นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แบ่งออกเป็น 2 ส่วน ได้แก่

ส่วนที่ 1 : ว่าด้วยการจัดทำนโยบาย

1. ผู้บริหาร พนักงาน ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย
2. นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบ และสามารถเข้าถึงได้อย่างสะดวกผ่านทางระบบการจัดเก็บข้อมูล Google Drive ของบริษัทฯ
3. กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน
4. มีการทบทวนและปรับปรุงนโยบาย ปีละ 1 ครั้ง

ส่วนที่ 2 : ว่าด้วยรายละเอียดของนโยบาย

1. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ
   มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานอย่างทั่วถึง โดยให้ผู้ใช้งานสามารถเข้าถึง และใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย
2. มีระบบสารสนเทศและระบบสำรองของสารสนเทศ
   มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งาน เพื่อให้สามารถทำงานได้อย่างต่อเนื่อง
3. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
   มีการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ ปีละ 1 ครั้ง
4. การสร้างความรู้ ความเข้าใจในการใช้ระบบสารสนเทศและ/หรือระบบคอมพิวเตอร์
   มีนโยบายในการสร้างความรู้ ความเข้าใจ โดยการจัดทำคู่มือจัดฝึกอบรมและเผยแพร่ในการใช้งานระบบสารสนเทศ และระบบคอมพิวเตอร์แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ 1 ข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) ดังนี้

1.1 มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

1.2 ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

1.3 ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญหรือความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ 2 การบริหารจัดการการเข้าถึงระบบสารสนเทศของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยของสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ที่ซึ่งไม่ได้รับอนุญาต ดังนี้

2.1 สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

2.2 การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากการลงทะเบียนของผู้ใช้งาน เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

2.3 การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy) โดยต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ อาทิ เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึง โดยผู้ซึ่งไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

2.4 ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับขององค์กร

ข้อ 3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาดังนี้

3.1 การใช้งานรหัสผ่าน (Password User) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งาน ในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

3.2 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

3.3 การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy) โดยต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ อาทิ เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

3.4 ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับขององค์กร

ข้อ 4 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ดังนี้

4.1 การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศ ได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

4.2 การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคล ก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

4.3 การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Network) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่าย และควรใช้อุปกรณ์บนเครือข่ายเป็นการยืนยัน

4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

4.5 การแบ่งแยกเครือข่าย (Segregation in Network) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้งานร่วมกัน หรือเชื่อมต่อระหว่างกัน ให้สอดคล้องกับแนวปฏิบัติการควบคุมเข้าถึง

4.7 การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านไหลเวียนของข้อมูลหรือสารสนเทศ สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง หรือการประยุกต์ใช้งานตามภารกิจ

ข้อ 5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ดังนี้

5.1 กำหนดขั้นตอนปฏิบัติ เพื่อให้การใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการที่จะต้องควบคุม โดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

5.2 ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรับรองการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

5.3 การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบการบริหารจัดการรหัสผ่าน ที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

5.4 การใช้งานโปรแกรมอรรถประโยชน์ (User of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัย

5.5 เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง ให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out)

5.6 การจำกัดเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อ เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ 6 การควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุม

6.1 การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึง หรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งาน ในการเข้าถึงสารสนเทศและฟังก์ชั่นต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยสอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

6.2 ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing WLAN Teleworking)

6.3 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสม เพื่อป้องกันสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

6.4 การปฏิบัติงานจากภายนอกหน่วยงานโดยใช้ VPN ต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติ เพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานภายนอกหน่วยงาน

ข้อ 7 จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

7.1 ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสม ให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

7.2 ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถดำเนินการได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการงานตามภารกิจ

7.3 ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรองและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอิเล็กทรอนิกส์

7.4 ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมฉุกเฉินอย่างสม่ำเสมอ ปีละ 1 ครั้ง

7.5 มีการปฏิบัติและทบทวนแนวทางการจัดทำระบบสำรอง ปีละ 1 ครั้ง

ข้อ 8 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาดังนี้

8.1 ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) ตามความเหมาะสมเมื่อมีความเสี่ยง

8.2 ในการตรวจสอบและประเมินความเสี่ยง จะต้องดำเนินการโดยหน่วยตรวจสอบภายใน (Internal Auditing Unit) ผู้ตรวจสอบภายในที่ได้รับมอบหมาย เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ 9 กำหนดผู้กำกับดูแลและความรับผิดชอบ

ต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวทางปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงที่มีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงาน เป็นผู้รับผิดชอบต่อความเสี่ยงและเสียหายหรืออันตรายที่เกิดขึ้น

ข้อ 10 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information System Acquisition, Development and Maintenance)

10.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

หน่วยงานดูแลระบบเทคโนโลยีสารสนเทศต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือซื้อมาใช้งาน

หน่วยงานดูแลระบบเทคโนโลยีสารสนเทศ จะต้องทำการวิเคราะห์ระบบเทคโนโลยีสารสนเทศ ว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้

- มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย อาทิ การสำรองข้อมูล ระบบเครือข่ายสำรอง

- มาตรการปฏิบัติหลังจากเกิดความเสียหาย อาทิ แผนการกู้คืนข้อมูล ระยะเวลาในการกู้คืนข้อมูล

10.2 ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)

ผู้พัฒนาระบบสารสนเทศต้องมีการป้องกันโอกาสการรั่วไหลของข้อมูล อาทิ การดักจับข้อมูลจากสายสัญญาณภายนอกบริษัทการปลอมแปลง การใช้ซอฟต์แวร์ที่มีความเสี่ยงในการ รั่วไหลของข้อมูล

ในการทำสัญญาว่าจ้างการพัฒนาระบบของบริษัทฯ ต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

ข้อ 11 การควบคุมความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

บุคคลภายนอกต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy) ของบริษัทอย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท

ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการด้านเทคโนโลยีสารสนเทศของหน่วยงานภายนอกโดยต้องประกอบไปด้วยรายละเอียดดังนี้

- การยอมรับนโยบายและการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท
- ขอบเขต รายละเอียด และระดับการให้บริการ (Service Level Agreement)
- เอกสารต่างๆ เกี่ยวกับมาตรการการควบคุมที่ใช้ทั้งด้านกายภาพและด้าน Logical
- เพื่อให้มั่นใจได้ว่าระบบงานของผู้ให้บริการจากภายนอกสามารถรักษาความมั่นคงปลอดภัยสารสนเทศได้ทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
- ข้อมูลที่หน่วยงานภายนอกสามารถเข้าถึงได้และขั้นตอนและวิธีการร้องขอข้อมูลของบริษัทฯ กรณีต้องการข้อมูลเพิ่มเติม
- การไม่เปิดเผยข้อมูลของบริษัทฯ
- ให้แผนกบริหารองค์กรทบทวนและตรวจสอบบริการจาก ผู้ให้บริการ ภายนอกตามข้อตกลงที่กำหนด
- ให้แผนกบริหารองค์กรเป็นผู้รับผิดชอบในการบริหารจัดการการเปลี่ยนแปลงในการให้บริการ จากผู้ให้บริการภายนอก

ข้อ 12 การควบคุม การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

มอบหมายให้ผู้จัดการแผนกบริการองค์กรเป็นผู้ควบคุม บริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ เพื่อให้เกิดความชัดเจนในการรับมือกับปัญหาที่เกิดกับระบบสารสนเทศของบริษัทฯ จัดทำขั้นตอนการปฏิบัติในการแก้ไขปัญหาทั้งสภาวะปกติ และ สภาวะการที่ต้องได้รับการแก้ไขอย่างเร่งด่วน

ข้อ 13 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)

กำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติงานของบริษัทฯ การบริหารจัดการและการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอ กำหนดให้มีการทดสอบกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติงานของบริษัทฯ อย่างสม่ำเสมอ เช่น จัดให้มีเครื่องคอมพิวเตอร์สำรองในกรณีที่มีเครื่องเสีย และ มีความจำเป็นเร่งด่วนที่ต้องใช้งาน

ข้อ 14 การปฏิบัติตามข้อกำหนด (Compliance)

14.1 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย (Compliance with Legal Requirements)

แผนกบริหารองค์กรต้องศึกษาและกำหนดรายการของนโยบาย กฎระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศของหน่วยงาน เจ้าหน้าที่ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของ นโยบาย กฎ ระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ ที่กำหนดขึ้นอย่างเคร่งครัด

14.2 การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยและรายละเอียดทาง เทคนิค (Reviews of Security Policy and Technical Compliance)

แผนกบริหารองค์กรต้องจัดให้มีการตรวจสอบระบบทั้งหมดของหน่วยงานตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและระยะเวลาที่กำหนดไว้ ได้แก่ การตรวจดูว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และทดสอบการ โจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบ เมื่อมีความเสี่ยงด้วย