นายธนพล วงศ์อาษา 62010356

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง ให้ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน และต้องปฏิบัติเพิ่มเติม ดังนี้

ข้อ ๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ หน่วยงานต้องวางแผนการติดตามและประเมินผลการใช้งานความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ เพื่อปรับปรุงหากมีการเปลี่ยนแปลงใด ๆ ภายในหน่วยงาน ทั้งนี้ เพื่อให้เหมาะสมกับสถานการณ์การใช้งาน และคงความมีประสิทธิผลอยู่เสมอ จัดให้มีการประชุมเพื่อตรวจสอบสถานะด้านความปลอดภัยของระบบสารสนเทศหน่วยงานอย่างสม่ำเสมอ

ข้อ ๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๒.๑ มีการกำหนดเนื้องานหรือหน้าที่ความรับผิดชอบต่าง ๆ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจน

๒.๒ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน

๒.๓ จัดให้มีการพิจารณาทบทวนแนวทางในการบริหารจัดการงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ในการดำเนินงาน ทั้งนี้ การพิจารณาทบทวนดังกล่าวควรดำเนินการโดยผู้ไม่มีส่วนได้เสียกับงานที่มีการพิจารณาทบทวน

ข้อ ๓. การบริหารจัดการทรัพย์สินสารสนเทศ

๓.๑ มีการกำหนดบุคคลผู้มีหน้าที่ดูแลควบคุมการใช้งานและรับผิดชอบทรัพย์สินสารสนเทศไว้ชัดเจน แต่งตั้งมอบหมายให้มีแผนกทำงานด้านระบบความปลอดภัยสารสนเทศและแต่งตั้งให้มี CISO

๓.๒ มีการกำหนดกฎระเบียบในการใช้งานทรัพย์สินสารสนเทศไว้อย่างชัดเจน โดยจัดทำเป็นเอกสาร และมีการประกาศใช้ในหน่วยงาน

๓.๓ มีการจำแนกประเภทของข้อมูลสารสนเทศ โดยจำแนกตามมูลค่าของข้อมูล ข้อกำหนดทางกฎหมายระดับชั้นความลับและความสำคัญต่อหน่วยงาน

๓.๔ มีการกำหนดและประกาศใช้ขั้นตอนที่เหมาะสมในการจำแนกประเภทของข้อมูลสารสนเทศและจัดการข้อมูลสารสนเทศ โดยให้สอดคล้องกับแนวทางการจำแนกประเภทของข้อมูลสารสนเทศที่หน่วยงานประกาศใช้

ข้อ ๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร พนักงาน หน่วยงานหรือบุคคลภายนอกต้องได้รับการอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตน และได้รับการสื่อสารให้ทราบถึงนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่หน่วยงานประกาศใช้อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลง อบรมพนักงานให้รู้เท่าทันภัยคุกคามต่าง ๆ และจัดให้มีการทดสอบความรู้พนักงานสม่ำเสมอ เช่น การทดลองส่ง Phishing email หรือการโทรศัพท์หลอกลวงเป็นต้น

ข้อ ๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

๕.๑ มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันพื้นที่หรือสถานที่ปฏิบัติงาน หรืออุปกรณ์สารสนเทศต่าง ๆ การติดตั้งกล้องวงจรปิด ราวเหล็ก ป้ายเตือนกันชน กระจกนูน เทปเรืองแสง ถังดับเพลิงและระบบ sprinkler

๕.๒ ไม่ควรนำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของหน่วยงานหากมิได้รับอนุญาต ควบคุมสิทธิในการใช้งานระบบสารสนเทศและซอฟต์แวร์ต่าง ๆ เช่น การห้ามใช้อุปกรณ์ external storage หรือการบังคับใช้ Proxy ของบริษัทในการติดต่อกับอินเทอร์เน็ต

ข้อ ๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๖.๑ มีการจัดการควบคุมการเปลี่ยนแปลงของระบบสารสนเทศ เมื่อมี software/hardware เวอร์ชันใหม่กว่าที่มีการแก้ปัญหาความปลอดภัย ให้ทำการอัพเกรดระบบให้ไปใช้เวอร์ชันใหม่นั้นถ้าเป็นไปได้

๖.๒ มีการติดตามผลการใช้งานทรัพยากรสารสนเทศ และวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม ตรวจสอบการเข้าถึงทรัพยากรต่าง ๆ ของระบบอย่างสม่ำเสมอ โดยหากเป็น server ที่ดูแลเอง อาจเช็คได้จาก utilization percentage และ log หากเป็น cloud computing service ต่าง ๆ เช่น AWS อาจตรวจสอบได้จาก dashboard ที่แสดงให้เห็นถึงอัตราการใช้งาน ณ ช่วงเวลาต่าง ๆ และทำการเลือก scale-up/scale-down ตามความจำเป็น

๖.๓ มีขั้นตอนการปฏิบัติงานในการจัดการและจัดเก็บข้อมูลสารสนเทศเพื่อมิให้ข้อมูลรั่วไหลหรือถูกนำไปใช้ผิดประเภท การเก็บข้อมูลในฐานข้อมูล โดยข้อมูลมีการเข้ารหัสลับและสิทธิ์การอ่านข้อมูลให้เฉพาะผู้ที่มีสิทธิเกี่ยวข้องกับงานบริหารฐานข้อมูลเท่านั้น

๖.๔ มีการจัดเก็บ Log ที่เกี่ยวข้องกับข้อผิดพลาดใด ๆ ของระบบสารสนเทศ มีการวิเคราะห์ Log ดังกล่าวอย่างสม่ำเสมอ และมีการจัดการแก้ไขข้อผิดพลาดที่ตรวจพบอย่างเหมาะสม

๖.๕ ระบบเวลาของระบบสารสนเทศต่าง ๆ ที่ใช้ในหน่วยงานหรือในขอบเขตงานด้านความมั่นคงปลอดภัย (Security domain) ต้องมีความสอดคล้องกัน (Synchronization) โดยให้มีการตั้งค่าพร้อมกับเวลาจากแหล่งเวลาที่เชื่อถือได้ ทำการตั้งค่าเวลาของระบบให้ตรงกับตามนโยบายของบริษัท หรืออาจใช้ NTP เพื่อตั้งเวลา server ให้ตรงกันทั่วโลก

ข้อ ๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๗.๑ มีข้อบังคับให้ผู้ใช้งานปฏิบัติตามขั้นตอนเพื่อการเลือกใช้รหัสผ่านอย่างมั่นคงปลอดภัยตามที่หน่วยงานกำหนด เช่น รหัสผ่านต้องเปลี่ยนทุกกี่เดือน มีความยาวตั้งแต่กี่ตัวอักษรขึ้นไป ต้องประกอบด้วยอักขระพิเศษใดบ้าง

๗.๒ ผู้ใช้งานสามารถเข้าถึงเฉพาะบริการทางเครือข่ายคอมพิวเตอร์ที่ตนเองได้รับอนุญาตให้ใช้ได้เท่านั้น กำหนดสิทธิการใช้งานของผู้ใช้งานทุกคนโดยใช้หลักการ Least Privilege

๗.๓ ให้มีการกำหนดวิธีการตรวจสอบตัวตนที่เหมาะสมเพื่อควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล การบังคับใช้งาน VPN เพื่อเชื่อมต่อกับระบบต่าง ๆ ในบริษัท อาจใช้บริการ VPN ของผู้ให้บริการได้หลายเจ้าเช่น Cisco AnyConnect

๗.๔ มีการควบคุมการเข้าถึงช่องทางการดูแลระบบสารสนเทศทั้งทางกายภาพและการเชื่อมต่อผ่านคอมพิวเตอร์สำหรับระบบสารสนเทศที่สามารถเข้าถึงจากระยะไกลได้ เช่น Remote diagnostic หรือ Configuration facility ของอุปกรณ์เครือข่ายคอมพิวเตอร์ ตั้งค่าให้ระบบสามารถเข้าถึงผ่านระยะไกลโดยบุคคลที่มีสิทธิดูแลด้วยเครื่องมือที่ปลอดภัยเช่น SSH

๗.๕ มีการจัดกลุ่มตามประเภทของข้อมูลสารสนเทศที่ให้บริการ ระบบสารสนเทศ กลุ่มผู้ใช้งาน โดยมีการแบ่งแยกบนเครือข่ายคอมพิวเตอร์อย่างเป็นสัดส่วน เลือกใช้ Identity Provider เช่น AWS IAM หรือ Azure AD เพื่อบริหารจัดการ role ของผู้ใช้งานและสิทธิการทำงานต่าง ๆ

๗.๖ กำหนดให้มีการควบคุมเส้นทางการไหลของข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์เพื่อไม่ให้ขัดแย้งกับนโยบายควบคุมการเข้าถึงของแอพพลิเคชั่น

๗.๗ กำหนดขั้นตอนการ Log-on เพื่อควบคุมการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์

๗.๘ ให้จัดทำหรือจัดให้มีระบบการบริหารจัดการรหัสผ่านที่สามารถทำงานแบบเชิงโต้ตอบกับผู้ใช้งาน (Interactive) และสามารถรองรับการใช้งานรหัสผ่านที่มีความมั่นคงปลอดภัย ใช้งาน password manager ต่าง ๆ เช่น LastPass

ข้อ ๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบ

คอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๘.๑ ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ ที่จะรับเข้าสู่แอพพลิเคชั่นก่อนเสมอ เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม ทำการเขียนโค้ดให้มีความปลอดภัยจากประเด็นการโจมตีในหมวดหมู่ injection เช่น SQL Injection, XSS เป็นต้น ทั้งนี้อาจมีการใช้ library ภายนอกเพื่อช่วยจัดการปัญหาดังกล่าวก็ได้ และอาจจัดให้มีการวิเคราะห์ source code เพื่อความปลอดภัยโดยใช้เครื่องมือเช่น SonarQube

๘.๒ ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ อันเป็นผลจากการประมวลผลของแอพพลิเคชั่นเพื่อให้มั่นใจได้ว่า ข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม จัดให้มีการทำ software testing ที่ครอบคลุมตั้งแต่ unit testing ไปจนถึง end-to-end testing และติดตั้งการ testing ใน CI/CD Pipeline โดยอาจใช้ library เช่น Jest, Cypress

๘.๓ จัดให้มีแนวทางการบริหารจัดการกุญแจ (Key) เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของหน่วยงาน

๘.๔ ให้เลือกชุดข้อมูลสารสนเทศที่จะนำไปใช้เพื่อการทดสอบในระบบสารสนเทศอย่างระมัดระวัง รวมทั้งมีแนวทางควบคุมและป้องกันข้อมูลรั่วไหล จัดทำชุดข้อมูลที่ไม่มีอยู่จริงขึ้นมาเพื่อใช้งานใน development environment และใช้งานในการ demo โดยเก็บแยกกันจากข้อมูลจริง

๘.๕ ให้มีการจำกัดการเข้าถึงซอร์สโค้ด (Source code) ของโปรแกรม การใช้ version control system ต่าง ๆ โดยอาจเลือกใช้รูปแบบที่ทางบริษัทนำมา host เองได้เช่น GitLab และกำหนดการเข้าถึง repository ของโค้ดเหล่านั้น

๘.๖ หากมีการเปลี่ยนแปลงใด ๆ ในระบบปฏิบัติการคอมพิวเตอร์ ให้มีการตรวจสอบทบทวนการทำงานของโปรแกรมที่มีความสำคัญ และทดสอบการใช้งานเพื่อให้มั่นใจว่าผลของการเปลี่ยนแปลงดังกล่าว จะไม่ส่งผลกระทบใด ๆ ต่อความมั่นคงปลอดภัยของระบบสารสนเทศและการให้บริการของหน่วยงาน จัดทำให้มีการใช้งาน regression test โดยอาจนำไปใส่เป็นส่วนหนึ่งของ CI/CD Pipeline

ข้อ ๙. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

๙.๑ จัดให้มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่จำเป็น โดยกำหนดให้เป็นส่วนหนึ่งของขั้นตอนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน

๙.๒ กำหนดให้มีกรอบงานหลักสำหรับการพัฒนาแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน เพื่อให้การพัฒนาแผนต่าง ๆ เป็นไปในทิศทางเดียวกัน รวมทั้งสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัย ตลอดจนมีการจัดลำดับความสำคัญก่อนหลังในการทดสอบและการดูแล

๙.๓ ให้มีการทดสอบและปรับปรุงแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉินอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าแผนดังกล่าวเป็นปัจจุบันและมีประสิทธิผลอยู่เสมอ ศึกษาจากกรณีศึกษาต่าง ๆ เช่นเหตุการณ์น้ำท่วมในปี 2554 และนำปัญหาที่เกิดขึ้นมาปรับปรุง รวมทั้งคาดการณ์เหตุการณ์ที่อาจก่อความเสียหายในอนาคตด้วย

ข้อ ๑๐. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

๑๐.๑ จัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆของหน่วยงาน

๑๐.๒ ใช้เทคนิคการเข้ารหัสลับ ที่สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

๑๐.๓ ให้มีการทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอเพื่อให้สอดคล้องกับมาตรฐานการพัฒนางานด้านความมั่นคงปลอดภัยด้านสารสนเทศ จ้างบริษัทภายนอกให้เข้ามาตรวจสอบความปลอดภัยของระบบทุกปี

๑๐.๔ วางแผนและจัดให้มีข้อกำหนดการตรวจสอบและกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ เพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของการให้บริการ

๑๐.๕ ป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise) กำหนดให้ผู้ที่มีสิทธิ์ใช้งานเครื่องมือตรวจสอบให้ใช้งานได้เท่านั้น และอาจต้องมีการทำการยื่นคำร้องไปทางบริษัทเพิ่มเติมก่อนเรียกใช้งานเครื่องมือเหล่านี้ได้