

บทคัดย่อ

ชื่อเรื่อง : แนวทางการจัดการความเสี่ยง ด้านเทคโนโลยีสารสนเทศ ของกรมการสื่อสารทหาร กองบัญชาการกองทัพไทย

โดย : พันเอก อธิษฐ์ รัชชกิจดิอนันต์

อาจารย์ที่ปรึกษาเอกสารวิจัย : พันเอก

(ขวลิต ประดิษฐ์นวกุล)

กรกฎาคม ๒๕๖๕

การวิจัยเรื่อง แนวทางการจัดการความเสี่ยง ด้านเทคโนโลยีสารสนเทศ ของกรมการสื่อสารทหาร กองบัญชาการกองทัพไทย มีวัตถุประสงค์ในการวิจัย ๑) เพื่อศึกษาสภาพปัญหาการจัดการความเสี่ยงเทคโนโลยีสารสนเทศ และประเมินความเสี่ยงเทคโนโลยีสารสนเทศ ของกรมการสื่อสารทหาร กองบัญชาการกองทัพไทย ๒) เพื่อศึกษาแนวคิดและหลักการ รวมถึงการดำเนินการในการจัดการความเสี่ยงเทคโนโลยีสารสนเทศ ๓) เพื่อศึกษาแนวทางการจัดการความเสี่ยงเทคโนโลยีสารสนเทศของกรมการสื่อสารทหาร กองบัญชาการกองทัพไทย

การวิจัยนี้ใช้กระบวนการวิจัยเชิงคุณภาพ ประกอบไปด้วย กระบวนการศึกษาและวิเคราะห์ข้อมูลจากการวิจัยเชิงเอกสาร และกระบวนการสัมภาษณ์เชิงลึกผู้ทรงคุณวุฒิจำนวน ๕ ท่าน

ผลการวิจัย พบว่า แนวทางการจัดการความเสี่ยง เทคโนโลยีสารสนเทศ ของ สส.ทหาร ใน ๕ มิติ ประกอบไปด้วย ๑) ด้านข้อมูล ต้องมีการบริหารจัดการระบบฐานข้อมูลสารสนเทศ ให้เป็นระบบ กำหนดระเบียบ ข้อบังคับให้มีรหัสผ่านของแต่ละบุคคลในการเข้าถึงการใช้งานคอมพิวเตอร์หรือระบบสารสนเทศ มีมาตรการที่ชัดเจนในการดูแลและป้องกันการใช้งานสื่อบันทึกข้อมูลภายนอก ที่สามารถนำมาใช้บันทึกข้อมูลภายในออกไปได้ ๒) ด้านฮาร์ดแวร์ ต้องกำหนดและพิจารณาในเรื่องของพื้นที่สำหรับการติดตั้งอุปกรณ์สำคัญ ให้มีความมั่นคงปลอดภัย มีระบบป้องกันอัคคีภัย หรือป้องกันไฟฟ้ากระชาก หรือป้องกันไฟฟ้าดับ ๓) ด้านซอฟต์แวร์ ต้องกำหนดมาตรการให้มีการอัปเดตระบบปฏิบัติการ หรือซอฟต์แวร์ต่างๆ อย่างต่อเนื่อง กำหนดให้ใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ ถูกต้องตามกฎหมาย และต้องมีการอัปเดตโปรแกรมอยู่เสมอ ๔) ด้านบุคลากร ต้องมีการส่งเสริมให้กำลังพลมีความรู้ ความเข้าใจที่ชัดเจนในการใช้งานระบบสารสนเทศขององค์กร สร้างความตระหนักรู้ เกี่ยวกับการใช้งานระบบสารสนเทศขององค์กร ๕) ด้านเครือข่าย

ต้องควบคุมเกี่ยวกับเครือข่าย ไม่ให้สัญญาณ กระจายสัญญาณออกนอกพื้นที่ และต้องกำหนดแผนรองรับ
ในการจัดการเกี่ยวกับเครือข่ายจากเหตุการณ์ที่ไม่คาดคิดที่อาจเกิดขึ้นกับเครือข่าย

ABSTRACT

Title : Guidelines For Managing Risks In Information Technology Of The Directorate
Of Joint Communication, Royal Thai Armed Forces Headquarters.

By : COLONEL. ATHIRAT TAWATKITTIANUN

Research Advisor : Colonel

(Chavalit Praditnawakul)

July 2022

The objectives of research subject Guidelines For Managing Risks In Information Technology Of The Directorate Of Joint Communication, Royal Thai Armed Forces Headquarters were 1) to study information technology risk management problems and assessment of information technology risks of the Directorate of Joint Communication, Royal Thai Armed Forces Headquarters. 2) To study concepts and principles including the implementation of information technology risk management. 3) To study information technology risk management guidelines of the Directorate of Joint Communication, Royal Thai Armed Forces Headquarters.

This research use a qualitative research Methodology, comprising the process of studying and analyzing data from documented research and In-depth interview process with 5 qualified persons.

The results of this research found Risk Management Approach Information technology of the Royal Thai Army in 5 dimensions consists of 1) In the field of information, there must be a systematic management of the information database system. Establish rules and regulations for each person's password to access the computer or information system. There are clear measures to maintain and prevent the use of external storage media. used to save internal data. 2) Hardware side Must determine and consider the area for the installation of important equipment. to be secure There is a fire protection system. or protection against power

surges or prevent power failure. 3) Software Measures must be taken to update the operating system. or software continually. Required to use licensed software Legitimate And the program must always be updated. 4) As for personnel, personnel must be encouraged to have knowledge. A clear understanding of the use of corporate information systems. As for personnel, personnel must be encouraged to have knowledge. A clear understanding of the use of corporate information systems. Raise awareness about the use of corporate information systems. 5) Network side Must control about the network not to distribute the signal outside the area and must establish a support plan to manage the network from unexpected incidents that may occur to the network.