นโยบายความมั่นคงสารสนเทศ
(Information Security Policy)

เหตุผลและความจำเป็นของนโยบายความมั่นคงสารสนเทศ

องค์กรทั้งหลายในปัจจุบัน ต่างได้ดำเนินการด้านระบบสารสนเทศเพื่อรองรับการดำเนินงานและการวางแผนในระดับต่างๆขององค์กร. การดำเนินการระบบฯมีการประยุกต์ใช้เทคโนโลยีสารสนเทศอย่างกว้างขวางในระดับต่างๆ และอาจทำให้เกิดช่องว่างระหว่าง การป้องกันระบบที่ควรจะมีและการดำเนินการป้องกันระบบที่เกิดขึ้นจริง จนกลายเป็นจุดอ่อนหรือภาวะคุกคามในระบบได้. ช่องว่างเหล่านี้อาจนำมาซึ่งความสูญเสียหรือความเสียหายต่อระบบสารสนเทศ และอาจเกิดได้จากหลายสาเหตุ เช่น การใช้เทคโนโลยีอย่างกว้างขวางโดยไม่มีการควบคุม, ระบบมีการเชื่อมต่อได้อย่างทั่วถึงผ่านระบบ LAN หรือจากระบบ Internet ทำให้การเข้าถึงเป็นไปได้โดยไม่มีข้อจำกัดด้าน เวลา สถานที่, การบริหารจัดการและการควบคุมระบบฯอยู่ในสภาวะถดถอยหรือล้าหลังไม่ทันต่อเหตุการณ์และยุคสมัย, องค์กรมีสิ่งจูงใจให้เกิดการโจมตีระบบฯโดยบุคคลภายในและภายนอกองค์กร หรือข้อกำหนดด้านกฎระเบียบหรือกฎหมายมีการเปลี่ยนแปลง เป็นต้น.

ในองค์กรหรือหน่วยงานใดๆนั้นจะเกิดความมั่นคงสารสนเทศได้ก็ต่อเมื่อระบบฯนั้น มี

1. สภาพพร้อมใช้งาน (availability) เพราะสารสนเทศมีให้ใช้และสามารถใช้ได้ยามต้องการ โดยที่ระบบฯสามารถรับมือต่อการโจมตีและถ้ามีการโจมตีก็สามารถกู้คืนได้
2. การเก็บรักษาความลับ (confidentiality) เพราะข้อมูลและสารสนเทศในระบบฯนั้นมีการใช้งานเฉพาะในบรรดาผู้ที่เกี่ยวข้องและผู้มีสิทธิรับรู้ในข้อมูลเท่านั้น
3. บูรณภาพ (integrity) เพราะการลงบันทึกและการเปลี่ยนแปลงแก้ไขข้อมูล การกระทำโดยผู้ได้รับอนุญาตเท่านั้น

การดำเนินการเพื่อทำให้เกิดความมั่นคงของระบบสารสนเทศเป็นหลักประกันว่า องค์กรมีระบบสารสนเทศให้ใช้งานได้อย่างต่อเนื่องไม่หยุดชะงัก และสามารถควบคุมความเสียหายให้เกิดน้อยที่สุดในกรณีที่มีเหตุด้านความมั่นคง (security incident).

ในการจัดการด้านความมั่นคงของสารสนเทศนั้น มีกิจกรรมสำคัญ 6 ประการที่พึงได้รับการดำเนินการในแต่ละองค์กรไปอย่างพร้อมเพรียงกันเพื่อเป็นหลักประกันว่า ระบบสารสนเทศจะมีความมั่นคง. กิจกรรมเหล่านี้ได้แก่

1. การพัฒนานโยบายด้านความมั่นคง (policy development) องค์กรมีการใช้วิสัยทัศน์ พันธะกิจ วัตถุประสงค์และหลักการต่างๆที่องค์กรยึดถือมาเป็นกรอบในการพัฒนานโยบายฯ
2. บทบาทและความรับผิดชอบของบุคลากรในระดับต่างๆ (roles and responsibilities) ผู้บริหารองค์กรได้มีการกำหนดบทบาทอำนาจหน้าที่ ความรับผิดชอบ ให้แก่ทุกคนตั้งแต่

ระดับผู้บริหาร ประธานฝ่ายสารสนเทศ เจ้าหน้าที่ความมั่นคง บุคลากรอื่นๆขององค์กรทุกส่วนรวมทั้งผู้ใช้งานระบบทุกคน และมีความเข้าใจตรงกัน

3. การออกแบบระบบสารสนเทศ (systems design) ระบบฯได้รับออกแบบมาโดยอ้างอิงกรอบความมั่นคงและการควบคุมที่จำเป็นต่างๆ ได้แก่ มาตรฐาน (standards) มาตรการ (measures) การปฏิบัติ (practices) และกระบวนงาน (procedures). กระบวนการนี้อาจดำเนินมาตั้งแต่ต้นแล้ว หรือสำหรับบางองค์กรอาจประยุกต์แนวคิดหรือเทคโนโลยีทันสมัยโดยการติดตั้งหรือปรับระบบใหม่
4. การดำเนินงานระบบสารสนเทศ (system implementation) หน่วยงานสารสนเทศขององค์กรได้ดำเนินการแก้ไขปัญหาต่างๆในระบบฯอย่างทันกาล และมีการบำรุงรักษาระบบฯอย่างเหมาะสม ใช้ปรัชญาเชิงรุกเป็นตัวนำมากกว่าการตั้งรับแก้ปัญหาหาแต่เพียงอย่างเดียว
5. การเฝ้าสังเกตระบบสารสนเทศ (system monitoring) เพราะว่าระบบฯอาจมีปัญหาจากอุปกรณ์สารสนเทศต่างหรือจากการทำงานเองและส่งผลกระทบต่อสภาพพร้อมใช้งาน บูรณภาพและการเก็บรักษาความลับ จำเป็นต้องมีระบบการเฝ้าสังเกตเพื่อตรวจสอบและตรวจหาความผิดปรกติ. ในการนี้องค์กรใช้มาตรการเพื่อเฝ้าสังเกตว่ามีการละเมิดหรือฝ่าฝืนด้านนโยบาย, มาตรฐานหรือกระบวนงานด้านความมั่นคงโดยที่สามารถตรวจพบได้อย่างรวดเร็วและทันกาล, มีการสืบสวนสอบสวน และดำเนินการ รวมทั้งมีการดำเนินงานที่สอดคล้องกับนโยบาย มาตรฐาน และการปฏิบัติด้านความมั่นคง
6. การสร้างความตื่นตัว การฝึกอบรมและการให้การศึกษาแก่บุคลากรในองค์กร (awareness, training and education) องค์กรได้มีการดำเนินการในรูปแบบต่างๆเพื่อสร้างความตื่นตัวในบุคลากรให้ตระหนักในความสำคัญและความจำเป็นของการอารักขาสารสนเทศ อีกทั้งมีการจัดให้มีการฝึกอบรมที่จำเป็นสำหรับการดำเนินงานระบบสารสนเทศที่มีความมั่นคง และให้การศึกษาเกี่ยวกับมาตรการและการปฏิบัติด้านความมั่นคง อย่างต่อเนื่องเป็นประจำ.

กิจกรรมเหล่านี้ทั้ง 6 ประการจำเป็นต้องได้รับการพัฒนาควบคู่กันไปพร้อมกัน แต่ในที่นี้จะเป็นการเน้นเรื่องการพัฒนานโยบายความมั่นคงสารสนเทศเท่านั้น.

บุคลากรในองค์กรที่รับผิดชอบด้านนโยบายความมั่นคงสารสนเทศ

เพื่อให้เกิดความมั่นคงสารสนเทศขององค์กร จำเป็นต้องมีความร่วมมือจากทุกหน่วยงานอย่างทั่วถึง ไม่ใช่เฉพาะจากผู้บริหารและบุคลากรด้านไอทีเท่านั้น แต่ยังรวมถึงทุกคนที่ปฏิบัติงานในระบบฯอีกด้วย. นอกจากนี้แล้วเพื่อให้แน่ใจได้ว่ามีการดำเนินการตามนโยบายจริง จำเป็นต้องมีการร่วมมือจาก หน่วยงานตรวจสอบ (auditor), ผู้เชี่ยวชาญด้านความมั่นคง (security professionals) และผู้เชี่ยวชาญด้านเทคโนโลยี (technology experts).

บทบาทของผู้บริหารองค์กร

ในการดำเนินงานด้านระบบสารสนเทศนั้นผู้บริหารองค์กรพึงมีความเข้าใจอย่างถ่องแท้ว่าระบบฯ ที่กำลังดำเนินการอยู่นั้นมีประสิทธิภาพการทำงานและมีการลงทุนในด้านต่าง ๆมากน้อยเพียงไร ทั้งที่เป็นอยู่ในปัจจุบันและทิศทางที่องค์กรจะพัฒนาและดำเนินต่อไปในอนาคต; นอกจากนี้แล้วผู้บริหารองค์กรพึงตระหนักว่า ระบบสารสนเทศนั้นมีศักยภาพในการเปลี่ยนแปลงการดำเนินธุรกิจและวิธีปฏิบัติงาน การสร้างโอกาสทางธุรกิจ และการลดต้นทุนของการผลิต กิจกรรมหรือการบริการต่าง ๆ ขององค์กรได้อย่างไร. ผลที่ติดตามมาของการดำเนินการระบบฯคือ วิถีการดำเนินงานขององค์กรจะต้องพึ่งพาอาศัยสารสนเทศและระบบฯรวมทั้งการสื่อสารมากยิ่งขึ้น, การควบคุมระบบฯจะมีความซับซ้อนมากขึ้นตามไปด้วยเพราะเทคโนโลยีมีการเปลี่ยนแปลงและจำเป็นต้องดำเนินการเพื่อประกันความมั่นคงระบบฯ และเมื่อระบบฯไม่ทำงานจะสามารถส่งผลกระทบต่อ ภาพพจน์ ชื่อเสียงและการดำเนินงานขององค์กรได้. ดังนั้นเพื่อให้ระบบสารสนเทศสามารถรองรับภารกิจขององค์กรได้อย่างมีประสิทธิภาพและมีปัญหาน้อยที่สุด จำเป็นต้องมีความเข้าใจอย่างชัดเจนและเป็นเอกภาพในการดำเนินการ และการบังคับใช้ซึ่งนโยบายความมั่นคงสารสนเทศทั่วทั้งองค์กรโดยไม่มีข้อยกเว้น. นั่นหมายถึงว่าการละเลยไม่ปฏิบัติตาม หรือการละเมิดฝ่าฝืนนโยบายความมั่นคงสามารถส่งผลต่อสภาพพร้อมใช้งาน, บูรณภาพและการเก็บรักษาความลับ และผู้บริหารจำเป็นต้องดำเนินมาตรการทางวินัยสำหรับการละเลยหรือการฝ่าฝืนนั้น. การมีนโยบายที่ไม่ได้มีการบังคับใช้ ก็เปรียบเหมือนไม่มีนโยบายและทำให้ความมั่นคงของระบบสารสนเทศแห่งองค์กรอยู่ในสภาพที่มีความเสี่ยง. เมื่อความมั่นคงสารสนเทศอ่อนแอลง อาจทำให้ระบบฯไม่สามารถบริการได้ตามข้อกำหนดเพราะสภาพพร้อมใช้งานเสียไป, ข้อมูลในระบบไม่น่าเชื่อถือเพราะบูรณภาพเสียไปและไม่สามารถนำมารองรับภารกิจขององค์กร, และถ้าการเก็บรักษาความลับไม่เกิดขึ้นตามข้อกำหนด และยินยอมให้ผู้คนเข้าถึงข้อมูลได้อย่างไม่จำแนกและไม่มีการควบคุม จะทำให้ระบบสารสนเทศมีความเสี่ยงต่อภาพพจน์, ชื่อเสียงและล่อแหลมต่อการข้องเกี่ยวกับคดีความในกรณีที่มีการร้องเรียนหรือฟ้องร้องเกิดขึ้น.

สาระสำคัญของนโยบายความมั่นคงสารสนเทศ

สาระสำคัญของนโยบายความมั่นคงสารสนเทศโดยทั่วไปประกอบด้วยเนื้อหา 2 ส่วนคือ ส่วนที่หนึ่งว่าด้วยมาตรฐานในการดำเนินงานเพื่อป้องกันและอารักขาระบบสารสนเทศ โดยมีการกำหนดอำนาจหน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้องต่าง ๆไว้อย่างชัดเจน, และส่วนที่สองว่าด้วยกฎระเบียบ (rules) แนวปฏิบัติ (guidelines) และนิยาม (definitions) ต่าง ๆเพื่อทำให้เกิดความเข้าใจที่เป็นเอกภาพทั่วทั้งองค์กร.

สาระเหล่านี้ของนโยบายฯ จัดเป็นเครื่องมือสำคัญเพื่อทำให้เกิดความคล้องจองและหลีกเลี่ยงความขัดแย้งในการดำเนินงานทั้งหลายที่อาจเป็นความเสี่ยง อีกทั้งยังเป็นพื้นฐานสำคัญสำหรับการบังคับใช้ด้านกฎระเบียบและกระบวนงาน. ทั้งนี้นโยบายที่เหมาะสมพึงสามารถรองรับความแตกต่าง

และความหลากลายด้าน ข้อมูล, กิจกรรม, และทรัพยากรซึ่งอาจมีความแตกต่างกันได้มากในส่วนต่างๆขององค์กร. ดังนั้นการพัฒนานโยบายจึงจำเป็นต้องมีข้อคิดเห็นจากบุคลากรทุกระดับ รวมทั้งเจ้าหน้าที่ด้านไอทีและเจ้าหน้าที่ผู้รับผิดชอบด้านความมั่นคงสารสนเทศประกอบกัน.

นโยบายความมั่นคงสนเทศหมายถึงการตัดสินใจต่างๆที่เกี่ยวข้องกับสารสนเทศซึ่งโดยทั่วไปแล้วอยู่ในรูปของเอกสารบันทึก. นโยบายความมั่นคงสารสนเทศโดยทั่วไปแบ่งออกได้เป็น 3 ระดับคือ

ก. นโยบายทั่วไป (governing policy) เป็นนโยบายที่รองรับปัญหาพื้นฐานในการดำเนินงานขององค์กร จัดเป็นแม่บทสำหรับบังคับใช้ทั่วไป

ข. นโยบายด้านเทคนิค (technical policy) เป็นนโยบายที่รองรับประเด็นปัญหาด้านเทคนิคในระบบสารสนเทศและเทคโนโลยีที่เกี่ยวข้อง

ค. นโยบายสำหรับผู้ใช้งานระบบ (end-user policy) เป็นนโยบายที่รองรับการดำเนินงานของบุคลากรทุกระดับขององค์กร.

เนื่องจากนโยบายเป็นข้อความที่กำหนดไว้อย่างกว้างๆ จึงจำเป็นที่จะต้องมีการพัฒนา มาตรฐาน (standards), แนวปฏิบัติ (guidelines) และกระบวนงาน (procedures) ประกอบนโยบาย เพื่อให้บุคลากรทุกระดับสามารถปฏิบัติตามและบรรลุเป้าหมายขององค์กรได้. ตัวมาตรฐาน (standard) และแนวปฏิบัติ (guideline) เป็นสิ่งระบุว่าเทคโนโลยีและระเบียบวิธี (methodology) ของระบบที่มั่นคงนั้นมีอะไรบ้าง ในขณะที่กระบวนงาน (procedure) นั้นกำหนดขั้นตอนในรายละเอียดว่าจะปฏิบัติกิจที่เกี่ยวข้องกับความมั่นคงให้สำเร็จได้นั้นต้องทำอย่างไร.

องค์ประกอบสำคัญของนโยบายความมั่นคงสารสนเทศ

1. วัตถุประสงค์ (purpose) มีการกำหนดวัตถุประสงค์ให้ชัดเจน เช่น เพื่อทำให้เกิดสภาพพร้อมใช้งาน, การเก็บรักษาความลับและบูรณภาพของสารสนเทศในองค์กร เป็นต้น. บางองค์กรอาจกำหนดให้เป็นรูปธรรมชัดเจนมากขึ้น เช่น การลดความผิดพลาด การลดความสูญเสียด้านข้อมูล และการกู้คืนระบบ เป็นต้น.
2. ขอบเขต (scope) มีการกำหนดให้ชัดเจนว่านโยบายมีผลบังคับใช้กับทรัพยากรด้านใดบ้างขององค์กร เช่น อาคารสถานที่ ฮาร์ดแวร์ ซอฟต์แวร์ สารสนเทศและบุคลากร.
3. ความรับผิดชอบ (responsibilities) กำหนดให้ชัดเจนว่า ผู้ใดมีความรับผิดชอบในภารกิจใด. คณะกรรมการความมั่นคงขององค์กร (information security committee) ซึ่งรวมเอาผู้ทำหน้าที่รับผิดชอบด้านความมั่นคงสารสนเทศในองค์กรหนึ่งๆ อาจประกอบด้วย
   a. ผู้บริหารสูงสุด (chief executive officer, CEO) ขององค์กรนั้นๆ เช่น ผู้อำนวยการโรงพยาบาล, ผู้อำนวยการสำนัก, ผู้อำนวยการกอง, และอธิบดีกรม เป็นต้น

b. เจ้าหน้าที่ความมั่นคงระดับองค์กร (chief/senior security officer หรือ CSO) ทำหน้าที่เป็นตัวแทนหัวหน้าองค์กรในการจัดการและกำกับดูแลเรื่องนโยบายความมั่นคงสารสนเทศ และการดำเนินการว่าด้วย มาตรฐาน แนวปฏิบัติและกระบวนงาน. ในบางองค์กรอาจมอบหมายให้ ประธานฝ่ายสารสนเทศ (chief information officer, CIO) เป็นผู้ทำหน้าที่นี้.
c. เจ้าหน้าที่ความมั่นคงระดับกลุ่มงาน (departmental security officer หรือ DSO) หมายถึง เจ้าหน้าที่ความมั่นคงระดับกลุ่มงาน เช่น โรงพยาบาลอาจมีกลุ่มงานเภสัชกรรม กลุ่มงานพยาบาล กลุ่มงานแพทย์ กลุ่มงานห้องปฏิบัติการ กลุ่มงานการเงิน ฯลฯ จำเป็นต้องมีเจ้าหน้าที่ความมั่นคงของแต่ละกลุ่มที่ไม่ใช่ตัวหัวหน้ากลุ่มงานเอง แต่อาจมอบหมายให้หัวหน้ากลุ่มงานปฏิบัติหน้าที่นี้ก็ได้.
d. เจ้าหน้าที่งานสารสนเทศ (head of information service) เช่น หัวหน้างานสารสนเทศ หรือกลุ่มงานที่เทียบเท่า
e. ที่ปรึกษาหรือผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ, ความมั่นคงสารสนเทศ
f. อื่นๆ

4. การคงแบบ (compliance) ประเด็นสำคัญของการคงแบบหรือการปฏิบัติตามกฎระเบียบ เพื่อดูว่ามีความสอดคล้องกับข้อกำหนดเพียงใดนั้น มี 2 ประการ. ประการที่หนึ่งคือดูว่ามีการดำเนินการที่สอดคล้องกับนโยบาย มาตรฐาน แนวปฏิบัติและกระบวนงานมากน้อยเพียงไร โดยมีการตรวจสอบด้านระบบสารสนเทศทีและความมั่นคง (information system & security audit) และประการที่สองดูว่า องค์กรมีบทลงโทษสำหรับการละเมิดฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายหรือไม่อย่างไร เพราะการไม่ปฏิบัติตามนโยบายอาจทำให้เกิดความเสี่ยงและความเสียหายตามมา ส่งผลให้องค์กรไม่สามารถปฏิบัติภารกิจได้.

หัวข้อรายละเอียดของนโยบายความมั่นคงสารสนเทศที่พึงได้รับการพัฒนา

นโยบายความมั่นคงสารสนเทศ ที่องค์กรดำเนินการพัฒนาพึงมีสาระดังต่อไปนี้

1. เอกสารข้อความว่าด้วยนโยบายความมั่นคงสารสนเทศ (information security policy statement), มาตรฐาน (standards) และกระบวนงาน (procedures) ในเนื้อหาต่างๆที่เกี่ยวข้องกับความมั่นคงสารสนเทศ
2. หน่วยงานที่รับผิดชอบและโครงสร้างพื้นฐานด้านความมั่นคงสารสนเทศ (organization and infrastructure)
3. การจำแนกและการจัดระดับสารสนเทศ (information classification)
4. การบริหารความเสี่ยง (risk management)
5. กรอบโครงสร้างด้านความมั่นคง (security framework) สำหรับการระบุและพิสูจน์ตัวจริง (identification and authentication), การให้สิทธิ์และการควบคุมการเข้าถึง (authorization

and access control), ภาระความรับผิด (accountability), บูรณภาพและสภาพพร้อมใช้งาน (integrity and availability), ความมั่นคงของสารสนเทศ (information security) และการบริหารจัดการความมั่นคง (security administration)

6. ความมั่นคงด้านบุคลากร (personnel security)
7. ความมั่นคงทางกายภาพและสิ่งแวดล้อม (physical and environmental security)
8. การกู้ระบบสารสนเทศจากภัยพิบัติ (disaster recovery)
9. การรายงานเหตุ (incident reporting)
10. การคงแบบ (compliance) และการจัดการด้านวินัยเมื่อมีการละเมิดหรือละเลย (disciplinary action)
11. การฝึกอบรมและการจัดการศึกษา (education and training)
12. การตรวจสอบด้านความมั่นคง (security audit) รวมทั้งการพัฒนาคู่มือ (manual) เพื่อรองรับกระบวนการตรวจสอบด้านระบบสารสนเทศ (information system & security audit) ด้วย.

ทีมงานพัฒนานโยบายความมั่นคงสารสนเทศ

การพัฒนานโยบายฯ พึงดำเนินการโดยคณะทำงานนโยบายความมั่นคงสารสนเทศซึ่งอาจประกอบด้วยบุคลากรด้านความมั่นคงของหน่วยงานต่างๆ (เช่น กรมสนับสนุนบริการสุขภาพ) รวมทั้งนิติกร (legal department), บุคลากรที่รับผิดชอบด้านทรัพยากรบุคคล (human resource department), ตัวแทนหน่วยงานที่รับผิดชอบด้านการตรวจสอบภายใน (internal audit) และกลุ่มผู้ใช้งานระบบ (user group) เป็นต้น. คณะทำงานฯทำหน้าที่พัฒนานโยบาย, มาตรฐานและกระบวนงานแล้วจึงนำไปสู่การดำเนินการในหน่วยงานต่างๆ (เช่น โรงพยาบาลระดับต่างๆของกระทรวงสาธารณสุข) ต่อไป.

เนื้อหาและสาระสำคัญของความมั่นคงสารสนเทศตามมาตรฐาน ISO 17799

ดูภาคผนวกประกอบ.

เรียบเรียงโดย
ดำรงศักดิ์ บุลยเลิศ
กุมภาพันธ์ 2549

เอกสารอ้างอิง

1. An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12. Accessed from http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf, October 14 2004.
2. CMS Information Systems Security Policy, Standards and Guidelines Handbook. Centers for Medicare and Medicaid Services, Department of Health and Human Services. July 19, 2004. Accessed from http://www.cms.hhs.gov/it/security/docs/handbook.pdf
3. An Information Security Policy Development Guide for Large Companies. Sorcha Canavan, SANS Institute 2004, November 18th, 2003. Accessed October 14 2004, from www.sans.org.
4. Security Architecture. Nebraska Information Technology Commission. Accessed October 14, 2004, from http://www.nitc.state.ne.us/tp/workgroups/security/security_policies.htm
5. Information Technology Security Techniques: Code of practice for information security management. ISO-17799, 2005.

ภาคผนวก

Information Security Management Outline (Based on ISO-17799, 2005)

Information Technology Security Techniques: Code of practice for information security management

0 INTRODUCTION

0.1 WHAT IS INFORMATION SECURITY?

0.2 WHY INFORMATION SECURITY IS NEEDED?

0.3 HOW TO ESTABLISH SECURITY REQUIREMENTS

0.4 ASSESSING SECURITY RISKS

0.5 SELECTING CONTROLS

0.6 INFORMATION SECURITY STARTING POINT

0.7 CRITICAL SUCCESS FACTORS

0.8 DEVELOPING YOUR OWN GUIDELINES

1 SCOPE

2 TERMS AND DEFINITIONS

3 STRUCTURE OF THIS STANDARD

3.1 CLAUSES

3.2 MAIN SECURITY CATEGORIES

4 RISK ASSESSMENT AND TREATMENT

4.1 ASSESSING SECURITY RISKS

4.2 TREATING SECURITY RISKS

5 SECURITY POLICY

5.1 INFORMATION SECURITY POLICY

5.1.1 Information security policy document

5.1.2 Review of the information security policy

6 ORGANIZATION OF INFORMATION SECURITY

6.1 INTERNAL ORGANIZATION

6.1.1 Management commitment to information security

6.1.2 Information security co-ordination

6.1.3 Allocation of information security responsibilities

6.1.4 Authorization process for information processing facilities

6.1.5 Confidentiality agreements

6.1.6 Contact with authorities

6.1.7 Contact with special interest groups

6.1.8 Independent review of information security

6.2 EXTERNAL PARTIES

6.2.1 Identification of risks related to external parties

6.2.2 Addressing security when dealing with customers

6.2.3 Addressing security in third party agreements

7 ASSET MANAGEMENT

7.1 RESPONSIBILITY FOR ASSETS

7.1.1 Inventory of assets

7.1.2 Ownership of assets

7.1.3 Acceptable use of assets

7.2 INFORMATION CLASSIFICATION

7.2.1 Classification guidelines

7.2.2 Information labeling and handling

8 HUMAN RESOURCES SECURITY

8.1 PRIOR TO EMPLOYMENT

8.1.1 Roles and responsibilities

8.1.2 Screening

8.1.3 Terms and conditions of employment

8.2 DURING EMPLOYMENT

8.2.1 Management responsibilities

8.2.2 Information security awareness, education, and training

8.2.3 Disciplinary process

8.3 TERMINATION OR CHANGE OF EMPLOYMENT

8.3.1 Termination responsibilities

8.3.2 Return of assets

8.3.3 Removal of access rights

9 PHYSICAL AND ENVIRONMENTAL SECURITY

9.1 SECURE AREAS

9.1.1 Physical security perimeter

9.1.2 Physical entry controls

9.1.3 Securing offices, rooms, and facilities

9.1.4 Protecting against external and environmental threats

9.1.5 Working in secure areas

9.1.6 Public access, delivery, and loading areas

9.2 EQUIPMENT SECURITY

9.2.1 Equipment siting and protection

9.2.2 Supporting utilities

9.2.3 Cabling security

9.2.4 Equipment maintenance

9.2.5 Security of equipment off-premises

9.2.6 Secure disposal or re-use of equipment

9.2.7 Removal of property

10 COMMUNICATIONS AND OPERATIONS MANAGEMENT

10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES

10.1.1 Documented operating procedures

10.1.2 Change management

10.1.3 Segregation of duties

10.1.4 Separation of development, test, and operational facilities

10.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT

12.5.2 Technical review of applications after operating system changes

12.5.3 Restrictions on changes to software packages

12.5.4 Information leakage

12.5.5 Outsourced software development

12.6 TECHNICAL VULNERABILITY MANAGEMENT

12.6.1 Control of technical vulnerabilities

13 INFORMATION SECURITY INCIDENT MANAGEMENT

13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES

13.1.1 Reporting information security events

13.1.2 Reporting security weaknesses

13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS

13.2.1 Responsibilities and procedures

13.2.2 Learning from information security incidents

13.2.3 Collection of evidence

14 BUSINESS CONTINUITY MANAGEMENT

14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

14.1.1 Including information security in the business continuity management process

14.1.2 Business continuity and risk assessment

14.1.3 Developing and implementing continuity plans including information security

14.1.4 Business continuity planning framework

14.1.5 Testing, maintaining and re-assessing business continuity plans

15 COMPLIANCE

15.1 COMPLIANCE WITH LEGAL REQUIREMENTS

15.1.1 Identification of applicable legislation

15.1.2 Intellectual property rights (IPR)

15.1.3 Protection of organizational records

15.1.4 Data protection and privacy of personal information

15.1.5 Prevention of misuse of information processing facilities

15.1.6 Regulation of cryptographic controls

15.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE

15.2.1 Compliance with security policies and standards

15.2.2 Technical compliance checking

15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS

15.3.1 Information systems audit controls

15.3.2 Protection of information systems audit tools