• T-NET IT Security Plan Service

การจัดทำแผน นโยบายการรักษาความมั่นคง ตามมาตรฐานและกฎเกณฑ์สากล ประกอบด้วยงาน 5 ส่วน ได้แก่.

1. การทำ Security Policy ในองค์กร

คือ การเข้าไปศึกษาและสำรวจการใช้งานระบบข้อมูลและเครือข่ายของลูกค้า เพื่อนำมาจัดทำนโยบายการรักษาความมั่นคงข้อมูลและเครือข่ายในองค์กร (Security Policy) ซึ่งในแต่ละองค์กรจะมีรูปแบบธุรกิจ วัฒนธรรมในการดำเนินงาน ที่แตกต่างกันออกไป นอกจากนี้ยังมีรูปแบบและการจัดแบ่งชั้นความลับของข้อมูลที่แตกต่างกัน ดังนั้นในแต่ละองค์กรจึงมีความจำเป็นที่จะต้องอาศัยผู้เชียวชาญทางด้านการรักษาความมั่นคงปลอดภัยเข้าไปให้คำปรึกษา คำแนะนำ หรือช่วยเหลือในการร่างและจัดทำนโยบายการรักษาความมั่นคงปลอดภัยในองค์กร ซึ่งนโยบายการรักษาความมั่นคงปลอดภัยถือเป็นสิ่งสำคัญ ที่ทุกองค์กรต้องจัดทำขึ้นเพื่อเป็นแนวทาง และเป็นเข็มทิศชี้นำองค์กรในการรักษาความมั่นคงปลอดภัยข้อมูลและเครือข่าย นอกจากนี้การจัดทำนโยบายยัง ครอบคลุมไปถึงการจัดทำระเบียบปฏิบัติ ในการใช้งานข้อมูลและเครือข่าย (Code of Conduct) ข้อตกลงการใช้งาน ข้อห้าม และบทลงโทษต่างๆ ในกรณีเกิดความเสียหายทางด้าน Information Security ขึ้น ในส่วนขององค์กรที่มีความจำเป็นหรือต้องการเข้าสู่กระบวนการรับรองมาตรฐานในการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ (Security Standard) เพื่อผ่านข้อกำหนดในการประกอบธุรกิจองค์กรจะต้องจัดทำนโยบายนี้ เพราะเป็นข้อกำหนดเบื้องต้นในการเข้าสู่กระบวนการทางมาตรฐานสากล

2. การทำ Risk Assessment

การประเมินความเสียง ถือเป็นจุดเริ่มต้นของกระบวนการรักษาความมั่นคงปลอดภัยข้อมูลและเครือข่ายในองค์กร โดย T-NET จะส่งทีมงานเข้าไปทำการศึกษา วิเคราะห์ และประเมินว่าทรัพย์สินสารสนเทศขององค์กรมีความเสี่ยงต่อการเกิดความเสียหายมากน้อยเพียงใด โดยพิจารณาจากระดับความสำคัญของทรัพย์สิน ภัยคุกคามที่อาจเกิดขึ้นต่อทรัพย์สิน และจุดอ่อนของทรัพย์สินเหล่านั้น ซึ่งผลลัพธ์จากการประเมินจะทำให้ทราบระดับความเสี่ยงต่อทรัพย์สินแต่ละอย่าง ทั้งที่ยอมรับได้และยอมรับไม่ได้ โดยจะต้องผ่านการอนุมัติจากผู้บริหารขององค์กรจากนั้นจึงสามารถบริหารจัดการกับความเสี่ยงโดยกำหนดมาตรการอันเหมาะสมในการแก้ไขจุดอ่อน และป้องกันภัยคุกคามโดยอ้างอิงตามมาตรฐานความปลอดภัยสากล ISO/IEC 17799, BS7799 และ ISO/IEC 27001

3. Risk Management ด้าน IT

บริการนี้ประกอบด้วยการแนะนำวิธีการและการทำสัมมนาเชิงปฏิบัติการ เพื่อให้ตัวแทนขององค์กรได้ฝึกปฏิบัติและเรียนรู้วิธีการบริหารจัดการความเสี่ยงที่มีต่อสารสนเทศ โดยอาศัยเทคนิคการบริหารจัดการความเสี่ยงอ้างอิงตามข้อกำหนดในมาตรฐาน ISO/IEC 17799, BS7799 และ ISO/IEC 27001 รวมทั้งสามารถวางแผนเพื่อบริหารความเสี่ยงที่มีต่อสารสนเทศขององค์กรต่อไป

ทั้งนี้งาน Risk Assessment และ Risk Management ทาง T-NET จะจัดผู้เชี่ยวชาญและมีประสบการณ์ที่ได้รับประกาศนียบัตร การผ่านการฝึกอบรมหลักสูตร Information Security Management System (ISMS) Auditor/Lead Auditor ซึ่งอ้างอิงมาตรฐานความปลอดภัยสากล ISO/IEC 17799 , BS7799 และ ISO/IEC 27001 เข้าไปดำเนินการจัดทำ Risk Assessment และ Risk Management ด้าน IT ให้กับลูกค้า

4. Business Continuity Planning (BCP) *และ* 5. Disaster Recovery Plan (DRP)

เป็นการวางแผนสร้างความต่อเนื่องให้กับธุรกิจเพื่อเตรียมการรองรับผลกระทบที่รุนแรงที่อาจเกิดขึ้นกับธุรกิจ เช่น กรณียึดทำเนียบรัฐบาล ยึดท่าอากาศยานดอนเมือง และ สุวรรณภูมิ เป็นต้น รวมทั้งปัญหาการเกิดภัยโรคภัยไข้เจ็บที่ส่งผลให้พนักงานในองค์กรไม่สามารถมาทำงานได้เป็นระยะเวลานาน เช่น การเกิดโรคซาร์ล โรคไข้หวัดนก และอื่นๆ ที่องค์กรอาจจะต้องเตรียมแผนสำรองการทำงานจากนอกสถานที่ เพื่อให้ธุรกิจสามารถดำเนินงานต่อไปได้ โดย T-NET จะส่งทีมงานผู้เชียวชาญ เข้าไปศึกษาการดำเนินงานทางด้านสารสนเทศในองค์กร ประเมินความเสี่ยง จัดประชุมเชิงปฏิบัติการขึ้น เพื่อทำแผนร่วมกับพนักงานและผู้บริหารในองค์กรนั้นๆ และสร้างกระบวนการในการจัดทำแผนเพื่อสร้างความต่อเนื่องทางธุรกิจ(BCP) และแผนรับมือกับความหายนะ (DRP) ที่เหมาะสำหรับธุรกิจหรือการดำเนินงานขององค์กรนั้นๆ