยอมรับให้ข้อมูลสูญเสียเมื่อเกิดเหตุ (RPO) : 24 ชั่วโมง

- คำอธิบายการคำนวณ RPO : 24 ชั่วโมง หากทำการสำรองข้อมูล วันที่ 1 เวลา 20.00 น. แล้วเกิดระบบเสียหาย วันที่ 2 เวลา 17.00 น. สามารถกู้คืนข้อมูลที่เป็นของวันที่ 1 เวลา 20.00 น. ซึ่งหมายถึงข้อมูลจะสูญหายไปเป็นระยะเวลา 21 ชั่วโมง
- ระยะเวลาที่ยอมรับให้ระบบหยุดทำงานเมื่อเกิดเหตุเพื่อให้ระบบทำการกู้คืน (RTO) : 1 ชั่วโมง

3. ระยะเวลาการให้บริการ

ดำเนินการตามคำร้องขอและแก้ไขเหตุการณ์ผิดปกติ เฉพาะวันทำการ เวลา 8.30 น. – 16.30 น.

4. ระยะเวลาในการให้บริการได้อย่างต่อเนื่องของการให้บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Private Server) ไม่น้อยกว่าร้อยละ 97

IDT-SDIS-001
(14/03/2025)

5. หน้าที่ของผู้ขอรับบริการ

5.1. ผู้ขอรับบริการ จะต้องเข้าสู่ระบบจากชื่อบัญชีที่ผู้ให้บริการที่ออกให้ เพื่อใช้งานเครื่องคอมพิวเตอร์แม่ข่ายเสมือน และทำการติดตั้งโปรแกรมอื่น ๆ ที่ต้องการใช้งาน พร้อมทำการเก็บรหัสชื่อบัญชีอื่น ๆ ที่ต้องการด้วยตนเอง

5.2 ผู้ขอรับบริการมีหน้าที่การสำรองข้อมูล (Backup) และเพื่อความปลอดภัยมากขึ้น ผู้ขอรับบริการควรทำการสำรองข้อมูลเป็นประจำเก็บไว้ภายนอกอีกชุดหนึ่ง

5.3. ผู้ขอรับบริการต้องรับผิดชอบในการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายเสมือนของตน และยอมรับว่า ผู้ให้บริการไม่ต้องรับผิดชอบต่อผู้ขอรับบริการในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายเสมือนของผู้ขอรับบริการไม่ว่าจะเป็นกรณีใด ๆ ในกรณีที่เกิดปัญหากับเครื่องคอมพิวเตอร์แม่ข่ายเสมือนของผู้ขอรับบริการไม่ว่าจะเกิดจากอุบัติเหตุทางด้านฮาร์ดแวร์ ซอฟต์แวร์ การติดไวรัส หรือการถูกแฮกเข้าระบบ เนื่องจากเหตุการณ์ที่อยู่นอกเหนือความควบคุมของผู้ให้บริการ

5.4. ผู้ขอรับบริการ จะต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมถึงกฎหมายอื่น ๆ ที่เกี่ยวข้องทั้งการใช้บริการอย่างเคร่งครัด และต้องปฏิบัติตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของสถาบันพัฒนาบริหารศาสตร์ พ.ศ. 2564 ข้อกำหนดและเงื่อนไขการให้บริการนี้ และไม่กระทำการใด ๆ ที่อาจก่อให้เกิดความเสียหายแก่ผู้ให้บริการ โดยผู้ให้บริการจะไม่รับผิดชอบต่อความสูญหายหรือความเสียหายของข้อมูลของผู้ขอรับบริการ ในกรณีที่ผู้ขอรับบริการ ไม่ปฏิบัติตาม เงื่อนไขที่กำหนดไว้ข้างต้น

5.5 หากผู้ขอรับบริการ พบว่าเกิดความผิดปกติใด ๆ เกิดขึ้นกับเครื่องที่ใช้บริการ ผู้ขอรับบริการ จะต้องแจ้งผู้ให้บริการทราบโดยทันที เพื่อป้องกันหรือบรรเทาความเสียหายที่อาจเกิดขึ้นแก่ทรัพย์สินของผู้ขอรับบริการหรือผู้ให้บริการ

5.6 ผู้ขอรับบริการจะต้องดูแลเครื่องคอมพิวเตอร์แม่ข่ายเสมือน ไม่ให้เป็นแหล่งแพร่ข้อมูลที่ผิดกฎหมาย หรือโจมตีระบบของเครื่องคอมพิวเตอร์แม่ข่ายอื่น หรือบุคคลอื่น เช่น mail bomb, hack, crack, DoS, spamming, port scanning และวิธีอื่นๆ ที่มีลักษณะเหมือนหรือจุดประสงค์คล้ายกัน หากมีการนำไปใช้บริการในทางลักษณะดังกล่าว จะถูกปิดกั้นการให้บริการทันที โดยผู้ขอรับบริการไม่สามารถเรียกร้องค่าเสียหายใด ๆ

5.7 ในกรณีที่สิ้นสุดการใช้บริการ ผู้ขอรับบริการ จะต้องเป็นผู้ขอคำอนุญาตปิดกั้นข้อมูลเพื่อขอเก็บข้อมูลจากบริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Private Server) และเป็นผู้รับผิดชอบในการถ่ายโอนข้อมูลลงในอุปกรณ์ที่จัดหา

5.8 ผู้ขอรับบริการ ต้องอ่านและทำความเข้าใจข้อกำหนดและเงื่อนไขการให้บริการนี้เป็นอย่างดี จึงลงนามในแบบฟอร์มขอใช้บริการ

6. เงื่อนไขและข้อจำกัดในการให้บริการ

6.1 ผู้ให้บริการจะเก็บรักษาข้อมูลของผู้ขอรับบริการเป็นอย่างดี ตามข้อกำหนดและเงื่อนไขการให้บริการ และจะไม่ทำการเปิดเผยต่อบุคคลใด เว้นแต่ข้อมูลดังกล่าวเป็นข้อมูลที่กำหนดให้ต้องเปิดเผยโดยกฎหมายหรือโดยคำสั่งศาล

6.2. ผู้ให้บริการจะไม่รับผิดชอบต่อความสูญหายหรือความเสียหายของข้อมูลหรือแฟ้มข้อมูลของผู้ขอรับบริการ เว้นแต่มีเหตุความเสียหายอันเนื่องมาจากผู้ขอรับบริการ หรือความเสียหายที่เกิดจากเหตุการณ์ไม่คาดคิด

6.3 หลังจากที่ผู้ให้บริการได้แจ้งชื่อบัญชีและรหัสผ่านของเครื่องแม่ข่ายคอมพิวเตอร์เสมือนแล้ว สิทธิ์การเข้าถึงบริหารจัดการ และใช้งานเป็นของผู้ขอรับบริการทั้งหมด

6.4 การให้บริการจะไม่ครอบคลุมปัญหาที่เกิดขึ้นจากการใช้หรือติดตั้งซอฟต์แวร์ที่ผู้ขอรับบริการทำการติดตั้งเอง

6.5. ผู้ให้บริการขอสงวนสิทธิ์ในการตรวจสอบค้นหาข้อเท็จจริงของระบบที่ใช้งาน ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันบัณฑิตพัฒนบริหารศาสตร์ พ.ศ. 2564

6.6. ผู้ให้บริการขอสงวนสิทธิ์ระงับการให้บริการ รวมถึงการเชื่อมต่อระหว่างเครือข่ายคอมพิวเตอร์ของผู้ให้บริการในทันที หากตรวจพบจุดเกิดเหตุดังต่อไปนี้

6.6.1. เครื่องคอมพิวเตอร์แม่ข่ายเสมือนของผู้ขอรับบริการก่อให้เกิดผลกระทบต่อการทำงานการใช้งานของอุปกรณ์คอมพิวเตอร์ ระบบเครือข่ายของผู้ให้บริการหรือมีปัญหาทางด้านความมั่นคงปลอดภัย

6.6.2. ผู้ขอรับบริการกระทำการฝ่าฝืนกฎหมายที่เกี่ยวข้องกับการให้บริการหรือละเมิดต่อข้อกำหนดและเงื่อนไขการให้บริการ

6.6.3. มีเหตุจำเป็นซึ่งผู้ให้บริการไม่สามารถจัดการหรือควบคุมให้เกิดขึ้น

6.6.4. มีเหตุจำเป็นต้องทำนุบำรุงรักษาหรือแก้ไขระบบสารสนเทศที่ใช้ในการให้บริการ

6.7. ผู้ให้บริการขอสงวนสิทธิ์ในการพิจารณาความเหมาะสมในการจัดสรรทรัพยากร เพื่อให้การใช้งานทรัพยากรมีประสิทธิภาพ

6.8 หากมีการเปลี่ยนแปลงผู้ประสานงาน ผู้ขอรับบริการต้องแจ้งให้ผู้ให้บริการทราบเป็นลายลักษณ์อักษรโดยทันที ทั้งนี้ ผู้ให้บริการจะไม่รับผิดชอบความเสียหายที่อาจเกิดขึ้นจากการไม่แจ้งเปลี่ยนผู้ประสานงานให้ผู้ให้บริการทราบ

6.9. การที่ผู้ขอรับบริการยินยอมให้ข้อมูลซึ่งอาจเข้าถึงข้อมูลส่วนบุคคล ข้อมูลองค์กร และข้อมูลใด ๆ ของผู้ขอรับบริการแก่ผู้ให้บริการ เพื่อประโยชน์ในการตรวจสอบปัญหา ให้คำปรึกษา หรือแก้ไขปัญหาสำหรับการใช้งานต่าง ๆ จะถือว่าผู้ให้บริการได้รับข้อมูลที่จะเข้าถึงข้อมูลต่าง ๆ ภายใต้การอนุญาตเพื่อขอรับบริการตรวจสอบปัญหา ให้คำปรึกษา หรือแก้ไขปัญหาโดยผู้ขอรับบริการ จึงไม่ถือเป็นการที่ผู้ให้บริการเข้าถึงข้อมูลของผู้รับบริการอันเป็นความผิดต่อกฎหมาย และไม่ถือเป็นการละเมิดสิทธิ์ใด ๆ ของผู้ขอรับบริการ ภายหลังจากที่ผู้ขอรับบริการได้รับบริการจากผู้ให้บริการ ในการดำเนินการต่าง ๆ ดังกล่าวเสร็จเรียบร้อยแล้ว เพื่อเป็นการรักษาความปลอดภัยในข้อมูลของผู้ขอรับบริการ ผู้ขอรับบริการหรือเจ้าหน้าที่ของหน่วยงาน ผู้ใช้บริการมีหน้าที่ต้องรับผิดชอบในการดำเนินการเปลี่ยนแปลงรหัสข้อมูลดังกล่าว ใหม่โดยทันที โดยผู้ให้บริการขอสงวนสิทธิ์ไม่รับผิดชอบในความสูญหายหรือเสียหายใด ๆ จากการดำเนินการ หรือความเสียหายใด ๆ ที่เกิดขึ้นกับข้อมูล โปรแกรม สิทธิ์ในทรัพย์สินทางปัญญา สิทธิ์อื่นใดและประโยชน์ทางธุรกิจ หรือการหยุดชะงักทางธุรกิจของผู้ขอรับบริการ ในทุกกรณี

7. ผู้ให้บริการขอสงวนสิทธิ์ในการแก้ไขเปลี่ยนแปลง แก้ไขเพิ่มเติมหรือตัดออก ซึ่งส่วนใดส่วนหนึ่งของข้อกำหนดและเงื่อนไขการให้บริการนี้ได้ตลอดเวลา และถือว่าผู้ขอรับบริการได้ตกลงรับข้อกำหนดและเงื่อนไขการให้บริการใหม่โดยปริยาย ตลอดระยะเวลาที่ผู้ขอรับบริการยังคงใช้บริการและรับบริการของผู้ให้บริการ

8. การรายงานผลการให้บริการ

ผู้ให้บริการจะจัดส่งรายงานผลการให้บริการตามขอบเขตการให้บริการแก่ผู้ขอรับบริการเมื่อได้รับคำร้องขอจากผู้ขอรับบริการ

(3) **ข้อกำหนดและเงื่อนไขการให้บริการรับฝากเครื่องคอมพิวเตอร์แม่ข่าย (Colocation)**

ข้อกำหนดและเงื่อนไขการให้บริการรับฝากเครื่องคอมพิวเตอร์แม่ข่าย (Colocation)
สำนักเทคโนโลยีดิจิทัลและสารสนเทศ สถาบันบัณฑิตพัฒนบริหารศาสตร์

การให้บริการรับฝากเครื่องคอมพิวเตอร์แม่ข่าย (Colocation) คือ บริการรับฝากเครื่องคอมพิวเตอร์แม่ข่ายของผู้ใช้บริการ เพื่อใช้บริการระบบเครือข่ายอินเทอร์เน็ตหรือบริการอื่นๆ ภายในศูนย์ข้อมูลหลัก (Data Center) โดยผู้ใช้บริการเป็นผู้จัดหาเครื่องคอมพิวเตอร์แม่ข่ายสำหรับใช้บริการด้วยตนเอง

ผู้ให้บริการ หมายถึง สำนักเทคโนโลยีดิจิทัลและสารสนเทศ
ผู้ขอรับบริการ หมายถึง หน่วยงานต่าง ๆ ภายในสถาบัน

1. **ขอบเขตการให้บริการ**
   ผู้ให้บริการจะจัดเตรียม พื้นที่สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายอินเทอร์เน็ตหรือบริการอื่น ๆ ภายในศูนย์ข้อมูลหลัก (Data Center) สำหรับให้บริการตามรูปแบบที่ผู้ขอรับบริการร้องขอ โดยผู้ให้บริการจะทำการจัดสรรทรัพยากรให้ผู้ขอรับบริการ ตามความเหมาะสม
2. **ระยะเวลาการให้บริการ**
   ดำเนินการตามคำร้องขอและแก้ไขเหตุการณ์ผิดปกติ เฉพาะวันทำการ เวลา 8.30 น. – 16.30 น.
3. **ระยะเวลาในการให้บริการได้อย่างต่อเนื่องของให้บริการรับฝากเครื่องคอมพิวเตอร์แม่ข่าย (Colocation)**
   ไม่น้อยกว่าร้อยละ 97
4. **หน้าที่ของผู้ขอรับบริการ**
   4.1. ผู้ขอรับบริการควรทำการสำรองข้อมูล (Backup) อย่างสม่ำเสมอและเพื่อความปลอดภัยมากขึ้น ผู้ขอรับบริการควรทำการสำรองข้อมูลเป็นประจำเก็บไว้ภายนอกอีกชุดหนึ่ง
   4.2. ผู้ขอรับบริการต้องรับผิดชอบในการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายของตน และตกลงยอมรับว่าผู้ให้บริการไม่ต้องรับผิดชอบต่อผู้ขอรับบริการในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย ไม่ว่าจะเป็นกรณีใด ๆ ในกรณีที่เกิดปัญหากับเครื่องคอมพิวเตอร์แม่ข่ายของผู้ขอรับบริการไม่ว่าจะเกิดจากอุปกรณ์ทางด้านฮาร์ดแวร์ ซอฟต์แวร์ การติดไวรัส หรือการถูกเจาะเข้าระบบ เนื่องจากเหตุการณ์ที่อยู่นอกเหนือความควบคุมของผู้ให้บริการ
   4.3. ผู้ขอรับบริการ จะต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมถึงกฎหมายอื่น ๆ ที่เกี่ยวข้องกับการใช้บริการอย่างเคร่งครัด และต้องปฏิบัติตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของสถาบันบัณฑิตพัฒนบริหารศาสตร์ พ.ศ. 2564 ข้อกำหนดและเงื่อนไขการให้บริการนี้ และไม่กระทำการใด ๆ ที่อาจก่อให้เกิดความเสียหายแก่ผู้ให้บริการโดยผู้ให้บริการจะไม่รับผิดชอบต่อความสูญหายหรือความเสียหายของข้อมูลของผู้ขอรับบริการ ในกรณีที่ผู้ขอรับบริการ ไม่ปฏิบัติตาม เงื่อนไขที่กำหนดไว้ข้างต้น
   4.4. หากผู้ขอรับบริการ พบว่ามีความผิดปกติใด ๆ เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย ผู้ขอรับบริการจะต้องแจ้งผู้ให้บริการทราบโดยทันที เพื่อป้องกันหรือบรรเทาความเสียหายที่อาจเกิดขึ้นแก่ทรัพย์สินของผู้ขอรับบริการ หรือผู้ให้บริการ

IDT-SO-IS-002
(14/03/2025)

4.5. ผู้ขอรับบริการจะต้องดูแลเครื่องคอมพิวเตอร์แม่ข่าย ไม่ให้เป็นแหล่งแพร่ข้อมูลที่ผิดกฎหมาย หรือโจมตีระบบของเครื่องคอมพิวเตอร์แม่ข่ายอื่น หรือบุคคลอื่น เช่น mail bomb, hack, crack, DoS, spamming, port scanning และวิธีอื่นๆ ที่มีลักษณะหรือจุดประสงค์ที่คล้ายกัน หากมีการนำไปใช้บริการไปในทางลักษณะดังกล่าว จะถูกยกเลิกทันทีการให้บริการทันที โดยผู้ขอรับบริการไม่สามารถเรียกร้องค่าเสียหายใดๆ

4.6. ระบบจะสามารถรับรองการใช้งาน Remote จากภายนอก ผู้ขอรับบริการสามารถ Remote จาก IP Address และ Port ที่ผู้ให้บริการกำหนด ในกรณีผู้ขอรับบริการต้องการเข้าพื้นที่ Data Center กรุณาแจ้งล่วงหน้าอย่างน้อย 1 วันทำการ และหากต้องการนำอุปกรณ์ออกจากห้องต้องนำหนังสือจากหน่วยงานมาแสดง

4.7. หากผู้ขอรับบริการไม่ประสงค์จะใช้บริการนี้ต่อไป ผู้ใช้บริการจะต้องแจ้งให้ผู้ให้บริการทราบเป็นลายลักษณ์อักษร ล่วงหน้าอย่างน้อย 7 วัน

4.8. ผู้ขอรับบริการ ต้องอ่านและทำความเข้าใจข้อกำหนดและเงื่อนไขการให้บริการนี้เป็นอย่างดี จึงลงนามในแบบฟอร์มขอใช้บริการ

5. **เงื่อนไขและข้อจำกัดในการให้บริการ**

5.1. ผู้ให้บริการจะดำเนินการรักษาข้อมูลของผู้ขอรับบริการ ตามข้อกำหนดและเงื่อนไขการให้บริการ และจะไม่ทำการเปิดเผยต่อบุคคลใด เว้นแต่ข้อมูลดังกล่าวเป็นข้อมูลที่กำหนดให้ต้องเปิดเผยโดยกฎหมายหรือโดยคำสั่งศาล

5.2. ผู้ให้บริการจะไม่รับผิดชอบต่อความสูญหายหรือความเสียหายของข้อมูลของผู้ขอรับบริการ เว้นแต่ความเสียหายอันเนื่องมาจากผู้ขอรับบริการ หรือความเสียหายที่เกิดจากเหตุการณ์ไม่คาดคิด

5.3. การให้บริการจะไม่ครอบคลุมปัญหาที่เกิดขึ้นจากการใช้งานหรือติดตั้งซอฟต์แวร์ที่ผู้ขอรับบริการทำการติดตั้งเอง

5.4. ผู้ให้บริการขอสงวนสิทธิ์ในการตรวจสอบค้นหาช่องโหว่ของระบบที่ใช้งาน ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับปรับปรุงล่าสุด ประจำปี พ.ศ. 2566

5.5. ผู้ให้บริการขอสงวนสิทธิ์ระงับการให้บริการ รวมทั้งการเชื่อมต่อระหว่างเครือข่ายคอมพิวเตอร์ของผู้ให้บริการในทันที หากตรวจพบโดยกรณีดังต่อไปนี้

5.5.1 เครื่องคอมพิวเตอร์แม่ข่ายของผู้ขอรับบริการก่อให้เกิดผลกระทบต่อสภาพการใช้งานของอุปกรณ์คอมพิวเตอร์ ระบบเครือข่ายของผู้ให้บริการหรือมีปัญหาทางด้านความมั่นคงปลอดภัย

5.5.2 ผู้ขอรับบริการกระทำการฝ่าฝืนกฎระเบียบที่เกี่ยวข้องกับการให้บริการหรือละเมิดต่อข้อกำหนดและเงื่อนไขการให้บริการ

5.5.3 มีเหตุจำเป็นซึ่งผู้ให้บริการไม่สามารถจัดการหรือควบคุมได้เกิดขึ้น

5.5.4 มีเหตุจำเป็นต้องบำรุงรักษาหรือแก้ไขระบบสารสนเทศที่ใช้ในการให้บริการ

5.6. หากมีการเปลี่ยนแปลงผู้ประสานงาน ผู้ขอรับบริการต้องแจ้งให้ผู้ให้บริการทราบเป็นลายลักษณ์อักษรในทันที มิฉะนั้น ผู้ให้บริการจะไม่รับผิดชอบความเสียหายที่อาจเกิดขึ้นจากการไม่แจ้งเปลี่ยนผู้ประสานงานให้ผู้ให้บริการทราบ

5.7. การที่ผู้ขอรับบริการยินยอมให้ข้อมูลซึ่งอาจเข้าถึงข้อมูลส่วนบุคคล ข้อมูลอ่อนไหว หรือข้อมูลใดๆ ของผู้ขอรับบริการแก่ผู้ให้บริการ เพื่อประโยชน์ในการเข้าตรวจสอบปัญหา ให้คำปรึกษา หรือแก้ไขปัญหาสำหรับการใช้งานต่างๆ จะถือว่าผู้ให้บริการได้รับหรือข้อมูลซึ่งอาจเข้าถึงข้อมูลต่างๆ ภายใต้การอนุญาตเพื่อการรับบริการตรวจสอบปัญหา ให้คำปรึกษา หรือแก้ไขปัญหาโดยผู้ขอรับบริการ จึงไม่ถือเป็นการ

ผู้ใช้บริการเข้าถึงข้อมูลของผู้รับบริการอันเป็นความผิดต่อกฎหมาย และไม่ถือเป็นการละเมิดสิทธิในฐานะผู้รอรับบริการ กรณีดังกล่าวผู้ให้บริการได้รับบริการจากผู้ให้บริการ ในการดำเนินการต่าง ๆ ดังกล่าวเครียบร้อยแล้ว เพื่อเป็นการรักษาความปลอดภัยในข้อมูลของผู้ขอรับบริการ ผู้ขอรับบริการหรือเจ้าหน้าที่ของหน่วยงาน ผู้ใช้บริการมีหน้าที่ต้องรับผิดชอบในการดำเนินการและเปลี่ยนแปลงข้อมูลดังกล่าว ให้เป็นปัจจุบัน โดยผู้ให้บริการขอสงวนสิทธิ์ไม่รับผิดชอบในความสูญหายหรือเสียหายใด ๆ จากการดำเนินการ หรือค่าเสียหายใด ๆ ที่เกิดขึ้นกับข้อมูล โปรแกรม สิทธิบัตรหรือลิขสิทธิ์ปัญญา สิทธิอื่นใด ผลประโยชน์ทางธุรกิจ หรือการหยุดชะงักทางธุรกิจของผู้ขอรับบริการ ในทุกกรณี

6. ผู้ให้บริการขอสงวนสิทธิ์ในการเปลี่ยนแปลง แก้ไขเพิ่มเติม หรือลดออก ซึ่งส่วนใดส่วนหนึ่งของข้อกำหนดและเงื่อนไขการให้บริการนี้ได้ตลอดเวลา (และสิ้นสุดว่าผู้ขอรับบริการได้ยอมรับข้อกำหนดและเงื่อนไขการให้บริการใหม่โดยปริยาย ตลอดระยะเวลาที่ผู้ขอรับบริการยังคงใช้บริการและรับบริการของผู้ให้บริการ)
7. การรายงานผลการให้บริการ
ผู้ให้บริการจะจัดส่งรายงานผลการให้บริการตามหลักเกณฑ์การให้บริการแก่ผู้ขอรับบริการเมื่อได้รับเรื่องร้องขอจากผู้ขอรับบริการ

(4) **ขอบเขตของงานและคุณลักษณะ (Term of Reference : TOR) ระบบการให้บริการการศึกษาแบบเปิด (Open System for Lifelong Learning) รองรับการเรียนรู้ตลอดชีวิตเพื่อการพัฒนาที่ยั่งยืน ระยะที่ 2**