เอกสารประกอบการจัดประชุมเพื่อระดมความคิดเห็นกลุ่มย่อย (Focus Group)
“ร่างมาตรฐานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศระบบคลาวด์ภาครัฐ
(Government Cloud Security Standard)”
โดยสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สรอ.

วันอังคารที่ 15 กันยายน 2558 เวลา 8.30 -16.30 น.
ณ ห้องโพเดียม ชั้น 7 โรงแรมโหมดสาทร

1. หลักการและเหตุผล

กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ พ.ศ. 2554 – 2563 ในยุทธศาสตร์ที่ 1 “พัฒนาโครงสร้างพื้นฐาน ICT ที่เป็นอิเทอร์เน็ตความเร็วสูงหรือการสื่อสารรูปแบบอื่นที่เป็น Broadband ให้มีความทันสมัย มีการกระจายอย่างทั่วถึง และมีความมั่นคงปลอดภัยสามารถรองรับความต้องการของภาคส่วนต่างๆ ได้” ซึ่งเป็น 1 ใน 6 ยุทธศาสตร์ที่รัฐบาลตั้งเป้าหมายในการพัฒนาประเทศไทย กล่าวโดยสรุปคือ ประเทศไทยในปี พ.ศ.2563 จะมีการพัฒนาอย่างฉลาด การดำเนินกิจกรรมทางเศรษฐกิจและสังคมจะอยู่บนพื้นฐานของความรู้และปัญญา โดยให้โอกาสแก่ประชาชนทุกคนมีส่วนรวมในกระบวนการพัฒนาอย่างเสมอภาค นำไปสู่การเติบโตอย่างสมดุล และยั่งยืน (Smart Thailand 2020)

นโยบาย Smart Thailand 2020 มีการกำหนดนโยบายเร่งด่วนไว้ 3 ด้านได้แก่ (1) Smart Network (2) Smart Government และ (3) Smart Business โดยรัฐมนตรีว่าการกระทรวงไอซีทีได้มอบหมายให้สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สรอ. ดำเนินการให้สัมฤทธิ์ผลโดยเร็ว ดังนั้นเพื่อตอบสนองนโยบายของรัฐบาล สรอ. จึงได้มีการดำเนินงานในส่วนของ Smart Government อาทิ เช่น โครงการบริการคลาวด์ภาครัฐ หรือ Government Cloud Service (G-Cloud Service) ซึ่งเป็นการประยุกต์แนวทางการให้บริการแบบ Cloud Computing โดย สรอ. ดำเนินการโครงการดังกล่าวตั้งแต่ช่วงกลางปี พ.ศ.2555 เป็นต้นมา

Cloud computing คือ รูปแบบของการเข้าถึงระบบเพื่อใช้งานที่สะดวกและหลากหลายตามความต้องการของผู้ใช้งาน ในรูปแบบของการใช้ทรัพยากรร่วมกัน เช่น ส่วนประมวลผล พื้นที่สำหรับเก็บข้อมูล และเครือข่าย เป็นต้น รวมทั้งบริการอื่นๆ ที่สามารถจัดเตรียมเพื่อให้บริการได้อย่างรวดเร็ว เพื่อลดภาระการบริหารจัดการของผู้ดูแลระบบให้น้อยที่สุด

การให้บริการของ G-Cloud Service นั้นเป็นการให้บริการในรูปแบบของโครงสร้างพื้นฐาน ซึ่งจะประกอบด้วยเครื่องคอมพิวเตอร์แม่ข่าย ซอร์ฟแวร์ลิขสิทธ์ ระบบปฏิบัติการ รวมถึงฐานข้อมูล ซึ่งหน่วยงานที่ใช้งานสามารถบริหารจัดการเครื่องได้ด้วยตนเอง เสมือนเป็นเครื่องที่หน่วยงานมีใช้งานอยู่ โดยการใช้งานในกรณีทรัพยากรไม่เพียงพอ สามารถเพิ่มเติมได้อย่างรวดเร็ว ทั้ง CPU, Memory, Storage โดยการใช้งานสามารถใช้งานผ่านทางโครงข่ายสารสนเทศภาครัฐ (GIN) หรือผ่านทางเครือข่าย Public Internet ซึ่งเครือข่ายนี้เป็นการให้บริการลิงค์ขนาดใหญ่สำหรับใช้งานเฉพาะโครงการ G-Cloud เท่านั้น และในด้านของความมั่นคงปลอดภัย มีการป้องกันทั้งภายนอกและภายใน โดยการแยกส่วนที่ให้บริการของแต่ละหน่วยงานออกจากกัน

จากที่กล่าวมาข้างต้น สรอ. ตระหนักถึงการสร้างความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศในการให้บริการ และความสำคัญเป็นอย่างยิ่งในการจัดทำร่างมาตรฐานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศระบบคลาวด์ภาครัฐ (Government Cloud Security Standard) จึงมีความประสงค์ที่จะดำเนินงานตามขอบเขตการดำเนินโครงการจัดจ้างในการจัดทำร่างมาตรฐานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศระบบคลาวด์ภาครัฐ

(Government Cloud Security Standard) เพื่อให้โครงการบริการคลาวด์ภาครัฐสามารถให้บริการแก่หน่วยงานและประชาชนได้อย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศตามมาตรฐานสากล

2. วัตถุประสงค์

2.1 เพื่อจัดทำร่างมาตรฐานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศระบบคลาวด์ภาครัฐ (Government Cloud Security Standard) ที่มีความเป็นกลาง

2.2 เพื่อยกระดับการบริการคลาวด์ภาครัฐให้มีประสิทธิภาพและมีความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศตามมาตรฐานสากล

3. คลาวด์คอมพิวติ้ง (Cloud Computing)

3.1 กลุ่มหน้าที่ที่เกี่ยวข้องกับคลาวน์ (Role and Responsibility)

บทบาท	หน้าที่
ผู้ถือครองสิทธิ์ความเป็นเจ้าของระบบคลาวน์ (Cloud Owner)	ผู้ทำหน้าที่จัดทำ ประกาศ นโยบาย ขั้นตอนปฏิบัติ ข้อตกลง สัญญาหรืออื่นๆ ที่เกี่ยวข้องกับระบบคลาวน์ เพื่อทำหน้าที่เป็นผู้ให้บริการคลาวน์
ผู้ให้บริการระบบคลาวน์ (Cloud Service Provider)	ผู้ที่ทำหน้าที่ช่วยอำนวยความสะดวกและความพร้อมใช้งานต่างๆ ของระบบคลาวน์แก่ Cloud Owner
ผู้ใช้บริการคลาวน์ (Cloud Customer)	องค์กรหรือหน่วยงานที่มีความประสงค์ใช้บริการคลาวน์

3.2 คุณลักษณ์ที่สำคัญของคลาวน์ (5 Essential Characteristics)

3.2.1 การบริการตนเองตามความต้องการ (On-demand self-service)

ผู้ใช้บริการคลาวน์สามารถกำหนดและจัดการระบบประมวลผลได้เอง เช่น สามารถกำหนดเวลาประมวลผลของเครื่องแม่ข่าย และพื้นที่เก็บเครือข่ายที่ต้องการได้อย่างอัตโนมัติ โดยปราศจากการติดต่อโดยบุคคลกับผู้ให้บริการ

3.2.2 การเข้าถึงเครือข่ายได้อย่างกว้างขวาง (Broad Network Access)

ความสามารถด้านความพร้อมใช้ทางด้านเครือข่าย เพื่อรองรับการเข้าถึงผ่านกลไกมาตรฐานที่ส่งเสริมการใช้งานที่แตกต่างกันจากลูกข่ายในหลายๆแพรตฟอร์ม (เช่น โทรศัพท์เคลื่อนที่ คอมพิวเตอร์พกพา และพีดีเอ PDA) รวมถึงการเข้าถึงจากบริการซอฟต์แวร์บนคลาวด์หรือการเข้าถึงเครือข่ายแบบดั้งเดิม

3.2.3 การใช้ทรัพยากรร่วมกัน (Resource Pooling)

ทรัพยากรคอมพิวเตอร์ในหลายๆส่วนของผู้ให้บริการถูกนำมารวมกัน เพื่อให้บริการกับผู้บริโภคหลายรายในรูปแบบเช่าใช้บริการร่วมกัน ด้วยทรัพยากรทั้งแบบกายภาพและแบบเสมือนที่ถูกกำหนดตามความต้องการ

ของผู้บริโภค ผู้ใช้บริการไม่สามารถควบคุมหรือรู้ในเรื่องตำแหน่งที่แน่นอนของทรัพยากรที่จัดให้ได้ แต่สามารถระบุได้เพียงตำแหน่งในระดับกว้าง (เช่น ประเทศ เมือง หรือศูนย์ข้อมูล) ตัวอย่างของทรัพยากรที่ถูกรวมเข้าด้วยกันเช่น ที่เก็บข้อมูล หน่วยประมวลผล หน่วยความจำ แบนวิดธ์ของเครือข่าย และเครื่องจำลองเสมือน แม้คลาวด์ส่วนตัวก็ยังมีแนวโน้มที่จะรวมทรัพยากรระหว่างแผนกต่างๆภายในองค์กรเดียวกัน

3.2.4 ความยืดหยุ่นที่รวดเร็ว (Rapid Elasticity)

ความสามารถจัดหาเปลี่ยนแปลงทรัพยากรได้อย่างยืดหยุ่นและรวดเร็ว ในบางกรณีทำได้โดยอัตโนมัติเพื่อที่จะขยาย และลดขนาดอย่างรวดเร็ว สำหรับลักษณะนี้จะทำให้ผู้บริโภคสามารถปรับเปลี่ยนขนาดอย่างไม่จำกัดเท่าที่ผู้บริโภคสามารถจ่ายได้ตลอดเวลา

3.2.5 การบริการที่วัดผลได้ (Measured Service)

ระบบคลาวด์มีความสามารถในการวัดค่าการใช้งานทรัพยากรตามความเหมาะสมของประเภทของบริการ (เช่น การจัดเก็บ ประมวลผล แบนวิดธ์ และบัญชีผู้ใช้งานที่ใช้งานได้) การใช้งานทรัพยากรสามารถตรวจสอบ ควบคุมและรายงานได้ทำให้เกิดความโปร่งใสในการบริการทั้งระหว่างผู้บริโภคและผู้ให้บริการ

3.3 โมเดลสำหรับอ้างอิงบริการคลาวด์ (Cloud Reference Model)

3.3.1 การให้บริการซอฟต์แวร์คลาวด์ (Cloud Software as a Service, SaaS)

บริการที่จัดเตรียมให้ผู้บริโภคสามารถใช้แอปพลิเคชันของผู้ให้บริการที่ทำงานบนโครงสร้างพื้นฐานคลาวด์ แอปพลิเคชันสามารถเข้าถึงได้จากอุปกรณ์ลูกข่าย (Client Devices) ที่หลากหลายรูปแบบ ผ่านส่วนเชื่อมต่อของผู้ใช้บริการเช่น เว็บบลาวด์เซอร์ (ตัวอย่างเช่น อีเมล์ผ่านเว็บ หรือ Web-based email) ผู้บริโภคไม่ต้องจัดการหรือควบคุมโครงสร้างพื้นฐานคลาวด์รวมถึงเครือข่าย เครื่องแม่ข่าย ระบบปฏิบัติการ ที่เก็บข้อมูล หรือกระทั่งความสามารถของแอปพลิเคชันแต่ละอัน โดยที่อาจมีข้อยกเว้นบ้างในกรณีการตั้งค่าแอปพลิเคชันตามผู้ใช้งานที่จำกัด

3.3.2 การให้บริการแพรตฟอร์มคลาวด์ (Cloud Platform as a Service, PaaS)

บริการที่จัดเตรียมให้ผู้บริโภคสามารถปรับปรุงโครงสร้างพื้นฐานคลาวด์ที่ผู้บริโภคสร้างขึ้น หรือแอปพลิเคชันสร้าง โดยใช้ภาษาโปรแกรมและเครื่องมือที่สนับสนุนจากผู้ให้บริการ ผู้บริโภคไม่ต้องจัดการหรือควบคุมโครงสร้างพื้นฐานที่ใช้ รวมถึงเครือข่าย เครื่องแม่ข่าย ระบบปฏิบัติการ และที่เก็บข้อมูล แต่สามารถควบคุมปรับใช้แอปพลิเคชันและตั้งค่าภายในสภาพแวดล้อมของแอปพลิเคชัน

3.3.3 การให้บริการโครงสร้างพื้นฐานคลาวด์ (Cloud Infrastructure as a Service, IaaS)

บริการที่จัดเตรียมให้ผู้บริโภคในการประมวลผล การจัดเก็บข้อมูล เครือข่าย และทรัพยากรคอมพิวเตอร์พื้นฐาน ที่ผู้บริโภคนำซอฟต์แวร์มาใช้งานและปรับใช้ได้ตามใจ ซึ่งอาจรวมถึงระบบปฏิบัติการและแอปพลิเคชัน ผู้บริโภคไม่ได้จัดการหรือควบคุมโครงสร้างพื้นฐานคลาวด์แต่ควบคุม

ระบบปฏิบัติการ ที่เก็บข้อมูล แอปพลิเคชันที่ใช้ และยังสามารถควบคุมส่วนประกอบบางอย่างของเครือข่ายได้ (เช่น host firewalls)

3.4 รูปแบบการติดตั้งคลาวด์ (Cloud Deployment Model)

ไม่ว่าจะเป็นโมเดลการบริการแบบใด (SaaS, PaaS หรือ IaaS) คลาวด์จะมีโมเดลการติดตั้งทั้งหมด 4 แบบ รวมถึงรูปแบบแยกย่อยสำหรับความต้องการที่เฉพาะเจาะจง

3.4.1 คลาวด์สาธารณะ (Public Cloud)

โครงสร้างพื้นฐานคลาวด์เปิดให้บริการแก่บุคคลทั่วไปหรือกลุ่มอุตสาหกรรมขนาดใหญ่ โดยองค์กรผู้ให้บริการคลาวด์เป็นเจ้าของโครงสร้างพื้นฐานคลาวด์

3.4.2 คลาวด์ส่วนบุคคล (Private Cloud)

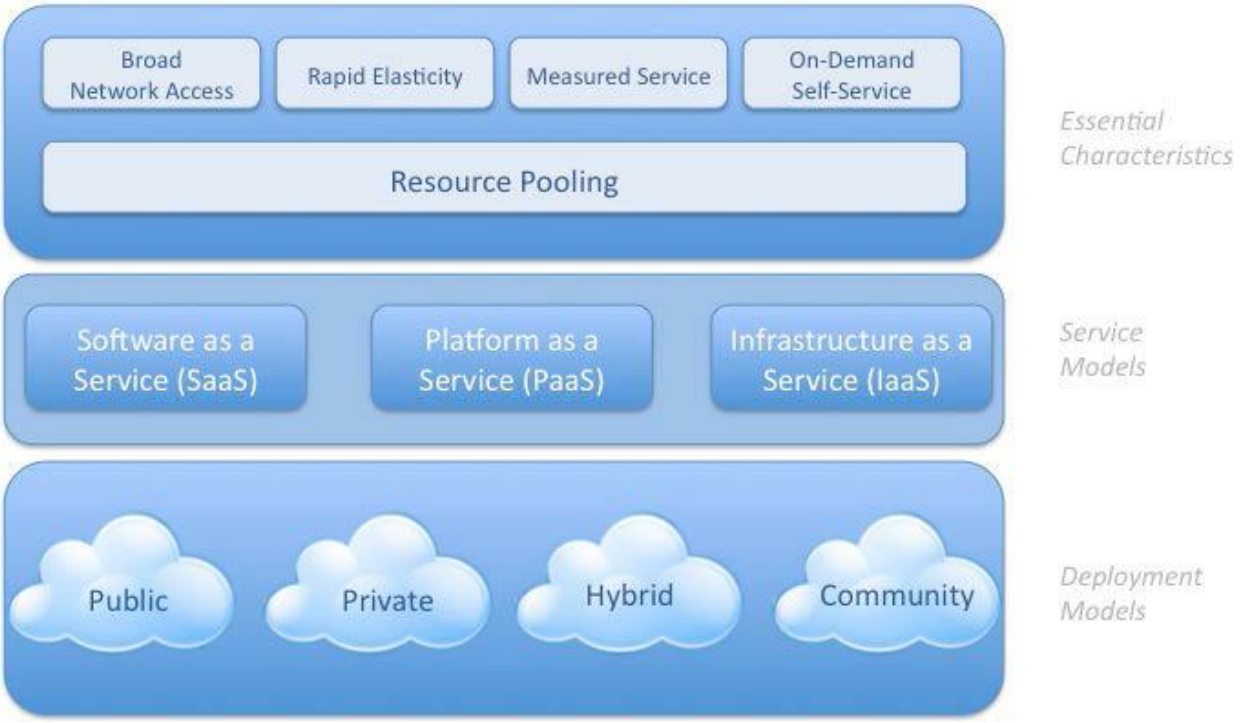
โครงสร้างพื้นฐานคลาวด์เปิดให้บริการแก่องค์กรเดียว อาจจะถูกบริหารจัดการโดยองค์กรเองหรือให้บุคคลที่สามจัดการและอาจตั้งอยู่ในสถานที่ในองค์กร (On-premise) หรือนอกองค์กร (Off-premise)

3.4.3 คลาวด์ชุมชน (Community Cloud)

โครงสร้างพื้นฐานคลาวด์ถูกใช้งานร่วมกันหลายองค์กรและรองรับชุมชนเฉพาะที่มีจุดประสงค์ร่วมกัน (เช่น ภารกิจ ความต้องการการรักษาความมั่นคงปลอดภัย นโยบาย หรือพิจารณาการปฏิบัติตามกฎระเบียบ) มันถูกบริหารจัดการโดยกลุ่มองค์กรหรือบุคคลที่สาม อาจตั้งอยู่ในสถานที่ในองค์กร (On-premise) หรือนอกองค์กร (Off-premise)

3.4.4 คลาวด์ลูกผสม (Hybrid Cloud)

โครงสร้างพื้นฐานคลาวด์เป็นการผสมระหว่างสองคลาวด์หรือมากกว่า (ส่วนบุคคล, ชุมชน หรือสาธารณะ) โดยคงรูปแบบเฉพาะตัวของตัวเองอยู่ แต่จะผูกพันกันด้วยเทคโนโลยีที่เป็นมาตรฐาน (Standardized) หรือเทคโนโลยีเฉพาะ (Proprietary) ที่ช่วยให้ข้อมูลและแอปพลิเคชันเคลื่อนย้ายถ่ายโอนได้ (ตัวอย่าง cloud bursting สร้างสมดุลของโหลดการทำงาน (Load-balancing) ระหว่างคลาวด์)



รูปที่ 1 : แสดงลำดับรูปแบบโครงสร้างของคลาวน์

จากรูปที่ 1 แสดงถึงลำดับโครงสร้างของระบบคลาวน์ ซึ่งระดับบนสุดประกอบด้วย 5 คุณลักษณ์สำคัญของคลาวน์ ลำดับต่อมาคือรูปแบบการให้บริการ (Service Models) และ รูปแบบการติดตั้ง (Deployment Models) ซึ่งขึ้นอยู่กับมุมมองกระบวนการทางธุรกิจของผู้ให้บริการและความต้องการการใช้บริการของผู้ใช้บริการ

การทำความเข้าใจถึงความสัมพันธ์ ระหว่างโมเดลคลาวด์คอมพิวติ้งต่างๆ มีความสำคัญอย่างมากต่อความเข้าใจด้านความเสี่ยงของการรักษาความมั่นคงปลอดภัยของคลาวด์คอมพิวติ้ง IaaS เป็นพื้นฐานของการบริการคลาวด์อื่นๆ ทั้งหมด PaaS สร้างอยู่บนฐานของ IaaS และ SaaS ก็สร้างอยู่บนฐานของ PaaS อีกที ตามที่แสดงในแผนภาพโมเดลสำหรับอ้างอิงบริการคลาวด์ ด้วยเหตุนี้ขีดความสามารถต่างๆ จะถูกถ่ายทอดมาเป็นลำดับชั้น รวมถึงปัญหาและความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยด้วย สิ่งสำคัญที่ควรทราบคือผู้ให้บริการคลาวด์อาจไม่ได้สอดคล้องกับโมเดลการให้บริการเป็นชั้นๆ อย่างพอดิบพอดี อย่างไรก็ตามโมเดลอ้างอิงเป็นสิ่งสำคัญที่เชื่อมโยงระหว่างการบริการจริงกับโครงสร้างสถาปัตยกรรมของคลาวด์ และทำให้เกิดความเข้าใจถึงการวิเคราะห์การรักษาความมั่นคงปลอดภัยต่อทรัพยากรและการบริการที่ถูกต้องเหมาะสม

IaaS ได้รวมชั้นโครงสร้างพื้นฐานทั้งหมดจากสิ่งอำนวยความสะดวกจนถึงแพรตฟอร์มฮาร์ดแวร์ บริการนี้จะรวมความทรัพยากรเข้าด้วยกันและเชื่อมโยงการเข้าถึงทั้งทางกายภาพ (physical) และลอจิคอล (logical) บริการ IaaS จะเชื่อมโยงติดต่อกับผู้ใช้บริการผ่านชุดสั่ง API (Application Programming Interface) ซึ่งเป็นช่องทางให้ผู้ใช้บริการสามารถบริหารจัดการและติดต่อสื่อสารกับโครงสร้างพื้นฐานเหล่านี้ได้

PaaS ซ้อนอยู่บนฐานของชั้น IaaS และเพิ่มชั้นที่เกี่ยวข้องกับโครงสร้างของการพัฒนาแอปพลิเคชัน (Application Development Frameworks) Middleware และฟังก์ชั่น เช่น ฐานข้อมูล (Database) ข้อความ (Messaging) และการจัดลำดับ (Queuing) การบริการเหล่านี้ช่วยให้นักพัฒนาสามารถสร้างแอปพลิเคชันบนแพลตฟอร์มด้วยโปรแกรมภาษาและเครื่องมือที่รองรับโดยบริการ PaaS

SaaS สร้างบนฐานของชั้น IaaS และชั้น PaaS โดย SaaS ให้สภาพแวดล้อมของระบบปฏิบัติการที่ครบถ้วนในตัวเองซึ่งถูกนำมาใช้ในการสร้างประสบการณ์ที่สมบูรณ์แบบแก่ผู้ใช้ ซึ่งรวมถึง เนื้อหา การนำเสนอแอปพลิเคชัน และความสามารถในการจัดการ

คุณสมบัติของการทำงานเข้ากันได้ (integrated features) ความซับซ้อน (Complexity) เปรียบเทียบกับการเปิดกว้าง (Openness) (การขยายต่อ) และการรักษาความมั่นคงปลอดภัย เป็นปัจจัยในการเลือกบริการคลาวด์ในแต่ละโมเดล โดยทั่วไป SaaS จะให้ฟังก์ชั่นที่มีมาพร้อมมากที่สุดโดยผู้บริโภคไม่ต้องเพิ่มเติมอะไรมาก และมีระบบการรักษาความมั่นคงปลอดภัยในระดับสูง (ผู้ให้บริการเป็นผู้ทำหน้าที่ในการดูแลรักษาความมั่นคงปลอดภัย)

PaaS มีจุดมุ่งหมายที่จะให้นักพัฒนาซอฟต์แวร์สร้างแอปพลิเคชันของตัวเองบนแพรตฟอร์มที่กำหนดให้ ผลคือ PaaS จะเปิดกว้างได้มากกว่า SaaS แต่จะสูญเสียคุณสมบัติสำเร็จรูปบางอย่างสำหรับผู้ใช้บริการไป โดยความสูญเสียคุณสมบัติดังกล่าวนี้เปิดโอกาสให้ผู้ใช้บริการสามารถเพิ่มเติมคุณสมบัติด้านการรักษาความมั่นคงปลอดภัยได้เองอย่างยืดหยุ่น

IaaS ให้คุณสมบัติสำเร็จรูปน้อยแต่จะสามารถต่อขยายได้มาก โดยทั่วไปหมายถึงมีคุณสมบัติและฟังก์ชั่นด้านการรักษาความมั่นคงปลอดภัยนอกเหนือจากการปกป้องโครงสร้างพื้นฐานของตัวมันเองที่น้อยลง โมเดลนี้ต้องการระบบปฏิบัติการ แอปพลิเคชัน และ การจัดการเนื้อหาและการรักษาความลับโดยผู้ใช้บริการคลาวด์

กุญแจสำคัญสำหรับสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยคือจุดที่ผู้ให้บริการคลาวด์ดูแลและบริการในระดับชั้นยิ่งต่ำลงเท่าใด ขีดความสามารถในการรักษาความมั่นคงปลอดภัยและการจัดการโดยผู้ใช้ต้องรับผิดชอบในการดำเนินงานและการจัดการด้วยตัวเองมากขึ้นเท่านั้น

4. ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศคลาวน์ (Security G-Cloud Requirements)

เพื่อให้บริการระบบคลาวด์ภาครัฐสามารถให้บริการแก่หน่วยงานและประชาชนได้อย่างมีประสิทธิภาพมีความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศตามมาตรฐานสากล โดยมีรายละเอียดที่จะกล่าวต่อจากนี้

4.1 คำนิยามกลุ่มของมาตรฐานการควบคุม (Control Area Definitions)

กลุ่มของมาตรการการควบคุม (Control Area)	ตัวย่อ	คำอธิบาย (Description)
Application and Interface Security	AIS	การพัฒนาด้านความมั่นคงปลอดภัยของแอปพลิเคชันและส่วนติดต่อเพื่อพัฒนาโปรแกรม

กลุ่มของมาตรการการควบคุม (Control Area)	ตัวย่อ	คำอธิบาย (Description)
Audit Assurance and Compliance	AAC	การตรวจสอบความเชื่อมั่นของระบบคลาวน์และการปฏิบัติตาม
Business Continuity Management and Operational Resilience	BCR	การบริหารจัดการความต่อเนื่องทางธุรกิจ และการกลับคืนสู่สภาวะการดำเนินงานปกติ
Change Control and Configuration Management	CCC	การบริหารจัดการควบคุมการเปลี่ยนแปลง และการบริหารจัดการข้อมูลคอนฟิกูเรชัน
Data Security and Information Lifecycle Management	DSI	การบริหารจัดการวงจรข้อมูลและการรักษาความมั่นคงปลอดภัย
Datacenter Security	DCS	ความมั่นคงปลอดภัยสำหรับห้องดาต้าเซ็นเตอร์
Encryption and Key Management	EKM	การเข้ารหัสลับและการบริหารจัดการกุญแจรหัสลับ
Governance and Risk Management	GRM	การกำกับดูแลและการบริหารความเสี่ยง
Human Resources	HRS	ทรัพยากรบุคคลล
Identity and Access Management	IAM	การบริหารจัดการตัวตนและการเข้าถึง
Infrastructure and Virtualization Security	IVS	ความมั่นคงปลอดภัยระบบโครงสร้างพื้นฐานและระบบเสมือน
Interoperability and Portability APIs	IPY	การถ่ายโอนและการทำงานร่วมกันของส่วนติดต่อเพื่อพัฒนาโปรแกรม
Mobile Security	MOS	ความมั่นคงปลอดภัยของอุปกรณ์เคลื่อนที่
Security Incident Management, E-Discovery and Cloud Forensics	SEF	การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย การสืบสวนและกู้ข้อมูลอิเล็กทรอนิกส์บนระบบคลาวน์
Supply Chain Management, Transparency and Accountability	STA	การจัดการโซ่อุปทาน ความโปร่งใสและความรับผิดชอบ
Threat and Vulnerability Management	TVM	การบริหารจัดการภัยคุกคามและช่องโหว่

4.2 ร่างมาตรฐานการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศระบบคลาวน์ภาครัฐ (Draft Government Cloud Security Standards)

Control Area	Control ID	Control Notes
4.2.1 การพัฒนาด้านความมั่นคงปลอดภัยของแอปพลิเคชัน และส่วนติดต่อเพื่อพัฒนาโปรแกรม (Application & Interface Security : AIS)		
แนวทางการพัฒนาแอปพลิเคชันอย่างมั่นคงปลอดภัย (Application Security)	AIS-01	- แอปพลิเคชัน และ ส่วนติดต่อเพื่อพัฒนาโปรแกรม (APIs) ต้องได้รับการออกแบบ พัฒนา ติดตั้ง และทดสอบให้สอดคล้องกับมาตรฐานอุตสาหกรรมชั้นนำ เช่น OWASP สำหรับการพัฒนาเว็บแอปพลิเคชัน เป็นต้น รวมทั้งต้องให้สอดคล้องกับกฎหมาย แนวทางการกำกับดูแล แนวปฏิบัติ ภาระผูกพันอื่นๆ ที่เกี่ยวข้องกับการให้บริการ
การกำหนดความต้องการด้านความมั่นคงปลอดภัยของการเข้าถึงของผู้เช่าใช้บริการ (Customer Access Requirements)	AIS-02	- การเข้าถึงข้อมูลหรือทรัพย์สินสารสนเทศใดๆ ของผู้ใช้บริการภายใต้บริการต้องถูกกำหนดให้สอดคล้องกับความต้องการด้านความมั่นคงปลอดภัย ความต้องการที่เกิดขึ้นจากสัญญา หรือความต้องการที่ตรงกับกฎระเบียบ ที่ตกลงกันไว้ระหว่างผู้ให้บริการ และผู้ใช้บริการ
การตรวจสอบความถูกต้องครบถ้วนของข้อมูล (Data Integrity)	AIS-03	- แอปพลิเคชันและส่วนติดต่อเพื่อพัฒนาโปรแกรม (APIs) ต้องมีกระบวนการสำหรับการตรวจสอบความถูกต้องครบถ้วนของข้อมูลนำเข้า (Input) และส่งออก (Output)

Control Area	Control ID	Control Notes
การสร้างความมั่นคงปลอดภัยให้กับข้อมูล (Data Security / Integrity)	AIS-04	- ต้องจัดทำนโยบายและขั้นตอนปฏิบัติที่สนับสนุนการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศ (Confidentiality, Integrity and Availability) ให้ครอบคลุมในทุกการเชื่อมโยงของการพัฒนาแอปพลิเคชันและส่วนติดต่อเพื่อพัฒนาโปรแกรม (APIs)
4.2.2 การตรวจสอบความเชื่อมั่นของระบบคลาวน์และการปฏิบัติตาม (Audit Assurance & Compliance)		
การวางแผนการตรวจสอบ (Audit Planning)	AAC-01	- องค์กรต้องจัดทำแผนการตรวจสอบระบบคลาวน์และระบบอื่นๆ ที่เกี่ยวข้องโดยคำนึงถึงความเสี่ยงที่จะทำให้เกิดการหยุดชะงักของกระบวนการทางธุรกิจ โดยแผนการตรวจสอบต้องมุ่งเน้นที่การตรวจสอบประสิทธิภาพของการดำเนินงานด้านการรักษาความปลอดภัยและกิจกรรมการตรวจสอบทั้งหมดต้องได้รับการเห็นชอบจากผู้ที่เกี่ยวข้องกับการตรวจสอบก่อนดำเนินกิจกรรมการตรวจสอบ
การตรวจสอบความสอดคล้องกับนโยบายอย่างเป็นอิสระ (Independent Audits)	AAC-02	- ต้องมีการดำเนินการการทบทวนหรือการประเมินความสอดคล้องอย่างเป็นอิสระระหว่างการปฏิบัติเปรียบเทียบกับนโยบาย ขั้นตอนปฏิบัติ มาตรฐาน และข้อกำหนดที่องค์กรต้องปฏิบัติตาม โดยต้องดำเนินการทบทวนหรือประเมินอย่างน้อยปีละ 1 ครั้ง หรือตามรอบระยะเวลาที่กำหนดไว้

Control Area	Control ID	Control Notes
การปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และสิ่งที่กำหนดในสัญญาจ้าง (Information System Regulatory Mapping)	AAC-03	- องค์กรต้องจัดทำกรอบการควบคุมให้เป็นไปตามตามกฎหมาย ระเบียบ ข้อบังคับ และสิ่งที่กำหนดในสัญญาจ้างที่ต้องปฏิบัติตามความต้องการของธุรกิจ (เช่น การเก็บข้อมูลล็อกตาม พรบ. ขั้นตอนปฏิบัติสำหรับการติดตั้งระบบ การป้องกันไวรัส การสำรองข้อมูล นโยบายการป้องกันการละเมิดทรัพย์สินทางปัญญา การดูแลและบริหารจัดการระบบคลาวน์ที่ผู้ให้บริการเป็นผู้ดำเนินการให้ ข้อปฏิบัติต่างๆ ที่ผู้ใช้บริการต้องปฏิบัติตามให้สอดคล้อง และอื่นๆ) รวมทั้งต้องดูแลและบำรุงรักษากรอบการควบคุมดังกล่าวด้วยอีกทั้งกรอบการควบคุมต้องได้รับการทบทวนความถูกต้องและทันสมัยอยู่เสมืออย่างน้อยปีละ 1 ครั้งเพื่อให้มั่นใจว่าการเปลี่ยนแปลงกรอบการควบคุมไม่มีผลต่อกระบวนการทางธุรกิจ

Control Area	Control ID	Control Notes
4.2.3 การบริหารจัดการความต่อเนื่องทางธุรกิจ และการกลับคืนสู่สภาวะการดำเนินงานปกติ (Business Continuity Management & Operational Resilience)		
แผนสร้างความต่อเนื่องทางธุรกิจ (Business Continuity Planning)	BCR-01	- องค์กรต้องดำเนินการกำหนดกรอบการจัดทำแผนสร้างความต่อเนื่องทางธุรกิจ และจัดทำแผนสร้างความต่อเนื่องทางธุรกิจทุกอย่างให้เป็นลายลักษณ์อักษรและแผนทุกฉบับที่จัดทำขึ้นต้องมีความสอดคล้องกัน ทั้งนี้แผนสร้างความต่อเนื่องทางธุรกิจควรครอบคลุมประเด็น ดังนี้ 1. จุดประสงค์และขอบเขตของแผนฯ 2. ผู้ที่สามารถเข้าถึงได้ 3. ผู้ที่รับผิดชอบในการจัดทำ ทบทวน ปรับปรุง และอนุมัติ 4. โครงสร้างและบทบาทหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง 5. ช่องทางการของผู้ที่อยู่ในโครงสร้างทั้งหมดและผู้เกี่ยวข้อง 6. ขั้นตอนปฏิบัติในการกู้คืนซึ่งรวมถึงการปฏิบัติงานโดยวิธีการ manual และข้อมูลแหล่งอ้างอิงที่เกี่ยวข้อง 7. วิธีการเรียกใช้แผน

Control Area	Control ID	Control Notes
การทดสอบแผนสร้างความต่อเนื่องทางธุรกิจ (Business Continuity Testing)	BCR-02	- ต้องมีการดำเนินการการทดสอบแผนสร้างความต่อเนื่องทางธุรกิจ (Business Continuity Plan) แผนรับมือเหตุฉุกเฉิน (Incident Response Plan) ตามรอบระยะเวลาที่กำหนด เพื่อตรวจสอบสภาพความพร้อมใช้งานเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กรหรือมีการเปลี่ยนสภาพแวดล้อมขององค์กร อีกทั้งแผนรับมือเหตุฉุกเฉินต้องเกี่ยวข้องกับผลกระทบที่มีต่อผู้ใช้บริการหรือผู้ที่เกี่ยวข้องกับการดำเนินธุรกิจ
การบำรุงรักษาและเฝ้าระวังอุปกรณ์สนับสนุนการทำงานของห้องดาต้าเซ็นเตอร์ (Datacenter Utilities / Environmental Conditions)	BCR-03	- อุปกรณ์สนับสนุนการทำงานของห้องเดต้าเซ็นเตอร์และสภาพแวดล้อม เช่น น้ำ, ไฟ, การควบคุมอุณหภูมิและความชื้น, การสื่อสาร, และการเชื่อมต่อระบบอินเตอร์เน็ต เป็นต้น ต้องได้รับการดูแลให้ปลอดภัย, การเฝ้าระวัง, การบำรุงรักษาและการทดสอบตามรอบระยะเวลาที่กำหนด เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต หรือป้องกันความเสี่ยหายที่อาจเกิดขึ้นได้ หรือเพื่อให้มีการออกแบบตำแหน่งการติดตั้งอุปกรณ์ให้รองรับการทำงานทดแทนกันในกรณีที่อุปกรณ์หลักเกิดความเสียหาย
เอกสาร (Documentation)	BCR-04	- เอกสารที่เกี่ยวข้องกับระบบสารสนเทศ เช่น เอกสารคู่มือสำหรับผู้ดูแลระบบ คู่มือการใช้งานและแผนผังสถาปัตยกรรม เป็นต้น ต้องจัดเก็บให้มีความพร้อมใช้งานและสามารถเข้าถึงให้เฉพาะผู้ได้รับอนุญาตเท่านั้น เพื่อให้สามารถปฏิบัติตามได้เมื่อเกิดเหตุการณ์ฉุกเฉิน ควรประกอบด้วยรายละเอียดดังต่อไปนี้ - การคอนฟิก, การติดตั้ง และดำเนินงานระบบสารสนเทศ - ใช้คุณสมบัติด้านความปลอดภัยของระบบอย่างมีประสิทธิภาพ

Control Area	Control ID	Control Notes
ความเสี่ยงจากสภาพแวดล้อม (Environmental Risks)	BCR-05	- ต้องมีการป้องกันทางกายภาพสำหรับความเสี่ยงทั้งที่เกิดจากทางธรรมชาติและโดยมนุษย์ เช่น ไฟไหม้ น้ำท่วม ฟ้าผ่า พายุสุริยะ ลมพายุ แผ่นดินไหน สึนามิ อุบัติเหตุนิวเคลียร์ การระเบิด ภูเขาไฟระเบิด ฝูงชนที่บ้าคลั่ง โคลนถล่ม และอื่นๆ
ที่ตั้งของอุปกรณ์ (Equipment Location)	BCR-06	- สำหรับระบบและอุปกรณ์ที่เป็นส่วนหนึ่งของกระบวนการสำคัญซึ่งอาจได้รับความเสียหายจากความเสี่ยงด้านภาพแวดล้อมและการเข้าถึงระบบ/อุปกรณ์โดยไม่ได้รับอนุญาต ต้องติดตั้งระบบ/อุปกรณ์ไว้ในสถานที่ปลอดภัยจากความเสี่ยงและต้องระบบและอุปกรณ์สำรองซึ่งติดตั้งในสถานที่ที่อยู่ในระยะห่างที่เพียงพอ
การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)	BCR-07	- ต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติสำหรับการบำรุงรักษาอุปกรณ์ เพื่อทำให้คลาวน์สามารถให้บริการมีความต่อเนื่องและความพร้อมใช้ รวมถึงการบริหารจัดการผู้ปฏิบัติงานที่เกี่ยวข้องด้วย เช่น จัดผู้ปฏิบัติงานสำรองในกรณีที่ผู้ปฏิบัติงานหลักไม่สามารถปฏิบัติงานได้ เป็นต้น
การบริหารจัดการความต่อเนื่องทางธุรกิจ และการกลับคืนสู่สภาวะการดำเนินงานปกติ : การป้องกันกรณีระบบไฟฟ้าไม่สามารถใช้งานได้ (Business Continuity Management & Operational Resilience : Equipment Power Failures)	BCR-08	- ต้องมีมาตรการรองรับเหตุการณ์กรณีระบบไฟฟ้าไม่สามารถใช้งานได้ซึ่งอาจเกิดจากภัยคุกคามทางธรรมชาติหรือมนุษย์ โดยมาตรการดังกล่าวต้องพิจารณาถึงผลกระทบทางธุรกิจด้านภูมิศาสตร์ เช่น กรณีห้องเดต้าเซ็นเตอร์ตั้งอยู่ในสถานที่เสี่ยงต่อไฟฟ้าดับเป็นระยะเวลานาน และมีการใช้เครื่องผลิตกระแสไฟฟ้าเพื่อจ่ายไฟสำรอง เป็นต้น

Control Area	Control ID	Control Notes
การบริหารจัดการความต่อเนื่องทางธุรกิจ และการกลับคืนสู่สภาวะการดำเนินงานปกติ : การประเมินผลกระทบทางธุรกิจ (Business Continuity Management & Operational Resilience : Impact Analysis)	BCR-09	- ต้องมีการจัดทำวิธีการประเมินผลกระทบต่อกระบวนการสำคัญที่เกิดการหยุดชะงัก กำหนดไว้อย่างเป็นลายลักษณ์อักษร วิธีการครอบคุลมถึงรายละเอียด ดังนี้ 1. ระบุผลิตภัณฑ์และบริการสำคัญ 2. ระบุกระบวนการสำคัญและกระบวนการอื่นๆ ที่เกี่ยวข้อง ระบบงาน ผู้ที่มีส่วนได้ส่วนเสียกับธุรกิจและผู้ให้บริการภายนอก 3. ระบุภัยคุกคามที่มีผลต่อการหยุดชะงักของกระบวนการสำคัญ 4. ระบุผลกระทบจากการหยุดชะงักทั้งที่คาดคิดหรือไม่คาดคิดก็ตาม รวมทั้งแสดงให้เห็นถึงระดับผลกระทบเมื่อเวลาผ่านไป 5. กำหนดระยะเวลานานที่สุดที่องค์กรยอมรับด้านของการหยุดชะงัก และกำหนดระยะเวลาเป้าหมายในการกู้คืนกระบวนการและ/หรือระบบ (ภายในระยะเวลานานที่สุดนั้น) 6. กำหนดลำดับหรือขั้นตอนในการกู้คืนกระบวนการและ/หรือระบบ 7. กำหนดระยะเวลาเป้าหมายสำหรับการกู้คืนผลิตภัณฑ์และบริการสำคัญ 8. กำหนดทรัพยากรต่างๆ ที่จำเป็นต้องใช้สำหรับการสร้างความต่อเนื่องทางธุรกิจ

Control Area	Control ID	Control Notes
การบริหารจัดการความต่อเนื่องทางธุรกิจ และการกลับคืนสู่สภาวะการดำเนินงานปกติ : นโยบาย (Business Continuity Management & Operational Resilience: Policy)	BCR-10	- ต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติสำหรับการกำกับดูแลเทคโนโลยีสารสนเทศและการบริหารจัดการบริการเพื่อให้มั่นใจได้ว่าองค์กรมีการวางแผน การส่งมอบบริการและการสนับสนุนทางด้านเทคโนโลยีสารสนเทศขององค์กรที่รองรับการทำงานทางธุรกิจ กำลังคน และ/หรือผู้ใช้บริการตามมาตรฐานที่ยอมรับในอุตสาหกรรม (เช่น ITIL4 และ COBIT5) โดยที่นโยบายและขั้นตอนปฏิบัติดังกล่าวต้องมีการกำหนดบทบาทหน้าที่ความรับผิดชอบสำหรับผู้เกี่ยวข้อง รวมถึงต้องอบรมหน้าที่และความรับผิดชอบให้ผู้ที่เกี่ยวข้องให้รับทราบด้วย
นโยบายการจัดเก็บและระยะเวลาการจัดเก็บข้อมูล (Retention Policy)	BCR-11	- ต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติสำหรับการจัดเก็บและระยะเวลาการจัดเก็บข้อมูลสำคัญ เพื่อให้สอดคล้องกับกฎหมาย ระเบียบข้อบังคับ สิ่งที่อยู่ในสัญญาจ้าง ต้องมีมาตรการสำรองข้อมูล การกู้คืนในแผนการสร้างความต่อเนื่องทางธุรกิจพร้อมทั้งต้องมีการทดสอบข้อมูลที่ได้รับการสำรองไว้เพื่อให้สามารถใช้ข้อมูลสำรองได้อย่างมีประสิทธิภาพเมื่อมีความจำเป็นต้องกู้คืนระบบ

Control Area	Control ID	Control Notes
4.2.4 การบริหารจัดการควบคุมการเปลี่ยนแปลง และการบริหารจัดการข้อมูลคอนฟิกูเรชัน (Change Control & Configuration Management)		
การบริหารจัดการเพื่อพัฒนา และการจัดซื้อจัดจ้างระบบใหม่ (New Development / Acquisition)	CCC-01	- ผู้ให้บริการต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเพื่อรองรับการบริหารจัดการเพื่อพัฒนา และการจัดซื้อจัดจ้างระบบใหม่ในทุกองค์ประกอบของบริการ ที่ต้องกำหนดให้มีการอนุมัติโดยผู้บริหารขั้นสูงด้านธรุกิจขององค์กร
การควบคุมผู้ให้บริการภายนอกให้ปฏิบัติตามกระบวนการบริหารจัดการควบคุมการเปลี่ยนแปลง และการบริหารจัดการข้อมูลคอนฟิกูเรชัน (Change Control & Configuration Management Outsourced Development)	CCC-02	- คู่ค้าภายนอกต้องปฏิบัติตามนโยบาย และขั้นตอนปฏิบัติของผู้ให้บริการที่เกี่ยวข้องกับการบริหารจัดการการเปลี่ยนแปลง, การเปิดให้บริการใหม่ และการทดสอบ (Change management, release, and testing) ดังตัวอย่างของมาตรฐาน ITIL ในหัวข้อ service management processes
การกำหนดการทดสอบคุณภาพด้านความมั่นคงปลอดภัย (Quality Testing)	CCC-03	- ต้องมีการกำหนดคุณภาพด้านความมั่นคงปลอดภัยสำหรับกระบวนการเปลี่ยนแปลง และการทดสอบ (อ้างอิง ITIL หัวข้อ Service management) ของระบบและบริการ
การควบคุมการติดตั้งซอฟต์แวร์ในระบบของบริการ (Unauthorized Software Installations)	CCC-04	- ผู้ให้บริการต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ในอุปกรณ์ของตน และอุปกรณ์ของผู้ใช้บริการ(เช่น workstations, laptops, และ mobile devices) รวมถึงองค์ประกอบด้านโครงสร้างสารสนเทศในเครือข่าย และระบบงานต่างๆ ของบริการ

Control Area	Control ID	Control Notes
การบริหารจัดการการเปลี่ยนแปลงระบบเข้าสู่บริการจริง (Production Changes)	CCC-05	ผู้ให้บริการต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเพื่อบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการเปลี่ยนแปลงในประเด็นต่อไปนี้ 1. การเปลี่ยนแปลงของระบบสำคัญของบริการ หรือระบบสำคัญของผู้ใช้บริการ 2. การเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศ และระบบเครือข่าย โดยกระบวนการเปลี่ยนแปลงต้องได้รับการลงทะเบียนขอการเปลี่ยนแปลง (Registered change request), การอนุมัติการเปลี่ยนแปลงที่สอดคล้องกับ SLA ที่ได้กำหนดเอาไว้
4.2.5 การบริหารจัดการวงจรข้อมูลและการรักษาความมั่นคงปลอดภัย (Data Security & Information Lifecycle Management)		
การแบ่งระดับชั้นข้อมูล (Classification)	DSI-01	- ข้อมูลสารสนเทศภายใต้การบริการต้องได้รับการจัดแบ่งระดับชั้น โดยเจ้าของข้อมูล (data owner) เพื่อให้สอดคล้องกับชนิด มูลค่า ความอ่อนไหว ความสำคัญของข้อมูล ที่ผู้ให้บริการคลาวน์กำหนด
ทิศทางของข้อมูล (Data Inventory / Flows)	DSI-02	- ต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเพื่อควบคุมการไหลเวียนของข้อมูลภายใต้การให้บริการ และผู้ให้บริการต้องมั่นใจได้ว่าข้อมูลต้องไม่โอนย้ายไปยังภูมิภาคอื่นที่ไม่อนุญาต
การขนส่งข้อมูล e-Commerce (e-Commerce Transactions)	DSI-03	- ข้อมูลประเภท e-Commerce Transactions ที่วิ่งเข้าสู่ระบบเครือข่ายสาธารณะต้องได้รับการป้องกันด้านความมั่นคงปลอดภัยอย่างเหมาะสม
นโยบายการรักษาความปลอดภัย การทำสัญลักษณ์ และ การถือครอง	DSI-04	- ต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเพื่อควบคุมการ

Control Area	Control ID	Control Notes
(Handling / Labeling / Security Policy)		ถือครอง/การทำสัญลักษณ์กับข้อมูลอย่างมั่นคงปลอดภัย
การแบ่งแยกข้อมูลระหว่างระบบจริงและระบบทดลอง (Non-Production Data)	DSI-05	- ข้อมูลของการให้บริการจริงต้องไม่ถูกสำเนาเข้าสู่หรือใช้งานโดยระบบที่ไม่ให้บริการจริง (non-production environments)
การระบุความเป็นเจ้าของ (Ownership / Stewardship)	DSI-06	- ข้อมูลทั้งหมดที่จัดเก็บและใช้งานที่อยู่ในระบบคลาวน์ต้องได้รับการกำหนดเจ้าของ มีผู้ดูแลข้อมูลรับผิดชอบเป็นลายลักษณ์อักษรและต้องได้รับการสื่อสารอย่างทั่วถึง
การลบล้างหรือทำลายข้อมูลอย่างปลอดภัย (Secure Disposal)	DSI-07	- การถอดถอนข้อมูลออกจากระบบคลาวน์ต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้ใช้บริการ โดยต้องให้ปฏิบัติอย่างสอดคล้องกับกฎหมาย และเงื่อนไขข้อตกลงที่กำหนดไว้
4.2.6 ความมั่นคงปลอดภัยสำหรับดาต้าเซ็นเตอร์ (Datacenter Security)		
การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)	DCS-01	- ทรัพย์สินต้องได้รับการแยกลำดับชั้นความสำคัญตามข้อกำหนดด้านความสำคัญระดับการให้บริการ และความต่อเนื่องของการให้บริการ อีกทั้งทรัพย์สินที่มีความสำคัญทั้งหมดที่อยู่ใน/นอกพื้นที่ต้องมอบหมายผู้รับผิดชอบอย่างชัดเจนในการดูแลรักษาฐานข้อมูลทรัพย์สินดังกล่าวให้ทันสมัยอยู่เสมอ
การควบคุมการเข้าถึงทางกายภาพ (Controlled Access Points)	DCS-02	- ต้องมีมาตรการควบคุมทางกายภาพในบริเวณเขตกันชนกับภายนอก (Physical security perimeters) ให้มีความมั่นคงปลอดภัย
กระบวนการอนุมัติเพื่อนำอุปกรณ์ไปใช้นอกสถานที่ (Off-Site Authorization)	DCS-03	- ต้องกำหนดกระบวนการควบคุมการอนุญาตสำหรับการเคลื่อนย้ายฮาร์ดแวร์ซอฟต์แวร์หรือข้อมูลไปใช้นอกสถานที่

Control Area	Control ID	Control Notes
การระบุตำแหน่งของอุปกรณ์ (Equipment Identification)	DCS-04	- ต้องใช้ระบบบงบอกตำแหน่งของอุปกรณ์อย่างอัตโนมัติ (Automated equipment identification)เพื่อป้องกันการเคลื่อนย้ายอุปกรณ์โดยไม่ได้รับอนุญาต
กระบวนการนำอุปกรณ์ไปใช้นอกสถานที่ (Off-Site Equipment)	DCS-05	- ต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเพื่อบริหารจัดการอุปกรณ์ที่นำไปใช้นอกสถานที่ รวมถึงการทำลายข้อมูลในสื่อบันทึกข้อมูลต่างๆ ของอุปกรณ์ที่นำออกจากดาต้าเซ็นเตอร์
นโยบายด้านความมั่นคงปลอดภัยด้านกายภาพห้องเดต้าเซ็นเตอร์ (Policy)	DCS-06	- ต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเพื่อบริหารพื้นที่ปฏิบัติงาน พื้นที่สำนักงาน ห้องปฏิบัติงาน ห้องสนับสนุน และพื้นที่ควบคุม และพื้นที่จัดเก็บข้อมูลให้มีความมั่นคงปลอดภัย
การควบคุมการเข้าถึงพื้นที่มั่นคงปลอดภัยสารสนเทศ (Secure Area Authorization)	DCS-07	- ต้องมีมาตรการการควบคุมการเข้าและออกไปยังพื้นที่รักษาความปลอดภัยด้วยกลไกกายภาพเพื่อให้แน่ใจว่าเฉพาะผู้ที่ได้รับอนุญาตเท่านั้นที่มีการเข้าถึง
การเข้าถึงพื้นที่ส่วนรวม (Unauthorized Persons Entry)	DCS-08	- ต้องมีมาตรการเฝ้าระวังและควบคุมที่ชัดเจนจุดเข้าและออก เช่น พื้นที่ให้บริการผู้ใช้บริการ หรืออื่นๆ ซึ่งบุคคลทั่วไปสามารถเข้าถึงได้ ในด้านข้อมูลควรแยกการเก็บข้อมูลและสิ่งอำนวยความสะดวกออกจากกันเพื่อป้องกันความผิดพลาดหรือสูญหายของข้อมูล
การอนุญาตเข้าถึงผู้ใช้งาน (User Access)	DCS-09	- ต้องมีมาตรการการควบคุมการเข้าถึงข้อมูลทรัพย์สินและส่วนที่เกี่ยวข้องด้านกายภาพ
4.2.7 การเข้ารหัสลับและการบริหารจัดการกุญแจรหัสลับ (Encryption & Key Management)		
สิทธิ์ถือครองกุญแจรหัสลับ (Entitlement)	EKM-01	- กุญแจรหัสลับ (Key) ต้องสามารถกำหนดบุคคลผู้รับผิดชอบได้ รวมถึงต้องมีการ

Control Area	Control ID	Control Notes
		กำหนดนโยบายบริหารจัดการกุญแจรหัสลับ
การสร้างกุญแจรหัสลับ (Key Generation)	EKM-02	- ต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเพื่อบริหารจัดการการเข้ารหัสลับสำหรับบริการที่ต้องใช้ระบบเพื่อสนับสนุนการเข้ารหัสลับข้อมูล (service's cryptosystem) โดยผู้ให้บริการต้องสื่อสารกับผู้ใช้บริการเพื่อตกลงให้สอดคล้องกับเงื่อนไขการให้บริการโดยยังคงปฏิบัติตามนโยบายและขั้นตอนปฏิบัติที่มีอยู่
การป้องกันข้อมูลสารสนเทศที่สำคัญ (Sensitive Data Protection)	EKM-03	- ต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเพื่อกำหนดรูปแบบการเข้ารหัสลับเพื่อเข้ารหัสข้อมูลในบริการให้สอดคล้องกับกฎหมาย แนวทางการกำกับดูแล แนวปฏิบัติ ภาระผูกพันอื่นๆ ที่เกี่ยวข้องกับการให้บริการ
การจัดเก็บและการเข้าถึงกุญแจรหัสลับ (Storage and Access)	EKM-04	- ควรใช้รูปแบบการเข้ารหัสที่เป็นมาตราฐานเปิด และเป็นที่ยอมรับ การเก็บรักษากุญแจเข้ารหัสลับต้องไม่เก็บในบริการคลาวน์แต่ควรเก็บไว้ที่ผู้ใช้บริการเอง หรือเก็บโดยผู้ให้บริการเก็บรักษากุญแจเข้ารหัสลับที่น่าเชื่อถือ การบริหารจัดการและการใช้งานกุญแจเข้ารหัสลับต้องได้รับการแยกหน้าที่ดูแลอย่างชัดเจน

Control Area	Control ID	Control Notes
4.2.8 การกำกับดูแลและการบริหารความเสี่ยง (Governance and Risk Management)		
การรักษาความปลอดภัยขั้นพื้นฐาน (Baseline Requirements)	GRM-01	- ต้องมีการกำหนดความต้องการการรักษาความปลอดภัยขั้นพื้นฐาน สำหรับการพัฒนาหรือจัดหาระบบงานสารสนเทศ ระบบที่องค์กรเป็นเจ้าของเองหรือองค์กรบริหารจัดการ ระบบทางกายภาพ เช่น อุปกรณ์ฮาร์ดแวร์ของระบบต่างๆ เป็นต้น หรือระบบเสมือน (virtual) เช่น VM Ware เป็นต้น แอพลิเคชันและโครงสร้างพื้นฐานของแอปพลิเคชันและส่วนประกอบต่างๆ ของเครือข่าย โดยการรักษาความปลอดภัยขั้นพื้นฐานที่จัดทำขึ้นนั้นต้องสอดคล้องกับข้อบังคับทางกฎหมาย กฎระเบียบและข้อสัญญาต่างๆ - ในกรณีที่ไม่สามารถปฏิบัติตามการรักษาความปลอดภัยขั้นพื้นฐานได้ก่อนการดำเนินการต้องได้รับการอนุมัติตามกระบวนการบริหารจัดการการเปลี่ยนแปลงก่อน เช่น ไม่สามารถปรับค่าของระบบให้เป็นไปตามค่าของการรักษาความปลอดภัยขั้นพื้นฐานเนื่องจากมีผลกระทบต่อการทำงานของโปรแกรม ก่อนการดำเนินการปรับค่าต้องขออนุมัติการละเว้นการปรับแต่งค่าเฉพาะข้อที่ไม่สามารถดำเนินการได้ตามค่าของการรักษาความปลอดภัยขั้นพื้นฐาน เป็นต้น - การกำหนดค่าของระบบต้องได้รับการตรวจประเมินอย่างน้อยปีละ 1 ครั้งหรือตามรอบระยะเวลาที่องค์กรกำหนด เพื่อตรวจสอบความสอดคล้องกับค่าของการรักษาความปลอดภัยขั้นพื้นฐาน

Control Area	Control ID	Control Notes
การประเมินความเสี่ยงโดยมุ่งเน้นความสำคัญของข้อมูล (Data Focus Risk Assessments)	GRM-02	- ต้องมีการดำเนินการประเมินความเสี่ยง การประเมินความเสี่ยงที่เกี่ยวข้องกับข้อมูลความต้องการการกำกับดูแลจะต้องดำเนินการในช่วงเวลาที่วางแผนไว้และจะต้องพิจารณาต่อไปนี้: - ความตระหนักในเรื่องการจัดเก็บและการส่งข้อมูลที่มีความละเอียดอ่อน (Sensitive) เช่น การจัดเก็บข้อมูลลงในฐานข้อมูล - การปฏิบัติตาม - ระยะเวลาการเก็บรักษาและการสิ้นสุดของชีวิตต้องการกำจัด - การส่งผ่านข้อมูลดังกล่าวบนระบบเครือข่าย app, หรือข้าม application เป็นต้น - การกำหนด retention periods การทำลายข้อมูลตาม retention periods - การแบ่งชั้นความลับของข้อมูล (Data classification) การป้องกันข้อมูลจากการเข้าถึง ใช้งาน ทำลาย โดยไม่ได้รับอนุญาต
การกำกับดูแลของผู้บังคับบัญชา (Management Oversight)	GRM-03	ผู้บังคับบัญชามีหน้าที่ความรับผิดชอบในการกำกับดูแลผู้ใต้บังคับบัญชาเพื่อให้มีความตระหนักปฏิบัติตามนโยบายและขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับงานของตนเอง

Control Area	Control ID	Control Notes
ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Management Program)	GRM-04	- ต้องจัดทำ ขออนุมัติและประกาศใช้งานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ผู้เกี่ยวข้องปฏิบัติตามระบบบริหารฯ โดยการปฏิบัติตามระบบบริหารฯ ครอบคลุมถึงมาตรการการจัดการ (เช่น มีนโยบายความมั่นคงปลอดภัยบังคับใช้งาน) มาตรการทางเทคนิค และมาตรการทางกายภาพ ทั้งนี้เพื่อป้องกันข้อมูลและทรัพย์สินสารสนเทศจากการสูญหาย การใช้ผิดวัตถุประสงค์ การเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูล การเปลี่ยนแปลงข้อมูล และการทำลายข้อมูลโดยไม่ได้รับอนุญาต ระบบบริหารฯ ต้องครอบคลุมในเรื่องหรือหัวข้อเหล่านี้ - การบริหารความเสี่ยง - นโยบายความมั่นคงปลอดภัย - โครงสร้างการจัดการความมั่นคงปลอดภัย - ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล - ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม - การบริหารจัดการด้านการสื่อสารและการดำเนินงาน - การควบคุมการเข้าถึง - การจัดหา พัฒนา และบำรุงรักษาระบบงานสารสนเทศ หมายเหตุ ระบบบริหารฯ ในเอกสารฉบับนี้เทียบเท่ากับคำว่า Information Security Management Program (ISMP)

Control Area	Control ID	Control Notes
การสนับสนุนและการให้ความสำคัญกับการรักษาความมั่นคงปลอดภัย (Support/ Involvement)	GRM-05	- ผู้บริหารและผู้บังคับบัญชาตามสายงานต้องมีการกำหนดทิศทางด้านความมั่นคงปลอดภัย (เช่นวัตถุประสงค์ เป้าหมาย เป็นต้น) มีการมอบหมายงาน และการกำกับดูแลให้เป็นไปตามทิศทางที่กำหนดไว้ - ผู้บริหารและผู้บังคับบัญชาตามสายงานมีการติดตาม ดำเนินการ สั่งการ และสนับสนุนให้เป็นไปตามทิศทางที่กำหนดไว้
การกำกับดูแลและการบริหารความเสี่ยงนโยบาย (Governance and Risk Management : Policy)	GRM-06	- นโยบายความมั่นคงปลอดภัยสารสนเทศ และขั้นตอนปฏิบัติที่เกี่ยวข้อง ต้องได้รับการจัดทำและพร้อมที่จะได้รับการทบทวนจากบุคคลที่มีส่วนเกี่ยวข้องและองค์กรภายนอกที่เกี่ยวข้อง อีกทั้งนโยบายความมั่นคงปลอดภัยสารสนเทศต้องรับการลงนามอนุมัติประกาศใช้งานโดยผู้บริหาร (หรือผู้บังคับบัญชาตามสายงาน) และต้องมีความสอดคล้องกับแผนกลยุทธทางธุรกิจ แผนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ รวมทั้งนโยบายต้องกำหนดบทบาทหน้าที่ความรับผิดชอบของผู้บริหารที่เกี่ยวข้องกับความมั่นความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจนด้วย
การกำกับดูแลและการบริหารความเสี่ยง : การบังคับใช้นโยบาย (Governance and Risk Management : Policy Enforcement)	GRM-07	- ต้องสร้างความตระหนักให้พนักงานทราบหรือไม่เกี่ยวกับขั้นตอนการลงโทษ หรือการดำเนินการเมื่อพบว่าพนักงานกระทำความผิด พร้อมทั้งกำหนดบทลงโทษสำหรับผู้ที่ละเมิดนโยบายและขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยที่กำหนดไว้
การกำกับดูแลและการบริหารความเสี่ยง (Governance and Risk Management Policy Impact on Risk Assessments)	GRM-08	- ผลการประเมินความเสี่ยงต้องมีเรื่องที่เกี่ยวกับนโยบายและขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยที่ไม่ทันสมัย เช่น ขั้นตอนปฏิบัติกำหนดเรื่องความมั่นคงปลอดภัยสำหรับการตั้งรหัสผ่านไว้ไม่แข็งแกร่งเพียงพอส่งผลให้เกิดความเสี่ยงในระดับสูงขึ้น เป็นต้น

Control Area	Control ID	Control Notes
การทบทวนนโยบายความมั่นคงปลอดภัย (Policy Reviews)	GRM-09	- ผู้บริหารขององค์กรต้องทบทวนนโยบายความมั่นคงปลอดภัยตามรอบระยะเวลาที่กำหนดไว้ เช่น ปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงกับองค์กร เพื่อให้นโยบายความมั่นคงปลอดภัยมีความสอดคล้องกับกลยุทธ์ด้านความมั่นคงปลอดภัยขององค์กร รวมถึงสอดคล้องกับกฎหมาย ระเบียบต่างๆที่องค์กรต้องปฏิบัติด้วย
การประเมินความเสี่ยง (Risk Assessments)	GRM-10	- ต้องมีประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้งหรือตามแผนที่กำหนด หรือทุกครั้งที่มีการเปลี่ยนระบบสารสนเทศ เพื่อกำหนดโอกาสและผลกระทบของความเสี่ยงทั้งหมดโดยใช้วิธีการเชิงปริมาณและคุณภาพ โดยที่โอกาสและผลกระทบของความเสี่ยงที่มีอยู่ธรรมชาติ (Inherent Risk) และความเสี่ยงที่เหลืออยู่ (Residual Risk) ต้องได้รับการระบุอย่างอิสระ
กรอบหรือวิธีการบริหารจัดการความเสี่ยง (Risk Management Framework)	GRM-11	- ต้องมีการกำหนดระดับความเสี่ยงที่ยอมรับได้ตามเกณฑ์ความเสี่ยงขององค์กร และความเสี่ยงต้องได้รับการบริหารจัดการเพื่อให้ระดับความเสี่ยงลดลงจนถึงระดับที่องค์กรยอมรับได้ การจัดทำกรอบหรือวิธีการบริหารจัดการความเสี่ยงในระดับองค์กรต้องดำเนินการโดยผู้ที่มีส่วนเกี่ยวข้อง
4.2.9 ทรัพยากรบุคคลล (Human Resources)		
การคืนทรัพย์สินขององค์กร (Asset Returns)	HRS-01	- ต้องจัดทำเอกสารคู่มือและข้อกำหนด และประกาศใช้งานแก่พนักงาน ลูกจ้าง ผู้ให้บริการภายนอกและผู้ที่เกี่ยวข้องอื่นๆ เมื่อสิ้นสุดหรือเปลี่ยนการจ้างงาน/สัญญาจ้าง/ข้อตกลงการจ้าง ในการคืนทรัพย์สินที่ตนเองถือครอง ในระยะเวลาที่กำหนดไว้เป็นลายลักษณ์อักษร

Control Area	Control ID	Control Notes
การคัดเลือกบุคลากร (Background Screening)	HRS-02	- มีกลไกการคัดเลือกบุคลากร เช่น การตรวจสอบคุณสมบัติและประวัติการทำงานของผู้ที่จะเข้ามาปฏิบัติงานหรือไม่ ทั้งในส่วนของพนักงาน ลูกจ้าง และผู้ให้บริการภายนอก พร้อมทั้งมี การตรวจสอบประวัติเพื่อวัดความเหมาะสมต่อชั้นความลับของข้อมูลที่จะอนุญาตให้เข้าถึงหรือไม่ ซึ่งอาจต้องตรวจสอบจากลายนิ้วมือโดยนำไปที่สถานีตำรวจ
เงื่อนไขและข้อตกลงการจ้างงาน (Employment Agreements)	HRS-03	- ก่อนการจ้างงานหรือเริ่มต้นปฏิบัติงาน มีการลงนามในสัญญาจ้างซึ่งประกอบด้วยเงื่อนไขและข้อตกลงต่างๆ ของการจ้างงาน หรือไม่ เงื่อนไขหรือข้อตกลงครอบคลุมถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ
การสิ้นสุดการจ้างงาน (Employment Termination)	HRS-04	- มีการระบุหน้าทีและความรับผิดชอบเมื่อสิ้นสุดหรือเปลี่ยนการจ้างงานไว้อย่างเป็นลายลักษณ์อักษร (ทั้งในส่วนของพนักงาน ลูกจ้าง และผู้ให้บริการภายนอก) มีการสื่อสารให้บุคลากรทราบ มีการมอบหมายให้ปฏิบัติตามนั้น
การบริหารจัดการอุปรณ์พกพา (Mobile Device Management)	HRS-05	- ต้องมีการจัดทำ ขออนุมัติ ประกาศใช้งานนโยบายและขั้นตอนปฏิบัติที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงของการอนุญาตให้ใช้งานอุปกรณ์เคลื่อนที่ในการเข้าถึงทรัพยากรต่างๆขององค์กร นอกจากการจัดทำนโยบายขั้นตอนปฏิบัติแล้ว องค์กรอาจพิจารณาการควบคุมเพิ่มเติม เช่น การจัดทำและให้ผู้เกี่ยวข้องลงนามเอกสารยอมรับ ปฏิบัติตามนโยบายขององค์กร (AUP) การอบรมสร้างความตระหนักเรื่องการใช้งานอุปกรณ์เคลื่อนที่ให้ปลอดภัย การเฝ้าระวังการใช้งานอุปกรณ์ การตั้งรหัสผ่านที่แข็งแกรงมากขึ้น การควบคุมการเข้าถึง เป็นต้น

Control Area	Control ID	Control Notes
สัญญาการไม่เปิดเผยความลับ (Non-Disclosure Agreements)	HRS-06	- มีการระบุความจำเป็นในการทำสัญญาไม่เปิดเผยความลับระหว่างองค์กรกับผู้รับจ้าง (ซึ่งแสดงว่ามีความเสี่ยงของการเปิดเผยข้อมูลขององค์กรโดยไม่ได้รับอนุญาต) มีการทำสัญญาการไม่เปิดเผยความลับ - มีการทบทวนและปรับปรุงข้อความที่เกี่ยวข้องกับการไม่เปิดเผยความลับในสัญญาจ้าง เช่น อย่างน้อยปีละ 1 ครั้ง
หน้าที่ความรับผิดชอบ (Roles / Responsibilities)	HRS-07	- ต้องมีการกำหนดบทบาทและหน้าที่ความรับผิดชอบในส่วนที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของพนักงาน ลูกจ้าง ผู้ให้บริการภายนอกและผู้ที่เกี่ยวข้องอื่นๆไว้อย่างเป็นลายลักษณ์อักษร
การใช้เทคโนโลยีขององค์กรอย่างเหมาะสม (Technology Acceptable Use)	HRS-08	- นโยบายและขั้นตอนปฏิบัติต้องได้รับการจัดทำ และรองรับกับกระบวนการทางธุระกิจ และการดำเนินการทางเทคนิค เพื่อกำหนดงบประมาณและเงื่อนไขสำหรับการอนุญาตใช้งานอุปกรณ์ต่างๆที่องค์กรเป็นเจ้าของ หรือบริหารจัดการการใช้งานอุปกรณ์ (เช่น สถานที่ทำงาน เครื่องคอมพิวเตอร์ อุปกรณ์พกพา) และเครือข่ายสารสนเทศ และส่วนประกอบของระบบ - เพิ่มเติม การกำหนดงบประมาณและเงื่อนไขสำหรับการอนุญาตใช้งานอุปกรณ์พกพาส่วนบุคคล และที่เกี่ยวข้องการการใช้งานแอพพลิเคชันที่เข้าถึงการใช้ทรัพยากรขององค์กร (เช่น BYOD) ต้องได้รับการพิจารณาจากบริษัทอย่างเหมาะสม

Control Area	Control ID	Control Notes
การอบรม/สร้างความตระหนัก (Training / Awareness)	HRS-09	- มีการจัดทำแผนการอบรมเพื่อสร้างความตระหนักและให้ความรู้แก่พนักงาน ลูกจ้าง ผู้ให้บริการภายนอก หรือผู้ที่เกี่ยวข้องอื่นๆ เพื่อสร้างความตระหนักมีการอบรมในส่วนของนโยบายและขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัย รวมทั้งในส่วนที่เกี่ยวข้องกับการปฏิบัติงาน อย่างสม่ำเสมอเพื่อทบทวนในประเด็นใหม่ๆ เพิ่มเติม
ทรัพยากรบุคคลล : ความรับผิดชอบของผู้ใช้งาน (Human Resources :User Responsibility)	HRS-10	- ต้องมีการสร้างความตระหนักให้กับผู้ใช้งานในเรื่องของการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยที่กำหนดไว้ เช่น ความตระหนักในเรื่องของการปฏิบัติงานในพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย
ทรัพยากรบุคคล : (Human Resources : Workspace)	HRS-11	- ต้องมีการกำหนดนโยบายและขั้นตอนปฏิบัติเพื่อป้องกันเอกสารสำคัญในขณะที่ไม่มีผู้ดูแล และมีนโยบายบังคับการ logout ออกจากระบบโดยอัตโนมัติหลังจากที่ไม่มีการใช้งานมาช่วงระยะเวลาหนึ่ง เช่น 15 นาที
4.2.10 การบริหารจัดการตัวตนและการเข้าถึง (Identity & Access Management)		
การเข้าถึงเครื่องมือตรวจสอบ (Audit Tools Access)	IAM-01	- การเข้าถึงและการใช้งานเครื่องมือสำหรับการตรวจสอบ (Audit Tools) ซึ่งมีการเชื่อมต่อกับระบบข้อมูลขององค์กรต้องมีการแยกออกจากระบบขององค์กรและจำกัดการเข้าถึงอย่างเหมาะสมเพื่อป้องกันกันการเข้าถึงโดยไม่ได้รับอนุญาต (Compromise) และป้องกันการนำข้อมูลล็อกไปใช้งานในทางที่ไม่ถูกต้อง (Misuse)
การบริหารจัดการข้อมูลประจำตัวของบัญชีผู้ใช้งาน (Credential Lifecycle / Provision Management)	IAM-02	- ต้องมีการจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติ รวมทั้งประยุกต์ใช้เชิงเทคนิค สำหรับการควบคุมการเข้าถึงจากผู้ใช้บริการมายัง

Control Area	Control ID	Control Notes
		องค์ประกอบของระบบและข้อมูลของบริการ ซึ่งเน้นหนักในส่วนของการให้บริการ โดยควรคำนึงถึงประเด็นต่อไปนี้ • กำหนดบทบาท และหน้าที่สำหรับการจัดเตรียม และการถอดถอนบัญชีผู้ใช้งาน โดยต้องกำหนดสิทธิ์ให้น้อยที่สุด • เงื่อนไขการพิจารณาระดับความสำคัญจำเป็นในการใช้รูปแบบการยืนยันตัวตนจากหลายแหล่ง(multi-factor authentication) ในการให้บริการ • กำหนดรูปแบบการจัดแบ่งการเข้าถึงให้เหมาะสมตามโครงสร้างการให้บริการเช่าใช้ร่วมกัน (multi-tenant architectures) • กำหนดกระบวนตรวจสอบการยืนยันตัวตนในระดับ API ให้มีความน่าเชื่อถืออย่างมั่นคงปลอดภัย (เช่น SSO หรือ Federation) • กำหนดการบริหารจัดการวงจรชีวิตของข้อมูลประจำตัวของบัญชีผู้ใช้งาน (Account credential lifecycle management) • กำหนดให้ข้อมูลประจำตัวของบัญชีผู้ใช้งานต้องถูกเรียกใช้ได้น้อยที่สุดเท่าที่จำเป็น • กำหนดรูปแบบมาตรการด้านความมั่นคงปลอดภัยที่เหมาะสมสำหรับกระบวนการยืนยันตัวตน การกำหนดสิทธิ์ และการบันทึกการใช้งาน (Authentication, authorization, and accounting (AAA)) เช่น การใช้การเข้ารหัสที่แข็งแกร่งของ multi-factor authentication , การกำหนดระยะเวลาการใช้งาน หรือการไม่แชร์รหัสผ่าน เป็นต้น

Control Area	Control ID	Control Notes
		• กำหนดรูปแบบกระบวนการยืนยันตัวตน การกำหนดสิทธิ์ และการบันทึกการใช้งาน(Authentication, authorization, and accounting (AAA)) ที่เหมาะสมสำหรับกรณีที่ผู้ใช้บริการต้องการเสริมในบริการ • กำหนดเงื่อนไข กฎหมาย ระเบียบที่จำเป็นต้องปฏิบัติตามให้สอดคล้อง
การวินิจฉัยหรือเข้าถึงระบบผ่านช่องทางเฉพาะ (Diagnostic / Configuration Ports Access)	IAM-03	- ต้องควบคุมการเข้าถึงผู้ใช้บริการผ่าน Diagnostic/Configuration ports อย่างเหมาะสม โดยต้องกำหนดให้มีการอนุมัติก่อนการดำเนินการเข้าถึงเสมอ
นโยบายและขั้นตอนปฏิบัติการระบุตัวตนและการเข้าถึง (Policies and Procedures)	IAM-04	- ต้องมีการจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติสำหรับการจัดเก็บและบริหารจัดการข้อมูลอัตลักษณ์ (Identity) ของผู้ที่มีสิทธิ์เข้าถึงโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการกำหนดระดับสิทธิ์การเข้าถึงระบบ นอกจากนี้นโยบายดังกล่าวต้องระบุถึงการควบคุมการเข้าถึงทรัพยากรทางเครือข่ายตามอัตลักษณ์ (Identity) ที่กำหนดไว้ด้วย
การแบ่งแยกหน้าที่ (Segregation of Duties)	IAM-05	- ต้องมีการจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติการเข้าถึงของผู้ใช้งาน เพื่อจำกัดการเข้าถึงของผู้ใช้งานตามบทบาทหน้าที่ที่ได้กำหนดไว้
การจำกัดการเข้าถึงข้อมูลทรัพย์สินทางปัญญา (Source Code Access Restriction)	IAM-06	- ต้องมีการจำกัดการเข้าถึง แอปพลิเคชัน โปรแกรม ซอร์สโค้ด หรือสิ่งอื่นใดที่เป็นทรัพย์สินทางปัญญา รวมถึงการใช้งานซอฟต์แวร์ลิขสิทธิ์ต่างๆ ตามหลักการการให้สิทธิ์น้อยที่สุดตามหน้าที่ความรับผิดชอบตามที่กำหนดไว้ในนโยบายการเข้าถึงของผู้ใช้
การจำกัดสิทธิ์การเข้าถึงโดยผู้ให้บริการภายนอก (Third Party Access)	IAM-07	- ต้องระบุ ประเมิน และจัดลำดับความเสี่ยงที่เกิดจากการเข้าถึงข้อมูล และระบบสำคัญทางธุรกิจจากผู้ให้บริการภายนอก โดยการใช้มาตรการด้านความมั่นคง

Control Area	Control ID	Control Notes
		ปลอดภัยอย่างเหมาะสมเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
การกำหนดแหล่งที่มาที่น่าเชื่อถือ (Trusted Sources)	IAM-08	- ต้องมีการจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติสำหรับการบริหารจัดการการยืนยันตัวตน ให้ครอบคลุมการจัดเก็บข้อมูลบ่งชี้ตัวตน และกระบวนการพิสูจน์ตัวตน เพื่อให้มั่นใจว่าการเข้าถึงมีความถูกต้องครบถ้วนตามเงื่อนไขที่กำหนดในการให้บริการ
การยืนยันตัวตนผู้ใช้งาน (User Access Authorization)	IAM-09	- การจัดเตรียมให้สิทธิในการการเข้าถึงระบบต่างๆ ให้แก่ผู้ใช้งาน (เช่น พนักงาน พนักงานสัญญาจ้าง ผู้ใช้บริการระบบคลาวด์ คู่ค้าทางธุรกิจ ผู้ให้บริการภายนอก เป็นต้น) ต้องได้รับอนุญาตจากผู้บริหารก่อนที่จะสร้างบัญชีรายชื่อให้แก่ผู้ใช้งานโดยต้องกำหนดสิทธิตามนโยบาย ขั้นตอนปฏิบัติ - ในกรณีที่ข้อมูลของผู้ใช้งานถูกใช้เป็นส่วนหนึ่งของบริการ ผู้ใช้บริการสามารถร้องขอให้ผู้ให้บริการแจ้งข้อมูลการให้สิทธิการเข้าถึงแก่ผู้ใช้งานให้แก่ผู้ใช้งานได้รับทราบ เนื่องจากผู้ใช้งานมีหน้าที่ร่วมรับผิดชอบต่อการนำมาตรการควบคุมนำมาใช้งาน
การทบทวนสิทธิ์การเข้าถึง (User Access Reviews)	IAM-10	- การเข้าถึงระบบของผู้ใช้งานต้องได้รับการทบทวนและตรวจสอบสิทธิการเข้าถึงอย่างสม่ำเสมอตามระยะเวลาที่กำหนด โดยผู้บริหารหรือผู้รับผิดชอบต้องสนับสนุนหลักฐานเพื่อแสดงให้เห็นว่าองค์กรปฏิบัติตามกฎการให้สิทธิผู้ใช้งานน้อยที่สุดเพื่อให้สามารถปฏิบัติงานได้ตามหน้าที่ ในกรณีที่พบการละเมิดการเข้าถึง ต้องดำเนินการแก้ไขตามนโยบายเข้าถึงของผู้ใช้งาน

Control Area	Control ID	Control Notes
การยกเลิกหรือถอดถอนสิทธิ์การเข้าถึง (User Access Revocation)	IAM-11	- ต้องมีการดำเนินการถอดถอนสิทธิ์การเข้าถึงระบบต่างๆ ของผู้ใช้งานตามระยะเวลาที่เหมาะสม - การดำเนินการถอดถอนสิทธิ์ต้องปฏิบัติตามแนวทางที่ระบุไว้ในนโยบายและขั้นตอนปฏิบัติและการดำเนินการถอดถอนสิทธิ์ตามการเปลี่ยนแปลงสถานะของผู้ใช้งาน (เช่น สิ้นสุดการเป็นพนักงานหรือสิ้นสุดความสัมพันธ์ทางธุรกิจ มีการเปลี่ยนงานหรือโยกย้ายงาน เป็นต้น) - ในกรณีที่ข้อมูลของผู้ใช้งานถูกใช้เป็นส่วนหนึ่งของบริการ ผู้ใช้บริการสามารถร้องขอให้ผู้ให้บริการแจ้งข้อมูลการเปลี่ยนสิทธิการเข้าถึงแก่ผู้ใช้งานให้แก่ผู้ใช้งานได้รับทราบเนื่องจากผู้ใช้งานมีหน้าที่ร่วมรับผิดชอบต่อการนำมาตรการควบคุมนำมาใช้งาน

Control Area	Control ID	Control Notes
การบริหารจัดการหนังสือรับรองของผู้ใช้งาน (User ID Credentials)	IAM-12	- ข้อมูลประจำตัวของบัญชีผู้ใช้งานจำเป็นต้องได้รับการป้องกันอย่างเคร่งครัด การเข้าถึงเพื่อใช้งานในกระบวนการยืนยันตัวตนจำเป็นต้องกำหนด นโยบาย และขั้นตอนปฏิบัติอย่างชัดเจน โดยต้องระบุประเด็นต่อไปนี้ • กำหนดกระบวนตรวจสอบการยืนยันตัวตนในระดับ API ให้มีความน่าเชื่อถืออย่างมั่นคงปลอดภัย (เช่น SSO หรือ Federation) • กำหนดการบริหารจัดการวงจรชีวิตของข้อมูลประจำตัวของบัญชีผู้ใช้งาน (Account credential lifecycle management) • กำหนดให้ข้อมูลประจำตัวของบัญชีผู้ใช้งานต้องถูกเรียกใช้ได้น้อยที่สุดเท่าที่จำเป็น • กำหนดรูปแบบกระบวนการยืนยันตัวตน การกำหนดสิทธิ์ และการบันทึกการใช้งาน(Authentication, authorization, and accounting (AAA)) ที่เหมาะสมสำหรับกรณีที่ผู้ใช้บริการต้องการเสริมในบริการ
การจำกัดการเข้าถึงผ่านโปรแกรมช่วยเหลือ (Utility Programs Access)	IAM-13	- ต้องมีการจำกัดการใช้งานโปรแกรมยูทิลิตี้ที่มีความสามารถละเมิดมาตรการการควบคุม(Control) ของระบบ เครื่องคอมพิวเตอร์เสมือน(VM) ระบบเครือข่าย และแอปพลิเคชัน

Control Area	Control ID	Control Notes
4.2.11 ความมั่นคงปลอดภัยระบบโครงสร้างพื้นฐานและระบบเสมือน (Infrastructure & Virtualization Security)		
การป้องกันภัยคุกคามและการเก็บข้อมูลล็อคตรวจสอบ (Audit Logging / Intrusion Detection)	IVS-01	- ผู้ให้บริการต้องจัดเตรียมระบบที่สนับสนุนการตรวจสอบล็อก(Audit Log) ที่สอดคล้องกับ กฎหมาย และระเบียบที่กำหนดในเงื่อนไขการให้บริการ และมีระบบตรวจจับการบุกรุก(Intrusion detection) ที่มีประสิทธิ์ภาพ ที่สามารถสนับสนุนการสืบค้นข้อมูลเชิงลึก (forensic investigative)
การแจ้งเตือนเหตุการณ์เปลี่ยนแปลง (Change Detection)	IVS-02	- ผู้ให้บริการต้องสร้างความมั่นใจได้ว่า Virtual Machine ที่ให้บริการมีความถูกต้องครบถ้วนตลอดเวลา ต้องมีการบันทึกล็อกของกิจกรรมหากมีการปรับปรุงเปลี่ยนแปลงใดๆ กับ Virtual Machine โดยบริการต้องมีการแจ้งเตือนให้ผู้ใช้บริการทราบผ่านช่องทางอิเล็กทรอนิกส์ เช่น Portal หรือ e-mail เป็นต้น
การอ้างอิงเวลาที่สอดคล้องกัน (Clock Synchronization)	IVS-03	- องค์ประกอบของโครงสร้างพื้นฐานด้านระบบ Virtualization ต้องได้รับการเทียบเวลาที่เป็นมาตรฐานเดียวกัน และมีความน่าเชื่อถือ
เอกสารแสดงรายละเอียดความมั่นคงปลอดภัยระบบสารสนเทศ (Information System Documentation)	IVS-04	- การประเมินปริมาณการใช้งานทรัพยากรของระบบต้องได้รับการตรวจวัด และติดตามอย่างต่อเนื่องให้สอดคล้องกับสัญญา ข้อตกลง กฎหมาย กฎระเบียบของการให้บริการ การประเมินปริมาณการใช้งานทรัพยากรมีความจำเป็นเพื่อเป็นการลดความเสี่ยงต่อการหยุดชะงักของการให้บริการ
การบริหารจัดการพื้นฐานและช่องโหว่ (Management - Vulnerability Management)	IVS-05	- ต้องประยุกต์ใช้เครื่องมือ หรือระบบที่ใช้สำหรับการบริหารจัดการ ตรวจสอบช่องโหว่ของระบบ โดยต้องเป็นเครื่องมือที่เข้าใจและทำงานเข้ากันได้กับเทคโนโลยี

Control Area	Control ID	Control Notes
		Virtualization
ความมั่นคงปลอดภัยสารสนเทศของเครือข่าย (Network Security)	IVS-06	ระบบเครือข่ายของระบบ Virtualization ต้องได้รับการออกแบบและตั้งค่าเพื่อควบคุม และเฝ้าระวังระหว่างเครือข่ายสำคัญและไม่สำคัญ (trusted and untrusted connections) ด้วยมาตราการที่เหมาะสม เช่น Firewall โดยการควบคุม(Firewall rules) service, protocol, port ต้องได้รับการอนุมัติเป็นลายลักษณ์อักษร และต้องได้รับการทบทวนการควบคุมทุกปี
การเสริมสร้างความมั่นคงปลอดภัยให้แก่ระบบปฏิบัติการ และ การควบคุมพื้นฐาน (OS Hardening and Base Controls)	IVS-07	- ระบบปฏิบัติการในระบบ Virtualization ต้องได้รับการเสริมสร้างความแข็งแกร่งโดยอ้างอิงแหล่งข้อมูลที่น่าเชื่อถือในการเสริมสร้างความแข็งแกร่ง
การแบ่งแยกการระหว่าง Production และ non-Production (การแยก Production / Non-Production)	IVS-08	- ระบบ Production และระบบ non-production ต้องได้รับการแยกกันด้วยมาตรการที่เหมาะสมเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
การแบ่งกลุ่มในระบบ Virtualization (Segmentation)	IVS-09	- การถือครองร่วมกัน (Mullti-tenant) ต้องได้รับการจัดแบ่งอย่างเหมาะสมทั้ง Physical และ Virtual
การป้องกันข้อมูลในกระบวนการ vMotion (VM Security - vMotion Data Protection)	IVS-10	- กระบวนการ vMotion ต้องได้รับการควบคุม และต้องเข้ารหัสลับช่องทางการเชื่อมต่อ
การเสริมสร้างความแข็งแกร่งให้แก่ระบบ Hypervisor (VMM Security - Hypervisor Hardening)	IVS-11	ระบบ Hypervisor ต้องได้รับการเสริมสร้างความแข็งแกร่งโดยอ้างอิงแหล่งข้อมูลที่น่าเชื่อถือในการเสริมสร้างความแข็งแกร่ง
การรักษาความมั่นคงปลอดภัยสำหรับการเชื่อมโยงเครือข่ายไร้สาย (Wireless Security)	IVS-12	- ต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเพื่อการรักษาความมั่นคงปลอดภัยสำหรับการเชื่อมโยงเครือข่ายไร้สาย โดยประกอบด้วยประเด็นต่อไปนี้

Control Area	Control ID	Control Notes
		1. การใช้ Firewall ในการควบคุมการเข้าถึงเครือข่าย 2. การตั้งค่าการเข้ารหัสของการเชื่อมต่อเครื่อข่ายไร้สายที่มีความมั่นคงปลอดภัย 3. กำหนดแนวทางการป้องกัน และตรวจสอบการปลอมแปลงเครือข่ายไร้สาย (Rouge)
โครงสร้างความมั่นคงปลอดภัยของสถาปัตยกรรมเครือข่าย (Network Architecture)	IVS-13	- โครงสร้างสถาปัตยกรรมเครือข่ายต้องได้รับการออกแบบเพื่อกำหนดมาตรการควบคุมอย่างเหมาะสมสำหรับการการป้องกันการโจมตีในเครือข่ายสำคัญ เช่น MAC spoofing, ARP poisoning, DDoS เป็นต้น
4.2.12 การถ่ายโอนและการทำงานร่วมกันของส่วนติดต่อเพื่อพัฒนาโปรแกรม (Interoperability & Portability)		
การทำงานร่วมกันของส่วนติดต่อเพื่อพัฒนาโปรแกรม (APIs)	IPY-01	- ผู้ให้บริการต้องใช้งาน API ที่มีการใช้งานกันแพร่หลายเพื่อให้มั่นใจว่า API สามารถทำงานร่วมกันระหว่างส่วนประกอบต่างๆและเพื่อความสะดวกในการโยกย้ายแอปพิลเคชัน
การร้องขอข้อมูล (Data Request)	IPY-02	- ข้อมูลที่มีโครงสร้างและไม่มีโครงสร้างต้องสามารถส่งให้ผู้ใช้บริการได้ในรูปแบบมาตรฐานตามการร้องขอของผู้ใช้บริการ (เช่น .doc, .xls, .pdf, logs เป็นต้น)
นโยบายและกฎหมาย (Policy & Legal)	IPY-03	- นโยบาย ขั้นตอนปฏิบัติ และข้อตกลงที่จัดทำร่วมกัน และ/หรือ ข้อตกลงต่างๆ ต้องได้รับการจัดทำเพื่อกำหนดข้อตกลงที่ชัดเจนในการใช้ API สำหรับการเชื่อมโยงข้อมูลของผู้ใช้บริการเพื่อให้เกิดความเชื่อมั่นในการรักษาความถูกต้องครบถ้วนของข้อมูล

Control Area	Control ID	Control Notes
มาตรฐานการเชื่อมต่อระหว่างระบบเครือข่าย Standardized Network Protocols	IPY-04	- ผู้ให้บริการต้องใช้โปรโตคอลของระบบเครือข่ายที่เป็นมาตรฐานและมีความมั่นคงปลอดภัยสำหรับการนำเข้าและส่งออกข้อมูล และใช้สำหรับบริหารจัดการบริการ เช่น การส่งข้อมูลสำหรับพิสูจน์ตัวตนต้องไม่ส่งข้อมูลแบบ Clear text เป็นต้น และต้องมีการจัดทำเอกสารรายละเอียดมาตรฐานของโปรโตคอลทางเครือข่ายที่มีการใช้งานกับระบบอื่นๆ และการใช้งานข้ามระบบ (Interoperability & Portability) เพื่อจัดส่งให้ผู้ใช้งานตามที่ร้องขอ
การเชื่อมต่อระหว่างระบบเสมือน (Virtualization)	IPY-05	- ผู้ให้บริการต้องใช้รูปแบบแพลตฟอร์มการทำงานแบบเสมือนที่ได้รับการยอมรับและรูปแบบการทำงานแบบเสมือนที่เป็นมาตรฐาน (เช่น OVF) เพื่อให้สามารถนำข้อมูลไปใช้กับระบบอื่นได้ และต้องจัดทำเอกสารให้กับผู้ใช้บริการตรวจสอบหากมีการปรับแต่งค่าใดๆ บน Hypervisor
4.2.13 ความมั่นคงปลอดภัยบนอุปกรณ์เคลื่อนที่ (Mobile Security)		
การป้องกันมัลแวร์ (Anti-Malware)	MOS-01	- ต้องมีการให้ความเกี่ยวกับการป้องกันมัลแวร์โดยเฉพาะบนการป้องกันมัลแวร์บนอุปกรณ์เคลื่อนที่ไว้เป็นส่วนหนึ่งในการอบรมสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการ
แอปพลิเคชันสโตร์ (Application Stores)	MOS-02	- จัดทำเอกสารระบุรายการแอปพลิเคชันสโตร์ซึ่งได้รับการอนุมัติให้สามารถติดตั้งลงบนอุปกรณ์เคลื่อนที่ที่สามารถเข้าถึงหรือบันทึกข้อมูลขององค์กรได้
การอนุมัติใช้งานแอปพลิเคชัน (Mobile Security : Approved Applications	MOS-03	- องค์กรต้องมีการจัดทำนโยบายห้ามติดตั้งใช้งานแอปพลิเคชันที่ไม่ผ่านการอนุมัติหรือแอปพลิเคชันที่ผ่านการอนุมัติแล้วแต่ไม่อยู่ในแอปพลิเคชันสโตว์ที่ได้รับอนุญาต

Control Area	Control ID	Control Notes
การอนุมัติซอฟต์แวร์สำหรับอุปกรณ์ BYOD (Approved Software for BYOD)	MOS-04	- ต้องมีการจัดทำนโยบาย BYOD โดยระบุไว้อย่างชัดเจนถึงการอนุญาตให้ผู้ใช้งาน BYOD สามารถใช้งาน/ติดตั้ง แอปพลิเคชัน แอปพลิเคชันสโตว์ ส่วนขยายของแอปพลิเคชันและส่วนเพิ่มเติม (Plug-in) เฉพาะรายการที่ผ่านการอนุมัติแล้วเท่านั้น และต้องมีการจัดการอบรมสร้างความตระหนักถึงนโยบาย BYOD ดังกล่าวให้แก่ผู้ใช้งาน
การอบรมสร้างความตระหนักด้านความมั่นคงปลอดภัยการใช้อุปกรณ์เคลื่อนที่ (Awareness and Training)	MOS-05	- ต้องจัดทำและประกาศใช้งาน นโยบายการใช้งานอุปกรณ์เคลื่อนที่โดยในนโยบายต้องมีการระบุคำนิยามของอุปกรณ์เคลื่อนที่และการยอมรับการใช้งานอุปกรณ์เคลื่อนที่ และความต้องการสำหรับอุปกรณ์เคลื่อนที่ทั้งหมด - ผู้ให้บริการต้องสื่อสารนโยบายและความต้องการดังกล่าวผ่านการอบรมสร้างความตระหนักให้แก่ผู้ใช้งานรับทราบ
การคัดเลือกอุปกรณ์สำหรับการใช้บริการคลาวน์ (Cloud Based Services)	MOS-06	- ต้องมีการขออนุมัติใช้งานบริการคลาวด์ในอุปกรณ์เคลื่อนที่หรือ BYOD
ความเข้ากันได้ของแอปพลิเคชัน (Compatibility)	MOS-07	- องค์กรต้องมีการจัดทำเอกสารกระบวนการตรวจสอบเพื่อทดสอบความเข้ากันได้ของอุปกรณ์เคลื่อนที่ ระบบปฏิบัติการ และแอปพลิเคชัน
การคัดกรองเครื่องมือที่เหมาะสมสำหรับการใช้งาน (Device Eligibility)	MOS-08	- นโยบาย BYOD ต้องกำหนดคุณสมบัติที่เหมาะสมของอุปกรณ์ที่จะอนุญาตให้ใช้งาน
บัญชีรายการอุปกรณ์ (Device Inventory)	MOS-09	- ต้องจัดทำ จัดเก็บ และบำรุงรักษาบัญชีรายการอุปกรณ์เคลื่อนที่ซึ่งมีการเข้าถึงและจัดเก็บข้อมูลขององค์กร - บัญชีรายการอุปกรณ์ต้องมีการบันทึกรายละเอียดของอุปกรณ์ และรวมถึงการเปลี่ยนแปลงสถานะของอุปกรณ์ (เช่น เปลี่ยนระบบปฏิบัติการ หรือโปรแกรมแก้ไขช่องโหว่ สถานะสูญหายหรือสถานะยกเลิกการใช้งาน ชื่อเจ้าของอุปกรณ์)
การบริหารจัดการอุปกรณ์เคลื่อนที่ (Device Management)	MOS-10	- ต้องติดตั้ง และใช้งานระบบบริหารจัดการอุปกรณ์เคลื่อนที่แบบรวมศูนย์ (Mobile

Control Area	Control ID	Control Notes
		Device Management)
การเข้ารหัสลับข้อมูลบนอุปกรณ์เคลื่อนที่ (Encryption)	MOS-11	- นโยบายการใช้งานอุปกรณ์เคลื่อนที่ต้องกำหนดให้มีการเข้ารหัสข้อมูลทั้งหมดหรือเฉพาะข้อมูลสำคัญบนอุปกรณ์และองค์กรต้องบังคับการเข้ารหัสตามนโยบายข้างต้นผ่านการควบคุมด้วยเทคโนโลยี
การป้องกันและแจ้งเตือนการละเมิดสิทธิ์ของระบบปฏิบัติการอุปกรณ์เคลื่อนที่ (Jailbreaking and Rooting)	MOS-12	- นโยบาย Mobile Device ต้องกำหนดไม่ให้ผู้ใช้งานละเมิดระบบควบคุมภายในอุปกรณ์เคลื่อนที่ (เช่น การ Jailbreak หรือ root) โดยต้องกำหนดมาตรการการตรวจสอบและป้องกันที่ปฏิบัติได้ หรือใช้ระบบ centralized device management system ในการควบคุม
กฎระเบียบด้านความมั่นคงปลอดภัยอุปกรณ์เคลื่อนที่ (Legal)	MOS-13	- นโยบาย BYOD ต้องมีการกล่าวถึงการยอมรับในเงื่อนไขด้านกฎหมายต่อข้อมูลขององค์กรที่อยู่ในอุปกรณ์ BYOD รวมทั้งต้องกล่าวถึงการยอมรับในเงื่อนไขที่จะถูกลบข้อมูลส่วนตัวหากเกิดกรณีที่ต้องถูกล้างข้อมูลในอุปกรณ์ (Wipe Device)
มาตรการกำหนดการล็อคหน้าจอ (Lockout Screen)	MOS-14	- อุปกรณ์เคลื่อนทีหรืออุปกรณ์ BYOD ต้องได้รับการปรับค่าให้ Lock Screen อย่างอัตโนมัติ และกำหนดมีการตั้งค่าทางเทคนิคเพื่อบังคับให้มีการ Lock Screen โดยอัตโนมัติ
ระบบปฏิบัติการ (Operating Systems)	MOS-15	- การเปลี่ยนระบบปฏิบัติการ การติดตั้งโปรแกรมแก้ไขช่องโหว่ และ/หรือแอปพลิเคชันของอุปกรณ์เคลื่อนที่ต้องดำเนินการตามขั้นตอนการบริหารจัดการการเปลี่ยนแปลง (change management processes) ขององค์กร

Control Area	Control ID	Control Notes
รหัสผ่าน (Mobile Security : Passwords)	MOS-16	- ต้องจัดทำและประกาศใช้งาน นโยบายการกำหนดรหัสผ่าน (Password policies) สำหรับอุปกรณ์เคลื่อนที่ (Mobile device policy) และบังคับใช้งานผ่านการควบคุมทางเทคนิคโดยมีผลกับอุปกรณ์เคลื่อนที่ (Mobile device policy) ขององค์กรรวมถึงอุปกรณ์ BYOD และต้องห้ามเปลี่ยนความยาวของรหัสผ่าน/PIN รวมถึงต้องใช้รหัสผ่านในการเข้าถึงอุปกรณ์ทุกครั้ง
ความมั่นคงปลอดภัยบนโมบาย : นโยบาย (Mobile Security : Policy)	MOS-17	นโยบายสำหรับอุปกรณ์เคลื่อนที่ (Mobile device policy) ต้องกำหนดให้ผู้ใช้งาน BYOD ต้องดำเนินการสำรองข้อมูล โดยห้ามใช้งาน application stores ที่ไม่ได้รับอนุญาต และต้องติดตั้งซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดีที่องค์กรกำหนด
การลบล้างข้อมูลจากระยะไกล (Remote Wipe)	MOS-18	อุปกรณ์เคลื่อนที่ (Mobile devices) ทั้งหมด BYOD ที่องค์กรอนุญาตให้ใช้งาน ผู้ใช้งานต้องอนุญาตให้องค์กรสามารถล้างข้อมูลบนอุปกรณ์เหล่านั้นได้จากระยะไกล (Remote Wipe)
การติดตั้งโปรแกรมแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัย (Security Patches)	MOS-19	- ก่อนการเข้าถึงระบบเครือข่ายขององค์กรอุปกรณ์เคลื่อนที่ (Mobile devices) ต้องได้รับการติดตั้งโปรแกรมแก้ไขช่องโหว่ (Patch) ล่าสุดที่องค์กรกำหนด
ผู้ใช้งาน (Users)	MOS-20	นโยบาย BYOD ต้องมีการกำหนดระบบและเซิร์ฟเวอร์ที่อนุญาตให้ใช้งานหรือเข้าถึงไว้อย่างชัดเจน

Control Area	Control ID	Control Notes
4.2.14 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย การสืบสวนและกู้ข้อมูลอิเล็กทรอนิกส์บนระบบคลาวน์ (Security Incident Management, E-Discovery & Cloud Forensics)		
การซ่อมบำรุงรายชื่อหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Contact / Authority Maintenance)	SEF-01	- ต้องมีการจัดทำ ปรับปรุง และดูแลรักษา ช่องทางการติดต่อกับหน่วยงานด้านกฎหมาย หน่วยงานที่มีอำนาจในการบังคับใช้กฎหมายระดับประเทศและท้องถิ่น รวมถึงหน่วยงานอื่นที่มีอำนาจตัดสินคดีความ หรือหน่วยงานที่เกี่ยวข้องกับกฎหมายต่างๆ ให้ทันสมัย เพื่อให้สามารถนำมาใช้ในการติดต่อหน่วยงานที่เกี่ยวข้องได้อย่างรวดเร็วเมื่อต้องมีการตรวจสอบทางนิติวิทยาศาสตร์
การบริหารจัดการเหตุการณ์ฉุกเฉิน (Incident Management)	SEF-02	- ต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติสำหรับการรับแจ้งและจัดการกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยเพื่อให้มีการคัดกรองเหตุการณ์เหตุการณ์ด้านความมั่นคงปลอดภัยและดำเนินการตอบสนองได้ภายในเวลาที่เหมาสม
การรายงานเหตุการณ์ฉุกเฉิน (Incident Reporting)	SEF-03	- ต้องมีการแจ้งหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างรวดเร็วและทันเวลาให้พนักงานและผู้เกี่ยวข้องได้รับทราบ โดยต้องรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยผ่านทางช่องทางที่กำหนดไว้อย่างรวดเร็วและเหมาะสม
การเตรียมหลักฐานเหตุการณ์ฉุกเฉิน (Incident Response Legal Preparation)	SEF-04	- ต้องมีการจัดทำกระบวนการทางนิติวิทยาศาสตร์ทางดิจิตอลสำหรับระบบคลาวด์ที่เหมาะสม โดยต้องมีขั้นตอนปฏิบัติสำหรับการจัดเก็บหลักฐานทางคอมพิวเตอร์

Control Area	Control ID	Control Notes
		เพื่อให้สามารถจัดเก็บและนำเสนอหลักฐานในชั้นศาลได้อย่างถูกต้อง ผู้ใช้บริการและ/หรือผู้เกี่ยวข้องที่ได้รับผลกระทบจากการละเมิดความปลอดภัยต้องได้รับโอกาสในการเข้ามีส่วนร่วมในการตรวจสอบทางนิติวิทยาศาสตร์ด้วย
กลไลการตอบสนองเหตุการณ์ฉุกเฉิน (Incident Response Metrics)	SEF-05	- ต้องมีกลไกในการติดตามเหตุการณ์ความมั่นคงปลอดภัยโดยแยกตามประเภท นับจำนวนเหตุการณ์ตามประเภท และสรุปค่าใช้จ่ายของเหตุการณ์เหล่านั้น (เพื่อใช้ในการเรียนรู้และป้องกันการเกิดขึ้นซ้ำในอนาคต)
4.2.15 การจัดการโซ่อุปทาน ความโปร่งใสและความรับผิดชอบ (Supply Chain Management, Transparency and Accountability)		
ความถูกต้องและคุณภาพของข้อมูล (Data Quality and Integrity)	STA-01	- ผู้ให้บริการต้องตรวจสอบ และปฏิบัติงานร่วมกับผู้เกี่ยวข้องเพื่อแก้ไขความผิดพลาดของข้อมูลและความเสี่ยงที่เกี่ยวข้อง โดยผู้ให้บริการต้องออกแบบและดำเนินการควบคุมเพื่อลดและจำกัดความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลโดยผ่านการควบคุมต่างๆ เช่น การแบ่งแยกตามหน้าที่ความรับผิดชอบ การเข้าถึงข้อมูลตามสิทธิ์ของผู้ใช้งานและการให้สิทธิเข้าถึงให้น้อยที่สุดเท่าที่ผู้ใช้งานจะสามารถดำเนินงานได้

Control Area	Control ID	Control Notes
การรายงานเหตุการณ์ (Incident Reporting)	STA-02	- ผู้ให้บริการควรมีการรายงานข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยเป็นระยะให้แก่ผู้ใช้บริการหรือผู้ให้บริการทั้งหมดที่ได้รับผลกระทบผ่านระบบอัตโนมัติ เช่น portals เป็นต้น หมายเหตุ : การรายงานข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยต้องการความรวดเร็วในการรายงานและการแก้ไข จึงแนะนำให้ใช้งานระบบอัตโนมัติ
บริการโครงสร้างพื้นฐาน และเครือข่าย (Supply Chain Management, Transparency and Accountability :Network / Infrastructure Services)	STA-03	- แอปพลิเคชัน API โครงสร้างพื้นฐานของระบบสารสนเทศและเครือข่ายซึ่งสนับสนุนบริการที่สำคัญหรือผู้ใช้งาน (ผู้ใช้บริการ) ที่สำคัญต้องได้รับการกำกับดูแลและบริหารจัดการบริการ ตั้งแต่การออกแบบ พัฒนา และติดตั้ง เพื่อให้งานบริการสำคัญมีความสอดคล้องระดับการให้บริการและระดับความสามารถ (capacity) ของบริการที่ตกลงไว้
การประเมินภายในโดยผู้ให้บริการ (Provider Internal Assessments)	STA-04	ผู้ให้บริการต้องจัดให้มีการตรวจสอบภายในเพื่อประเมินการปฏิบัติตามนโยบายขั้นตอนปฏิบัติ ที่เกี่ยวข้องกับการบริหารจัดการผู้ให้บริการภายนอกอย่างน้องปีละ 1 ครั้ง
ข้อตกลงของโซ่อุปทาน (Supply Chain Agreements)	STA-05	ต้องมีการจัดทำข้อตกลงของโซ่อุปทาน เช่น ข้อตกลงระดับการให้บริการ (SLA) ระหว่างผู้ให้บริการและผู้ใช้บริการ (ผู้เช่า) โดยอย่างน้อยต้องมีหัวข้อดังต่อไปนี้ - ขอบเขตการให้บริการ (เช่น ข้อมูลผู้ใช้บริการ การแลกเปลี่ยนและการใช้งานบุคลากร เครือข่าย เซิร์ฟเวอร์ บทบาทหน้าที่และความรับผิดชอบ การจ้างช่วง

Control Area	Control ID	Control Notes
		สถานที่ในการให้บริการ กฎหมาย ระเบียบ ข้อบังคับ ที่ต้องปฏิบัติตาม และ อื่นๆ ในการให้บริการ เป็นต้น) - ความต้องการด้านความมั่นคงปลอดภัย ข้อมูลติดต่อ (กรณีจำเป็น) ของทั้งผู้ให้บริการและผู้ใช้บริการ กระบวนการที่เกี่ยวข้องและมาตรการในการกำกับกับดูแลบริหารความเสี่ยง การปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ ที่เกี่ยวข้อง - การแจ้งและ/หรือการขออนุมัติล่วงหน้าต่อผู้ให้บริการ กรณีที่มีความจำเป็นต้องมีการเปลี่ยนแปลงระบบซึ่งจะกระทบต่อผู้ใช้บริการ - การแจ้งเหตุการณ์หรือการละเมิดความมั่นคงปลอดภัยอย่างทันกาลให้ผู้ใช้บริการและผู้ที่เกี่ยวข้องได้รับทราบ การแจ้งอาจจำเป็นต้องแจ้งผู้ที่เกี่ยวข้องในห่วงโซ่การให้บริการให้ครบถ้วน - การประเมินและการตรวจสอบอย่างอิสระถึงความสอดคล้องกับเงื่อนไขตามข้อตกลงในสัญญาจ้าง (อาทิ อาจใช้การตรวจเพื่อออกใบรับรอง การตรวจสอบและออกรายงาน หรือรูปแบบอื่นๆ ที่เท่าเทียมกัน) - การสิ้นสุดสัญญาจ้างและการดำเนินการต่างๆ กับผู้ใช้บริการที่อาจได้รับผลกระทบ - ความต้องการด้านระบบงานที่มีการเชื่อมโยงและติดต่อกัน การย้ายข้อมูลหรือแอปพลิเคชันไปอยู่อีกแพลตฟอร์มหนึ่ง ที่ผู้รับจ้างต้องดำเนินการ
การทบทวนการกำกับดูแลโซ่อุปทาน (Supply Chain Management, Transparency and Accountability : Supply	STA-06	- ผู้ให้บริการต้องทบทวนการบริหารจัดการความเสี่ยงและกระบวนการการกำกับดูแลผู้เกี่ยวข้อง (Partner) เพื่อให้การปฏิบัติมีความสอดคล้องกับความเสี่ยงที่สืบ

Control Area	Control ID	Control Notes
Chain Governance Reviews)		ทอดมาจากผู้เกี่ยวข้องรายอื่นของห่วงโซ่อุปทาน
การวัดโซ่อุปทาน (Supply Chain Management, Transparency and Accountability : Supply Chain Metrics)	STA-07	ต้องมีการทบทวน SLA ที่จัดทำขึ้นระหว่างผู้ให้บริการและผู้ใช้บริการต้องสอดคล้องเหมาะสมกับ UC (Underpinning Contract) ที่จัดทำขึ้นระหว่างผู้ให้บริการและผู้ให้บริการภายนอก อย่างสม่ำเสมอย่างน้อยปีละ 1 ครั้ง
การประเมินผู้ให้บริการภายนอก (Supply Chain Management, Transparency and Accountability : Third Party Assessment)	STA-08	- ผู้ให้บริการต้องดำเนินการประเมินการให้บริการของผู้ให้บริการภายนอกอย่างน้องปีละ 1 ครั้ง
การตรวจสอบการปฏิบัติงานของผู้ให้บริการภายนอก (Supply Chain Management, Transparency and Accountability : Third Party Audits)	STA-09	- ผู้ให้บริการภายนอกต้องแสดงให้เห็นว่าการให้บริการเป็นไปตามข้อตกลงด้านความมั่นคงปลอดภัย(Information Security UC) ที่กำหนดไว้อย่างน้อยปีละ 1 ครั้ง
4.2.16 การบริหารจัดการภัยคุกคามและช่องโหว่ (Threat and Vulnerability Management)		
แอนติไวรัส/ซอฟแวร์ที่เป็นอันตราย (Anti-Virus / Malicious Software)	TVM-01	- ต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติ เพื่อป้องกันการทำงานของมัลแวร์บนอุปกรณ์ต่างๆ ขององค์กรหรือของผู้ใช้งาน เช่น เวิร์คสเตชั่น แล็ปท็อปและ อุปกรณ์เคลื่อนที เป็นต้น และบนโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ระบบเครือข่ายและส่วนประกอบของระบบเทคโนโลยีสารสนเทศ
ช่องโหว่/การบริหารจัดการการปิดช่องโหว่ (Vulnerability / Patch Management)	TVM-02	- ต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติสำหรับการตรวจสอบช่องโหว่ตามระยะเวลาที่เหมาะสม โดยการตรวจสอบช่องโหว่ต้องดำเนินการกับทุกองค์ประกอบทั้งหมดภายใต้บริการ เพื่อให้การควบคุมความมั่นคงปลอดภัยมีประสิทธิภาพ

Control Area	Control ID	Control Notes
โปรแกรมประสงค์ร้าย (Mobile Code)	TVM-03	- ต้องจัดทำ ประกาศใช้งาน ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติที่เกี่ยวข้องกับการป้องกันการรันโปรแกรมประสงค์ร้าย (Mobile Code) โดยไม่ได้รับอนุญาตบนอุปกรณ์ต่างๆขององค์กร (เช่น เครื่องคอมพิวเตอร์ แล็ปท็อป และอุปกรณ์เคลื่อนที่) และบนระบบเครือข่ายและส่วนประกอบต่างๆของระบบ หมายเหตุ mobile code หมายถึงซอฟต์แวร์ที่สามารถส่งข้ามระหว่างระบบโดยผ่านระบบเครือข่ายทั้งที่น่าเชื่อถือหรือไม่น่าเชื่อถือได้ และสามารถรันบนระบบได้โดยไม่จำเป็นต้องติดตั้ง(Install) หรืออาจติดตั้งโดยผู้รับได้

หมายเหตุ ในวันที่ 15 กันยายน 2558 มีจัดประชุมเพื่อระดมความคิดเห็นกลุ่มย่อย (Focus Group) ซึ่งผู้ที่เข้าร่วมงานจะได้รับเอกสารแบบสอบถามความคิดเห็นร่างมาตรฐานความมั่นคงปลอดภัยสารสนเทศระบบคลาวน์ภาครัฐ (Government Cloud Security Standard) อีกครั้ง

ขอความร่วมมือทุกท่านช่วยกรอกแบบสอบถามร่างมาตรฐานความมั่นคงปลอดภัยสารสนเทศระบบคลาวน์ภาครัฐ เพื่อเป็นประโยชน์ในการพัฒนาต่อไป