ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้ออกประกาศกำหนดหลักเกณฑ์และรายละเอียดของมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในแต่ละระดับชั้น ซึ่งมาตรฐานดังกล่าวจะครอบคลุมการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องความครบถ้วน (Integrity) และ การสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศ และให้ความสำคัญกับการดูแลรักษาความมั่นคงปลอดภัยของระบบสารสนเทศใน 11 เรื่อง ได้แก่

1) การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

2) การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

3) การบริหารจัดการทรัพย์สินสารสนเทศ

4) การสร้างความมั่นคงปลอดภัย ของระบบสารสนเทศด้านบุคลากร

5) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ แระบบสารสนเทศ

7) การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

8) การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

9) การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

10) การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

11) การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

เพื่อให้องค์กรผ่านมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง ต่อไปนี้คือขั้นตอนและกิจกรรมที่ควรดำเนินการ

1. **การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ**
    - กำหนดนโยบายความมั่นคงปลอดภัยและกระบวนการที่เชื่อมโยงกับวัตถุประสงค์และปรัชญาขององค์กร
    - จัดฝึกอบรมและการฝ่ายที่เกี่ยวข้องเพื่อเพิ่มความเข้าใจและการปฏิบัติตามนโยบายและกระบวนการ
2. **การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ**
    - ทบทวนและปรับปรุงโครงสร้างทางอิเล็กทรอนิกส์เพื่อตอบสนองกับความต้องการของมาตรฐาน
    - ติดตั้งระบบความปลอดภัยที่สอดคล้องกับมาตรฐาน
3. **การบริหารจัดการทรัพย์สินสารสนเทศ**
    - จัดทำแผนการบริหารจัดการทรัพย์สินสารสนเทศที่ครอบคลุมการจัดเก็บ การเข้าถึง และการรักษาความปลอดภัยของข้อมูล
4. **การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร**
    - จัดประชุมและสัมมนาเพื่อเสริมสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยของข้อมูล
    - บังคับมาตรฐานด้านความปลอดภัยและติดตามการปฏิบัติตามมาตรฐานนั้น
5. **การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม**
    - ตรวจสอบและปรับปรุงสภาพแวดล้อมที่มีผลกระทบต่อความปลอดภัยของระบบสารสนเทศ
    - ปรับปรุงระบบความปลอดภัยที่เกี่ยวข้องกับสภาพแวดล้อม
6. **การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์**
    - กำหนดนโยบายการใช้งานเครือข่ายที่ปลอดภัย
    - ตรวจสอบและปรับปรุงระบบเครือข่ายตามมาตรฐานความปลอดภัย

7. **การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์**
    - กำหนดนโยบายและกระบวนการควบคุมการเข้าถึงที่มีความปลอดภัย
    - ติดตั้งและบริหารจัดการระบบควบคุมการเข้าถึง
8. **การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์**
    - กำหนดแผนการพัฒนาและการบำรุงรักษาระบบเครือข่าย
    - ทำการปรับปรุงตามการทดสอบและประเมินผลจากกิจกรรมที่ดำเนินการ
9. **การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด**
    - กำหนดแผนการตอบสนองที่รวดเร็วในกรณีเหตุการณ์ที่ไม่พึงประสงค์
    - ทำการฝึกอบรมและทดสอบแผนการตอบสนองเป็นประจำ
10. **การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กร**
    - กำหนดแผนการดำเนินงานที่มีความต่อเนื่องในด้านความปลอดภัย
    - ตรวจสอบและปรับปรุงกระบวนการทำงานตามมาตรฐาน
11. **การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการ:**
    - ตั้งคณะกรรมการตรวจสอบและประเมินผลการปฏิบัติตามมาตรฐาน
    - ทำการตรวจสอบประจำเพื่อตรวจพบข้อบกพร่องและปรับปรุงตามต้องการ

การดำเนินการเหล่านี้จะช่วยให้องค์กรมีการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศตามมาตรฐานที่กำหนดไว้ในประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2555 อย่างมีประสิทธิภาพและต่อเนื่อง

เพื่อเสริมสร้างความมั่นคงปลอดภัยของระบบสารสนเทศตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 องค์กรสามารถดำเนินกิจกรรมต่อไปนี้

1. **การจัดทำแผนปฏิบัติการฉุกเฉิน**
    - สร้างแผนการที่เน้นการปฏิบัติในกรณีเหตุฉุกเฉินที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศ
2. **การฝึกอบรมความปลอดภัยทางไซเบอร์**
    - จัดกิจกรรมฝึกอบรมและเสวนาเพื่อเพิ่มความรู้และความเข้าใจในการป้องกันอันตรายทางไซเบอร์
3. **การทดสอบระบบความปลอดภัย**
    - ทำการทดสอบความทนทานและความปลอดภัยของระบบสารสนเทศตามมาตรฐาน
4. **การตรวจสอบความปลอดภัยของโครงสร้างทางอิเล็กทรอนิกส์**
    - ประเมินความปลอดภัยของโครงสร้างทางอิเล็กทรอนิกส์และทำการปรับปรุงตามความต้องการ
5. **การพัฒนานโยบายความปลอดภัย**
    - ทบทวนและปรับปรุงนโยบายความปลอดภัยเพื่อทำให้เป็นไปตามมาตรฐานที่กำหนด
6. **การตรวจสอบการบริหารจัดการทรัพย์สินสารสนเทศ**
    - ตรวจสอบและปรับปรุงกระบวนการบริหารจัดการทรัพย์สินสารสนเทศเพื่อความมั่นคงปลอดภัย
7. **การจัดกิจกรรมสัมมนาเชิงวิชาการ**
    - จัดกิจกรรมสัมมนาหรือการนำเสนอเพื่อแลกเปลี่ยนความรู้และประสบการณ์ในด้านความปลอดภัย
8. **การแลกเปลี่ยนข้อมูลเชิงปฏิบัติการ**
    - สร้างกิจกรรมแลกเปลี่ยนข้อมูลระหว่างทีมความปลอดภัยเพื่อเรียนรู้จากประสบการณ์ทางการปฏิบัติ
9. **การจัดการประชุมประจำทางความปลอดภัย**
    - จัดประชุมประจำเพื่อทบทวนความก้าวหน้าและปัญหาทางความปลอดภัย

10. การสร้างความตระหนักรู้ในพนักงาน

- จัดกิจกรรมที่เน้นการสร้างความตระหนักรู้ในพนักงานเกี่ยวกับความปลอดภัยทางไซเบอร์และการป้องกันอันตรายทางอิเล็กทรอนิกส์

ทั้งนี้เพื่อให้การดำเนินกิจกรรมดังกล่าวเป็นไปอย่างมีประสิทธิภาพ ควรมีการวิเคราะห์ความเสี่ยง และการประเมินผลเพื่อปรับปรุงแผนการต่อไป

เพื่อให้บรรลุเป้าหมายในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และดำเนินกิจกรรมต่าง ๆ อย่างมีประสิทธิภาพมีหลายเครื่องมือและโปรแกรมที่สามารถใช้งานได้ ต่อไปนี้คือบางตัวอย่าง:

1. **Security Information and Event Management (SIEM):**
   - ตัวอย่างโปรแกรม: Splunk, IBM QRadar, ArcSight
   - ช่วยในการรวบรวม วิเคราะห์ และรายงานข้อมูลที่เกี่ยวข้องกับความมั่นคงปลอดภัย
2. **Vulnerability Scanning Tools:**
   - ตัวอย่างโปรแกรม: Nessus, Qualys, OpenVAS
   - ช่วยในการสแกนและตรวจหาช่องโหว่ทางความปลอดภัยที่อาจเป็นจุดอ่อนของระบบ
3. **Intrusion Detection and Prevention Systems (IDPS):**
   - ตัวอย่างโปรแกรม: Snort, Suricata
   - ช่วยตรวจจับและป้องกันการบุกรุกทางไซเบอร์
4. **Data Loss Prevention (DLP) Solutions:**
   - ตัวอย่างโปรแกรม: Symantec DLP, McAfee DLP
   - ช่วยป้องกันการสูญเสียข้อมูลที่มีความลับ
5. **Endpoint Protection Software:**
   - ตัวอย่างโปรแกรม: Symantec Endpoint Protection, McAfee Endpoint Security
   - ช่วยป้องกันและตรวจจับมัลแวร์ที่อาจเข้าสู่ระบบผ่านทางอุปกรณ์ Endpoint

6. **Encryption Tools:**
    - ตัวอย่างโปรแกรม: VeraCrypt, BitLocker
    - ช่วยในการเข้ารหัสข้อมูลเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
7. **Network Security Tools:**
    - ตัวอย่างโปรแกรม: Wireshark, Nmap
    - ช่วยในการวิเคราะห์และตรวจสอบความมั่นคงปลอดภัยของเครือข่าย
8. **Patch Management Software:**
    - ตัวอย่างโปรแกรม: WSUS (Windows Server Update Services), Patch My PC
    - ช่วยในการจัดการและปรับปรุงทุกข์อาการที่เกี่ยวข้องกับความปลอดภัย
9. **Security Awareness Training Platforms:**
    - ตัวอย่างโปรแกรม: KnowBe4, Sophos Phish Threat
    - ช่วยในการฝึกอบรมพนักงานเพื่อเพิ่มความตระหนักรู้ในด้านความปลอดภัย
10. **Password Management Tools:**
    - ตัวอย่างโปรแกรม: LastPass, Dashlane
    - ช่วยในการจัดการและเพิ่มความปลอดภัยของรหัสผ่าน

การใช้เครื่องมือเหล่านี้ร่วมกับแผนการที่ดีในการบริหารจัดการความมั่นคงปลอดภัยจะช่วยให้องค์กรมีการป้องกันและตอบสนองต่ออุบัติเหตุทางความปลอดภัยได้อย่างเหมาะสมและมีประสิทธิภาพ